COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Informe Propuesta Normativa:

Norma que modifica NCG N°514 e incorpora Anexo N°3

Julio 2025

www.CMFChile.cl

Informe Propuesta Normativa:

Norma que modifica NCG N°514 e incorpora Anexo N°3

ACTUALIZACIONES:

Modificaciones introducidas mediante acuerdos adoptados por el Consejo de la Comisión para el Mercado Financiero:

Circular N° XXX de XX de XX de 2025

CONTENIDO:

Índice Informe Normativo

INTRODUCCIÓN

La presente propuesta normativa aborda elementos que se incorporan al Anexo N°3 de la NCG 514 que regula el Sistema de Finanzas Abiertas emitida el 3 de julio de 2024, especialmente en lo referido a Intercambio de Información. Otros elementos propios del mencionado Anexo, como lo relacionado con Iniciación de Pagos, serán abordados en una próxima publicación.

En términos resumidos, la norma en consulta presentada, que cubre aquellos aspectos propios del Anexo N°3 según el alcance antes especificado, dice relación con los siguientes asuntos o materias:

- Sobre la Infraestructura del sistema: Especificaciones y funciones del Directorio de participantes, Certificados, Firmas, Mantenciones programadas, entre otros.
- Sobre las Especificaciones de las APIs: la naturaleza de estas, nomenclaturas, códigos de respuesta y paginación.
- Sobre elementos de disponibilidad, rendimiento y TPM/TPS.
- Sobre el Consentimiento: mecanismos de generación y administración de este.
- Sobre las Certificaciones y pruebas: la vigencia de estas y las condiciones de otorgamiento.
- Sobre el mecanismo alternativo: marco general y condiciones.
- Sobre aspectos de monitoreo, reporte y pruebas de calidad de la información.
- Sobre interrupciones e incidentes se detalla el RIO del SFA y aspectos relativos a suspensiones.

Se destaca como parte esencial del proceso normativo la instalación, que realizó la CMF, del Foro del Sistema de Finanzas Abiertas con diversas industrias participantes del Sistema que, en su carácter consultivo, permitió a este Organismo recibir propuestas respecto de especificaciones y elementos técnicos a incorporar en la presente actualización normativa.

El presente informe normativo, en su Capítulo II contiene las contribuciones al proceso consultivo cuyo objetivo es capturar aquellas materias o aspectos específicos que son de interés de la CMF. El Capítulo III resume el marco regulatorio vigente e identifica las fuentes legales y normativas que se deben tener como referencia para sustentar las disposiciones del marco regulatorio

propuesto para el SFA. En el Capítulo IV, se identifica el potencial impacto regulatorio de la propuesta. Finalmente, el Capítulo V contiene la propuesta normativa que se somete a consulta pública, la que incorpora algunos elementos del Anexo N°3: "Anexo Técnico".

I. CONTRIBUCIONES AL PROCESO CONSULTIVO

Sin perjuicio de los demás elementos, sugerencias u observaciones que los distintos actores o usuarios del mercado financiero pudieren manifestar en el proceso consultivo a que se somete la presente propuesta, se espera recibir comentarios por parte de quienes presten o quieran prestar alguno de los servicios o roles regulados por el Título III de la Ley Fintec, sobre:

a) Si existiese algún costo de cumplimiento de las instrucciones incorporadas en la propuesta que fuere tan relevante como para hacer inviable el surgimiento de nuevos actores o el desarrollo de un modelo de negocio.

b) Si se percibe algún elemento del marco planteado que pueda ser un obstáculo relevante para que el sistema logre sus objetivos.

c) Si existieren aspectos en que por estar comprometida la fe pública en el mercado, la estabilidad del mercado financiero, o la protección de los clientes, fuere pertinente establecer exigencias adicionales a las ya incorporadas en la propuesta.

d) Si se identifican elementos que no están incorporados en esta regulación y que se considere que deban ser normados.

e) Si existieren elementos que no permiten una adecuada comprensión o que requieran mayor precisión para su adecuada aplicación.

f) Si existieran elementos técnicos indispensables en el desarrollo del SFA relacionados a las temáticas abordadas que no están siendo consideradas.

II. MARCO REGULATORIO VIGENTE

Fuente legal del proyecto normativo

Las normas que contiene el presente proyecto normativo se impartirán en virtud de lo establecido en el Título III (artículos 17 a 27) y en los artículos tercero y cuarto transitorios de la Ley Fintec. Asimismo, han sido consideradas para su confección las disposiciones atingentes contenidas en el D.L. 3538 de 1980, la Ley N°20.009, y la Ley N°19.628.

Normativa vigente relevante

Para la confección de la presente propuesta normativa, se ha considerado un conjunto relevante de normativa secundaria de carácter sectorial que atañe a uno o más grupos o tipos de Participantes del SFA, con el propósito de propender

a la coherencia regulatoria en atención a los desarrollos normativos vigentes, en conjunción con los fines previstos en la Ley Fintec:

N.C.G. N°502*,* que regula el registro, autorización y obligaciones de los prestadores de servicios financieros de la Ley Fintec.

Recopilación Actualizada de Normas para bancos (RAN)

Capítulo 1-7. Sobre transferencia de información y fondos. Se refiere a la prestación de servicios bancarios y la realización de operaciones interbancarias que se efectúan mediante transmisiones de mensajes o instrucciones a un computador conectado por redes de comunicación propias o de terceros, efectuadas desde otro computador o mediante el uso de otros dispositivos electrónicos (cajeros automáticos, teléfonos, PINPAD, etc.).

Capítulo 1-13*.* Establece disposiciones generales relativas a la evaluación de la Administración de Riesgo Operacional realizada por los bancos. De acuerdo con las exigencias establecidas, la entidad debe identificar claramente los principales activos de información e infraestructura física y definir políticas para el manejo del riesgo operacional, teniendo en consideración la naturaleza, el volumen y la complejidad de sus actividades; el nivel de tolerancia al riesgo del Directorio; y las líneas específicas de responsabilidad.

Capítulo 20-7*.* Contiene pautas de carácter general relativas a servicios externalizados y, en forma particular, a la tercerización de servicios de procesamiento de datos y resguardos adicionales en el caso de servicios en la nube. La norma señala las condiciones que debe cumplir una entidad ante la decisión de externalizar un servicio; y establece requisitos esenciales respecto a los sitios de procesamiento, los aspectos de continuidad del negocio, seguridad de la información propia y de sus clientes, entre otros.

Capítulo 20-8*.* Establece lineamientos para la información que las entidades supervisadas, a las que aplica, deben remitir ante incidentes operacionales relevantes que afecten la continuidad del negocio; la seguridad de la información o la imagen de la institución. También señala las condiciones mínimas a considerar para desarrollar y mantener bases de información respecto de incidentes de ciberseguridad.

Capítulo 20-9*.* Contempla lineamientos para la gestión de los riesgos de continuidad del negocio, considerando la naturaleza, el volumen y la complejidad de las operaciones de las entidades supervisadas a las que aplica. De esta manera, indica la debida existencia de una estrategia aprobada por la máxima

instancia de la entidad; de una función de riesgos que se encargue de este ámbito en conjunto con instancias colegiadas de alto nivel; de una estructura para el manejo de situaciones de crisis; de la evaluación de escenarios mínimos de contingencia, entre otros.

Capítulo 20-10. Contiene disposiciones, basadas en las mejores prácticas internacionales, que deben considerarse para gestionar la seguridad de la información y ciberseguridad. Se definen lineamientos específicos respecto del papel que debe tener el Directorio para la gestión adecuada, de seguridad de la información y de ciberseguridad, otorgándole como responsabilidad la aprobación de la estrategia institucional en esta materia, y de asegurar que las entidades mantengan un sistema de gestión de la seguridad de la información y ciberseguridad. Asimismo, se establece principios y procedimientos para detección de las amenazas y vulnerabilidades de ciberseguridad; la respuesta ante incidentes; y la recuperación de la operación normal de la entidad, entre otros.

Normativa en materia de Valores y Seguros

Circular N°2054, sobre control interno y gestión de riesgos para intermediarios de valores. En esta circular se establecen requerimientos mínimos tendientes a formalizar y fortalecer los sistemas de control y gestión de riesgo de los intermediarios de valores, los que, además, permiten una mejor administración de los riesgos inherentes a sus modelos de negocio y el adecuado desarrollo de sus actividades.

N.C.G. N°309**,** que establece los principios de gestión de riesgo y control interno en las entidades aseguradoras y reaseguradoras, incluyendo los riesgos de mercado, riesgos operativos, riesgos legales, entre otros.

N.C.G. N°325, relativo al sistema de gestión de riesgos de las aseguradoras y evaluación de solvencia de estas compañías, donde se establecen los principios y buenas prácticas de gestión de riesgos en las aseguradoras, enmarcada en el contexto de la aplicación de adecuados principios de gobierno corporativo en las compañías.

N.C.G. N°507, establece instrucciones sobre el gobierno corporativo y gestión de riesgos de administradoras generales de fondos. Deroga Circular N° 1.869

Normativa aplicable a Cooperativas de Ahorro y Crédito

Circular N°108 de Cooperativas. Contiene la compilación de instrucciones generales para Cooperativas de Ahorro y Crédito fiscalizadas por la Comisión, en temas tales como su fiscalización, régimen legal, requisitos prudenciales, sistemas contables, actividades comerciales, gestión de riesgos, externalización de servicios, y notificación de incidentes operacionales, entre otros.

Normativa sobre emisión y operación de tarjetas de pago

Circular N°1 Empresas Emisoras de Tarjetas de Pago No Bancarias. Desarrolla las normas generales sobre registro y fiscalización de los emisores no bancarios de tarjetas de pago, incluyendo requisitos patrimoniales, obligaciones dentro de la cadena de pagos, y reportería de información para el ejercicio de las funciones de la Comisión.

Circular N°1 Empresas Operadoras de Tarjetas de Pago. Contiene las disposiciones asociadas al registro, fiscalización y ejercicio de actividades económicas por parte de operadoras de tarjetas de pago, considerando requisitos prudenciales, operativos, y de gestión.

Circular N°1 Empresas Emisoras de Tarjetas No Bancarias y Operadoras de Tarjetas de Pago. Contiene normas comunes en materia de resguardos operacionales, externalización de servicios, continuidad de negocios, y seguridad de la información y ciberseguridad.

Compendio de Normas Financieras del Banco Central de Chile

Capítulo III.J.1. – Emisión de Tarjetas de Pago. Contiene las disposiciones impartidas en materia de emisión de tarjetas de crédito, tarjetas de débito y tarjetas de pago con provisión de fondos, en materias tales como requisitos patrimoniales, gestión de riesgos y obligaciones de las entidades emisores con los establecimientos afiliados y los tarjetahabientes. Las instrucciones particulares para la emisión de cada instrumento de pago se encuentran incorporadas en subcapítulos respectivos.

Capítulo III.J.2. – Operación de Tarjetas de Pago. Contiene las disposiciones que rigen la operación de tarjetas de pagos, considerando las diversas modalidades de operación. Se establecen en lo medular requerimientos patrimoniales, de gestión, y de relacionamiento con otros intervinientes de la cadena de pagos.

III. EVALUACIÓN DE IMPACTO REGULATORIO

Esta propuesta normativa permite implementar elementos del Anexo Técnico N° 3 de la NCG sobre materias relacionadas a infraestructura, especificaciones de las APIs, especificaciones sobre disponibilidad y rendimiento, forma de generar y administrar el consentimiento, certificaciones y pruebas, marco general de aplicación del mecanismo alternativo y su definición, mecanismos de reporte y reporte de incidentes operacionales en el contexto de SFA.

El impacto regulatorio general ya está considerado a nivel agregado en la NCG 514 ya emitida, siendo este informe normativo una profundización de los estándares considerados en dicha NCG y entrega especificaciones necesarias para su correcta implementación y funcionamiento.

Se considera que el impacto de esta normativa debe ser acotado por cuanto la mayoría de los estándares aquí propuestos fueron parte de la discusión del Foro y sus grupos técnicos, y son estándares conocidos por sus participantes.

IV. PROPUESTA NORMATIVA: NORMA QUE MODIFICA NCG N°514 E INCORPORA ANEXO N°3

Texto Propuesto:

REF.: ACTUALIZACIÓN NORMA DE CARÁCTER GENERAL N°514, DE 3 DE JULIO DE 2024. INCORPORACIÓN ANEXO N°3.

NORMA DE CARÁCTER GENERAL N° XX

XX de xxxx de 2025

Modifica Norma de Carácter General N°514, de fecha 3 de julio de 2024, que regula el Sistema de Finanzas Abiertas, en los términos que indica.

Esta Comisión, en uso de las facultades que le confieren los artículos 1, 3, 5 en sus numerales 1, 8 y 18, y 20 en su numeral 3 del Decreto Ley N°3.538, los artículos 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27 y tercero y cuarto transitorios de la Ley N°21.521 ("Ley Fintec"), y lo acordado por el Consejo de la Comisión en Sesión Ordinaria N°[XXX] de [XX] de [XXXX] de 2024, ha estimado pertinente actualizar las siguientes instrucciones respecto de la implementación del Sistema de Finanzas Abiertas (en adelante también e indistintamente el "Sistema" o "SFA") al que se refiere el Título III de la Ley Fintec, (en adelante también la "Norma"):

MODIFICACIONES NCG

1. REFERENCIA A LA REACTIVACIÓN DE UN PARTICIPANTE

En la Sección V: Otras Disposiciones, letra A. Suspensiones Temporales, se precisa el proceso de reactivación de un Participante posterior a una suspensión, incorporando un párrafo al final, de la siguiente manera:

"SECCIÓN V: OTRAS DISPOSICIONES

A. SUSPENSIONES TEMPORALES

La Comisión, en conformidad con el buen funcionamiento del Sistema, y lo dispuesto en el inciso penúltimo del artículo 27 de la Ley Fintec, podrá suspender temporalmente, de forma parcial o total, la participación de las entidades o sus interfaces cuando se verifiquen alguna de las siguientes circunstancias:

a) Entidades que muestren deficiencias en la calidad de la información que suministren a través de sus interfaces.
b) Entidades que ~~sufren~~ se vean afectadas por algún tipo de incidente de ciberseguridad que ~~afecte o~~ comprometa los activos de información asociados al SFA o que involucre una vulneración de los datos personales de los clientes ~~financieros~~.
c) Entidades que hayan ~~sufrido~~ enfrentado algún incidente operacional que les impida la transferencia y/o intercambio de datos en forma segura o que afecte el correcto funcionamiento del Sistema.
d) Entidades que presenten deficiencias en su gestión de riesgos operacionales o de ciberseguridad.
e) Entidades que presenten otros inconvenientes o evidencien problemas que puedan generar un efecto negativo sobre el Sistema.

En línea con lo anterior, los Participantes del SFA, bajo ninguna circunstancia, deben afectar los activos de información asociados al SFA, entre ellos, los datos personales de los clientes financieros. Por lo anterior, en caso de que un Participante del SFA estime que existe un riesgo relevante de afectación de tales activos que requiera acciones urgentes, deberá tomar medidas preventivas inmediatas, tales como la desconexión de sus propios sistemas del SFA o la denegación de solicitudes en sus interfaces y sistemas a otros participantes. Junto con lo anterior, deberá enviar ~~de inmediato~~ a la brevedad un reporte a la CMF informando las medidas adoptadas con los fundamentos explicativos pertinentes, así como adoptar a la brevedad las acciones correctivas para solucionar la situación que la motivó y mantener informada a la Comisión sobre estas acciones.

Una vez solucionada la situación que motivó las medidas, el Participante del SFA deberá informar a la CMF esta situación y reestablecer el servicio.

Respecto a las medidas preventivas adoptadas y sus acciones correctivas, el Participante deberá mantener a disposición de la Comisión todos los antecedentes que fundamenten tales decisiones, a fin de que ~~la Comisión~~ esta pueda evaluar su pertinencia, oportunidad e idoneidad y, si corresponde, ejercer las acciones necesarias según sus facultades legales.

Reactivación de un Participante posterior a una suspensión por parte de la CMF

Respecto a la reactivación de un participante de forma posterior a una suspensión, esta acción solo será posible de realizar por la Comisión. Para estos efectos, la institución deberá entregar un informe de cierre y superación del evento respectivo el que será evaluado por este Organismo para determinar la pertinencia de la reactivación de un Participante dentro del SFA.

2. CAMBIOS EN EL PLAZO DE LA ENTREGA DE LOS CERTIFICADOS DE SEGURIDAD

En la Sección V: Otras Disposiciones, letra C. Plazos de implementación del Sistema, se incorpora un literal e), en el último párrafo, respecto a los plazos para presentar los certificados de seguridad, de la siguiente manera:

"SECCIÓN V: OTRAS DISPOSICIONES

C. PLAZOS DE IMPLEMENTACIÓN DEL SISTEMA

El SFA tendrá un periodo de implementación en dos etapas. La primera de ella, que durará 24 meses, considera la preparación tecnológica y desarrollo de las tareas propias que corresponden a los participantes y a la Comisión. Este periodo de 24 meses comienza con la publicación de la presente normativa. Una vez terminado dicho periodo, la presente norma entrará en vigencia.

Los hitos de la implementación gradual, una vez vigente esta normativa, consideran los siguientes plazos de cumplimiento de disponibilidad de las APIs de información dentro del marco establecido por la Ley Fintec:

- Los bancos, los emisores de tarjetas de crédito y emisores de tarjetas de pago con provisión de fondos deberán cumplir con los siguientes plazos:

  a) 6 meses para implementación de APIs sobre Canales de Atención y APIs sobre Términos y Condiciones Generales.

  b) 15 meses para implementación de APIs sobre Condiciones Comerciales y Uso e Historial de Producto, en lo referido a clientes personas naturales. Tratándose de información sobre líneas de crédito asociadas a cuentas corriente, cuentas vista y tarjetas de crédito, deberá estar disponible a los 18 meses de entrada en vigencia de esta norma.

  c) 18 meses para implementación de APIs sobre Condiciones Comerciales y Uso e Historial de Producto, en lo referido a clientes personas jurídicas.

  d) 18 meses para implementación de APIs sobre Iniciación de Pagos.

- Para las entidades indicadas en el inciso segundo, letras (a) a la (h) del artículo 18 de la Ley Fintec, los plazos correspondientes para que deban tener disponibles sus APIs serán:

a) 24 meses para implementación de APIs sobre Canales de Atención y Términos y Condiciones Generales.

b) 36 meses para implementación de APIs sobre Condiciones Comerciales y Uso e Historial de Producto.

La Comisión considerará que se ha cumplido con los plazos cuando, a las fechas estipuladas, las IPI e IPC:

a) Hayan desarrollado las APIs de acuerdo con el ~~al~~ calendario de implementación antes indicado, y el respectivo mecanismo alternativo indicado en la Norma.

b) Hayan proporcionado la información ~~documentación~~ pertinente al Directorio de Participantes.

c) Hayan realizado las respectivas pruebas funcionales.

d) Tengan la información efectiva de lo~~a~~s clientes ~~asociadas a cada API~~ (no solo información de pruebas) ya disponible en el Sistema.

e) Cuenten con el certificado de implementación de perfiles de seguridad de interfaces.

f) Cuenten con los certificados digitales que acreditan identidad provistos por un CA valido.

En el caso de entidades indicadas en el inciso segundo, letras (a) a la (h) del artículo 18 de la Ley Fintec, que emitan directamente tarjetas de pago o ~~aperturen~~ abran cuentas vistas, aplicará el plazo de 18 meses para iniciación de pagos.

3. CAMBIOS EN LA ESPECIFICACIÓN DEL MECANISMO ALTERNATIVO

Mecanismo alternativo

Las IPI e IPC deberán contar con el ~~un~~ mecanismo alternativo de entrega de información, que opere en caso de los eventos de indisponibilidad de las interfaces descritas en el Anexo 3 de esta norma. ~~en esta sección, *infra*.~~

Para lo anterior, las IPI y las IPC deberán dar cuenta a la Comisión, al momento de solicitar su incorporación en la nómina, ~~los antecedentes que acrediten el desarrollo efectivo del mecanismo alternativo que determina la presente Norma~~ la acreditación de la existencia de este mecanismo y la realización de las pruebas de funcionamiento respectivas~~,~~ cuyos detalles técnicos se indican en el Anexo N°3 y que deberán ser parte de la evaluación del certificador como parte del requisito de la letra c de la Sección I.E.1 de la norma.

~~El mecanismo alternativo deberá considerar los siguientes requisitos técnicos, los que serán debidamente especificados en el Anexo N°3 de la Norma:~~

a) ~~Capacidad de mantener el servicio y la entrega de información.~~
b) ~~Métricas de rendimientos de respuesta a la solicitud o consulta de información.~~
c) ~~Medidas de seguridad tales que permitan monitorear el tráfico de la información en el mecanismo alternativo, así como la detección activa de intrusos y la vulneración o exceso de permisos.~~
d) ~~Canales seguros de transmisión de información.~~
e) ~~Uso de credenciales que identifiquen a los Participantes al momento de descargar la información y que permitan la adecuada trazabilidad respecto a la información accedida, escrita, o recuperada, cada vez que aquellos se conecten.~~

~~Las especificaciones del mecanismo alternativo podrán considerar variantes o elementos particulares conforme la naturaleza de la información a intercambiar y los detalles técnicos de la interfaz principal respectiva. Con todo, el mecanismo alternativo y las especificaciones del Anexo 3 serán uniformes para todos los Participantes, asegurando así la interoperabilidad del Sistema.~~

~~La entidad deberá acreditar como parte de su proceso de habilitación o incorporación a la nómina respectiva, la implementación del mecanismo alternativo cuyas especificaciones se indiquen en el Anexo N°3, el que deberá ser sometido a a pruebas funcionales en los términos indicados para el proceso de inscripción~~

~~La existencia de este mecanismo alternativo es independiente de los requerimientos de continuidad operacional de la interfaz principal que da cuenta la Sección III.A.3. de esta Norma.~~

~~El uso del mecanismo alternativo en caso alguno habilita al Participante a tratar datos distintos de los que se encuentran disponibles en las interfaces del SFA, debiendo para todos los efectos ceñirse a los términos del consentimiento otorgado por el Cliente.~~

El mecanismo alternativo especificado en el Anexo N°3 no sustituye los requisitos de planes de contingencia que deberá tener el Mecanismo Principal.

~~Las condiciones de activación y uso del mecanismo alternativo, incluyendo eventos desencadenantes, rol de los Participantes, y la duración de su funcionamiento, deberán cumplir las exigencias y requerimientos que indique el Anexo N°3 de esta Norma~~. El mecanismo alternativo deberá resguardar la continuidad de entrega de información en dos escenarios: la vulneración de la información y fallas en el sistema de entrega de información.

Se activará cuando este indisponible el mecanismo principal y su contingencia.

~~Con todo, para efectos de esta disposición, no aplicará la activación del mecanismo alternativo en los siguientes casos:~~

- ~~Mantenciones programadas debidamente informadas y justificadas por la IPI o IPC a la CMF, que condicionen operativamente el mecanismo alternativo. Lo anterior según los estándares que se indiquen en el Anexo N°3.~~
- ~~Suspensiones temporales que mandate la Comisión y que involucren el mecanismo alternativo.~~

4. CAMBIOS EN LAS REFERENCIAS AL DIRECTORIO Y LA COPIA LOCAL

C. Directorio de Participantes

Para la adecuada interacción de los diversos participantes en el contexto del SFA, la CMF implementará un Directorio de Participantes (en adelante "DP"), de consulta obligatoria por parte de las entidades.

El acceso, consulta, y actualización de la información del DP se someterá a las directrices, requisitos operativos, e instrucciones incorporadas en el manual del DP, que estará disponible para ser consultado, en su versión vigente y actualizada, a través de los canales tecnológicos dispuestos por la Comisión.

Será obligación y responsabilidad exclusiva de cada participante el cerciorarse que la información sobre sí mismo contenida en el DP resulte correcta y no haya experimentado cambios sustantivos que afecten su vigencia o veracidad. En particular, deberá considerar las especificaciones de la copia local que debe mantener el participante respecto del Directorio, así como los hitos de actualización respectivos que se indican en el Anexo N°3 de la presente norma.

Sin perjuicio de otros elementos que en el futuro se incorporen dentro de la plataforma de DP, cada participante deberá suministrar la ~~siguiente~~ información que se detalla en el Anexo 3 para efectos de una correcta incorporación al sistema.~~:~~

~~a) Información sobre la entidad y las personas naturales que figurarán como responsable funcional y contacto técnico en el SFA, así como de quien detente la calidad de encargado ante consultas de otros participantes, de acuerdo con lo dispuesto en la Sección II.D.~~

~~b) Información sobre el o los certificados digitales que empleará la entidad para su operación en el SFA, considerando vínculos de descarga o repositorio de certificados, e información de la o las claves públicas respectivas.~~

~~c) Información sobre los endpoints de cada API implementada por la entidad, conforme con las especificaciones técnicas de denominación de rutas que se establezcan en el Anexo Nº3 de esta Norma.~~

~~Para la incorporación de un participante en el Directorio, junto con haber cumplido exitosamente los procesos de registro o inscripción en la nómina, según sea el caso, deberá obtener de una CA un certificado digital que cumpla con los atributos y campos que se indiquen en el Anexo Nº3 de esta Norma.~~

~~El referido Anexo Nº3 indica los requisitos que deberán cumplir las CA, así como las prácticas o lineamientos de validación extendida a consideraren la emisión de los respectivos CD a cada Participante, incluyendo exigencias y consideraciones legales de las cadenas de confianza y certificados raíces a ser utilizados para fines de seguridad, integridad y no repudiación.~~

5. REFERENCIA AL SANDBOX COMO EL ÁREA DE PRUEBAS DEL SFA

C. Registro de Prestadores de Servicios Basados en Información

1. Inscripción en el Registro

1.2 Antecedentes adjuntos

l) *Pruebas funcionales*. Documento que evidencie, a través de un reporte de evidencia de pruebas ~~reporte de hallazgos~~ provisto por un tercero, sobre la realización de Pruebas Funcionales de consumo de APIs en Áreas de Prueba. Tanto las condiciones que debe tener este tercero, como los elementos mínimos de prueba a efectuarse se deberán ajustar a las especificaciones del Anexo N°3 de esta Norma.

Para todos los efectos el área de prueba válida para las pruebas funcionales es el Sandbox que para estos efectos provee la CMF.

6. PRECISIÓN EN EL ALCANCE DE LA INFORMACIÓN A REPORTAR AL MOMENTO DE LA INSCRIPCIÓN DEL PSBI

C. Registro de Prestadores de Servicios Basados en Información
2. Inscripción en el Registro
1.2 Antecedentes adjuntos

c) Plan de negocios y actividades. Síntesis referencial del plan estratégico y de negocios, indicando las principales líneas de negocios y las actividades que pretende realizar, refiriéndose expresamente a los servicios que proveerá a clientes en su calidad de PSBI, indicando el o los segmentos o tipo de clientes concernidos en sus servicios, así como una descripción de las categorías o grupos de datos e información financiera disponible en el SFA que empleará para el desarrollo de su actividad, según lo indicado en la Sección IV.A. Como parte del Plan se deberá indicar, además de los servicios habilitados por información financiera, las actividades accesorias que llevará a cabo (de aplicar), incluyendo la prestación de servicios de iniciación de pagos, así como actividades económicas de otra índole. El Solicitante deberá siempre mantener a disposición de la Comisión una copia actualizada y vigente de este documento.

La descripción de las categorías o grupos de datos que se informe por parte del PSBI para el desarrollo de su negocio no son restrictivas respecto al conjunto de datos que este puede requerir en el Consentimiento a su cliente considerando el carácter dinámico que puede tener la información en la provisión de un servicio basado en información.

7. CAMBIO EN LA REFERENCIA A LAS VARIABLES DEL SFA

SECCIÓN VI. ANEXOS NORMATIVOS

ANEXO N°1: VARIABLES PARA CONJUNTOS DE INFORMACIÓN DEL SFA

~~1. Términos y condiciones~~

~~2. Canales de atención y ATM~~

~~3. Enrolamiento~~

~~4. Posiciones financieras históricas~~

~~5. Información transaccional~~

~~6. Productos Vigentes~~

~~7. Iniciación de Pagos~~

Las especificaciones de las variables aplicables en el SFA son aquellas disponibles en el Portal de Desarrolladores que tiene habilitado esta Comisión en la siguiente URL: https://cmfchile.atlassian.net/wiki/x/yIHiDw

8. SE MODIFICA LA LETRA D) CONSENTIMIENTO, DE LA SECCIÓN III

D. Consentimiento

1. Otorgamiento del consentimiento

Para efectos de lo establecido en el Título III de la Ley N°21.521, el consentimiento es otorgado por parte del titular de datos, tanto para la IPI e IPC, como para el PSBI y PSIP, cumpliéndose con las siguientes condiciones:

a) La voluntad haya sido manifestada de manera expresa, en los siguientes términos:

i. En el caso de Persona Natural: por el respectivo titular, su representante legal o mandatario con poder específico para autorizar la transmisión y tratamiento de los datos o para autorizar la iniciación de pagos, según corresponda.

ii. En el caso de Persona Jurídica: por él o los representantes legales o apoderados, autorizados ya sea para actuar conjunta o separadamente, en el caso de iniciación de pagos, o cualesquiera de los representantes legales o mandatarios con poder específico para autorizar la transmisión y tratamiento de los datos correspondientes.

iii. Que el PSBI o PSIP haya verificado y validado que la persona que está otorgando el consentimiento esté debidamente facultada para autorizar la transmisión y tratamiento de datos o para autorizar la iniciación de pagos a nombre del titular, es decir, que puede actuar a nombre del titular y autorizar el tratamiento de datos en el marco del Sistema de Finanzas Abiertas. De conformidad con lo establecido en el Titulo III de la Ley N°21.521, en el intercambio de información a través de las interfaces implementadas en virtud de ese Título por las entidades autorizadas, las IPI o IPC deberán cursar los requerimientos de información que le sean solicitados con la sola autenticación de la PSBI o PSIP y del usuario, no correspondiéndoles pronunciarse o verificar la capacidad legal del usuario autenticado o sus facultades para consentir el intercambio y tratamiento de datos, ni rechazar por falta de poderes la solicitud de intercambio de información o iniciación de pagos. Tampoco les corresponderá rechazar las solicitudes que se les presenten a pretexto de resguardar el principio de proporcionalidad. Serán las PSBI o PSIP las que, en virtud de los poderes que se les hubieren conferido, indicaran a la

IPI o IPC respectiva a qué usuarios deben autenticar para que se perfeccione el consentimiento. El hecho de que quien o quienes otorgaron el consentimiento contaban con poderes suficientes para ello deberá ser acreditado por la PSBI o PSIP, cuando ello sea requerido por esta Comisión en el marco de sus procesos de fiscalización, para lo cual deberán mantener la documentación de respaldo a lo menos por 6 años.

b) El PSBI y PSIP haya implementado el mecanismo de gestión del consentimiento en los términos y condiciones establecidas en la sección III.E.2 de esta normativa.

c) La voluntad sea almacenada en un soporte duradero, que sea apto para resguardar su seguridad, integridad y acceso, respecto de la identidad del titular de los datos, así como de las circunstancias y condiciones en que fue solicitado y otorgado, de manera que pueda verificarse posteriormente que dicho consentimiento fue manifestado de manera libre, informada, expresa y específica en cuanto al tipo de información requerida, la finalidad y el periodo máximo de validez de esa autorización.

d) La persona o sistema informático que interactúe con el titular de los datos o cliente no ejercerá ninguna influencia indebida sobre éste para inducirlo a manifestar su voluntad o a disentir el tratamiento o intercambio de datos, o forzar su consentimiento o disentimiento. Por ejemplo, el uso de interfaces que induzcan a los usuarios a tomar decisiones no intencionadas, involuntarias o potencialmente lesivas con respecto a sus datos personales; exigir que el consentimiento sea otorgado para la aplicación de un descuento u obtención de regalías, o avanzar en la interfaz; condicionarlo para la prestación del servicio a menos que sea inviable su prestación sin dicho consentimiento; o que las opciones empleadas para que éste se otorgue o rechace estén marcadas por defecto, estén con colores, tamaños o estilos de fuentes que las destaquen por sobre aquellas opciones que se refieran a no otorgar el consentimiento o respecto de aquellas establecidas para períodos más cortos, o que se le oculten ciertas opciones.

e) Al momento de solicitar el consentimiento para la transmisión, tratamiento o cesión de datos, o iniciación de pagos, se deberá poner en conocimiento del titular o cliente de manera precisa y clara ~~los datos sobre los cuales~~ el tipo de información para la que consiente el intercambio, tratamiento~~, cesión a terceros~~ o iniciación en el marco del SFA; el servicio que pretende prestar y que motiva el intercambio y tratamiento de información; a qué institución confiere la autorización para ello, o iniciar y cursar el o los pagos; por qué período o frecuencia; y para qué finalidad, la que deberá ser suficientemente clara y detallada

para que no haya confusión respecto del propósito para el que se requiere el intercambio y tratamiento de datos.
Dicha solicitud no podrá contener otra información o requerir el consentimiento del titular o cliente para actos o fines distintos.
f) Que los datos sobre los que versa el consentimiento y vigencia de éste sean los estrictamente necesarios para la finalidad respectiva, circunstancia que el PSBI o PSIP deberá acreditar cuando ello sea requerido por la Comisión en el marco de sus procesos de fiscalización, no correspondiendo a la IPI o IPC pronunciarse a ese respecto ni alterar el requerimiento original formulado por la PSBI o PSIP en el marco del SFA.
g) Que la información que se pone en conocimiento del titular o cliente para obtener el consentimiento esté expresada en un lenguaje sencillo, claro, preciso y evitando tecnicismos, salvo en los casos en que resulte estrictamente necesario, debiendo explicarlos claramente. Además, deberá disponer de mecanismos que permitan a personas en situación de discapacidad acceder a esta información.
h) Una vez que el titular o cliente haya otorgado el consentimiento se le deberá informar que, tanto el PSBI o PSIP como la IPI o IPC, pondrán a su disposición un panel de control y la forma en que podrá acceder al mismo, mediante el cual podrá conocer, verificar y revocar los consentimientos que haya otorgado.
i) Que el titular de los datos o cliente se haya autenticado conforme a los estándares que para ello se establecen en la sección III.C de esta normativa. Lo anterior, salvo en el caso de modificaciones en la finalidad o en el período de vigencia del consentimiento -sobre el mismo tipo de información-, en que no se requerirá que quien otorga el consentimiento ante la PSBI o PSIP deba autenticarse en la IPI o IPC.
Queda prohibido a la IPI o a la IPC alterar el contenido de la solicitud de consentimiento formulada por la PSBI o PSIP en el marco del SFA, pedir un consentimiento adicional para el mismo intercambio, tratamiento o iniciación, adoptar medidas o prácticas que desincentiven el otorgamiento del consentimiento por los titulares o clientes, o que deterioren la experiencia usuaria de esos titulares o clientes. Al momento de adoptar o implementar nuevas tecnologías, las IPI o IPC deberán propender al uso de aquellas que mejoren la experiencia usuaria y minimicen el número de direccionamientos del usuario en el marco del SFA. Ello no obsta a que en la interfaz que ponga la IPI o IPC a disposición de la persona para su autenticación se permita a ésta seleccionar el o los productos o tipos de productos para los cuales quiere acotar el intercambio o tratamiento de información. La interfaz de la IPI o IPC no podrá contener opciones pre marcadas o marcadas por defecto

ni tampoco incorporar otra información que no le haya sido comunicada por la PSBI o PSIP para efectos de producirse la autorización de intercambio de información debiendo tales IPI e IPC velar porque el proceso de autenticación ocurra en un solo paso. La interfaz de la PSBI o PSIP, con el objeto de facilitar la especificación del período, podrá dar opciones predeterminadas (Por ejemplo, un solo uso, 7 días, 1 mes, 3 meses, 6 meses y 12 meses), no obstante que, tratándose de intercambio de información, podrá incorporar la opción "mientras dure el contrato o prestación del servicio".

Una vez ~~otorgado el consentimiento~~ autenticado el o los usuarios, según corresponda, ~~deberá ser comunicado y almacenado simultáneamente tanto por la PSBI o PSIP como por la IPI o IPC respectiva~~ la IPI o IPC deberá comunicar ese hecho en tiempo real a la PSBI o PSIP, de manera que el consentimiento válidamente otorgado pueda quedar almacenado tanto en la IPI o IPC como la PSBI e PSIP respectiva.

Para efectos de lo establecido en esta normativa, la Finalidad es el propósito o motivo específico y explícito por el cual el usuario autoriza que sus datos financieros o los datos de la persona a la que está representando, sean compartidos dentro del SFA. En virtud de lo establecido en el artículo 19 de la Ley N°21.521, esa finalidad necesariamente debe tener relación con la prestación de un servicio toda vez que las consultas, acceso y recepción datos en el marco del SFA es para efectos de proveer servicios a los clientes. En tal sentido, no es una finalidad legítima en el marco del SFA la mera cesión de datos personales. Ello, en ningún caso obsta a que la PSBI o IPC pueda efectuar el tratamiento de datos a través de un tercero mandatario o encargado. La naturaleza secreta o reservada de dicha información deberá resguardarse en todo momento, incluso después de concluida la operación o de finalizada la relación que dio origen a su conocimiento.

1. Gestión del consentimiento y obligaciones de información

Las PSBI, PSIP, IPI e IPC deberán poner a disposición de los titulares de datos y clientes un panel de control a través del cual puedan conocer, verificar y revocar los consentimientos que hayan otorgado.

Este panel de control deberá cumplir las siguientes condiciones y requisitos, independiente de si es puesto a disposición de los titulares o clientes directamente por la institución o por terceros por cuenta de ésta:

a) Deben ser de acceso gratuito y remoto para el titular o cliente.

b) Deben contar con una interfaz fácil de utilizar, esto es, que permita al titular o cliente conocer y revocar los consentimientos de manera simple e intuitiva. Además, deberán considerar los mecanismos dispuestos en el numeral 1.g), anterior.

c) Deben contar con mecanismos de autenticación equivalentes a los exigidos en la Sección III.C de esta normativa.

d) La interfaz debe permitir obtener el detalle de cada consentimiento otorgado, de manera que ese titular o cliente pueda informarse respecto a:

   i. La institución a la que otorgó el consentimiento para intercambiar, tratar, ceder o adquirir sus datos, o iniciar y efectuar el pago. Para lo cual deberá indicarse el nombre comercial o de fantasía, así como razón social.

   ii. La finalidad específica para la cual se otorgó dicho consentimiento.

   iii. El tipo de información cuyo intercambio, tratamiento o cesión fue consentido.

   iv. Fecha en la que se otorgó el consentimiento, incluida la hora en que se registró el mismo, permitiendo así identificar adecuadamente la existencia de múltiples consentimientos otorgados durante un mismo día.

   v. Plazo, frecuencia o período para el que el consentimiento fue otorgado.

   vi. Estado actual del consentimiento respectivo, es decir, si está vigente, suspendido, caducado o revocado.

   vii. La identificación del o los representantes legales o mandatarios que otorgaron o revocaron el consentimiento por esa persona, en caso de que corresponda.

e) Contar con un sistema o mecanismo de registro que permita preservar, de manera íntegra y por al menos 5 años, los accesos e interacciones efectuadas por los titulares, que esté a disposición de la Comisión para sus procesos de fiscalización.

f) Permitir la visualización de todos los consentimientos que han sido otorgados, revocados o caducados durante los últimos 5 años.

g) Contar con un sistema destinado a prevenir y evitar que se continue efectuando iniciaciones de pago, intercambio o tratamiento de datos una vez revocado el consentimiento. Para lo anterior, dicho sistema deberá contar con un mecanismo de

comunicación asincrónica en tiempo real basada en eventos con los demás implementados por las PSBI, PSIP, IPI e IPC para ~~mantener actualizados~~ que cambios en los estados de los consentimientos sean comunicados a la IPI, IPC, PSBI o PSIP respectivas en tiempo real, de manera que el cliente pueda gestionar sus consentimientos indistintamente en la PSBI o IPI, PSIP o IPC respectiva.

En caso de que el titular de los datos o cliente no acceda al panel de control habilitado por la PSBI o PSIP por un periodo de más de un año calendario y existan consentimientos vigentes, se deberá enviar una comunicación al lugar o medio que el titular o cliente haya establecido para ese efecto en la que se le recuerde que existe dicho panel de control a través del cual puede gestionar el o los consentimientos otorgados, así como revisar los consentimientos caducados y revocados. Dicha comunicación se deberá remitir dentro de los cinco primeros días hábiles inmediatamente posteriores al cumplimiento de ese año de inactividad.”

9. SE INCORPORA LA SIGUIENTE INFORMACIÓN EN EL ANEXO 3:

En la Sección VI: Anexo Normativos, Anexo N°3: Anexo Técnico, se incorporan lo siguiente:

"SECCIÓN VI. ANEXOS NORMATIVOS

ANEXO 3: ANEXO TÉCNICO

I. INFRAESTRUCTURA Y FUNCIONAMIENTO: DIRECTORIO

A. ASPECTOS GENERALES DE FUNCIONAMIENTO DEL DIRECTORIO

El Directorio es un componente de arquitectura que permite validar a los participantes del SFA para interactuar entre ellos a través de APIs. Junto a lo anterior cumple la función de ser un repositorio de información necesaria para la interoperabilidad de los participantes. Este componente será administrado por la CMF.

Principios del directorio:

1. Este es bajamente acoplado (Directorio estará desacoplado de las transacciones), y sigue los principios once-only y de fuentes auténticas. Además, no debe afectar el flujo transaccional de intercambio de información entre los participantes.

2. El Directorio contará con servicios de verificación del estado de los participantes, pero que solo deberán ser utilizados en el proceso de DCR, y en ningún caso en el flujo transaccional de intercambio de información entre los participantes.

3. La API expone un segundo servicio liviano para obtener el timestamp de la última actualización del Directorio, que servirá al participante del SFA para saber si posee una copia actualizada. Este servicio debe ser consultado por los participantes al menos una vez cada 8 horas.

4. Cada participante debe implementar una interfaz, de manera que pueda recibir notificaciones cada vez que el Directorio se actualice. Para lo anterior, cada entidad deberá ingresar la dirección de su webhook para recibir esta notificación.

5. Los tipos de actualizaciones que podrán ser recibidas son las siguientes:

- Cuando se incorpora una entidad al Directorio
- Cuando se modifica el estado de un participante.
- Cuando una entidad tiene una cancelación del registro.
- Cuando se modifican los certificados digitales de identidad.
- Cuando se modifica información de los participantes relacionada a elementos necesarios para el intercambio de información.

B. REGISTROS DE INSTITUCIONES EN EL DIRECTORIO

El registro de las instituciones en el Directorio será un proceso a cargo de la CMF, quien tendrá credenciales para la organización dentro del Directorio, así como también datos de acceso de sus representantes para la gestión de información restante necesaria, como por ejemplo datos de registro, URL de endpoints, certificados digitales, entre otros.

C. SOBRE LA EXISTENCIA DE MÚLTIPLES MARCAS

Una IPI puede tener más de una marca en el Directorio. Esta opción permite que una entidad legal, que tenga más de una marca comercial con sus respectivos logos e imágenes, pueda mantener esta marca en la relación que sus clientes tengan con el Sistema de Finanzas Abiertas. Estas marcas adicionales deben ingresarse a la CMF por el mismo canal mediante el cual se ingresó el registro inicial. Cada una de estas marcas podrá tener un logo y servidor de autorización distintos. No obstante, para todos los efectos, habrá solo un participante registrado para aquellos que tengan más de una marca.

Cuando una entidad considere inscribir una nueva marca, debe haber antes realizado el proceso de autorización/visado de la CMF para utilizarla.

D. INFORMACIÓN DEL DIRECTORIO

El Directorio requiere dos tipos de información:

- **Información necesaria para funcionamiento**. Se define como información crítica aquella que es necesaria para que opere el SFA con normalidad, desde el punto de vista transaccional. Detalle en Tabla 1.
- **Información complementaria**. Información que no es estrictamente necesaria para que se pueda realizar un intercambio en el SFA, no obstante, que si es necesaria de compartir por temas normativos. Detalle en Tabla 2.

Tanto la información necesaria para el funcionamiento como aquella complementaria podrá siempre actualizarse vía WEB. En algunos casos, según

se especifica en las APIs del Directorio, cierto tipo de información adicionalmente se podrá actualizar vía APIs también.

Tabla 1: Información necesaria para funcionamiento

Descripción de la información	Modificado por
Identificador del participante dentro del SFA	CMF
Rut del participante, sin dígito verificador	CMF
Dígito verificador del participante	CMF
Nombre del participante	CMF
Marca del participante	CMF
Indica si es PSBI	CMF
Indica si es PSIP	CMF
Indica si es IPI	CMF
Indica si es IPC	CMF
Fecha de inscripción al SFA	CMF
Estado del registro del participante en el SFA	CMF
Estado de las API del participante	Participante
URL de la API que contiene los endpoints de producción del participante	Participante
URL de la API que contiene los endpoints alternativos del participante	Participante
Autoridad certificadora del participante	Participante
Validez del certificado del participante	Participante
Llaves públicas del participante	Participante
Lista de servidores de autorización	Participante
Lista de declaraciones de software	Participante

Tabla 2: Información complementaria

Variable	Descripción
Logo	Logo de la institución
Información contacto técnico	Información referente al contacto técnico del participante: Nombre, teléfono e email
Dirección	Dirección
Representantes	Información de los representantes
Mantenciones programadas	Calendario de mantenciones programadas

E. REGISTRO DE INFORMACIÓN DE INTEGRACIÓN

Todos los registros de información que no son de origen automatizado deben ser hechos vía portal WEB, pudiendo en algunos casos ser actualizables también desde una API.

Los cambios en estos registros serán puntuales, no necesitando de un desarrollo complejo para actualizarlos. Los representantes deben hacer la gestión utilizando credenciales entregadas por la CMF en el registro de la organización.

F. COPIA LOCAL

Los participantes serán notificados vía Webhook si hubo cambios del Directorio que impliquen actualizar la copia local. Acto seguido, el participante debe consumir el endpoint respectivo del Directorio para descargar en su copia local la versión actualizada del Directorio. La actualización del Directorio tiene un sistema de confirmación de recepción del mensaje enviado del tipo:

```
{
  "specversion": "1.0",
  "type": "cl.sfa.participant.new",
  "source": "directorio",
  "subject": "New participant",
  "id": "xkjskk3984jcka",
  "time": "2024-08-06T17:31:00Z",
  "datacontenttype": "application/json",
  "data": {
    "participantId": "ID"
  }
}
```

Cuando un participante tenga que notificar información al Directorio, deberá utilizar el endpoint /message-receiver del Directorio. Los tipos de actualizaciones soportadas por el sistema son los siguientes:

- cl.sfa.participant.new
- cl.sfa.participant.change.role
- cl.sfa.participant.change.cert
- cl.sfa.participant.left
- cl.sfa.participant.suspended
- cl.sfa.participant.cs.suspended
- cl.sfa.participant.cs.inactive
- cl.sfa.participant.cs.alternative

Donde “cl” hace referencia a Chile, “sfa” al Sistema de Finanzas Abiertas, “participant” a que es referido a un participante, y “cs” a que es un evento de ciberseguridad.

El payload del endpoint de participants, necesario para la actualización de la copia local se muestra a continuación:

```
[
  {
    "cmf_id": "xyz",
    "rut": 12345,
    "dv": "x",
    "name": "example",
    "brand": "example",
    "is_psbi": true,
    "is_psip": true,
    "is_ipi": true,
    "is_ipc": true,
    "enroll_date": "2025-01-11T17:09:17.759Z",
    "sfa_status": "ACTIVO",
    "sandbox_url": "string",
    "api_resources": [
      {
        "api_name": "ENROLAMIENTO",
        "api_status": "ACTIVO",
        "prod_api_endpoints_url": [
          "https://server.example/open-finance/v1/customer/pn",
          "https://server.example/open-finance/v1/customer/pj"
        ]
      }
    ]
  }
]
```


A su vez, los campos obtenidos a través de la API del Directorio serán los siguientes:

- logo uri (BLOB): Logo de la institucional
- technical contact uri (Array:String): información del contacto técnico del participante: teléfono, email.
- address uri (String): Dirección
- representatives uri (Array:String): Representantes del participante
- maintenance schedule uri (dateTimeString): Calendario de mantenciones programadas.

Por otro lado, el payload del endpoint public-keys es el siguiente:


```
[
  {
    "cmf_id": "string",
    "cert_ca": "string",
    "cert_val": "2025-11-11T23:59:59.999Z",
    "alg": "string",
    "key_ops": "string",
```

```
    "kid": "string",
    "kty": "string",
    "use": "string",
    "x5c": [
      "string"
    ],
    "x5t": "string",
    "x5thashS256": "string",
    "x5u": "string"
  }
]
```

G. API DEL DIRECTORIO

Las APIs que tendrá el Directorio son aquellas que la CMF tenga habilitadas en su Portal Desarrollador del SFA, que para todos los efectos administra la Comisión.

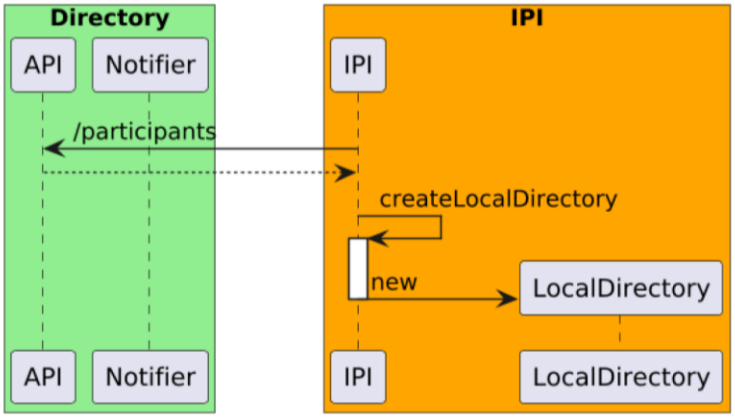
Cada participante del SFA tendrá una copia local del Directorio, la cual será actualizada periódicamente según se establece en la sección II, letra C de la norma. La responsabilidad de esta actualización es compartida:

- Es responsabilidad del participante del SFA consultar periódicamente el endpoint expuesto la última fecha de actualización del el Directorio (método head del endpoint del participante), de tal manera de verificar que la fecha y hora de actualización de la copia local corresponda con la fecha y hora de modificación entregada por el Directorio.
- Es responsabilidad del Directorio enviar una notificación a los participantes del SFA informando los cambios que hayan ocurrido.
- Para ello, es responsabilidad de cada participante mantener un endpoint /notifyupdate y /notify-incident, ambos de tipo POST operativo.
- Es responsabilidad del Directorio mantener el endpoint /message-receiver de tipo POST operativo.
- Cada participante del SFA consumirá el endpoint /lastupdate de manera periódica. En particular, la IPI, al menos cada 8 horas, deberá consumir el recurso /last-update, el cual le retorna un timestamp con el momento en que el Directorio fue actualizado por última vez. Con esta información la IPI compara la fecha de actualización de su copia local con respecto a la recibida, y prepara su copia local para ser actualizada. Se pedirá entonces la información de los participantes del SFA al Directorio a través del endpoint /participants. El Directorio responde con la información de los participantes al IPI, y este comienza el proceso de actualización de su copia local.

Flujos de información

A continuación, se presenta un flujo normal de información para cualquier caso de uso. El primer paso para cualquier participante que entra por primera vez al SFA es crear su copia local del Directorio. Dado que toda llamada al Directorio debe enviar el access-token en el header del request, por simplicidad en los diagramas no se explicita la interacción de la IPI para obtener el access-token correspondiente. En la Figura 1 se puede ver este proceso.

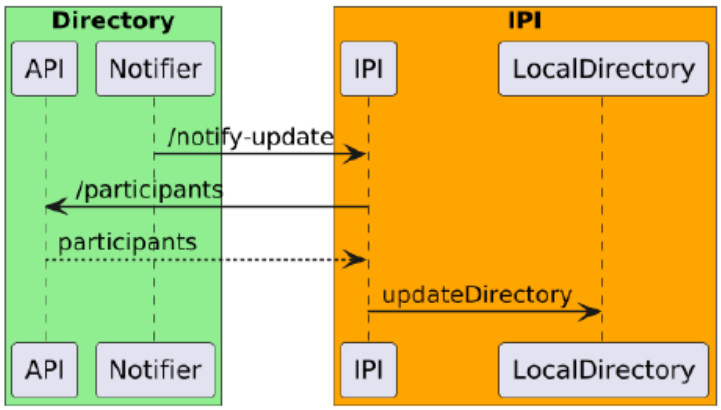
Figura 1: Proceso de creación de copia local



La Figura 1 muestra el proceso de creación del Directorio local. En este caso, una IPI (puede ser también una PSBI) está entrando por primera vez al sistema, y consume el recurso de participantes desde el Directorio a través de un método GET sobre el endpoint /participants. El Directorio responde a este REQUEST con la copia del Directorio. Cuando el participante del SFA recibe esta información por primera vez, gatilla un proceso de creación de copia local. Finalmente, luego de finalizado este proceso, el participante del SFA cuenta con una copia local actualizada en su servidor.

Cuando hay algún cambio en el Directorio, este se encarga de enviar un mensaje a los participantes del SFA, como muestra la Figura 2.

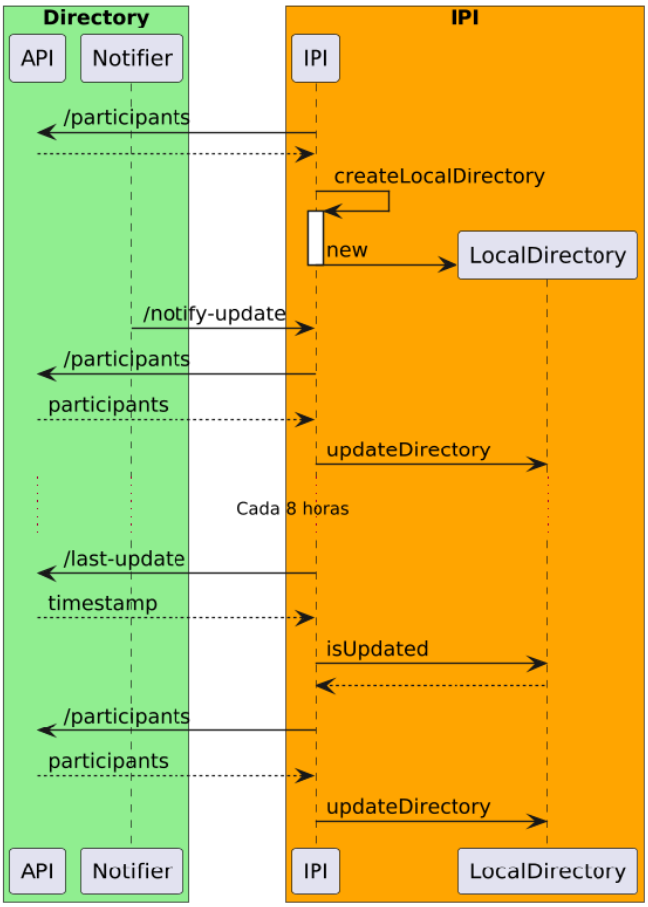
Figura 2: Actualización de la copia local del Directorio en un participante del SFA a través de una notificación del Directorio



La Figura 2 muestra la actualización de una copia local del Directorio de un participante del SFA debido a una actualización enviada desde el Directorio. Primero, el Directorio genera un notify-update mediante el cual avisa al IPI (o PSBI) que el Directorio ha tenido cambios. Luego de esto, la IPI (o PSBI) obtiene la copia del Directorio utilizando un método GET sobre el endpoint /participants del Directorio, para posteriormente actualizar su copia local. Siempre, luego de un notify-update existe por parte del integrante del SFA una petición GET para obtener los participantes del Directorio.

La Figura 3 muestra un ejemplo de interacción entre un participante del SFA y el Directorio durante su permanencia en el sistema. En esta figura puede verse la creación de la copia local del Directorio, la actualización producto de una notificación, y la actualización periódica de la copia local.

Figura 3: Interacción entre un participante del SFA y el Directorio durante su permanencia en el sistema



H. CONTINUIDAD DEL DIRECTORIO

Sobre el funcionamiento en caso de indisponibilidad del directorio.

En caso de indisponibilidad del Directorio por una contingencia no controlada, los participantes deberán ocupar la copia local con la última actualización disponible para continuar con los procesos de intercambio de información hasta que el servicio del directorio se encuentre reestablecido.

I. MÓDULO DE COMUNICACIONES

El Directorio tendrá dos fuentes de actualización. La primera son los cambios que introduce la CMF al Directorio para reflejar cambios en los Registros y Nóminas de las entidades participantes que mantiene la CMF. De esta manera es la CMF la que agregará entidades a los Registros y Nóminas, eliminará

entidades (ya sea por cancelación o por salida voluntaria) y establecerá cuales entidades están suspendidas. La segunda, son cambios ingresados al Directorio efectuados directamente por los propios participantes. Para incorporar esta información por parte de los participantes al Directorio deberá implementar una API POST.

De esta manera, el módulo de comunicaciones del Directorio quedará conformado por los siguientes componentes:

- APIs del Directorio: GET, POST, PUT.
- Mensajería del directorio para difundir información de actualizaciones a través de Webhook.
- Actualización de información mediante WEB o APIs por parte del participante.
- Canal de comunicación alternativa para eventos de continuidad y seguridad del Directorio o eventos de seguridad del sistema.

A su vez, la mensajería de la API POST del Directorio tendrá el estándar:

- Cuando se incorpora una entidad al Directorio “type”: cl.sfa.participant.new
- Cuando se modifica un rol “type”: cl.sfa.participant.change.role
- Cuando se modifican los certificados “type”: cl.sfa.participant.change.cert
- Cuando una entidad sale del Directorio “type”: cl.sfa.participant.left
- Cuando una entidad es suspendida “type”: cl.sfa.participant.suspended
- Cuando una entidad es suspendida por ciberseguridad “type”: cl.sfa.participant.cs.suspended
- Cuando una entidad es inactiva “type”: cl.sfa.participant.cs.inactive
- Cuando una entidad está en mecanismo alternativo “type”: cl.sfa.participant.cs.alternative.

Y de acuerdo con el siguiente payload:

```
{
  "specversion": "1.0",
  "type": "cl.sfa.participant.new",
  "source": "directorio",
  "subject": "New participant",
  "id": "xkjskk3984jcka",
  "time": "2024-08-06T17:31:00Z",
  "datacontenttype": "application/json",
  "data": {
    "participantId": "ID"
  }
}
```

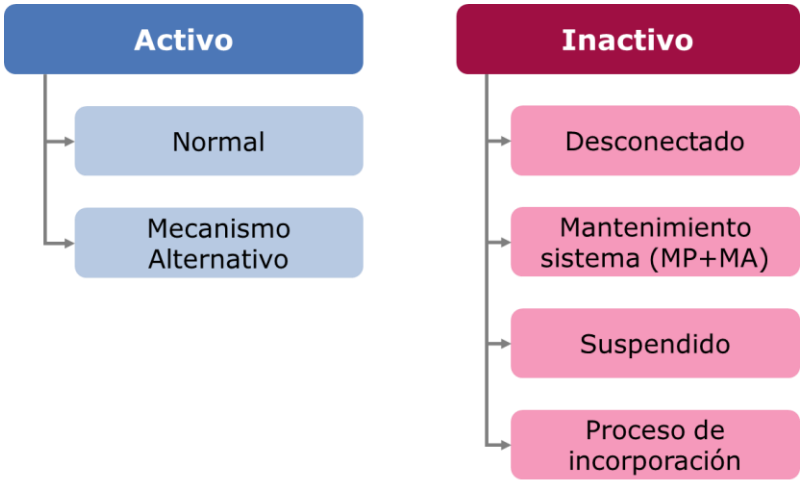
Cabe destacar que hay además canales de comunicación existentes en la CMF que se utilizan en el SFA:

- Canales de ingreso de información para la mantención de los Registros y Nóminas (mediante CMF Supervisa).
- Reporte de Incidentes Operacionales (RIO)

J. ESTADOS DE LOS PARTICIPANTES EN EL DIRECTORIO

Cada participante del Directorio estará en un estado, como se muestra en la Figura 4:

Figura 4: Estados de los Participantes del SFA



Como lineamientos generales se tiene que:

- Toda entidad que está ya sea en la lista de Nómina de IPI, Nómina de IPC, Registro PSIB o Registro PSIP, está en algún estado en el Directorio.
- Entidades que están aún en un proceso de licenciamiento no son parte del Directorio.
- Toda entidad que es cancelada sale del Directorio.

Hay 6 estados del directorio agrupados en: activos e inactivos. La diferencia entre ambos es que cuando hay un participante "activo" hay intercambio de información, versus cuando esta "inactivo" donde no hay intercambio de información. Cada uno de los 6 estados son excluyentes, es decir, no es posible que una entidad este en más de un estado al mismo tiempo.

El detalle de cada estado y un esquema de flujo de cambios se muestran en la siguiente Tabla 3:

Tabla 3: Estados de los Participantes del SFA y características

Estado	Descripción general	Quien lo activa	Quien lo desactiva	Método de activación y desactivación
Tipo: Activos				
Normal	Estado general, funcionamiento del mecanismos principal y alternativo en orden	CMF	No aplica	CMF de forma directa en el Directorio
Mecanismo alternativo	Cuando el participante no tiene habilitado el mecanismo principal y solo tiene habilitado el mecanismo alternativo	Participante (IPI/IPC)	Participante (IPI/IPC)	Propio participante mediante acceso a cambio de estado en Directorio
Tipo: Inactivos				
Desconectado	Cuando la entidad se autodesconecta del sistema por los motivos especificados en la normativa.	Participante (IPI/IPC/PSBI/PSIP)	Participante, a menos que la CMF haya aplicado el estado "suspendido", el cual tiene prioridad.	Propio participante mediante acceso a cambio de estado en Directorio. Si es que no está ahora en el estado "Suspendido"
Mantenimiento sistema (MP+MA)	Cuando el mantenimiento programado afecta tanto al mecanismo principal como alternativo.	Participante (IPI/IPC)	Participante (IPI/IPC)	Propio participante mediante acceso a cambio de estado en Directorio
Suspendido	Cuando la entidad es suspendida por la CMF	CMF	CMF	Lo activa y desactiva la CMF mediante su panel de control en el Directorio

Proceso de incorporación	Estado inicial de una entidad que entra al Directorio cuando es parte de un registro o nomina[1]	CMF	CMF	CMF de forma directa en el Directorio

[1] Considera este estado el proceso de actualización de elementos técnicos desde el entorno de pruebas a productivo, por ejemplo, la actualización de los certificados de identidad preliminares a finales.

II. CERTIFICADOS DIGITALES DE IDENTIDAD

A. AUTORIDADES CERTIFICADORAS DEL CERTIFICADO DIGITAL DE IDENTIDAD

Se considerarán dos capas de certificados SSL, entregados por entidades certificadoras raíz e intermedia.

Ambos tipos de autoridades certificadoras deberán contar con los requisitos necesarios para ejercer la actividad (tener un informe de auditoría o una declaración de certificación disponible publica que cumpla con el esquema WebTrust para CA[2] o posterior o ETSI EN 319 411[3]) y cumplir con las características de funcionamiento en sus respectivas jurisdicciones.

Los participantes además deberán implementar RFC8659[4] (DNS Certification Authority Authorization (CAA) Resource Record) con el fin de especificar cuáles son las Autoridades de certificación autorizadas para emitir certificados y DNSSEC con el fin de proteger contra ataques de falsificación de dominio entre otros.

B. SOBRE LA OBTENCIÓN DEL CERTIFICADO DIGITAL DE IDENTIDAD

Una vez las entidades estén registradas en el caso de los PSBI o inscritas en las nóminas en el caso de las IPI, las entidades deberán actualizar información en el Directorio, pasando su información a estado final y así poder activarse en el mismo.

Para el registro del Certificado en el Directorio se deben seguir los siguientes pasos:

1. Registro de la institución en el Directorio.
2. La institución genera manualmente un Certificate Signing Request (CSR), siguiendo las instrucciones definidas por la CA.
3. La institución debe registrar su certificado en el Directorio.
4. El Directorio confirmará, entre otras cosas, los datos del certificado y su validez.

[2] Se debe contar con la versión 2.7 -SSL Baseline con seguridad de red o posterior.
[3] Se considerará la versión ETSI EN 319 411-1 (v1.3.1 o más reciente) o ETSI EN 319 411-2 (v2.4.1 o más reciente)
[4] https://datatracker.ietf.org/doc/html/rfc8659

C. VALIDACIÓN DE FIRMAS

El flujo para validar las firmas contra el Directorio es:

1. Obtener clave pública que estará disponible en el Directorio de Participantes y validar la firma del mensaje. Esta validación debe ser hecha por los participantes durante el procesamiento del mensaje.
2. Validar la cadena del Certificado Digital X.509. Será hecho por el Directorio durante el registro del certificado.

D. REGISTRO DINÁMICO DE CLIENTES

Se utilizará para la implementación lo dispuesto en RFC7591[5] (DCR) y RFC7592[6] (DCRM), incluyendo el perfil de seguridad de OpenID connect.

El servidor de autenticación como requisito de funcionamiento del DCR, expondrá sus metadatos según RFC8414[7] (OAuth 2.0 Authorization Server Metadata), lo que garantiza el funcionamiento del DCR.

La firma de los SSA (Software Statement Assertion) será firmada por el directorio.

[5] https://datatracker.ietf.org/doc/html/rfc7591
[6] https://datatracker.ietf.org/doc/html/rfc7592
[7] https://datatracker.ietf.org/doc/html/rfc8414

III. PORTAL WEB DE DESARROLLADORES

Este portal se será proporcionado y gestionado por la CMF y considerará la siguiente información:

1. Documentación Técnica
   - Estándares de desarrollo: Especificaciones técnicas adoptadas por el ecosistema.
   - Especificaciones de las API: Guías detalladas para el desarrollo e integración de servicios.
   - Requerimientos no funcionales: Definición de límites operacionales, umbrales, TPS, TPM, etc.
   - Especificaciones de seguridad: Perfil de seguridad y lineamientos de implementación.
   - Directrices de implementación: Detalles técnicos de los componentes SFA.
   - Guías y manuales: Documentación de apoyo integral al ecosistema.
   - Glosario: Definición de términos técnicos y financieros clave.

2. Recursos para Desarrolladores
   - Referencias de codificación: Ejemplos y patrones de desarrollo.
   - Flujos de información/conexión: Diagramas y esquemas para la integración de APIs.
   - Sandbox: Entorno controlado para pruebas funcionales y de seguridad.
   - Servicio de iniciación de pagos: Recursos y especificaciones para habilitar pagos seguros.

3. Soporte y Comunidad
   - FAQ: Guía de preguntas frecuentes.
   - Recursos de soporte técnico: Contacto para resolver problemas de desarrollo.
   - Comunidad: Espacio colaborativo para desarrolladores, foros y eventos.

4. Actualizaciones del Portal
   - Nuevas versiones de las APIs: Publicaciones y cambios significativos.
   - Mejoras importantes: Ajustes y optimizaciones del ecosistema.
   - Actualización del sandbox: Notificaciones sobre cambios o nuevas funcionalidades.
   - Alertas en tiempo real: Cambios y mantenimientos comunicados oportunamente.

El contenido del portal del desarrollador será un proceso iterativo y evolutivo. No toda la información que se describe en este apartado necesariamente estará disponible en el portal en el momento de su implementación. Cada vez que se establezca una nueva versión del portal de desarrollador se informará a los participantes, indicando las modificaciones y desde cuando se hacen exigibles.

El portal web de desarrolladores estará disponible en la siguiente URL: https://cmfchile.atlassian.net/wiki/x/yIHiDw.

IV. AMBIENTE DE PRUEBAS DE LA CMF Y CERTIFICADOS FUNCIONALES

A. AMBIENTE DE PRUEBAS CMF

El Ambiente de Pruebas (en adelante, AP) provista por la CMF incluye todas las APIs del Sistema de Finanzas Abiertas:

- APIs del Directorio
- APIs de entrega de información
- Gestión del consentimiento

El AP tiene acceso restringido, el que será otorgado por la CMF a través de un proceso de solicitudes. Este AP cumple con dos funciones: permitir habilitar un área de prueba para los procesos de certificación que deberán realizar los certificadores externos, y servir como un Sandbox para PSBIs o IPIs que quieran desarrollar productos nuevos. De esta manera, el AP no realizará certificaciones, sino que provee un espacio tecnológico donde se pueden realizar. El AP estará actualizado y será consistente con el Portal del Desarrollador.

B. PRUEBAS FUNCIONALES DE IPIS EN EL AMBIENTE DE PRUEBAS DE LA CMF

Las IPIs deberán realizar pruebas contra todos componentes del sistema de finanzas abiertas. En particular deberán realizar las siguientes pruebas en AP:

- Probar actualizar información en el AP (cambios de estados e información general).
- Descarga del directorio de prueba local.
- Uso del sistema de mensajería en AP (por ejemplo, simular informar uso de mantenciones programadas).

Estas pruebas deberán ser parte del requisito de la sección I.E.1.c. de la norma.

C. PRUEBAS FUNCIONALES DE IPIS QUE NO SE REALIZAN EN EL AMBIENTE DE PRUEBAS DE LA CMF

Respecto a las otras pruebas que deben ejecutar los IPIs que no son realizables dentro del AP tenemos aquellas relacionadas al mecanismo alternativo y aquellas que no. Respecto a estas últimas, deberán considerarse al menos las siguientes:

- Validación de Endpoints de TyCs (urls, contenido, y formato)

- Validación de Endpoints de Canales de Atención (urls, contenido, y formato)
- Validación de Endpoints de consumo de datos (urls, autenticación, contenido y formato).
- Simulación de un registro de un PSBI como nuevo cliente.
- Prueba de flujo de entrega de Access token a PSBI en nombre de un usuario real.
- Validación de Access token emitido para consultar información.
- Pruebas funcionales del Panel de Control.

Estas pruebas deberán ser parte del requisito de la sección I.E.1.c. de la norma.

D. PRUEBAS FUNCIONALES DE PSBIs EN EL AMBIENTE DE PRUEBAS DE LA CMF

Las pruebas funcionales de los PSBI consideradas en la sección I.C.1.2.l de Consumo de APIs deberá ser realizadas en el área de pruebas que tiene a disposición la Comisión que para todos los efectos es el Sandbox. En función de los datos que desee consultar el PSBI en el sistema son las APIs que deberá probar en el Sandbox. Para poder acceder en producción a intercambiar información de una API, necesariamente debe haber probado esta API en el Sandbox.

La certificación que deberá realizar la entidad certificadora será integral y deberá abordar el siguiente listado de procesos:

- Uso de Directorio
- Registro de Clientes de las PSBI en las IPI
- Flujos de datos de términos y condiciones de las IPIs
- Flujo de consentimiento
- Obtención de datos personales de clientes

Estas pruebas deberán realizarse contra el AP provisto por la CMF. Un listado (no exhaustivo) del plan de pruebas a realizarse se presenta en las siguiente Tabla 4:

Tabla 4: Prueba de Integración

Título	Descripción	Plataforma	Operación	Resultado esperado
Pruebas de consumo	PSBI solicita autorización al IPI y verifica que la redirección al endpoint de autorización es exitosa.	PSBI	Solicitar autorización	PSBI debe ser redirigido correctamente a la página de autorización del IPI.
Verificar generación de token con client credentials grant	PSBI genera un token utilizando el flujo denominado 'client_credentials_grant'.	PSBI	Generar token	PSBI debe recibir un token de acceso, generado mediante el flujo 'client_credentials_grant'.
Verificar generación de token con authorization code	PSBI verifica que el IPI genere un token con el código de autorización.	PSBI	Generar token	PSBI debe recibir un token de acceso, utilizando el código de autorización.
Registrarse en el IPI: obtener client_id y client_secret	PSBI realiza el proceso de registro en el IPI y obtiene su client_id y client_secret.	PSBI	Registrar cliente	PSBI debe recibir un client_id y client_secret.
Solicitar o recuperar otro código de autorización	PSBI solicita un nuevo código de autorización con base en los parámetros enviados por el cliente.	PSBI	Obtener código	PSBI debe recibir un nuevo código de autorización.
Enviar uno o más mensajes a la CMF	PSBI envía uno o varios mensajes a la CMF con información del cliente.	PSBI	Enviar mensajes	PSBI debe recibir confirmación de que los mensajes fueron enviados correctamente.
Solicitar términos al IPI	PSBI solicita al IPI los términos y condiciones disponibles.	PSBI	Obtener términos	PSBI debe recibir los términos y condiciones disponibles.
Solicitar autorización masiva con información de cuentas, tarjetas, productos financieros	PSBI solicita autorización masiva con información del cliente.	PSBI	Solicitar autorización	PSBI debe recibir autorización para los datos de cuentas, tarjetas, productos financieros, etc.

Estas pruebas deberán ser parte del requisito de la sección I.C.1.l de la norma.

E. PRUEBAS FUNCIONALES DE LAS PSBI QUE NO SE REALIZAN EN EL AMBIENTE DE PRUEBAS DE LA CMF

Deberá considerarse dentro de las pruebas funcionales la realización de pruebas sobre los paneles de control de consentimiento.

Estas pruebas deberán ser parte del requisito de la sección I.C.1.l de la norma.

F. SOBRE LOS HITOS PARA PARTICIPAR EN EL DIRECTORIO Y SANDBOX.

Tanto las IPI como los PSBI deberán participar del Sandbox de la CMF para efectos de realizar sus pruebas funcionales como pruebas de integración con el Directorio. A continuación, se explican los requisitos mínimos de cumplimiento normativos para poder acceder a estas áreas de prueba.

IPI

En el caso de las IPI, ellas podrán participar del Sandbox desde el momento que presentan su solicitud de inscripción como IPI. Una vez entregados estos antecedentes, pueden iniciar pruebas funcionales en el Directorio/Sandbox.

PSBI

Para el caso de los PSBI se requerirá al menos haber entregado los siguientes antecedentes previo a la incorporación a las pruebas funcionales en el Sandbox:

- Todos los indicados en el punto "1.1 Contenido de la solicitud"
- Letras (a), (b), (c), (d), (e), (f), (g) y (h) indicadas en el punto "1.2 Antecedentes adjuntos"

Una vez entregados estos antecedentes pueden iniciar pruebas funcionales en el Directorio/Sandbox.

G. ELEMENTOS TECNICOS QUE DEBERAN CONSIDERAR LAS ENTIDADES PARA HACER PRUEBAS EN EL SANDBOX

Las entidades una vez cumplan con los elementos mínimos para acceder al área de pruebas deberán seguir las instrucciones y requisitos funcionales para la ejecución de estas que están descritas en los manuales técnicos que proveerá el Sandbox para estos efectos.

H. REQUISITOS DE LA ENTIDAD CERTIFICADORA DE LAS PRUEBAS FUNCIONALES

Las entidades certificadoras que podrán acreditar el requerimiento letras b y c de la sección I.E.1 en lo que respecta a las IPI y de la letra l de la sección I.C.1 en lo que respecta a las PSBI, deberán cumplir con los siguientes requisitos:

- Experiencia de al menos 3 años realizando pruebas tecnológicas
- Experiencia en APIs
- Experiencia en Cibserseguridad

Una misma entidad certificadora podrá dar cumplimiento a más de un proceso de certificación por entidad.

I. VALIDEZ DE LOS CERTIFICADOS FUNCIONALES

Los certificados de funcionamiento de las APIs y de los PSBI, que estas entidades emitan serán válidos hasta que:

1. Haya un cambio relevante en los estándares del Sistema de Finanzas Abiertas
2. Se incorporen nuevos datos o productos al Anexo 1 de la NCG Nº514
3. La entidad (IPI/PSBI) realice una actualización tecnológica que pueda afectar la interoperabilidad del sistema
4. En el caso de una PSBIs, haya un cambio en el listado de APIs que consumen en su modelo de negocio.
5. En el caso de las IPIs, haya un cambio en los productos que ofrecen.
6. En el caso que se identifiquen nuevas vulnerabilidades y avisos de obsolescencia que emiten los proveedores de las plataformas que soportan las APIs.

En los casos anteriormente listados, la revalidación deberá enfocarse en el cambio efectuado.

Los certificados de funcionamiento de las IPIs y PSBIs serán públicos.

V. INTERCAMBIO DE INFORMACIÓN

A. ESPECIFICACIONES DE LAS APIs

Las especificaciones técnicas que deben considerarse para la estructura de cada API son aquellas que la CMF tenga habilitadas en su Portal Desarrollador del SFA, que para todos los efectos administra la Comisión. Estas especificaciones en caso de tener actualizaciones serán informadas por la Comisión vía mensajería del Directorio y deberán considerarse sus implementaciones en los tiempos considerados e informados también en la misma mensajería.

En aquellos casos donde lo amerite, y sea necesario, estas actualizaciones implicarán la realización de nuevas pruebas funcionales por parte de los PSBI o nuevas certificaciones por parte de las IPIs.

B. CÓDIGOS DE ERROR

Se deben implementar los siguientes códigos de respuesta indicados en la Tabla 5:

Tabla 5: Lista de códigos de respuesta de APIs según RFC 7231

Código	Situación
200 OK	Consulta completada correctamente
201 Created	Ejecución estándar. La solicitud fue exitosa
204 No Content	La solicitud se completó correctamente, pero no hay contenido para devolver. Este código también puede ser utilizado para indicar que una operación de exclusión se completó exitosamente.
304 Not Modified	La respuesta no ha sido modificada desde la última llamada
308 Permanent Redirect	El recurso ha sido movido permanentemente a una nueva URL. El método HTTP no se modifica en la redirección.
400 Bad Request	Encabezado de autenticación ausente/invalido o token invalido. La solicitud fue malformada, omitiendo atributos obligatorios, ya sea en el payload o a través de atributos en la URL.
401 Unauthorized	Encabezado de autenticación ausente/inválido o token inválido
403 Forbidden	El token tiene un alcance incorrecto o se violó una política de seguridad
404 Not Found	El recurso solicitado no existe o no fue implementado
405 Method Not Allowed	El consumidor intento acceder al recurso con un método no soportado

406 Not Acceptable	La solicitud contenía un encabezado ‘Accept‘ diferente de los tipos de medios permitidos o un conjunto de caracteres diferente de UTF-8
409 Conflict	Conflicto en el estado del recurso
410 Gone	Recurso fue borrado o eliminado
415 Unsupported Media Type	La operación fue rechazada porque el payload está en un formato no soportado por el endpoint.
429 Too Many Requests	La operación fue rechazada, ya que muchas solicitudes se realizaron dentro de un período determinado o el límite global de solicitudes concurrentes se alcanzó
500 Internal Server Error	Ocurrió un error en el gateway de la API o en el microservicio
502 Bad Gateway	Problema con el servidor proxy o Gateway
503 Service Unavailable	El servicio no está disponible en este momento
504 Gateway Timeout	El servidor no pudo responder a tiempo
529 Service is overloaded	El servicio está sobrecargado

C. DISPONIBILIDAD Y RENDIMIENTO DE LAS APIS

SLAs de las APIs

Se medirá el tiempo de respuesta de cada solicitud como el tiempo transcurrido entre la recepción de una solicitud en el Gateway de la IPI y el momento en que la solicitud es completamente respondida por el Gateway de la IPI, o TTLB.

La medición se hace por endpoint, utilizando el percentil 95 (descartando el 5% de los peores valores).

Método de cálculo para disponibilidad

Cada IPI debe determinar el mecanismo para monitorear sus APIs, pudiendo ser por ejemplo mediante monitoreo “activo” (tiempo real) o “pasivo” (revisión ex-post de logs).

Respecto al reporte mensual que por norma deben entregar las IPIs con datos diarios, en este informe se deben detallar: tiempos de disponibilidad, momentos de indisponibilidad, cantidad de llamadas totales y cantidad de llamadas exitosas.

En el cálculo de la indisponibilidad se deberán excluir los códigos de error 429 y 529 y las mantenciones programadas. Respecto al error 529 deberá excluirse cuando se alcanza el límite operativo (TPM-TPS), pero no por otra razón.

La unidad de cuenta para medir disponibilidad serán milisegundos y se contará como disponibilidad la capacidad

D. TPM y TPS

Se considerarán como default 10 Transacciones por Segundo (TPS) de una IPI a todos los PSBI y 60 Transacciones por Minuto (TPM) de una IPI a cada PSBI. Lo anterior, considerando:

- Cada métrica a nivel de endpoint
- No se considera el uso del mecanismo alternativo.

Especificaciones adicionales sobre las TPM y TPS:

TPS:

- Se calculan agregando todos los requerimientos que recibe un PSBI/PSIP.
- Se calculan usando el segundo completo, es decir, desde el momento 000ms hasta el momento 999ms de cada segundo, independiente del momento en que el endpoint recibe la primera llamada dentro de ese intervalo
- Solo se contabilizan las llamadas aceptadas y procesadas correctamente, es decir, las que retornan un código HTTP 2XX.
- Si se superan los TPS definidos, cada llamada que lo supere podrá ser contestada con un código de error 529 (Site overloaded) y un header Retry-After con una fecha http en un número random (entre 0 y 5) de segundos para evitar que en episodio de sobrecarga muchos PSBI reintenten en el mismo instante.

TPM:

- Se calcula para cada par endpoint/PSBI o endpoint/PSIP por separado.
- Se calcula usando el minuto completo, es decir, desde el momento 0s000ms hasta el momento 59s999ms de cada minuto independiente del momento en que el endpoint recibe la primera llamada dentro de ese intervalo. Se considera el tiempo de recepción de la llamada para asignar el minuto al que corresponde.
- Solo se contabilizan las llamadas aceptadas y procesadas correctamente, es decir, las que retornan un código HTTP 2XX.
- Si un PSBI o PSIP supera las TPM definidas para un endpoint, cada llamada que lo supere podrá ser contestada con un código de error 429 (Too Many

Requests) y un header Retry-After con una fecha http en el siguiente minuto más un número random (entre 0 y 15) de segundos para evitar que en episodio de sobrecarga muchos PSBI o PSIP reintenten en el mismo instante.

E. MECANISMO ALTERNATIVO

Todas las IPI deberán implementar un mecanismo alternativo (MA) para la entrega de información. En términos técnicos el mecanismo alternativo deberá ser una réplica funcional de la API principal (MP), esto es una réplica de los servicios que esta entrega cumpliendo con los requisitos de seguridad, interoperabilidad y especificaciones técnicas asociados.

El mecanismo alternativo tendrá algunos elementos atenuados de exigibilidad, entre ellos:

- Disponibilidad: 90% de forma diaria por día calendario y de 95% de forma mensual, considerando una base de cálculo diario de 24 horas, empezando y terminando a medianoche. Respecto al tiempo de procesamiento de estas API, ellas deberán procesar transacciones en un tiempo máximo de 5.000 milisegundos.

- Actualización de los datos: hasta 60 minutos en promedio con respecto al mecanismo principal.

El mecanismo alternativo deberá activarse cuando el mecanismo principal y su contingencia no estén disponibles. Adicionalmente, el MA deberá estar ubicado de forma que no comparta los mismos riesgos que el MP y su contingencia, respecto a los objetivos de entrega de información indicados en su definición.

En lo relativo a las medidas se seguridad deberá cumplir con lo contemplado en la RAN 20-7 de la Comisión. El mecanismo alternativo deberá considerar su propio servidor de autorización el que deberá estar sincronizado con el servidor de autorización del mecanismo principal.

El cumplimiento de FAPI 2.0 se sigue requiriendo en la implementación alternativa de la API por parte de todos los participantes. Por otro lado, los identificadores de clientes OAuth (client_id) se mantienen idénticos para el mecanismo alternativo, facilitando la trazabilidad.

Para efectos de lo relativo a los servidores de recursos y mecanismos de acceso interno a la información, las IPI serán responsables de establecer los mecanismos más adecuados dada su infraestructura, tales como acceso directo a cores de negocios, acceso a API intermedias, acceso a portales de información de clientes, entre otros. Sera responsabilidad de la IPI optimizar este mecanismo

de recursos para que la información este siempre disponible en los términos indicados en esta normativa.

Pruebas funcionales del mecanismo alternativo

El mecanismo alternativo antes descrito debe ser probado y estas pruebas deben ser parte del requisito de la sección I.E.1.c. de la norma. En particular en este requisito debe darse cuenta en relación con el MA lo siguiente:

1. Que está correctamente integrado en términos tecnológicos y de infraestructura a la solución de continuidad operacional del IPI.

2. La realización de al menos una prueba de continuidad operacional donde se acredite que el mecanismo principal dejó de funcionar y que el servicio paso al mecanismo alternativo con todos los componentes antes descritos sincronizados correctamente.

F. PRUEBAS DE CALIDAD DE LA INFORMACIÓN

Las Pruebas de Calidad de datos que deben realizar las IPIs deberán:

- Validar los datos contra los datos en otras instancias de almacenamiento y de consulta de las IPIs.

- Realizarse sobre cada uno de las APIs de consulta de datos, a modo de generar una muestra representativa al 95%.

- Entregar el reporte de Calidad a la CMF.

- Mantener los microdatos de las pruebas. Lo anterior, por al menos 2 años.

Para la realización de la prueba de calidad de datos, las IPIs deberán considerar como mínimo los criterios de la Data Management Association (DAMA) indicados en la siguiente tabla:

Tabla 6: Matriz DAMA

Dimensión	Descripción	Métrica
Exactitud (*accuracy*)	Qué tan precisos son los datos en relación a otras instancias	% registros con errores y % de error de los datos
Completitud (*completeness*)	Qué tan completos son los registros en relación con otras instancias	% registros completos
Integridad (*integrity*)	Qué tan correctas son las relaciones entre distintos datos y en el tiempo	% registros íntegros

Actualización (*timelines*)	Qué 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

Todo lo anterior deberá ser provisto en un informe donde se expliquen las cifras y caminos de acción en casos donde se observen deficiencias. El contenido de este informe se encuentra en la sección VIII de este Anexo.

G. MARCHA BLANCA

Las IPI verán reducida la exigibilidad de sus APIs por un periodo de 6 meses a contar del momento de inicio operativo de cada APIs en el sistema. Los elementos que se verán atenuados en términos de exigibilidad son:

- Disponibilidad: 90% de forma diaria por día calendario y de 95% de forma mensual, considerando una base de cálculo diario de 24 horas, empezando y terminando a medianoche. Respecto al tiempo de procesamiento de estas API, ellas deberán procesar transacciones en un tiempo máximo de 5.000 milisegundos.

- Actualización de los datos: hasta 60 minutos en promedio con respecto al mecanismo principal.

Una vez terminados estos 6 meses aplicarán los requerimientos normales establecidos a cada API.

H. MANTENCIONES PROGRAMADAS

Las mantenciones programadas deben ser avisadas con anticipación mediante la mensajería asociada al Directorio y tendrán tiempos máximos considerados computables en el uptime del servicio. Para lo anterior, en la siguiente tabla se indican los tipos de mantención y las características de estas:

Tabla 7: Tipos de mantenciones programadas y características

Tipo de Mantención	Tiempo de aviso (previo a ejecución)	Plazo máximo de extensión en la frecuencia	Frecuencia máxima permitida
Correctiva	48 horas	4 horas	Mensual
Preventiva	7 días	8 horas	Trimestral

Evolutiva/ Actualización[8]	14 días	12 horas	Semestral
Urgente	4 horas	2 horas	Mensual

Los participantes del SFA deben revisar al menos diariamente los endpoints de mantenciones.

En cualquier caso, el participante no deberá hacer mantención del mecanismo principal y alternativo al mismo tiempo.

I. MECANISMOS DE MONITOREO

La siguiente Tabla 8 muestra las métricas, plazos e información que deberán enviar los IPI en un auto-reporte de entrega mensual:

Tabla 8: Información a ser reportada por las IPI respecto a rendimiento

Materia	Desagregación	Métrica	Periodo
Disponibilidad de las APIs	Separado por API. Separado entre mantenciones y bajas no programadas.	% del tiempo disponible	Diario y mensual
Time to Last Byte (TTLB) entre recepción de request y envío del último byte del response	Por API y PSBI.	Milisegundos. mediana, máximo, mínimo, y P90	Semanal
TPS y TPM	Por API y PSBI.	Mediana, máximo, mínimo, p90	Semanal
Tasa de error en APIs de Datos	Separado por API y PSBI.	% de llamados de datos con errores, separado por tipo de error	Semanal
Tasa de error en API consentimiento	Separado por PSBI.	% de llamados de consentimiento con errores, separado por tipo de error	Semanal

[8] Este tipo de mantenciones considera eventos tales como actualizaciones de seguridad, ampliación de capacidad, migración de infraestructura, pruebas de continuidad operativa, actualizaciones de API y mantenimientos de redes.

Las tablas especificas a completar por los IPI se encuentran en la sección VIII del presente Anexo.

VI. REQUERIMIENTOS DE SEGURIDAD

Tal como define la NCG 514, la comunicación de las APIs se realizará según las especificaciones técnicas presentes en el perfil de seguridad FAPI 2.0[9] que se complementa con el Modelo de atacante[10] (especificación final [19/02/2025]), ambos establecido por la Open ID Foundation (OIDF), basado en el marco de autorización OAuth 2.0 [RFC 6749][11]. Respecto a los mensajes con objetivo de no repudio, se deberá implementar el protocolo de Firma de mensajes[12] FAPI 2.0.

A continuación, se especificarán algunas características propias de cada área de seguridad de la API, en lo que no se mencione se aplicara el perfil de seguridad de FAPI 2.0.

i. Se usará como protocolo de encriptación Transport Layer Security TLS 1.3 [RFC8446][13].

ii. Se implementará como control de seguridad en la capa de transporte el método de autenticación mutual TLS (mTLS) [RFC8705][14].

iii. Se deberá implementar el protocolo de registro de clientes dynamic client registration [RFC7591].

iv. Los End Points utilizarán certificados emitidos por una autoridad certificadora que contenga una firma electrónica avanzada bajo el estándar X509v3, este certificado será del tipo de validación extendida (EV).

v. Pruebas y revisiones permanentes de seguridad. A modo de ejemplo y sin ser exhaustivos las implementaciones FAPI 2.0 debiese ser sometidas a revisiones periódicas en aspectos de autentificación y autorización, cifrado, gestión de errores, limitación de velocidad, y validación de entrada, así como en otros aspectos generales de seguridad de plataformas y sistemas.

VI. Certificación de OIDF.

[9] https://openid.net/specs/fapi-security-profile-2_0-final.html
[10] https://openid.net/specs/fapi-attacker-model-2_0-final.html
[11] https://www.rfc-editor.org/info/rfc6749
[12] https://openid.net/specs/fapi-2_0-message-signing-ID1.html
[13] El *Security profile* de FAPI 2.0 define el uso de TLS 1.2 o posterior, por lo que estamos exigiendo el uso de TLS 1.3 que es la última versión disponible.
[14] En *Security profile* de FAPI 2.0 se MTLS o DPoP para el uso de token de acceso restringido, esta implementación se decanta por el uso de MTLS, por sobre DPoP. Además, también define como valido el uso de MTLS o *private_key_*jwt para la autenticación de clientes, en este caso también se elige MTLS como método, ambas elecciones podrían ser revisadas en una etapa de implementación posterior considerando el avance de la implementación.

VII. CONSENTIMIENTO

A. GENERACIÓN Y ADMINISTRACIÓN DEL CONSENTIMIENTO

La forma en que se generará y administrará el consentimiento en el SFA será mediante Rich Authorization Requests (RAR) y Grant Management (GM) respectivamente. Para RAR la referencia es el RFC 9396.

Respecto a la estructura del Authorization Details se seguirá el estándar definido en el RFC 9396 y la CMF definirá lo correspondiente a Finalidad.

La Authorization Details es una estructura que describe de manera granular lo que se está autorizando.

Los elementos fijos de la authorization_details según el RFC 9396 son los siguientes:

- Type
- Locations
- Actions
- Datatypes
- Identifier
- Privileges

En la authorization_details, por ser parte del consentimiento en virtud del artículo 23 de la Ley Fintec, la finalidad será un "parámetro" dentro del objeto de la autorización.

El parámetro finalidad será expresado en inglés con el término "purpose", el cual consistirá en un campo libre de un largo máximo de 100 caracteres y deberá describirse con un lenguaje claro y en idioma español.

Un ejemplo de cómo se vería el parámetro "purpose" en la authorization details es el siguiente:

```
{
    "authorization_details": [
        {
            "purpose": "El objetivo de la información que se pedirá es
                        evaluar las condiciones de sus actuales créditos
                        para ofrecerle otra entidad que tenga mejores
                        condiciones, de manera que pueda repactar esos
                        créditos."
        }
    ]
}
```

B. AUTENTICACIÓN DEL CLIENTE POR PARTE DEL IPI

La forma en que deberá realizar este proceso es mediante un flujo redirigido.

VIII. REPORTES

A. REPORTE DE INCIDENTES OPERACIONALES

El Reporte de Incidentes Operacionales que deberán reportar los participantes del SFA considerara la siguiente estructura y formato.

En relación con los participantes que ya tienen requerimientos de RIO deberán considerar el reporte de un incidente solo una vez sin necesidad de duplicar la reportería.

REPORTE DE INCIDENTES OPERACIONES PARA EL SFA

1. Fecha y hora del inicio del incidente:

Se debe señalar la fecha (DD/MM/AAAA) y la hora (HH:MM:SS) en que comenzó el incidente.

2. Tipo de incidente:

En este campo se debe señalar el tipo de incidente, eligiendo entre las siguientes opciones:

- Afectación de instalaciones
- Ausencia de Colaboradores
- Sin acceso dependencias y otras áreas específicas
- Falla Sistemas Base (SO, BD)
- Falla aplicativos (negocio, web, batch)
- Falla de comunicaciones
- Falla Hardware
- Falla en servicios básicos (electricidad/agua)
- Pérdida de Recursos Monetarios de la entidad
- Pérdida de Recursos Monetarios de clientes
- Pérdida de Información de la entidad o de clientes
- Interrupción/ latencia en servicios otorgados en canales electrónicos
- Error de envío de información de cuentas de clientes
- Error en cobro de producto o servicios a clientes
- Interrupción de servicios en canales físicos
- Otros: especificar

3. Descripción detallada del incidente:

En este campo se debe detallar en qué consiste el incidente reportado.

4. Causa:

En este campo se debe señalar la causa probable/definitiva del incidente, eligiendo entre las siguientes opciones:

- Inundación por causas naturales
- Terremoto
- Tsunami
- Huelga
- Pandemia
- Incendio
- Corte de energía
- Corte de agua
- Asalto a dependencias
- Robo o hurto de activos físicos
- Robo o hurto de activos digitales
- Daño de infraestructura tecnológica
- Daño de infraestructura de comunicaciones
- Ataque denegación de servicio
- Clonación
- Ataque de virus maliciosos
- Retraso/ Errores en procesos operativos/tecnológicos
- Otros: especificar

5. Dependencias afectadas:

En este campo se deben señalar las dependencias afectadas, eligiendo entre las siguientes opciones:

- Casa Matriz
- Sucursal
- Caja Auxiliar
- Sitio Producción
- Sitio Contingencia
- Dependencias proveedor
- Otros: especificar

6. Dirección dependencias afectadas (calle, comuna, región)

En este campo se debe informar la dirección de la dependencia afectada, incluyendo la calle, la comuna de acuerdo con la Tabla Nº65 del manual de sistema de información y la región considerando la Tabla Nº2 del manual de sistema de información. Si existe más de una dependencia afectada, se debe indicar la dirección de cada una de ellas, separándolas con un punto y coma (;).

7. Canales afectados

En este campo se deben seleccionar los canales afectados por el incidente:

- Sucursales
- Página web
- Aplicación móvil
- Cajeros automáticos
- Centro de atención telefónica
- POS
- Otros: especificar

8. Nombre de proveedores involucrados:

Corresponde al nombre o razón social del proveedor.

9. Tipo de proveedor involucrado:

- SAG
- Servicios básicos
- Telecomunicaciones
- Infraestructura tecnológica
- Transporte de valores y custodia
- Procesamiento
- N/A
- Otros: especificar

10. Existe afectación a clientes:

- Si
- No

11. Número de clientes que están siendo afectados:

En este campo se debe completar el número de clientes que fueron afectados por el incidente que se reporta.

12. Tipo de clientes afectados:

En este campo se debe seleccionar el tipo de cliente afectado, entre las siguientes opciones:

- Personas
- Empresas
- Ambos
- N/A

13. Se envió comunicación a clientes afectados:

- Sí
- No

14. Canal de envío de información a clientes:

- Correo electrónico
- Teléfono (WhatsApp, mensaje de texto)
- RRSS
- Página web
- App
- Otro (especificar)

15. Número de empleados afectados:

En este campo se debe completar con el número de empleados que fueron afectados por el incidente que se reporta.

16. Productos o servicios afectados:

En este campo se deben informar los productos y servicios afectados por el incidente.

17. Número de transacciones afectadas:

En este campo se debe completar el número de transacciones que fueron afectadas por el incidente que se reporta.

18. Medidas adoptadas:

En este campo se deben informar en detalle las acciones realizadas por la entidad para superar el incidente y sus actualizaciones.

19. Nombre y cargo del informante:

Corresponde a la persona que informa el incidente y su cargo.

20. Teléfono celular del informante:

Se debe señalar en este campo el número del teléfono celular de la persona que informa el incidente.

<u>Módulo específico SFA</u>

21. ¿El evento reportado afecta su funcionamiento en el SFA?

- Sí, solo nuestro funcionamiento en el SFA
- Sí, a nuestro funcionamiento general y funcionamiento en el SFA
- No

22. ¿En qué rol está informando este evento?

- IPI
- PSBI
- Ambos

23. ¿Está relacionado el evento a algunas de estas materias?:

- Deficiencias en la calidad de la información que se suministran a través de sus interfaces.
- Incidente de ciberseguridad que afecte o comprometa los activos de información asociados al SFA o involucre una vulneración de los datos personales de los clientes financieros.
- Incidente operacional que impida la transferencia y/o intercambio de datos en forma segura o que afecte el correcto funcionamiento del Sistema.
- Ninguno de los anteriores.

24. ¿Efectuó una denegación de llamadas a alguna contraparte[15]? (timestamp)

- Sí
- No

[15] Medida que puede tomar una participante del SFA respecto a otro participante del sistema que consiste en la denegación de solicitudes de información de sus interfaces y sistemas debido a la existencia de un riesgo relevante de afectación de activos del SFA, por parte de este otro participante.

25. Contraparte SFA: En caso de haber indicado "Sí" en el campo anterior indique código de contraparte.

26. ¿Ejecutó la medida de desconexión[16]? (timestamp)

- Sí
- No

<u>Variables de RIO de cierre:</u>

27. Fecha y hora de término del incidente:

Este campo se incluirá cuando se cierra el incidente. Se debe completar la fecha (DD/MM/AAAA) y la hora (HH:MM:SS) en que éste finalizó.

28. Tiempo de resolución del incidente:

Este campo se incluirá cuando se cierra el incidente. Se debe completar el tiempo que demoro el evento (HH:MM:SS) en ser superado contando desde que este fue reconocido por la institución.

29. Número de clientes afectados finales:

Este campo se incluirá cuando se cierra el incidente. En este campo se debe completar el número de clientes afectados totales al momento de cierre del incidente.

[16] Medida que puede tomar un participante que consiste en la desconexión de sus sistemas del SFA cuando estima que existe un riesgo relevante de afectación de los activos de información asociados al SFA, entre ellos, los datos personales de los clientes financieros.

REPORTE DE INCIDENTES MENSUAL

Las entidades, además de comunicar los incidentes a través de la plataforma Reporte de Incidentes Operacionales (RIO) del SFA, deberán remitir mensualmente el archivo I12 “Incidentes de Ciberseguridad”, del Manual de Sistema de Información.

B. REPORTE DE MANTENCIONES

Las entidades participantes del SFA deberán enviar el reporte mensual de mantenciones efectuadas durante el mes previo en el formato que se describe a continuación:

Tabla 9: Reporte Mensual de Mantenciones:

Tipo de mantención	**Número de mantenciones efectuadas en el periodo**	**Tiempo total de las mantenciones efectuadas (HH:MM:SS)**	**Tiempo máximo asociado a una mantención (HH:MM:SS)**
Correctiva			
Preventiva			
Evolutiva/Actualización			
Urgente			

C. REPORTE DE CALIDAD DE LA INFORMACIÓN

En los plazos indicados en la norma, los IPI deberán informar reportes de calidad de la información con la siguiente estructura:

Tabla 10: Reporte de Calidad de la Información:

Dimensión	**Descripción**	**Métrica**	**Valor (Porcentaje)**
Exactitud (*accuracy*)	Qué tan precisos son los datos en relación con otras instancias	Registros con errores	
		Error de los datos	
Completitud (*completeness*)	Qué tan completos son los registros en relación con otras instancias	Registros completos	
Integridad (*integrity*)	Qué tan correctas son las relaciones entre distintos datos y en el tiempo	Registros íntegros	
Actualización (*timelines*)	Qué 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	

D. REPORTE DE DISPONIBILIDAD Y RENDIMIENTO

Tabla 11: Reportes de disponibilidad y rendimiento

a) Disponibilidad de las APIs

API	Dia del mes	Disponibilidad total	Disponibilidad descontando tiempos de mantención programada
...	...	...	...

Donde los campos corresponden a:

- Disponibilidad total: Corresponde a la razón de tiempo total disponible en el periodo sobre el tiempo total del periodo. Expresado con dos decimales (ej: 99,99%).

- Disponibilidad descontando tiempos de mantención programada: Corresponde a la razón de tiempo total disponible en el periodo (considerando las mantenciones programadas de la API principal como tiempos de disponibilidad) sobre el tiempo total del periodo. Expresado con dos decimales (ej: 99,99%).

b) Time to Last Byte (TTLB), expresados en milisegundos.

API	Endpoint	PSBI	Mediana	Máximo	Mínimo	P95
...	...	...				

c) TPM y TPS, expresado en numero

Unidad	API	Endpoint	Mediana	Máximo	Mínimo	P90
TPM	...					
TPS	...					

d) Tasa de error de APIs de datos públicos:

API	PSBI	Tipo de Error	% de llamados con datos con errores
…	…		

e) Tasa de error en API de consentimiento:

API	PSBI	Tipo de Error	% de llamados de consentimiento con errores
…			

E. REPORTE DE ESTADO DE ACTIVIDAD EN EL SFA PARA IPI y PSBI

Como parte del monitoreo general del sistema las entidades deberán enviar mensualmente la siguiente información:

IPI

Tabla 12: Información mensual de actividad para IPIs

a) Información mensual de actividad para información pública

Número de llamadas recibidas en el mes	Número de llamadas en el mes exitosas

Donde los campos corresponden a:

- **Número de llamadas recibidas en el mes**: Corresponde al número total de llamadas recibidas por el IPIs por concepto de acceso a información de parte de los PSBI.

- **Número de llamadas recibidas en el mes exitosas**: Corresponde al número total de llamadas recibidas por el IPIs por concepto de acceso a información donde el intercambio fue efectivo sin códigos de error.

b) Información mensual de actividad para información de personas jurídicas y naturales

Tipo de persona (natural o jurídica)	Número de llamadas recibidas en el mes	Número de llamadas recibidas en el mes exitosas	Número de clientes únicos con consentimientos activos a fin de mes.	Número de clientes con algún intercambio de información en el mes.
Natural				
Jurídica				

Donde los campos corresponden a:

- **Tipo de persona (natural o jurídica)**: Corresponde al tipo de cliente del PSBI si es persona natural o jurídica.

- **Número de llamadas recibidas en el mes**: Corresponde al número total de llamadas recibidas por el IPIs por concepto de acceso a información de parte de los clientes de parte de los PSBI.

- **Número de llamadas recibidas en el mes exitosas**: Corresponde al número total de llamadas recibidas por el IPIs por concepto de acceso a información de parte de los clientes de los PSBI donde el intercambio fue efectivo sin códigos de error.

- **Número de clientes únicos con consentimientos activos a fin de mes**. Corresponde al número total de clientes que están activos con algún consentimiento por parte de un PSBI, independiente hayan realizado consultas de información en el periodo en cuestión.

- **Número de clientes con algún intercambio de información en el mes**: Respecto al campo "Número de llamadas en el mes" corresponde al total de clientes únicos asociados a esas llamadas que autorizaron el intercambio de información

PSBI

Tabla 13: Información mensual de actividad para PSBI

Tipo de persona (natural o jurídica)	Número de llamadas realizadas en el mes	Número de llamadas realizadas en el mes exitosas	Número de clientes únicos con consentimientos activos a fin de mes.	Número de clientes con algún intercambio de información en el mes

Donde los campos corresponden a:

- **Tipo de persona (natural o jurídica)**: Corresponde al tipo de cliente del PSBI si es persona natural o jurídica.

- **Número de llamadas realizadas en el mes**: Corresponde al número total de llamadas realizadas a IPIs por concepto de acceso a información de parte de los clientes.

- **Número de llamadas realizadas en el mes exitosas**: Corresponde al número total de llamadas a IPIs por concepto de acceso a información de parte de los clientes donde el intercambio fue efectivo sin códigos de error.

- **Número de clientes únicos con consentimientos activos a fin de**

mes: Corresponde al número total de clientes que tiene el PSBI, independiente hayan realizado consultas de información en el periodo en cuestión.

- **Número de clientes con algún intercambio de información en el mes**: Respecto al campo "Número de llamadas en el mes" corresponde al total de clientes únicos asociados a esas llamadas

COMISIÓN
PARA EL MERCADO
FINANCIERO

Regulador y Supervisor Financiero de Chile

www.cmfchile.cl