COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Informe Normativo:

Norma que actualiza el Anexo 3 e incorpora la Iniciación de Pagos

Enero 2026

www.CMFChile.cl

Índice Informe Normativo

I. INTRODUCCIÓN

A partir de la conversación constante con la industria y las instancias facilitadas por el Foro del SFA, más un exhaustivo análisis de las áreas internas de la CMF, se decidió realizar ajustes a la actual NCG 514 con su Anexo 3 propuesto con el fin de facilitar la implementación de este nuevo sistema. Junto a lo anterior se incorpora la Iniciación de Pagos en los estándares técnicos del SFA.

Estos ajustes, están asociados a las siguientes materias:

A. Principales modificaciones NCG 514

- Se incluye dentro de las causales para aplicar suspensiones temporales el infringir obligaciones legales o regulatorias de la CMF que comprometan la integridad, seguridad o transparencia del Sistema de Finanzas Abiertas.
- Se define el contenido mínimo del informe de cierre de incidentes operacionales y se clarifica que puede ser generado por la misma entidad.
- Se indica que aquellas entidades que no actualicen sus certificados pasan automáticamente al estado inactivas (suspendida).

B. Principales modificaciones Anexo 3:

I. Infraestructura

- Se clarifica que también los PSBI y PSIP pueden tener múltiples marcas y se detallan las condiciones registrales asociadas.
- Se clarifica que los estados de los participantes con más de un rol (por ejemplo, una institución que es IPI y PSBI al mismo tiempo) son independientes entre sí.
- Se indica que ante periodos de indisponibilidad del Directorio las entidades deben considerar información pública de suspensiones de participantes.

II. Certificados digitales de identidad

- Se indica que el Directorio revisará la vigencia en el tiempo (revocaciones) de los certificados, junto con enviar avisos tempranos ante no renovaciones. Se aclara, de todas formas, que es responsabilidad del participante verificar sus propias vigencias (revocaciones).

III. Perfil de seguridad

- Se indica el tipo de *token* de acceso para enviar o acceder a la información del campo *authorization details*.

IV. Ambiente de pruebas de la CMF y certificados funcionales

- Se detallan elementos que acrediten la experiencia en pruebas tecnológicas y en ciberseguridad del certificador de pruebas funcionales, y se indica que el propio participante debe argumentar el cumplimiento de estos requisitos en la entrega del certificado funcional.

- Se precisa las pruebas funcionales fuera del Sandbox deben considerar la continuidad operacional en el caso de IPI/IPC.
- Se elimina la causal general de invalidez de certificados funcionales y se agrega en el caso de vulnerabilidades que estas deben representar un "riesgo crítico y material para la operación del sistema".
- Se aclara que los datos del *Sandbox* no consideran información real de clientes.

En relación con la Iniciación de Pagos:

- Se incluyen nuevas pruebas funcionales ad-hoc para Iniciación de Pagos.

V. Intercambio de Información

- Se clarifican códigos de error que no deben ser considerados como indisponibilidad de la infraestructura de la IPI o IPC, así como que tampoco las mantenciones programadas constituyen *downtime.*
- Se modifica la frecuencia permitida de las mantenciones preventivas y evolutivas (más plazo de mantenciones por mes equivalente).
- Se corrigen las especificaciones de medición de TPS y TPM.
- Se indica que cada IPI/IPC deberá actualizar su TPS de forma trimestral (al cierre del primer año), considerando el percentil 90 de las llamadas efectivas.
- Se indica que las IPI/IPC podrán también aplicar la denegación cuando reciban un volumen significativo de llamadas erróneas (4xx) o repetitivas por parte de una PSBI o PSIP.
- Se pasan a anuales las pruebas de calidad de la información. Debiendo el primer informe ser parte de las pruebas funcionales.
- Se permite ahora que los PSBI/PSIP puedan informar deficiencias de información observadas en los IPI/IPC.

En relación con la Iniciación de pagos:

- Nuevos códigos de error relativos a la Iniciación de Pagos.
- Clarificación que los 800 milisegundos aplican a la ejecución del pago, pero no al ciclo completo del pago.
- Se definen las TPS que las IPC deben tener como capacidad de respuesta.

VII. Consentimiento

- Se mantiene que la forma en que se generará y administrará el consentimiento en el SFA será mediante *Rich Authorization Requests* (RAR) y *Grant Management* (GM), respectivamente (Referencia RAR RFC 9396).

- Los campos de la *Authorization Details*, con su respectiva obligatoriedad, se traspasan al Portal del Desarrollador.
- Se mantiene el "parámetro" (campo) "purpose" (finalidad) en la *Authorization Details*, pero se especifica que será un campo informativo (por ser parte del consentimiento) que no dará lugar a ninguna restricción por parte de la IPI/IPC.
- Se aumenta de 100 a 300 el número de caracteres para su descripción.
- Se incluyen los estados del consentimiento que serán considerados en el Panel de Control de Consentimientos para supuestos de intercambio de información y de iniciación de pagos.

Sobre la Iniciación de Pagos:

- Se mantiene como flujo de autenticación el tipo redirigido para pagos.
- Se incluyen estados de Consentimiento para casos de Iniciación de Pagos.

Sobre el Portal de Desarrolladores:

- Se consideran las especificaciones y diccionarios técnicos 5 APIs de pagos:

1. Pago único	Permite hacer pagos de PN/PJ* a PN/PJ en pesos.
2. Pago único programado	Permite hacer pagos PN/PJ a PN/PJ en pesos a una fecha futura que no exceda los 90 días.
3. Pago recurrente fijo	Permite hacer múltiples pagos PN/PJ a PN/PJ en pesos en fechas programadas mientras dure el contrato (cada 3 años nueva autenticación).
4. Pago recurrente variable	Permite hacer múltiples pagos PN/PJ a PN/PJ en pesos en fechas programadas mientras dure el contrato (cada 3 años nueva autenticación) con montos variables. El usuario puede indicar límite superior del pago.
5. Confirmación de fondos	Permite validar fondos antes de hacer la transferencia, especialmente útil en el caso de pagos recurrentes.

*Tanto para personas jurídicas firma simple como múltiple.

Adicionalmente:

- Inclusión de la API de Registro Dinámico de Clientes.
- Se agregan especificaciones del Funcionamiento de *Webhook*.
- Se incorpora política de versionamiento y registro de cambios del portal.
- Se definieron los parámetros concretos para idempotencia y responsabilidades PSBI/PSIP.

- Se alinea el uso del protocolo de seguridad a TLS 1.3 en lugar de TLS 1.2.
- Se revisaron y ajustaron las descripciones funcionales de *endpoints* de términos y condiciones.
- Se revisaron y ajustaron la obligatoriedad de *headers* y criterios en *request/response API*.
- Se alineó el catálogo de códigos de error entre portal, norma y especificaciones.
- Se agregaron las especificaciones del *Grant Management*.
- Se agregaron las especificaciones de los estados del Consentimiento.
- Otros ajustes y mejoras generales.

<u>Sobre la realización de consultas públicas</u>.

El SFA ha contado con 2 consultas públicas post emisión de la NCG 514 (dos consultas previas a la presente):

Consulta Pública	**Fechas de la consulta**
Consulta pública de norma que modifica NCG 514 que regula el Sistema de Finanzas Abiertas e incorpora Anexo Técnico	10/07/2025 al 18/08/2025
Consulta pública sobre norma que modifica NCG N°514.	12/11/2025 al 12/12/2025

Esta consulta pública recoge los comentarios de la industria en el proceso de consulta pública "*Consulta pública de norma que modifica NCG 514 que regula el Sistema de Finanzas Abiertas e incorpora Anexo Técnico*" e incorpora adicionalmente aquellos elementos técnicos propios de la Iniciación de Pagos.

Para mayor facilidad de lectura de la industria se muestran los cambios del Anexo 3 respecto a la primera versión del Anexo 3 publicada.

Adicionalmente, debe considerarse que elementos presentados en la "Consulta pública sobre norma que modifica NCG N°514" tales como aquellos relativos al mecanismo alternativo (en particular la sección V.E), la existencia de periodos pilotos y la disponibilidad previa de áreas de prueba están bajo análisis y, por ende, la actual consulta no considera cambios en estas materias a la versión vigente del Anexo 3.

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, para su confección han sido consideradas las disposiciones atingentes contenidas en el D.L. 3.538 de 1980, la Ley N°20.009 y la Ley N°19.628.

Normativa vigente relevante

Para la preparación de la presente propuesta normativa se ha considerado un conjunto relevante de normativa que considera a uno o más grupos o tipos de participantes del SFA, con el propósito de brindar coherencia regulatoria, además de dar cumplimiento a 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 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 deben remitir ante incidentes operacionales relevantes que afecten la continuidad del negocio, la seguridad de la información, o la imagen de la institución. Además, 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. De esta manera, considera la 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; y, de la evaluación de escenarios mínimos de contingencia, entre otros elementos.

Capítulo 20-10. Contiene disposiciones que deben considerarse con el fin de gestionar la seguridad de la información y la ciberseguridad. En este Capítulo se definen lineamientos específicos respecto del papel que debe tener el Directorio en relación con la seguridad de la información y la ciberseguridad, otorgándole a dicha instancia la responsabilidad de la aprobación de la estrategia institucional en la materia. Asimismo, establece principios y procedimientos para la detección de amenazas y vulnerabilidades de ciberseguridad; la respuesta ante incidentes; y, la recuperación de la operación normal de la entidad, entre otros aspectos.

Normativa en materia de Valores y Seguros

N.C.G. N°528. Imparte instrucciones sobre gobierno corporativo y gestión integral de riesgos para corredores de bolsa de valores, agentes de valores y corredores de bolsas de productos. Deroga circular N°2.054 de 2011.

N.C.G. N°309. 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. Se refiere 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 aspectos.

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.

N.C.G. N°538. Se refiere a las medidas de seguridad y autenticación de operaciones sometidas a la Ley N°20.009.

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.

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 requerimientos patrimoniales, de gestión y de relacionamiento con otros intervinientes de la cadena de pagos.

III. DESCRIPCIÓN DE LOS AJUSTES INCORPORADOS Y SU IMPACTO

En respuesta a los comentarios recibidos durante la consulta pública del Anexo 3, esta Comisión ha preparado una propuesta de ajustes con el fin de recibir nuevos comentarios de las partes interesadas.

Entre los cambios propuestos, se homologa la existencia de marcas en los PSBI/PSIP con los requisitos registrales correspondientes. Además, la Comisión aclara que las entidades con más de un rol (por ejemplo, una institución financiera que ejerce el rol de IPI y PSBI) podrán tener estados de participación diferenciados, si corresponde.

En cuanto a los certificados de identidad, uno de los cambios más relevantes es que, además de la responsabilidad de cada participante en la revisión de la vigencia de los certificados, el Directorio realizará periódicamente una revisión de estos, con la capacidad de detectar, entre otros aspectos, revocaciones. En los casos en que se observe una revocación, la institución será considerada como suspendida hasta que actualice su certificado. La inclusión del Directorio en la revisión periódica de vigencias se considera un avance importante para la supervisión del sistema y su buen funcionamiento. Además, el Directorio implementará un sistema de avisos previos a la fecha de caducidad de los certificados, lo que permitirá a las entidades recibir alertas tempranas y tomar las medidas correspondientes.

Respecto a los ambientes de prueba, a solicitud de la industria, se han aclarado las condiciones que deben cumplir los certificadores de pruebas funcionales. Estas condiciones deberán incluirse en el reporte de hallazgos. La Comisión considera que proporcionar mayor claridad sobre estos requisitos facilitará a las instituciones la selección de sus certificadores.

En relación con la sección de intercambio de información, se han realizado varias modificaciones. Entre ellas, se precisan los códigos de error y las mantenciones programadas, así como su contabilización en el tiempo de disponibilidad (*up time*) del sistema. Además, en el marco de la puesta en marcha del sistema, se han ampliado los periodos máximos de mantenciones programadas que se pueden implementar. También se ha clarificado la metodología para la actualización de los TPS mínimos que debe soportar cada IPI/IPC, haciendo que esta actualización sea funcional a las llamadas efectivas recibidas por la institución. Esta diferenciación en las reglas de actualización permite focalizar el aumento de infraestructura en las instituciones donde realmente es necesario.

En cuanto a la sección de consentimiento, se establece que el consentimiento en el SFA se generará mediante *Rich Authorization Requests* (RAR) y se gestionará a través de *Grant Management* (GM), conforme a la RFC 9396. Respecto de la *"Authorization Details",* sus campos con su respectiva obligatoriedad se trasladan al Portal del Desarrollador. El parámetro *"purpose"* (finalidad) se mantiene, pero se especifica que será un campo informativo que no dará lugar

a ninguna restricción por parte de la IPI/IPC. Adicionalmente, se aumenta su descripción de 100 a 300 caracteres.

Por parte de la autenticación requerida en ambiente de la IPI/IPC en el flujo del consentimiento, se mantiene el tipo redirigido para casos de iniciación de pagos, señalándose sus especificaciones en el Portal del Desarrollador. Por otro lado, se incorporan en este anexo los estados del consentimiento que serán considerados en el Panel de Control de Consentimientos para los casos de intercambio de información e iniciación de pagos, describiéndose los flujos de sincronización de estos estados en el Portal del Desarrollador. Estas modificaciones aportan mayor claridad sobre el alcance del consentimiento y permiten, por ejemplo, ofrecer una descripción más detallada de la finalidad del consentimiento para el cliente.

Adicionalmente, la propuesta de consulta incluye la incorporación de cinco nuevas APIs de pagos al SFA, lo que se considera un avance significativo en la preparación de las instituciones para su implementación. La inclusión de la iniciación de pagos también trae consigo una serie de modificaciones en el Anexo 3, como la adición de códigos de error específicos para esta actividad, pruebas funcionales en el *Sandbox* y en ambientes externos, así como la fijación de TPS. En este caso, la Comisión ha evaluado la información de llamadas efectivas para definir los niveles propuestos. Nuevamente, estas definiciones permitirán a la industria avanzar con sus implementaciones asociadas.

Finalmente, para mayor claridad de la industria, se han incluido en Portal del Desarrollador diversas especificaciones técnicas, tales como definiciones de versionamiento, funcionalidades del *Webhook,* implementación de la API del Registro Dinámico de Clientes, especificaciones de *Grant Management*, estados del Consentimiento, idempotencia, entre otros ajustes y mejoras. La Comisión considera que estas incorporaciones constituyen un aporte significativo para facilitar la implementación de estas herramientas por parte de la industria y su integración al SFA.

IV. PROPUESTA NORMATIVA: NORMA QUE ACTUALIZA EL ANEXO 3 E INCORPORA LA INICIACIÓN DE PAGOS

Texto Propuesto:

REF.: NORMA QUE ACTUALIZA EL ANEXO 3 E INCORPORA LA INICIACIÓN DE PAGOS

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 2025, 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"):

1. AJUSTES A LAS SUSPENSIONES TEMPORALES

NCG 514

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 infrinjan obligaciones legales o regulatorias de la CMF que comprometan la integridad, seguridad o transparencia del Sistema de Finanzas Abiertas.
f) 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~~ en 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. Acciones como auto desconexiones y denegaciones deben ser reportadas mediante RIO. Junto con lo anterior, deberá enviar ~~de inmediato~~ a la brevedad un reporte a la CMF, mediante una actualización del RIO respectivo, 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.

En particular, un IPI/IPC podrá también aplicar la denegación en estos casos cuando reciba un volumen significativo de llamadas erróneas (4xx) o repetitivas por parte de un PSBI o PSIP donde se pueda saturar la infraestructura de la IPI o IPC, comprometiendo su capacidad para procesar solicitudes legítimas de otros participantes y afectando la continuidad del servicio a los usuarios finales.

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.

Informe de Cierre del Incidente

Una vez cerrado el incidente, el Participante deberá emitir un informe de cierre de incidente, que incluya la información contenida en el Reporte de Incidentes Operacionales de finalización que haya sido adjuntado, más toda la información que respalde los planes recuperación y de acción correctivos llevados a cabo. El Participante deberá identificar e indicar en dicho informe qué acciones de mitigación se ejecutaron y/o ejecutarán para evitar que el incidente reportado se repita.

El informe de cierre lo puede generar la misma institución, no siendo exigido que sea emitido por un tercero.

Suspensión por no vigencia de certificados

En el caso de entidades que no tengan vigentes los certificados de identidad una vez caducados, tendrán automáticamente la condición de estado de participación “Suspendido”, la cual se levantará una vez que disponibilicen el certificado actualizado respectivo.

2. AJUSTES A LAS PRUEBAS DE CALIDAD DE LA INFORMACIÓN

NCG 514

SECCIÓN II: FUNCIONAMIENTO DEL SISTEMA

D. Calidad de información

Tanto las IPI como las IPC deberán realizar pruebas periódicas y aleatorias de calidad de los datos puestos a disposición de los participantes en el SFA. Las pruebas serán realizadas al menos con periodicidad ~~semestral~~anual y sus resultados serán entregados a la Comisión. El primer informe, previo a la entrada en operación de la API, será entregado a la Comisión en los plazos equivalentes a los que tienen para el desarrollo de las pruebas funcionales.

En caso de detectarse deficiencias significativas, las ~~entidades~~ IPI/IPC deberán informar a la CMF de la situación a través de los canales establecidos para informar eventos de continuidad operacional y presentar a la Comisión un plan de acción que les permita resolver estas deficiencias, sin perjuicio de las suspensiones temporales preventivas que la CMF pueda mandatar u otras acciones que la Comisión evalúe, incluyendo -entre otros- la imposición de sanciones conforme con los procedimientos dispuestos al efecto.

Las pruebas de calidad que realicen las IPI e IPC deben contener al menos los siguientes elementos:

- *Análisis de comparabilidad*: La información suministrada mediante interfaces adscritas al sistema debe cumplir con criterios de comparabilidad. Esto implica que la institución debe verificar que la información de sus clientes que comparte en el SFA es coherente con la información vigente en sus otras fuentes de almacenamiento y consulta.

- *Análisis de origen de errores*: Para aquellos casos en que se encuentren diferencias de información dependiendo de la fuente utilizada, la institución deberá revisar y verificar sus potenciales causas.

Sin perjuicio de lo anterior, en cualquier momento la Comisión podrá efectuar pruebas de calidad de la información, para cuya realización las entidades deberán poner a disposición la información solicitada para estos efectos.

Los requerimientos mínimos de las pruebas que deberán realizar las IPI e IPC son los considerados en el Anexo N°3. Lo anterior no obsta a que, para efectos de asegurar la calidad de la información que proveen en el SFA, voluntariamente las IPI e IPC realicen pruebas adicionales a las exigidas normativamente.

Sin perjuicio de la exigencia de pruebas de calidad periódicas de que trata la presente letra, las IPI e IPC deberán informar a la Comisión tan pronto tomen

conocimiento de su existencia, toda deficiencia significativa en la información que se transmite mediante sus interfaces adscritas al SFA, mediante comunicación conducida a través de los canales dispuestos al efecto en materia de reporte de incidentes operacionales.

Por su parte, las PSBI/PSIP también podrán informar deficiencias de calidad observadas en las APIs de las IPI e IPC.

3. AJUSTES AL PRINCIPIO DE NO DISCRIMINACIÓN

NCG 514

SECCIÓN III: SEGURIDAD Y RESGUARDOS DEL SISTEMA

E. Otros Estándares

1. Estándares de interoperabilidad

La interoperabilidad queda constituida con los siguientes principios:

a) Para el funcionamiento del SFA deberán cumplirse los estándares técnicos especificados por esta Comisión.

b) Las IPI o IPC no pueden dar un trato discriminatorio a los terceros receptores de datos y/o iniciadores de pagos. Esto quiere decir, por ejemplo, que no deben dar prioridad a determinadas instituciones por sobre otras al momento de dar acceso a la extracción de información, en tiempos de ejecución y confirmación de operaciones de pago, en tiempos de desarrollo, acceso a las APIs, servicios de respuestas a consultas, límites máximos de respuestas ante solicitudes igualitarias, entre otros.

c) Toda IPI o IPC, una vez que certifique la identidad de las entidades que proveen servicios ya sea basados en información o de iniciación de pagos, deberá brindar los servicios respectivos autorizados al usuario de información según sus perfiles, sin necesidad de acuerdo entre las partes.

d) Se deben publicar las condiciones de servicio para que todas las partes puedan acceder a ellas.

e) Cualquier criterio técnico adicional que sea indispensable, y que no esté contenido en los estándares, deberá velar por no imposibilitar el acceso a una PSBI o PSIP.

4. AJUSTES A PRIMERA VERSIÓN PROPUESTA DE ANEXO 3

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. Las especificaciones del *webhook* son las indicadas en el Portal de Desarrollador.

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/IPC/PSBI/PSIP 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~~SFA. 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.

El modelo de multimarca se basa en múltiples aplicaciones o declaraciones de software para las PSBI y PSIP, y múltiples servidores de autorización, para las IPI/IPC.

La solicitud de inscripción de una marca debe presentarse junto con la inscripción inicial en el caso de marcas vigentes. No obstante, podrá generarse dicha solicitud en etapas posteriores para nuevas marcas. El participante solo podrá activar la marca en el Directorio cuando esté aprobada.

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/PSIP/IPI/IPC	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:~~ se detalla en el Portal del Desarrollador.

```
[
  {
    "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 institución.
- 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:~~ también se encuentra detallado en el Portal del Desarrollador.

```
[
  {
    "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:

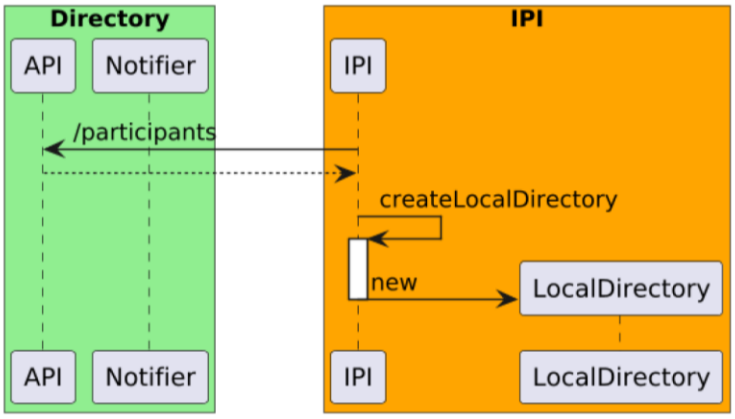
- Es responsabilidad del participante del SFA consultar periódicamente en el *endpoint* expuesto la última fecha de actualización del el Directorio (método *head del endpoint* del participante), de tal manera de verificar que la fecha y hora de actualización de la copia local corresponda con la fecha y hora de modificación entregada por el Directorio.
- Es responsabilidad del Directorio, administrado por la Comisión, 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/IPC/PSBI/PSIP, 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/IPC/PSBI/PSIP 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/IPC/PSBI/PSIP 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/IPC/PSBI/PSIP para obtener el *access-token* correspondiente. En la Figura 1 se puede ver este proceso.

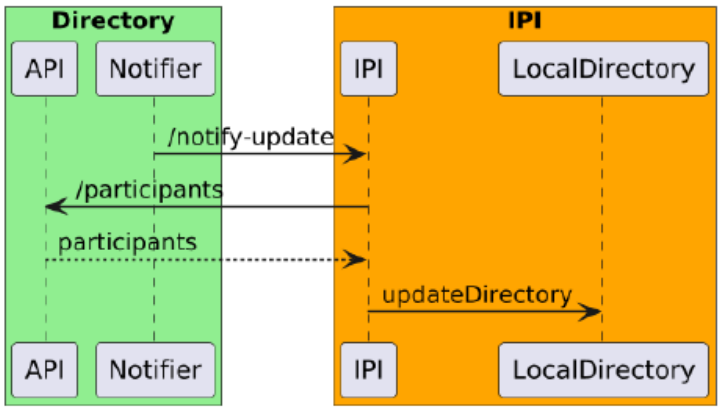
Figura 1: Proceso de creación de copia local



La Figura 1 muestra el proceso de creación del Directorio local. En este caso, una IPI/IPC/PSBI/PSIP 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.

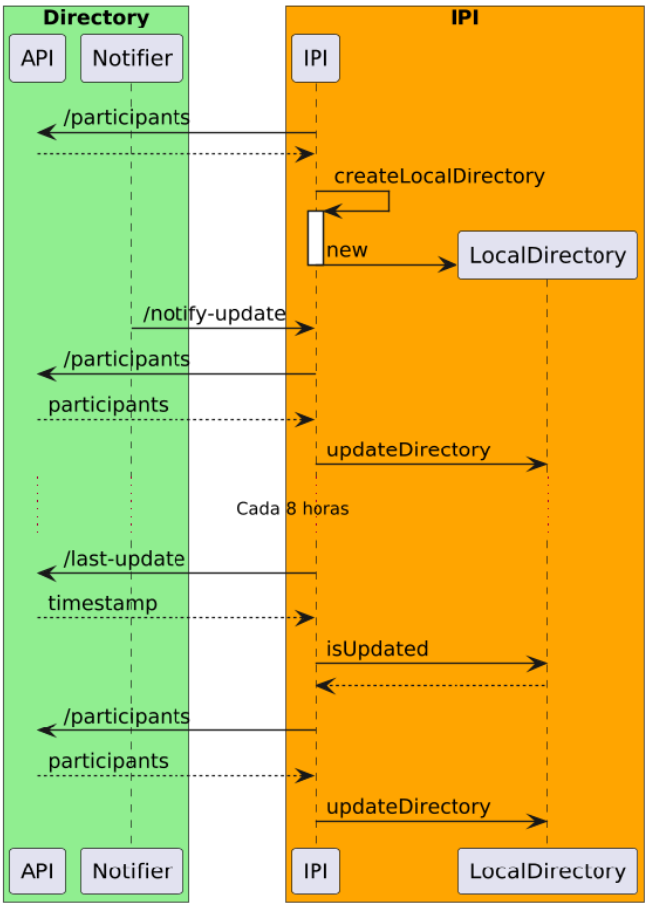
Figura 2: Actualización de la copia local del Directorio en un participante del SFA a través de una notificación del Directorio



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/IPC/PSBI/PSIP que el Directorio ha tenido cambios. Luego de esto, la IPI/IPC/PSBI/PSIP 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.

De todas formas, la entidad en estos momentos de indisponibilidad deberá acceder al Portal de Desarrolladores donde en la sección de Participantes deberá verificar si alguna entidad ha cambiado a un estado que inhabilite el intercambio de información o que la CMF haya tomado una decisión al respecto, en términos normativos, informada públicamente.

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 está 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* indicado para estos efectos en el Portal de desarrolladores.~~:~~

```
~~{~~
~~  "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"
  }
}
```

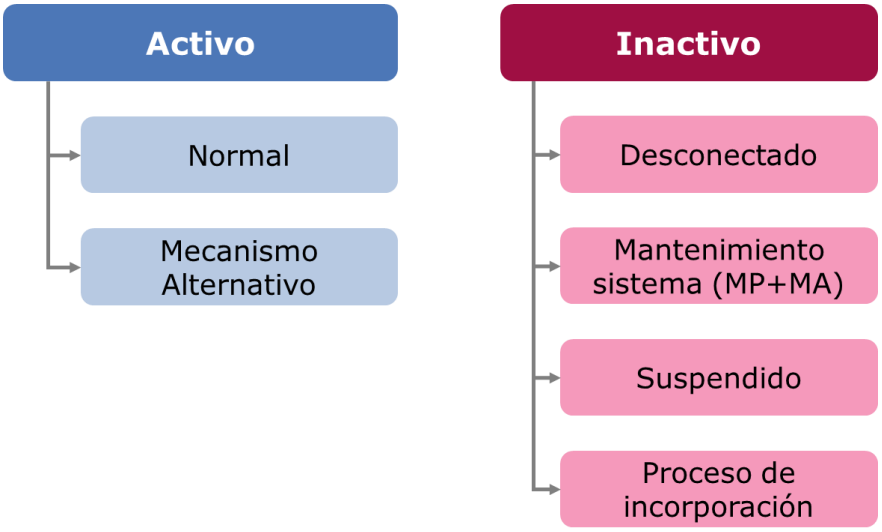
Cabe destacar que además hay canales de comunicación existentes en la CMF que se utilizan en el SFA:

- 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.

- Los estados están asociados a cada tipo de Participante de forma independiente. Entidades con más de un rol no necesariamente tendrán estados comunes para cada tipo de rol.

- 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 está "inactivo" donde no hay intercambio de información. Cada uno de los 6 estados son excluyentes, es decir, no es posible que una entidad para un rol específico esté 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 auto desconecta 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 nómina[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 pública 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 y PSIP o inscritas en las nóminas en el caso de las IPI e IPC, 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.

Las especificaciones del DCR a implementar son aquellas indicadas en el Portal del Desarrollador.

E. CERTIFICACIÓN DE VIGENCIA Y AVISOS TEMPRANOS

Las entidades son responsables de verificar en todo momento que sus certificados estén vigentes y no revocados, y deberán actualizarlos previo a su vencimiento en el Directorio.

Para estos efectos, los participantes deberán implementar y documentar procedimientos para la gestión del ciclo de vida de sus certificados digitales, incluyendo la renovación oportuna antes de su expiración, y la solicitud de revocación inmediata ante la Autoridad Certificadora en caso de compromiso de la clave privada, conforme a los estándares internacionales.

En el caso que una entidad tenga un certificado no vigente en el Directorio, ya sea por caducidad o revocación, esta deberá automáticamente

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

autodesconectarse del Sistema hasta que tenga un certificado vigente en el Directorio.

El Directorio por su lado, enviará avisos tempranos de vencimiento a los 30, 15 y 7 días previos a la fecha de caducidad respectiva de los certificados. La comunicación de estos avisos será mediante correo electrónico automático a los contactos técnicos registrados en el Directorio.

De forma complementaria al rol individual de verificación de vigencias de los certificados que tiene cada participante, el Directorio revisará de forma periódica la vigencia de los certificados, evaluando potenciales revocaciones.

En aquellos casos donde el Directorio encuentre revocaciones de vigencia, pasará el Participante automáticamente al estado Suspendido.

III. PORTAL WEB DE DESARROLLADORES

Este portal 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. Propuestas realizadas por la comunidad de desarrolladores a los diagramas de secuencia.
   - 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~~

https://openfinancechile.atlassian.net/wiki/spaces/OFAC/overview

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 y de pagos.
- Gestión del consentimiento.

El AP tiene acceso restringido, el que será otorgado por la CMF a través de un proceso de solicitud. 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.

Sobre los datos de prueba del Sandbox
La información que se transmitirá a modo de prueba en el *Sandbox* no considerará en ningún momento información real de personas ni sus datos personales. Solo se ocuparán datos generados con el propósito de la prueba, sin tener estos relación con clientes reales.

A. PRUEBAS FUNCIONALES DE IPI/IPC EN EL AMBIENTE DE PRUEBAS DE LA CMF

Las IPI/IPC 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.

B. PRUEBAS FUNCIONALES DE IPI/IPC QUE NO SE REALIZAN EN

EL AMBIENTE DE PRUEBAS DE LA CMF

Respecto a las otras pruebas que deben ejecutar los IPI/IPC 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:

- Para el caso de IPI:
  - 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.
- Para el caso de IPC:
  - Validación de *Endpoints* de APIs de Pagos.
  - Simulación de un registro de un PSIP como nuevo cliente.
  - Prueba de flujo de entrega de *Access token* a PSIP en nombre de un usuario real.
- Validación de *Access token* emitido para consultar información.
- Pruebas funcionales del Panel de Control de Consentimientos.

Las pruebas deben contemplar, además:

- La operación en contingencia.
- Procesos para manejar y resolver problemas de sus APIs que puedan afectar a otros participantes del SFA. Esto incluye proporcionar mensajes de error claros y concisos, como, asimismo, mecanismos para que los Participantes informen problemas y reciban respuestas y soluciones oportunas.

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

C. PRUEBAS FUNCIONALES DE PSBI/PSIP EN EL AMBIENTE DE PRUEBAS DE LA CMF

Las pruebas funcionales de los PSBI consideradas en la sección I.C.1.2.l 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*. Lo mismo ocurre en el caso de las pruebas funcionales de los PSIP consideradas en la sección I.D.1.2.o de consumo de APIs de pagos que también

deberán ser realizadas en esta área de pruebas. Los PSIP solo podrán realizar pagos en APIS que hayan probado 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/PSIP en las IPI/IPC.
- Flujos de datos de términos y condiciones de las IPI/IPC.
- Flujo de consentimiento.
- Obtención de datos personales de clientes.
- Flujo de iniciación de pagos.

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.~~

Tipo de prueba	Caso	API / Dominio	Título de la prueba	Descripción breve	Resultado visible en respuesta
Onboarding y seguridad base	1	Seguridad	Registro dinámico de cliente (DCR)	Registro con SSA y CSR; el AS valida estructura/firma y enlaza certificado.	201 Created. client_id, registration_access_token, token_endpoint_auth_method.
Onboarding y seguridad base	2	Seguridad	Verificación de canal mTLS	Acceso a discovery/OIDC presentando certificado cliente válido.	200 OK. Si falla: error SSL/TLS en Postman.
Onboarding y seguridad base	3	Seguridad	Token Client Credentials (Open Data)	Token para consumo de Open Data (mock).	200 OK. access_token, expires_in.
Autorización y consentimiento	4	Seguridad	Auth Code + PKCE + PAR + RAR	Flujo con PAR y authorization_details. Aprobación mock.	200 OK. Token con authorization_details + grantId/consentId mock.
Cumplimiento FAPI 2.0 (negative)	5	Seguridad	Petición insegura (policy violation)	Sin PKCE / sin PAR / redirect inválido / alg inseguro, etc.	400 Bad Request con error/política violada.
Controles transversales	6	Seguridad	Token ligado a mTLS	Usar token válido sin presentar certificado cliente.	401 Unauthorized.
Controles transversales	7	Seguridad	Permisos insuficientes (RAR)	Token sin authorization_details.actions para el recurso.	401/403 por permisos insuficientes.

Open Data	8	Open Data	Consumo Open Data (happy path)	GET a endpoint Open Data con token #3.	200 OK con payload mock.
Open Data (negative)	9	Open Data	Open Data sin token / token inválido	Validar control de acceso	401 o error definido.
APIs transaccionales – Cuentas, enrolamiento, recursos, tarjetas de crédito, operaciones de crédito, instrumentos de inversión y seguros	10	Cuentas	Movimientos / transacciones (mock)	Acceso a las informaciones de los endpoints y consultas.	200 OK con movimientos mock.
Iniciación de pagos – Pago único Inmediato	11	Pagos	Pago único inmediato – creación (mock)	Inicia pago sin mover fondos reales; retorna paymentId y estado simulado.	201/200 OK. paymentId, status.
Iniciación de pagos – Pago único Inmediato	12	Pagos	Pago único – consulta de estado (mock)	Consulta estado del paymentId con transiciones simuladas.	200 OK con status mock.
Iniciación de pagos – Programados	13	Pagos	Pago programado – creación (mock)	Pago con fecha futura, validación de formato y reglas.	201/200 OK. status=Scheduled.
Iniciación de pagos – Recurrentes	14	Pagos	Plan recurrente – creación (mock)	Alta de plan recurrente con parámetros válidos.	201/200 OK. recurringPaymentId, status.
Iniciación de pagos – Recurrentes de montos variables	15	Pagos	Plan recurrente variable – creación (mock)	Alta con límites/reglas. Rechazo si inválido.	201/200 OK o 400/422 si inválido.
Confirmación de fondos	16	Funds Confirmation	Fondos disponibles (mock)	Consulta con cuenta demo “saldo suficiente”.	200 OK. fundsAvailable=true.
Confirmación de fondos	17	Funds Confirmation	Fondos insuficientes (mock)	Consulta con cuenta demo “saldo insuficiente”.	200 OK. fundsAvailable=false (o error definido).
Controles transversales (gobierno)	18	Seguridad/Gobierno	Revocación de consentimiento (mock)	Revocar consentimiento y validar que	Revocación 200/204; reintento 401/403.

				recursos/pagos fallen después.	
Controles transversales (firma)	19	Firma (si aplica)	Firma inválida de payload (negative)	Payload sin firma o firma inválida (si el Sandbox la exige en ese endpoint).	400/401 por validación de firma.
Cierre	20	Global	Validación global de cumplimiento	Ejecutar happy paths + negativos: DCR/mTLS/PAR/PKCE/RAR + consumo dominios + pagos/fondos.	200/201 en happy path; 400/401/403 en negativos esperados.

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

D. PRUEBAS FUNCIONALES DE LAS PSBI/PSIP 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.1.2.l de la norma en el caso de los PSBI y de la sección I.D.1.2.o en el caso de los PSIP.

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

Tanto las IPI/IPC como los PSBI/PSIP 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/IPC

En el caso de las IPI/IPC, ellas podrán participar del Sandbox desde el momento que presentan su solicitud de inscripción como IPI/IPC. 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) y (k) indicadas en el punto "1.2 Antecedentes adjuntos".

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

PSIP

Para el caso de los PSIP 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), (f), (g), (h), (i), (j), (n) indicadas en el punto "1.2 Antecedentes adjuntos".

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

F. ELEMENTOS TECNICOS QUE DEBERÁN 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.

G. 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/IPC y de la letra l de la sección I.C.1.2 en lo que respecta a las PSBI y letra o de la sección I.D.1.2 en lo que respecta a los PSIP, deberán cumplir con los siguientes requisitos los cuales deberán ser verificados por el Participante cuando corresponda y ser reportado su cumplimiento en el reporte de hallazgos y de certificación de resultados de las pruebas funcionales de las APIs:

- Experiencia de al menos 3 años realizando pruebas tecnológicas en entornos de servicios digitales, con reconocido prestigio y experiencia en la evaluación de este tipo de servicios.
- Experiencia en APIs.
- Experiencia en Cibserseguridad (certificación ISO 27001 o estándar SOC2).

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

H. 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/IPC/PSBI/PSIP) 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.~~ Haya un cambio en el listado de APIs que consumen en su modelo de negocio, en el caso de PSBI/PSIP.
5. ~~En el caso de las IPIs, haya un cambio en los productos que ofrecen.~~ Haya un cambio en los productos que ofrecen, en el caso de las IPI/IPC.
6. ~~En el caso que se~~En caso de que se identifiquen nuevas vulnerabilidades y avisos de obsolescencia que emiten los proveedores de las plataformas que soportan las APIs que representen un riesgo crítico y material para la operación del sistema.

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

~~Los certificados de funcionamiento de las IPI/PSBI serán públicos.~~

La responsabilidad de la actualización y revalidación de las certificaciones radica en el Participante lo cual incluye el aviso respectivo y entrega del nuevo certificado.

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/PSIP o nuevas certificaciones por parte de las IPI/IPC.

B. CÓDIGOS DE ERROR

Se deben implementar los ~~siguientes~~ códigos de respuesta indicados en el Portal de Desarrolladores relativos a cada tipo de API. ~~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/IPC y el momento en que la solicitud es completamente respondida por el *Gateway* de la IPI/IPC, o TTLB.

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

Por otro lado, las APIs de iniciación de pagos deberán procesar las transacciones en un tiempo máximo de 800 milisegundos. Esto incluye validaciones del lado de la IPC (como saldos, bloqueos de cuenta, validación del PSIP, estado del consentimiento, idempotencia). Este tiempo no considera los lapsos necesarios para la ejecución y confirmación que las operaciones de pago requieran para la finalización en los sistemas de pago subyacentes a la iniciación de pagos efectuada.

Método de cálculo para disponibilidad

Cada IPI/IPC 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 IPI/IPC con datos diarios, en este informe se deben detallar: tiempos de disponibilidad, momentos de indisponibilidad, tiempos de respuesta, cantidad de llamadas totales y cantidad de llamadas exitosas.

Los errores con códigos 4xx y 529 no deben ser considerados como indisponibilidad de la infraestructura de la IPI o IPC, ~~En el cálculo de la indisponibilidad se deberán excluir los códigos de error 429 y 529 y las~~ así como tampoco 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

En el caso de las IPI, S~~s~~e 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. En el caso de las IPC se considerará como default 10 Transacciones por Segundo (TPS) de una IPC a todos los PSIP. Lo anterior, considerando:

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

No aplicará la medida de Transacciones por Minuto (TPM) en el caso de las IPC.

Especificaciones adicionales sobre las TPM y TPS:

TPS:

- Se calculan agregando ~~todos~~ los requerimientos que recibe un ~~PSBI/PSIP~~ IPI/IPC.
- 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. No obstante, se incluirán los códigos de error 4xx, 429 y 529, siempre que dichos códigos correspondan a condiciones atribuibles al PSBI/PSIP.
- 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 aleatorio ~~*random*~~ (entre 0 y 5) de segundos para evitar que en episodio de sobrecarga muchos PSBI/PSIP 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. No obstante, se incluirán los códigos de error 4xx, 429 y 529, siempre que dichos códigos correspondan a condiciones atribuibles a la PSBI.
- 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 aleatorio ~~*random*~~ (entre 0 y 15) de segundos para evitar que en episodio de sobrecarga muchos PSBI ~~o PSIP~~ reintenten en el mismo instante.

Actualización de TPS y TPM:

Los límites operativos de los TPS tendrán una vigencia trimestral después del primer año de vigencia operativa de la API. Para el trimestre siguiente al del primer año operativo, y con información del trimestre previo operativo, las TPS deberán dar respuesta al mayor valor entre el requerimiento de TPS vigentes al momento y el percentil 90 de la demanda de TPS en este trimestre previo. Lo anterior, para cada trimestre en adelante. Esto tanto para IPI como IPC.

Por su lado, las TPM serán proporcionales a las TPS. En concreto, la fórmula de las TPM será de TPM multiplicado por el valor de seis. Esto solo es válido para IPI ya que las IPC no tienen requerimientos de TPM.

Consideraciones Adicionales:

Si el PSIP recibe un código 429 como respuesta a una iniciación de pagos, entonces queda a discreción del PSIP la gestión del reintento de iniciación de pagos luego de transcurrido el tiempo recibido en el *header retry-after* de la respuesta.

E. MECANISMO ALTERNATIVO [Nota: Ver párrafo final explicativo de la sección introductoria de este informe normativo]

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 IPI/IPC deberán:

- Validar los datos contra los datos en otras instancias de almacenamiento y de consulta de las IPI/IPC.

- Realizarse sobre cada uno de las APIs de consulta de datos, y en cada de ellas ~~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~~4 años.

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

Tabla ~~6~~5: Matriz DAMA

Dimensión	Descripción	Métrica
Exactitud (*accuracy*)	Qué tan precisos son los datos en relación con 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 *up time* del servicio. Para lo anterior, en la siguiente tabla se indican los tipos de mantención y las características de estas:

Tabla ~~7~~6: 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~~ Mensual
Evolutiva/ Actualización[8]	14 días	12 horas	~~Semestral~~ Trimestral
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~~tabla muestra las métricas, plazos e información que deberán enviar las IPI/IPC en un auto-reporte de entrega mensual:

Tabla ~~8~~7: Información a ser reportada por las IPI/IPC respecto a rendimiento

Materia	Desagregación	Métrica	Periodo
Disponibilidad de las APIs de datos y pagos	Separado por API. ~~Separado entre mantenciones y bajas no programadas.~~ A nivel total y descontando tiempos de mantención programada	% 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/PSIP.	Milisegundos. mediana, máximo, mínimo, y P90	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.

TPS y TPM (datos y pagos en lo que aplique)	Por API y PSBI/PSIP.	Mediana, máximo, mínimo, p90	Semanal
Tasa de error en APIs de Datos públicos	Separado por API y PSBI/PSIP.	% de llamados de datos con errores, separado por tipo de error	Semanal
Tasa de error en API ~~de consentimiento~~ que implican consentimiento del cliente	Separado por PSBI/PSIP.	% de llamados de consentimiento con errores, separado por tipo de error	Semanal

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

J. IDEMPOTENCIA

Aplicará lo dispuesto para estos efectos en el Portal del Desarrollador.

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. El perfil de seguridad se complementa y detalla con lo indicado en el Portal del Desarrollador.

A continuación, se especificarán algunas características propias de cada área de seguridad de la API. En lo que no se mencione se aplicará 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 y RFC 7592].

iv. Los *endpoints* 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~~ Informe de conformidad de seguridad de OIDF.

VII. El token de acceso será en formato JWT (no opaco) para enviar o acceder

[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.

a la información del campo *authorization details*.

VII. CONSENTIMIENTO Y AUTENTICACIÓN

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.

B. ESTRUCTURA DEL *AUTHORIZATION DETAILS*

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. Sus campos con su respectiva obligatoriedad se señalan en el Portal del Desarrollador.

~~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. No obstante, es un campo informativo que no dará lugar a ninguna restricción por parte de la IPI/IPC.

El parámetro finalidad será ~~expresado~~ denominado en inglés con el término *"purpose",* el cual consistirá en un campo libre de un largo máximo de ~~100~~ 300 caracteres y deberá describirse con un lenguaje claro para el usuario final 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."

```
            }
        ]
    }
```

C. AUTENTICACIÓN DEL CLIENTE POR PARTE DEL IPI/IPC

La forma en que deberá realizar este proceso es mediante un flujo redirigido según las especificaciones señaladas en el Portal del Desarrollador.

D. PANEL DE CONTROL DE CONSENTIMIENTOS

Los estados del consentimiento que podrá ver el usuario final en este panel son los siguientes:

- **Autorización pendiente:** Este estado indica que el consentimiento ya fue creado en ambiente de la PSBI/PSIP, pero está pendiente de autenticación, autorización o aceptación por parte del usuario final en la IPI/IPC.

- **Firmas pendientes:** Este estado indica que el consentimiento ya fue creado en la PSBI/PSIP, pero aún no se encuentra perfeccionado al requerirse la manifestación de voluntad de más de un usuario final, quienes están habilitados para actuar de manera conjunta en la IPI/IPC. Este escenario aplica, por ejemplo, cuando se requiere firma conjunta para iniciar y aprobar pagos o para autorizar el intercambio de información en Persona Jurídica. Una vez que el acuerdo de voluntades esté completo mediante la autorización de los usuarios requeridos en ambiente de la IPI/IPC, el consentimiento pasará a tener el estado de "autorizado".

- **Incompleto:** Este estado indica que, en los casos de actuación conjunta, el consentimiento no logró perfeccionarse porque no concurrieron las demás firmas requeridas en ambiente de la IPI/IPC dentro del tiempo que cada institución considera para este fin, en virtud del tipo de servicio y por motivos de seguridad.

- **Autorizado**: Este estado indica que el consentimiento creado en ambiente de la PSBI/PSIP, fue autorizado por parte de él o los usuarios finales requeridos en la IPI/IPC mediante el proceso de autenticación, estando el consentimiento activo.

- **Rechazado**: Este estado indica que el consentimiento no logró

perfeccionarse, ya sea porque fue cancelado o rechazado por el usuario final en el proceso de autenticación sin mediar autorización; o bien, en los casos de actuación conjunta, porque fue cancelado o rechazado por el usuario que inicia el flujo de pago o de intercambio de información, o por los demás apoderados, antes de la concurrencia de todas las firmas requeridas en ambiente de la IPI/IPC.

- **Revocado:** Este estado indica que el consentimiento previamente autorizado fue revocado por el usuario final.

- **Expirado**: Este estado indica que el consentimiento expiró por haberse cumplido el plazo para el cual fue otorgado, que no puede ser superior al límite regulatorio.

Los flujos de sincronización de cada uno de estos estados entre los Paneles de Control de Consentimiento de las IPI/IPC y de los PSBI/PSIP se describen en el Portal del Desarrollador, considerando si el cambio o actualización fue generado desde las IPI/IPC o los PSBI/PSIP.

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:

- Sí.
- 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.

Módulo específico SFA

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? (selección múltiple)

- IPI.
- IPC.
- PSBI.
- PSIP.
- ~~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.

Variables de RIO de cierre:

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~~8: 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/IPC deberán informar reportes de calidad de la información con la siguiente estructura:

Tabla ~~10~~9: 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~~10: 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 número

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~~ asociados a consentimiento de clientes:

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

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

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

IPI/IPC

Tabla ~~12~~11: Información mensual de actividad para IPI/IPC

a) Información mensual de actividad para información pública de IPI

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 IPI 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/PSIP si es persona natural o jurídica.

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

- **Número de llamadas recibidas en el mes exitosas**: Corresponde al número total de llamadas recibidas por el IPI/IPC por concepto de acceso a información IPI/IPC de parte de los clientes de los PSBI/PSIP 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/PSIP, 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~~12: Información mensual de actividad para PSBI/PSIP

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 si el tipo de cliente del PSBI/PSIP es persona natural o jurídica.

- **Número de llamadas realizadas en el mes**: Corresponde al número total de llamadas realizadas a IPI/IPC 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 IPI/IPC por concepto de acceso a información

/pagos de parte de los clientes donde el intercambio/pago 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/PSIP, 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