

**REF.: MODIFICA NCG 514 QUE
REGULA EL SISTEMA DE
FINANZAS ABIERTAS, E
INCORPORA ANEXO N°3.**

NORMA DE CARÁCTER GENERAL N°569

1 de junio de 2026

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; lo dispuesto en el título III de la ley N°21.521; y lo acordado por el Consejo de la Comisión en Sesión Ordinaria N°498 de 28 de mayo de 2026, ejecutado mediante Resolución Exenta N°5.699 de 29 de mayo de 2026, ha estimado pertinente impartir las siguientes instrucciones que modifican la Norma de Carácter General N°514 que regula el Sistema de Finanzas Abiertas (SFA), en los siguientes términos:

Se reemplaza la sección I.C.1 numeral 1.2 por lo siguiente:

SECCIÓN I: PERÍMETRO DEL SISTEMA DE FINANZAS ABIERTAS

C. Registro de Prestadores de Servicios Basados en Información

1. Inscripción en el Registro

1.2 Antecedentes adjuntos

Se deberá acompañar con la solicitud los siguientes antecedentes:

- a) *Estatutos sociales*. Certificados de vigencia de la sociedad y copia con vigencia de estatutos sociales actualizado, expedido por el organismo competente conforme el régimen registral de la entidad.
 - i. *Régimen tradicional*. Copia de la escritura de constitución y de las escrituras modificatorias de los últimos 10 años, de las inscripciones, en el Registro de Comercio, de los extractos de cada una de éstas, y de la publicación de éstos en el Diario Oficial, junto con el certificado de vigencia de la sociedad y una copia de la inscripción social con constancia de las anotaciones marginales practicadas. Estos documentos no podrán tener una vigencia superior a 15 días desde su respectiva expedición.
 - ii. *Régimen de la Ley N°20.659*. Copia del certificado de vigencia de incorporación y de estatuto social actualizado expedido por el Registro de Empresas y Sociedades.
 - iii. *Agencia de una sociedad extranjera*. Se deberá adjuntar copia del extracto a que se refiere el artículo 123 de la Ley N°18.046 o el artículo 449 del Código de Comercio, según corresponda. Asimismo, se deberá adjuntar copia autorizada de la protocolización de documentos de que tratan los artículos 447 del Código de Comercio y 121 de la Ley N°18.046, según corresponda. Estos documentos no podrán tener una vigencia superior a 45 días desde su expedición.
- b) *Poder y representación del solicitante*. Copia del instrumento público o privado donde consta la designación del Solicitante como representante legal o convencional con poderes suficientes para representar a la entidad en el proceso de registro.
- c) *Plan de negocios y actividades*. Síntesis referencial del plan estratégico y de negocios, indicando las principales líneas de negocios y las actividades

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

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

- d) *Organigrama y estructura organizacional.* El Solicitante debe aportar una descripción general de la organización estructural de la entidad, con una descripción de las principales funciones de sus áreas. Asimismo, deberá detallar cargos claves, comités y estructura de responsabilidades de la o las áreas encargadas del cumplimiento de los requisitos de gestión, operativos y de seguridad que da cuenta esta Norma, la que deberá ser clara, coherente y transparente. En los casos que corresponda, considerar las estructuras de apoyo corporativas. El Solicitante deberá siempre mantener a disposición de la Comisión una copia actualizada y vigente de este documento.
- e) *Descripción de relacionamiento con clientes.* Se debe aportar un documento informativo que detalle (i) los servicios que se prestarán a los clientes y en qué condiciones; (ii) las medidas que adoptará la entidad para garantizar el correcto funcionamiento de sus sistemas en materia de gestión de consentimiento junto con la autorización y autenticación de clientes; (iii) los procedimientos que dispondrá la entidad para que los clientes ejerzan los derechos que le confiere la Ley Fintec. El Solicitante deberá siempre mantener a disposición de la Comisión una copia actualizada y vigente de este documento.
- f) *Consentimiento de Clientes y su gestión.* Se deberá aportar un documento que pormenore los términos que se emplearán para requerir el consentimiento de los clientes de conformidad con lo dispuesto en el artículo 23 de la Ley Fintec, como, asimismo, una descripción del o de los flujos de obtención, registro, mantención, resguardo y gestión del consentimiento que en cada caso implementará la entidad.

- g) *Tratamiento de datos personales.* Se deberá acompañar una descripción del procedimiento para registrar, controlar, rastrear y restringir el acceso a los datos de los clientes, incluyendo aquellos que califiquen como sensibles conforme con los términos de la Ley N°19.628. Como parte de este requisito, la entidad deberá acompañar una descripción de las medidas técnicas y organizativas de seguridad que implementará en atención a los riesgos detectados, así como el modelo de registro de actividades de tratamiento de datos (en adelante "RAT") que implementará, el que deberá, a lo menos, contar con la siguiente información: (i) el nombre y los datos de contacto del responsable del tratamiento y del oficial de protección de datos, de existir tal designación; (ii) los fines de cada tratamiento de datos; tiempo que mantendrán los datos; y la base o fuente de licitud que aplica a cada actividad; (iii) una descripción de las categorías de titulares de datos y de datos personales a tratar; (iv) los principales mecanismos de recolección de datos para cada actividad de tratamiento de datos; y (v) las categorías o tipos de destinatarios o terceros receptores de los datos.
- h) *No afectación de inhabilidad especial del artículo 19 de la Ley Fintec.* Se deberá acompañar declaración jurada simple, suscrita por el representante legal o convencional con poder suficiente, que indique que la entidad no se encuentra afecta a la inhabilidad de registro dispuesta en el inciso final del artículo 19 de la Ley Fintec. El solicitante deberá informar la existencia de modificaciones a este documento tan pronto tome conocimiento de la ocurrencia de alguna circunstancia que modifique el mismo.
- i) *Políticas de gestión.* Documento o conjunto de documentos que contenga las políticas a que se refiere la Sección III de esta norma.
- j) *Certificado de implementación de perfiles de seguridad de interfaces.* Documento que acredite la debida expedición y vigencia del certificado de correcta implementación técnica del estándar de seguridad conforme con los parámetros que se describan en el Anexo N°3 de esta Norma. Las condiciones que deberá cumplir el tercero que expida el respectivo certificado serán materia del referido Anexo N°3.
- k) *Certificado de procedimientos concursales vigentes o quiebras.* Documento expedido por la Superintendencia de Insolvencia y Reemprendimiento, en el que conste que la persona o entidad cuya inscripción se solicita no se encuentra en los registros de quiebra, ni está sometida a un procedimiento concursal de liquidación o de reorganización, de una antigüedad no superior a los 30 días. Para el caso de agencias, esta circunstancia estará referida a la entidad extranjera y se acreditará mediante declaración jurada expedida al efecto por el representante legal.

El solicitante deberá informar la existencia de modificaciones a este documento tan pronto tome conocimiento de la ocurrencia de alguna circunstancia que modifique el mismo.

- l) *Pruebas funcionales.* Documento que acredite, a través de un reporte de evidencia de pruebas provisto por un tercero, la realización de Pruebas Funcionales de consumo de APIs en Áreas de Prueba. Tanto las condiciones que debe tener este tercero, como los elementos mínimos de prueba a efectuarse se deberán ajustar a las especificaciones del Anexo N°3 de esta Norma. El ambiente de prueba válido para la realización de pruebas funcionales es el Sandbox, provisto para estos efectos por la CMF.

En el caso de los documentos expedidos en el extranjero, los mismos deben acompañarse con el respectivo Certificado de Apostilla, en el caso de otorgarse en países miembros del Convenio de la Apostilla de la Haya de 5 de octubre de 1961. En el caso de documentos expedidos en países no miembros del Convenio, los documentos, previo a su presentación, deben someterse al procedimiento de legalización y ratificación de firmas por vía consular o diplomática, establecido en el artículo 345 del Código de Procedimiento Civil. Asimismo, los documentos que originalmente se expidan en un idioma distinto al castellano, deben acompañarse con una traducción oficial al castellano, debidamente apostillada o legalizada, según sea el caso.

Ingresa la solicitud y verificada la completitud de los antecedentes requeridos en la presente sección, se procederá a la inscripción de la entidad en el Registro PSBI, previo pago por parte del Solicitante de los derechos establecidos en el artículo 33 del D.L. N°3.538.

Se reemplaza la sección I.D.1 numeral 1.2 por lo siguiente:

SECCIÓN I: PERÍMETRO DEL SISTEMA DE FINANZAS ABIERTAS

D. Registro de Proveedores de Servicios de Iniciación de Pagos

Los PSIP son aquellas entidades que pueden instruir, a nombre de un cliente y ante la Institución Proveedora de Cuentas respectiva, la ejecución de órdenes de pago o transferencias electrónicas de fondos, incluyendo pagos recurrentes predefinidos en favor de los terceros beneficiarios que los clientes indiquen, con cargo a sus respectivas cuentas y medios de pago.

1. Inscripción en el Registro

1.2 Antecedentes adjuntos

Se deberá acompañar con la solicitud los siguientes antecedentes:

- a) *Estatutos sociales*. Certificados de vigencia de la sociedad y copia con vigencia de estatutos sociales actualizado, expedido por el organismo competente conforme el régimen registral de la entidad.
 - i. *Régimen tradicional*. Copia de la escritura de constitución y de las escrituras modificatorias de los últimos 10 años, de las inscripciones de los extractos de cada una de éstas, y de la publicación de éstos en el Diario Oficial, junto con el certificado de vigencia de la sociedad y una copia de la inscripción social con constancia de las anotaciones marginales practicadas. Estos documentos no podrán tener una vigencia superior a 15 días desde su expedición, respectivamente.
 - ii. *Régimen de la Ley N°20.659*. Copia del certificado de vigencia de incorporación y de estatuto social actualizado expedido por el Registro de Empresas y Sociedades.
 - iii. *Agencia de una sociedad extranjera*. Se deberá adjuntar copia del extracto a que se refiere el artículo 123 de la Ley N°18.046 o el artículo 449 del Código de Comercio, según corresponda. Asimismo, se deberá adjuntar copia autorizada de estatutos y certificado de incorporación de la sociedad extranjera, expedido o visado por ministro de fe competente en la jurisdicción respectiva.
- b) *Poder y representación del solicitante*. Copia del instrumento público o privado donde consta la designación del solicitante como representante

legal o convencional con poderes suficientes para representar a la entidad en el proceso de registro.

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

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

- d) *Responsabilidad Ley N°20.009*. Se deberá proporcionar una descripción de las medidas adoptadas por la entidad para proteger y cautelar los fondos de los clientes que revistan la calidad de usuarios pagadores en el contexto de la iniciación de pagos, como, asimismo, los mecanismos de gestión de reclamaciones ante operaciones no autorizadas en los términos de la Ley N°20.009, incluyendo las medidas de prevención de ocurrencia de fraudes o uso malicioso de instrumentos de pago.
- e) *Custodia transitoria de fondos*. El Solicitante deberá indicar en su solicitud, a través de una declaración jurada simple preparada al efecto, si es su intención desarrollar modelos de negocios que impliquen la mantención o custodia transitoria de fondos en los términos del inciso cuarto del artículo 20 de la Ley Fintec. De ser efectivo lo anterior, de conformidad con lo dispuesto en la Sección I.D.2 de esta Norma, deberá acompañar los antecedentes que acrediten el cumplimiento de los requisitos que determine el Banco Central de Chile en conformidad con sus atribuciones legales.
- f) *Organigrama y estructura organizacional*. El Solicitante debe aportar una descripción de la organización estructural de la entidad, con una descripción de las principales funciones de sus áreas, cargos claves, comités y estructura de responsabilidades. En caso de que corresponda,

considerar las funciones de apoyo corporativas. El Solicitante deberá siempre mantener a disposición de la Comisión una copia actualizada y vigente de este documento.

- g) *Descripción sobre relacionamiento con Clientes.* Se debe aportar un documento informativo que detalle: (i) los servicios que se prestarán a los clientes y en qué condiciones; (ii) las medidas que adoptará la entidad para garantizar el correcto funcionamiento de sus sistemas en materia de gestión de consentimiento junto con la autorización y autenticación de clientes; y (iii) los procedimientos que dispondrá la entidad para que los clientes ejerzan los derechos que le confiere la Ley Fintec. El Solicitante deberá siempre mantener a disposición de la Comisión una copia actualizada y vigente de este documento.
- h) *Consentimiento de clientes y su gestión.* Se deberá aportar un documento que pormenore los términos que se emplearán para requerir el consentimiento de los clientes de conformidad con lo dispuesto en el artículo 23 de la Ley Fintec, como asimismo una descripción del o de los flujos de obtención, registro, mantención, resguardo y gestión del consentimiento que en cada caso implementará la entidad.
- i) *Tratamiento de datos personales.* Se deberá acompañar una descripción del procedimiento para registrar, controlar, rastrear y restringir el acceso a los datos de los clientes, incluyendo aquellos que califiquen como sensibles conforme con los términos de la Ley N°19.628. Como parte de este requisito, la entidad deberá acompañar una descripción de las medidas técnicas y organizativas de seguridad que implementará para este fin, incluyendo los procedimientos técnicos que garanticen el cumplimiento respecto de los datos de iniciación de pagos dispuesto en el inciso cuarto del artículo 20 de la Ley Fintec, así como el modelo de registro de actividades de tratamiento de datos que implementará, el que deberá, a lo menos, contar con la siguiente información: (i) el nombre y los datos de contacto del responsable de tratamiento y del oficial de protección de datos, de existir tal designación; (ii) los fines de cada tratamiento de datos, tiempo que mantendrá los datos y la base o fuente de licitud que aplica a cada actividad; (iii) una descripción de las categorías de titulares de datos y de datos personales a tratar; (iv) los principales puntos de captura asociados a cada actividad de tratamiento de datos; y (v) las categorías o tipos de destinatarios o terceros receptores de los datos.
- j) *No afectación de inhabilidad especial del artículo 20 de la Ley Fintec.* Se deberá acompañar declaración jurada simple, suscrita por el representante legal o convencional con poder suficiente, que indique que la entidad no se encuentra afecta a la inhabilidad de registro dispuesta en el inciso final del artículo 20 de la Ley Fintec. El Solicitante deberá

informar la existencia de modificaciones a este documento tan pronto tome conocimiento de la ocurrencia de alguna circunstancia que modifique el mismo.

- k) *Políticas de gestión*. Documento que contenga las políticas a que se refiere la Sección III esta norma.
- l) *Certificado de Implementación de Perfiles de Seguridad*. Documento que acredite la debida expedición y vigencia del certificado de correcta implementación técnica del estándar de seguridad conforme con los parámetros que se describan en el Anexo N°3 de esta Norma. Las condiciones que deberá cumplir el tercero que expida el respectivo certificado serán materia del referido Anexo N°3.
- m) *Garantías*. Se debe aportar la documentación que acredite la contratación de alguno de los instrumentos de garantía que da cuenta la Sección I.D.4. de esta Norma.
- n) *Certificado de procedimientos concursales vigentes o quiebras*. Documento expedido por la Superintendencia de Insolvencia y Reemprendimiento, en el que conste que la persona o entidad cuya inscripción se solicita no se encuentra en los registros de quiebra, ni está sometida a un procedimiento concursal de liquidación, reorganización o renegociación, de una antigüedad no superior a los 30 días. Para el caso de agencias, esta circunstancia estará referida a la entidad extranjera y se acreditará mediante declaración jurada expedida al efecto por el representante legal. El Solicitante deberá informar la existencia de modificaciones a este documento tan pronto tome conocimiento de la ocurrencia de alguna circunstancia que modifique el mismo.
- o) *Pruebas funcionales*. Documento que acredite, a través de un reporte de evidencia de pruebas provisto por un tercero, la realización de Pruebas Funcionales de consumo de APIs en Áreas de Prueba conforme con los elementos que se detallen en el Anexo N°3 de esta Norma. El ambiente de prueba válido para la realización de pruebas funcionales es el Sandbox, provisto para estos efectos por la CMF.

En el caso de los documentos expedidos en el extranjero, los mismos deben acompañarse con el respectivo "Certificado de Apostilla", en el caso de otorgarse en países miembros del Convenio de la Apostilla de la Haya de 5 de octubre de 1961. En el caso de documentos expedidos en países no miembros del referido convenio, los documentos, previo a su presentación, deben someterse al procedimiento de legalización y ratificación de firmas por vía consular o diplomática, establecido en el artículo 345 del Código de Procedimiento Civil. Asimismo, los documentos que originalmente se expidan en un idioma distinto al castellano, deben acompañarse con una traducción oficial al castellano, debidamente apostillada o legalizada, según sea el caso.

Ingresada la solicitud y verificada la completitud de los antecedentes requeridos en la presente sección, se procederá a la inscripción de la entidad en el Registro PSIP, previo pago por parte del Solicitante de los derechos establecidos en el artículo 33 del D.L. N°3.538.

Se reemplaza la sección I.D.4.a por lo siguiente:

SECCIÓN I: PERÍMETRO DEL SISTEMA DE FINANZAS ABIERTAS

D. Registro de Proveedores de Servicios de Iniciación de Pagos

4. Garantías asociadas

a. Póliza de Seguro

Esta deberá cubrir los daños y perjuicios causados a terceros, de los cuales sea civilmente responsable el PSIP, que resulten de la prestación de los servicios propios de iniciación de pagos, por actos, errores u omisiones ocurridos durante la vigencia de la póliza y que afecten a dichos terceros. Debe cubrir de forma particular las responsabilidades que se pudieran derivar de la actividad de iniciación de pagos por ejecución de órdenes de pago no autorizadas, ejecución tardía o defectuosa, y derecho de resarcimiento de que trata el inciso séptimo del artículo 5° de la Ley N°20.009. Deberá cubrir, asimismo, la responsabilidad civil de sus dependientes, de sus administradores, representantes, apoderados o de cualquier persona que participe en las funciones de su giro por cuenta del PSIP y, en general, la de toda persona por la cual sea civilmente responsable en el ejercicio de su actividad de iniciación de pagos.

La póliza deberá cubrir como mínimo el monto de garantía exigible determinado conforme con la fórmula en esta sección. En caso de que el monto de cobertura incluya cualquier franquicia, deducible o límite, ello no deberá afectar a los pagos que la entidad deba realizar en relación con las solicitudes de reembolso efectuadas por clientes o de resarcimiento por los Emisores que sean IPC.

La cobertura deberá comprender tanto los daños y perjuicios causados a terceros, como los gastos y costas del proceso que éstos o sus causahabientes promuevan en contra del asegurado.

También deberá ser de cargo de la compañía aseguradora los gastos de defensa del asegurado, incluso los honorarios respectivos, aun cuando se trate de reclamaciones infundadas.

Por último, el seguro deberá indicar que el pago de la indemnización al tercero perjudicado se efectuará en virtud de sentencia ejecutoriada, o de transacción judicial o extrajudicial celebrada por el asegurado con el consentimiento de la compañía.

Se reemplaza la sección I.E párrafo inicial y números 1, 2 y 3 por lo siguiente:

SECCIÓN I: PERÍMETRO DEL SISTEMA DE FINANZAS ABIERTAS

E. Nómina de Instituciones Proveedoras de Información y Proveedoras de Cuentas

Todas las entidades consideradas como IPI e IPC de conformidad con el artículo 18 de la Ley Fintec, tendrán que presentar los antecedentes que permiten acreditar el cumplimiento de las exigencias que la referida ley les hace aplicable, debiendo presentar los antecedentes a continuación mencionados para su incorporación y habilitación en un listado de entidades denominado como "Nómina IPI" y "Nómina IPC". Esta será una obligación de incorporación a la nómina aplicable a todas las IPI e IPC, que deberá ser cumplida conforme con los plazos de implementación y exigibilidad gradual del SFA que se estipula en la Sección V.D. de esta Norma.

1. Incorporación a la Nómina

La incorporación en esta nómina es obligatoria para las entidades que la Ley Fintec haya definido que deben ser parte del SFA, las que deberán dar cumplimiento al menos a los siguientes requisitos:

- a) Presentar los antecedentes de información asociados a su incorporación en el Directorio de Participantes.
- b) Acreditar el cumplimiento, respecto de las interfaces que le resulten exigibles, de los estándares y especificaciones técnicas que den cuenta esta norma y su Anexo N°3.
- c) Evidenciar a través de la emisión de un reporte de hallazgos y de certificación de resultados, provisto por un proveedor de acreditable prestigio y experiencia en materias de certificación técnica, desarrollo de proyectos tecnológicos, o aseguramiento de calidad de procesos empresariales, la realización de Pruebas Funcionales sobre sus APIs, considerando además los escenarios de contingencia, conforme con los elementos de prueba -entre los cuales se encuentran los requisitos sobre la cantidad de pruebas y certificaciones, los tipos de certificados y medios de acreditación de cumplimiento y, los roles y necesidad de participación de terceras entidades acreditadoras requeridos- que se detallan en el Anexo N°3 de esta Norma. Dicho reporte debe entregar una opinión sin observaciones de las pruebas realizadas.

- d) Acompañar la documentación sobre los mecanismos de ARC que tiene implementados, y la forma y requerimientos técnicos aplicables para su vinculación o redireccionamiento por parte de los PSBI o PSIP.
- e) Acompañar un certificado expedido por un tercero que cumpla los requisitos del Anexo N°3 de esta Norma, de implementación de perfiles de seguridad de interfaces que acredite la debida expedición y vigencia de la correcta implementación técnica del estándar de seguridad conforme con los parámetros que se describan en el referido anexo.
- f) Acreditar ante la Comisión la adopción e implementación de las políticas de gestión de riesgo indicadas en la Sección III de esta Norma. Los participantes que en virtud de otras disposiciones normativas ya cuenten o deban contar con políticas y procedimientos de gestión de riesgos y control interno, deberán complementar las mismas, incluyendo los aspectos asociados a la operación del SFA que se describen en la referida sección.

La IPI/IPC que no cumpla con los requisitos dispuestos para su incorporación en la respectiva Nómina IPI/IPC dentro de los plazos máximos establecidos en esta Norma, estará impedida de solicitar su habilitación en la Nómina PSBI, conforme lo dispuesto en la Sección I.C de esta Norma.

Lo indicado en el párrafo anterior será sin perjuicio de la eventual aplicación de sanciones por parte de la Comisión en ejercicio de sus facultades legales, por incumplimiento de los plazos establecidos en esta normativa, de conformidad con lo dispuesto en la Ley Fintec y las disposiciones de esta Norma.

Para estos efectos, habrá dos nóminas diferenciadas:

- Nómina de Instituciones Proveedoras de Información; y
- Nómina de Instituciones Proveedoras de Cuentas.

Las entidades que conforme a la Ley Fintec desempeñen más de un rol, deberán acreditar de forma separada, en lo que corresponda, los antecedentes para estar plenamente vigentes en ambas nóminas.

2. Plazos de incorporación a las Nóminas IPI e IPC

Las IPI obligadas por ley a compartir e intercambiar información en el SFA, así como los IPC obligados a cursar e intercambiar información respecto a órdenes de pago, deberán acreditar el cumplimiento de los requisitos y solicitar su incorporación en la Nómina IPI y la Nómina IPC, según corresponda, conforme con los siguientes plazos:

- *IPI del inciso primero del artículo 18, e IPC del artículo 20 de la Ley Fintec.* Deberán presentar su solicitud dentro de los primeros 60 días contados desde la entrada en vigencia de la presente Norma; e
- *IPI del inciso segundo del artículo 18 de la Ley Fintec (letras (a) a (h)).* Deberán presentar su solicitud dentro de los 15 meses siguientes a la entrada en vigencia de la presente Norma.

Los anteriores plazos no incluyen el cumplimiento de los elementos considerados en la sección V letra D, donde se especifican plazos específicos para aspectos de cumplimiento desarrollo de las APIs, entre ellas la realización de pruebas funcionales.

3. Participación simplificada en el SFA

Las IPI del inciso segundo del artículo 18 de la Ley Fintec (letras (a) a (h)) podrán voluntariamente solicitar a la Comisión, por la vía de un requerimiento, la aplicación del régimen de Participación Simplificada (PS) en el SFA. En caso de no hacerlo, deberán participar en el SFA con toda la información requerida en esta norma.

Para lo anterior, las entidades que soliciten la aplicación del régimen de PS deberán acreditar al momento de presentar su solicitud que tienen un número de clientes únicos totales inferior a 100 mil clientes durante el año móvil previo al momento de la postulación, ya sean personas naturales o jurídicas, con al menos un producto vigente conforme al Anexo 2 de la presente norma.

Las IPI que se incorporen al SFA bajo el régimen de PS deberán disponer únicamente de una API que contenga la información relativa a sus canales de atención, según los formatos especificados en el Portal de Desarrolladores.

Asimismo, aquellas IPI bajo el régimen de PS que, a su vez, participen como PSBI, solo podrán acceder a la información de los canales de atención de otras entidades del SFA, asegurándose así la reciprocidad entre los participantes.

La PS consistirá entonces en un atributo del Participante que no solo implicará la disponibilidad limitada de información por parte de la entidad IPI, sino también la restricción de la información a la que puede acceder en caso de participar como PSBI.

Quienes se acojan al régimen de PS estarán exceptuadas del desarrollo de APIs de términos y condiciones, así como de aquellas referidas a datos de clientes. En virtud de dicha excepción, las referidas entidades no estarán obligadas a la

generación e implementación de un Panel de Control de Consentimiento ni a la obtención de certificados de seguridad FAPI 2.0.

Para optar al régimen de PS, las entidades deberán presentar la solicitud en un plazo de 15 meses contado desde la entrada en vigencia de la norma, acreditando el número de clientes únicos totales, y que estos no superan el umbral en los términos ya especificados.

Aquellas entidades que hubiesen iniciado su participación bajo el régimen general y que registren durante 12 meses consecutivos un número de clientes inferior al umbral señalado, también podrán solicitar su incorporación al régimen de PS en el Sistema. Tras la aceptación de su solicitud de acceso a la PS, las entidades deberán notificar a sus clientes de esta nueva situación. También aplicará el principio de reciprocidad, por cuanto desde ese mismo momento cualquier PSBI asociado al IPI/IPC podrá acceder, de ahí en adelante, solo a la información de las APIs que considera la PS.

Por otro lado, aquellas entidades que se acojan al régimen de PS en el Sistema y que superen por 12 meses consecutivos el umbral establecido en esta sección, deberán incorporarse de manera completa al SFA, cumpliendo con todos los requerimientos establecidos en esta norma. Lo anterior deberá realizarse en un plazo máximo de 12 meses, contado desde la verificación de la superación del umbral. En caso de que la superación del umbral ocurra durante el proceso de implementación gradual del Sistema, se aplicará el plazo que resulte mayor entre: (i) los 12 meses antes señalados y (ii) los plazos establecidos en la sección V.D de la presente norma, considerando los hitos de implementación allí definidos.

Se reemplaza la sección II.A números 1 y 3 por lo siguiente:

SECCIÓN II: FUNCIONAMIENTO DEL SISTEMA

A. Medios de intercambio de información

1. Mecanismo principal

Las IPI e IPC deberán poner a disposición APIs para el SFA, junto con la documentación técnica asociada a éstas, necesarias para atender las solicitudes de acceso a los datos del SFA presentadas por los PSBI y PSIP.

En el contexto del SFA, las entidades fiscalizadas no podrán utilizar mecanismos diferentes a las API para atender solicitudes de acceso a datos. El desarrollo y mantención de las APIs será de exclusiva responsabilidad de las IPI e IPC.

Las APIs deberán estar habilitadas en sitios web que las propias instituciones proveerán para estos efectos, y sus direcciones y especificaciones técnicas (*endpoints*) serán comunicadas a la Comisión, quedando disponibles para el uso de los PSBI y los PSIP, según corresponda, en el Directorio del SFA y en los términos que se establezcan en el Anexo N°3 de esta normativa, de acuerdo con lo descrito en la Sección II.B.

Aun cuando el desarrollo de las APIs pueda ser delegado a otra empresa, para todos los efectos la IPI o IPC que participa en el Sistema será la única responsable por las mismas ante la Comisión.

La conexión e intercambio de información entre los Participantes del SFA será bilateral. Lo anterior, independientemente de las posibilidades de tercerización de uno o más componentes asociados a la comunicación o el procesamiento e intercambio de la información, conforme con las disposiciones aplicables.

3. Disponibilidad y rendimiento

Las APIs destinadas a la consulta de los datos asociados a los conjuntos de información indicados en los numerales 1 a 3 del artículo 17 de la Ley Fintec, deben estar disponibles para su uso con un tiempo de actividad mínimo del 95% de forma diaria por día calendario y de 99% 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 4.000 milisegundos, considerando el momento en que se realiza la consulta de la API y el tiempo TTLB transcurrido de la respuesta, conforme revelen las marcas de tiempo respectivas. Tratándose de *endpoints* que provean un número relevante de registros, y que sean debidamente identificados como tales en las especificaciones que da cuenta el

Anexo N°3 de esta Norma, la métrica de rendimiento exigida se aplicará por página de respuesta, considerando hasta 100 registros por cada página.

Las condiciones de paginación, incluyendo los atributos de la respuesta paginada, la indicación del total de páginas de la respuesta y el total de registros, y los vínculos de navegación entre cada una, deberán seguir las especificaciones y lineamientos que se desarrollen en el Anexo N°3 de esta Norma.

Por su parte, las APIs destinadas al servicio de iniciación de pagos por parte de una IPC deberán tener una disponibilidad mínima del 95% de forma diaria por día calendario y de 99,5% de forma mensual.

Las APIs de iniciación de pagos deberán procesar transacciones en un tiempo máximo de 800 milisegundos. El tiempo de procesamiento máximo señalado no considerará los tiempos de ejecución y confirmación que las operaciones de pago requieran para su finalización en los sistemas de pago subyacentes a la iniciación de pagos efectuada.

Los parámetros de disponibilidad y rendimiento de las APIs de Iniciación de Pagos deberán considerar las precisiones de cómputo indicadas en el párrafo primero y segundo de este numeral.

El tiempo de actividad mínimo tendrá como excepción para su cómputo las mantenciones y actualizaciones programadas, debidamente avisadas a la Comisión, así como las suspensiones temporales que mandate la Comisión en el ejercicio de sus facultades.

Las mantenciones programadas deberán cumplir con los requerimientos de tipo de mantención permitida, plazos de información, plazos máximos de extensión, formas de comunicación, entre otros elementos críticos, según lo que se consigna en el Anexo N°3 de la presente normativa. En ningún caso las mantenciones de los servicios podrán tener una frecuencia o programación tal que impidan la provisión regular del servicio provisto por los PSBI o PSIP.

Sin perjuicio que las entidades deberán contar con mecanismos y/o sistemas que les permitan monitorear permanentemente el rendimiento y disponibilidad de sus APIs, los reportes a la CMF de los respectivos estándares se deberán enviar de acuerdo sea establecido en la normativa correspondiente. Las IPI y IPC podrán contratar con terceros servicios de monitoreo y verificación de disponibilidad y rendimiento de sus interfaces, los que se someterán a las normas sobre tercerización de servicios impartidas por la Comisión que les resulten aplicables. En caso alguno la tercerización del monitoreo, en todo o en parte, afectará la responsabilidad que las IPI e IPC tienen frente a la Comisión respecto al reporte completo y oportuno de sus indicadores de disponibilidad y rendimiento.

El incumplimiento de los parámetros mínimos indicados en esta sección podrá ser sancionado por la Comisión de conformidad con sus atribuciones legales.

Con todo, los términos de rendimiento y disponibilidad aquí indicados resultarán aplicables, sin perjuicio de los límites operativos de transacciones máximas concurrentes por minuto para cada interfaz que se indiquen en el Anexo N°3 de esta Norma.

De forma excepcional, el primer año de vigencia de la presente Norma, las métricas de disponibilidad mínima mensual que da cuenta el presente numeral se medirán de forma trimestral, considerando una media móvil de 90 días.

Las IPI/IPC durante el periodo piloto no tendrán exigibilidad de disponibilidad y rendimiento ni de límites de TPM y TPS.

Se reemplaza la sección II.B por lo siguiente:

SECCIÓN II: FUNCIONAMIENTO DEL SISTEMA

B. Mecanismo alternativo

Para todos los efectos, y tanto respecto de las IPI como de las IPC, se entenderá por mecanismo alternativo de sus APIs aquel que opere en caso de contingencia del mecanismo principal, en el marco de las exigencias de continuidad operacional en esta norma.

Las IPI/IPC deberán garantizar la continuidad operacional de sus servicios, asegurando niveles de disponibilidad y resiliencia que cumplan, como mínimo, con los umbrales de respuesta definidos en la normativa vigente. Para tal efecto, deberán evaluar y adoptar mecanismos alternativos de resiliencia operacional que sean coherentes con su perfil de riesgo operacional en el ámbito del SFA, la naturaleza, el volumen y la complejidad de sus operaciones, así como con el nivel de tolerancia al riesgo establecido por su Directorio. Tales mecanismos debiesen incluir por ejemplo configuraciones de alta disponibilidad, despliegues en múltiples zonas geográficas que aseguren que el mecanismo alternativo no comparta los mismos factores de riesgo que el principal, y arquitecturas que incorporen redundancias en las capas superiores del servicio.

El mecanismo alternativo implementado deberá ser sometido a pruebas, al menos una vez al año, con el propósito de verificar su capacidad para asegurar la entrega de información y la ejecución de pagos del SFA con niveles de servicio conformes a los umbrales establecidos.

Se reemplaza la sección II.C por lo siguiente:

SECCIÓN II: FUNCIONAMIENTO DEL SISTEMA

C. Directorio de Participantes

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

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

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

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

Se reemplaza la sección II.D por lo siguiente:

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 anual y sus resultados serán entregados a la Comisión. El primer informe, previo a la entrada en operación de la API, deberá ser entregado en los mismos plazos que tienen las entidades para la entrega de los certificados funcionales en su proceso de inscripción en la nómina indicados en la sección V.D de la norma.

El informe de calidad de la información no requiere ser emitido por una entidad externa y el mismo participante puede desarrollarlo en función de las directrices descritas en el Anexo 3 de la presente norma.

En caso de detectarse deficiencias significativas, las 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 mandar 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 y las IPC. Lo anterior deberá ser complementario de la comunicación ante contingencias que debe realizar el PSBI/PSIP con la entidad IPI/IPC, según lo indicado en la sección II.E "Mecanismos de comunicación ante contingencia" de esta norma, mediante los contactos asignados para estos efectos.

Se incluye la siguiente letra G en la sección II:

SECCIÓN II: FUNCIONAMIENTO DEL SISTEMA

G. Periodo piloto

A partir del cumplimiento del límite de plazo dispuesto en la Sección V.D para el inicio del funcionamiento de cada API y por un plazo de 60 días, tanto para las APIs de IPI como de IPC, no se exigirán los SLA definidos en esta norma, así como tampoco límites de TPS/TPM. Todos los demás requisitos normativos sí serán exigibles en este periodo.

En cualquier caso, será deber de los IPI y los IPC mantener altos niveles de disponibilidad, con el objetivo de presentar una transición ordenada al régimen. Podrá ser sancionada la indisponibilidad que no se ajuste a un proceso justificado de adecuación y desarrollo de las APIs, considerando que la entidad, en esta etapa, ya debió dar cumplimiento a los requisitos técnicos propios de la inscripción y del registro asociado.

Adicionalmente, las entidades que habiliten sus APIs antes de los plazos máximos de implementación establecidos en la Sección V.D, tendrán la posibilidad de adelantar el inicio de su periodo piloto desde que se realice esta habilitación. En este periodo adicional, antes del límite de implementación, se permitirá, además:

- 1) Intercambiar información de conjuntos de clientes, definidos por la propia IPI/IPC.
- 2) Intercambiar información con PSBI acordados.
- 3) Realizar pruebas de intercambio "*in-house*" donde el PSBI de la propia IPI, en aquellos casos donde esto aplique, es el lector final de la información.

Todos los clientes financieros durante este periodo piloto deberán estar debidamente informados, lo cual no limita la responsabilidad de la IPI/IPC respecto del cumplimiento de los resguardos que la propia Ley establece.

Durante todo el periodo piloto las entidades deberán cumplir con los flujos regulados de acuerdo a esta norma, incluyendo el Directorio de Participantes.

Una IPI/IPC podrá mantener APIs en periodo piloto coexistiendo con APIs en funcionamiento normal. En particular, cuando las instituciones participantes se encuentren en este periodo piloto, esta circunstancia deberá informarse en el Directorio, incluyendo la fecha de inicio y de finalización respectiva de esta etapa.

Se incluye la siguiente letra H en la sección II:

SECCIÓN II: FUNCIONAMIENTO DEL SISTEMA

H. Habilitación de ambientes de pruebas previas a la entrada en vigencia.

El Sandbox y el Directorio deberán encontrarse habilitados para la realización de pruebas previas en un plazo de 9 meses antes de la entrada en vigencia de la normativa.

Las IPI e IPC podrán hacer uso de estos ambientes para efectos de sus pruebas funcionales, tanto en dichos roles como en el de PSBI.

En el caso de los PSIP o de las entidades que deban registrarse como PSBI para participar en el SFA, se habilitará, con anterioridad a la entrada en vigencia de la presente norma, un formulario de registro que permitirá a dichas entidades participar en el ambiente de pruebas.

El número de entidades que podrán ser seleccionadas para participar en estas pruebas previas estará sujeto a las capacidades técnicas de la Comisión. El registro tendrá carácter transitorio y habilitará únicamente el acceso al ambiente de pruebas previo a la entrada en vigencia de la norma. Una vez que esta entre en vigencia, el acceso al ambiente de pruebas estará disponible con carácter permanente para las entidades que cumplan los requisitos establecidos en la presente norma.

La participación en estas pruebas tendrá carácter voluntario, sin perjuicio de que los resultados obtenidos puedan ser considerados válidos para el proceso de inscripción en la nómina o de registro respectivo.

El ambiente de pruebas de la Comisión estará disponible de forma permanente desde la entrada en vigencia de la presente norma. En este contexto, la habilitación anticipada del ambiente señalada precedentemente tiene por único objeto permitir su utilización previa a dicha fecha, en las condiciones aquí establecidas.

Se reemplaza la sección III.D números 1 y 2 por lo siguiente:

SECCIÓN III: SEGURIDAD Y RESGUARDOS DEL SISTEMA

D. Consentimiento

1. Otorgamiento del consentimiento

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

- a) La voluntad haya sido manifestada de manera expresa, en los siguientes términos:
 - i. *En el caso de Persona Natural:* directamente por el respectivo titular de datos o titular de la cuenta; por su representante legal; o bien, por su mandatario.
 - ii. *En el caso de Persona Jurídica:* a través de su representante legal o bien, por sus apoderados o mandatarios.

Para los efectos de la iniciación de pagos, se entenderá que se encuentran facultadas aquellas personas que, conforme al poder o régimen de firma vigente, ya pueden efectuar pagos, transferencias u operaciones equivalentes a nombre de la empresa.

Serán las IPI/IPC quienes, mediante el proceso de autenticación regulado en la presente normativa, verificarán que la persona que está otorgando el consentimiento esté debidamente facultada para ello en los términos señalados en los literales i y ii anteriores.

- b) El PSBI y PSIP haya implementado el mecanismo de gestión del consentimiento en los términos y condiciones establecidas en la sección D.2 siguiente y haya autenticado al usuario final que está otorgando el consentimiento o se le está requiriendo.
- c) La voluntad sea almacenada en un soporte duradero, que sea apto para resguardar su seguridad, integridad y acceso, respecto de la identidad de: a) el titular de los datos/cuentas; o b) la identificación de la o las personas que dieron el consentimiento por la Persona Jurídica junto a la identificación de esta. Además, deberá almacenar las circunstancias y condiciones en que fue solicitado y otorgado, de manera que pueda verificarse posteriormente que dicho consentimiento fue manifestado de

manera previa, libre, informada, expresa y específica en cuanto al tipo de información requerida, la finalidad y el periodo máximo de validez de esa autorización. En los casos de iniciación de pago, además deberán almacenarse los datos de la instrucción de la orden de pago.

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

e) Al momento de solicitar el consentimiento para la transmisión, tratamiento o cesión de datos en el marco de un servicio vinculado al SFA¹, o para iniciar pagos, deberá poner en conocimiento del titular o usuario final de manera precisa y clara el tipo de información para la que consiente el intercambio, tratamiento, cesión antes referida o iniciación en el marco del SFA; el servicio que pretende prestar; a qué institución confiere la autorización para ello, o para iniciar y cursar el o los pagos; por qué período o frecuencia; y para qué finalidad, la que deberá ser suficientemente clara y detallada para que no haya confusión respecto del propósito para el que se requiere el intercambio, tratamiento, cesión de datos antes referida o iniciación de pagos.

El consentimiento no podrá requerirse para actos o fines distintos a los que se informan al otorgante. La concordancia y proporcionalidad entre tipo de información solicitada y la finalidad deberá ser acreditada por el PSBI/PSIP cuando sea requerido por la Comisión. No corresponderá a las IPI/IPC rechazar las solicitudes que las PSBI y PSIP les comuniquen, sin perjuicio de rechazos por razones estrictamente técnicas o de seguridad del Sistema.

¹ La cesión es instrumental para la prestación directa de un servicio al usuario final por parte del PSBI/PSIP

f) Que los tipos de datos sobre los que versa el consentimiento y vigencia de este sean los estrictamente necesarios para la finalidad respectiva, circunstancia que el PSBI o PSIP deberá acreditar cuando ello sea requerido por la Comisión en el marco de sus procesos de fiscalización, no correspondiendo a la IPI o IPC pronunciarse a ese respecto ni alterar el requerimiento original formulado por la PSBI o PSIP en el marco del SFA.

g) Que la información que se pone en conocimiento del titular o cliente para obtener el consentimiento esté expresada en un lenguaje sencillo, claro, preciso y evitando tecnicismos, salvo en los casos en que resulte estrictamente necesario, debiendo explicarlos claramente. Además, deberá disponer de mecanismos que permitan a personas en situación de discapacidad acceder a esta información.

h) Una vez que el titular de datos/cuentas o usuario final haya otorgado el consentimiento se le deberá informar que, tanto el PSBI o PSIP como la IPI o IPC, pondrán a su disposición un panel de control de consentimientos y la forma en que podrá acceder al mismo, mediante el cual podrá conocer y revocar los consentimientos que haya otorgado.

i) Que el titular de los datos/cuentas o usuario final se haya autenticado conforme a los estándares que para ello se establecen en la sección III.C N°2 de esta normativa.

Queda prohibido a la IPI o a la IPC alterar el contenido de la solicitud de consentimiento formulada por la PSBI o PSIP en el marco del SFA, pedir un consentimiento adicional para el mismo intercambio, tratamiento, cesión de datos en el marco de un servicio vinculado al SFA o iniciación de pago; o adoptar medidas o prácticas que desincentiven el otorgamiento del consentimiento por los titulares o usuarios finales, o que deterioren la experiencia usuaria de esos titulares o clientes.

Al momento de adoptar o implementar nuevas tecnologías, las IPI o IPC deberán propender al uso de aquellas que mejoren la experiencia usuaria y minimicen el número de direccionamientos del usuario en el marco del SFA. Ello no obsta a que en la interfaz que ponga la IPI o IPC a disposición de la persona como parte del proceso de autenticación, se incluya aquella información que facilite el intercambio de datos o la iniciación de pagos mejorando la experiencia usuaria como, por ejemplo, que se le permita seleccionar el o los productos o tipos de productos para los cuales quiere acotar el intercambio o tratamiento de información. Tampoco impide, por ejemplo, la selección de la cuenta sobre la cual se va a cursar el pago, si no fue informada por el PSIP o si el respectivo caso de uso requiere de una selección directa en ambiente de la IPC, o si en

ambiente de la IPC el usuario final desea modificar la elección de la cuenta previamente informada.

La interfaz de la IPI o IPC no podrá contener opciones pre marcadas o marcadas por defecto, ni tampoco presentar información distinta a la comunicada por el PSBI o PSIP, para efectos de producirse la autorización de intercambio de información, o la iniciación de pago, o incorporar elementos que no ayuden a la comprensión del usuario de lo que va a autorizar, o aumente el contenido del consentimiento más allá de los elementos necesarios para el intercambio, tratamiento, cesión de datos en el marco de un servicio vinculado al SFA o iniciación de pago en virtud del artículo 23 de la Ley 21.521, debiendo tales IPI e IPC velar porque el proceso de autenticación se desarrolle de forma eficiente y trazable, resguardando los niveles de seguridad exigidos y que ocurra en el menor número de pasos necesarios.

La interfaz usuaria del PSBI o PSIP, con el objeto de facilitar la especificación del período, podrá dar opciones predeterminadas (por ejemplo, un solo uso, 7 días, 1 mes, 3 meses, 6 meses, 12 meses o hasta 36 meses), o incorporar la opción "mientras dure el contrato o prestación del servicio" indicando la duración del respectivo contrato o servicio. En todo caso, el consentimiento no podrá tener una duración superior a 36 meses, aun cuando el contrato o servicio tenga una duración mayor.

Tratándose de servicios de iniciación de pagos que contemplen pagos recurrentes, la interfaz usuaria del PSIP podrá, adicionalmente, permitir al usuario final seleccionar la recurrencia o frecuencia con que se ejecutarán dichos pagos (por ejemplo, diaria, semanal, mensual u otra). La selección de dicha recurrencia no alterará el plazo máximo de vigencia del consentimiento, el que en todo caso no podrá exceder de 36 meses. Sólo en los casos de iniciación de pagos correspondientes a un pago único programado, el plazo máximo del consentimiento será de 90 días.

Lo anterior, en ningún caso limita la facultad que tiene el PSBI/PSIP de solicitar un nuevo consentimiento al usuario final antes de la expiración del consentimiento vigente con el objetivo de mantener la continuidad del servicio que se encuentre prestando. Dicho nuevo consentimiento deberá otorgarse conforme a las reglas generales establecidas en la presente normativa².

Por otro lado, la interfaz del PSIP debe permitir que el usuario indique los datos necesarios para la instrucción de la orden de pago, incluyendo la respectiva IPC, datos de la cuenta o medio de pago respectivo, valor de la transacción, fecha de pago y el tercero beneficiario de este pago. También se debe señalar al respectivo PSIP e individualizar al usuario titular de la cuenta, y en caso de estar actuando como representante legal, apoderado o mandatario de una Persona

² El nuevo consentimiento requerirá que el usuario final se autentique en ambiente de la IPI/IPC.

Jurídica, deberá señalar tanto su información como Persona Natural y también la de la correspondiente Persona Jurídica.

En los casos en que se requiera más de una firma por existir actuación conjunta, la IPI/IPC deberá notificar a la persona que inició la solicitud de intercambio de información o de iniciación de pago y a las demás personas que deban firmar dicha solicitud, en la forma y con los medios que ya emplea para informar operaciones a sus clientes, así como al PSBI/PSIP, del hecho que todos los firmantes dieron su autorización o, en su defecto, que dicha solicitud no haya podido ser autorizada por falta de alguna firma o por un error o falla del sistema u otra circunstancia que se indique, para que pueda completarse el proceso de firma o subsanarse el error, falla o circunstancia ante quien corresponda, incluido el PSBI/PSIP cuando proceda.

Para efectos de lo establecido en esta normativa, la Finalidad es el propósito o motivo específico y explícito por el cual el usuario autoriza que sus datos financieros o los datos de la persona natural o jurídica a la que está representando, sean compartidos dentro del SFA. En virtud de lo establecido en el artículo 19 de la Ley N°21.521, esa finalidad necesariamente debe tener relación con la prestación de un servicio, toda vez que las consultas, acceso y recepción de datos en el marco del SFA es para efectos de proveer servicios a los titulares de datos/cuentas o usuarios finales o su Persona Jurídica.

En tal sentido, no es una finalidad legítima en el marco del SFA la mera cesión de datos sin que esta se encuentre vinculada a la prestación de un servicio por parte del PSBI/PSIP en el marco del Sistema de Finanzas Abiertas.

La naturaleza secreta o reservada de la información deberá resguardarse en todo momento, incluso después de concluida la operación o de finalizada la relación que dio origen a su intercambio, cesión o tratamiento.

Finalmente, una vez autenticado según la sección III.C N°2 de esta normativa el o los usuarios, según corresponda, la IPI o IPC deberá comunicar ese hecho en tiempo real al PSBI o PSIP, de manera que el consentimiento válidamente otorgado pueda quedar almacenado tanto en la IPI o IPC como en la PSBI o PSIP respectivo.

2. Gestión del consentimiento y obligaciones de información

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

Este panel de control de consentimientos deberá cumplir las siguientes condiciones y requisitos, independiente de si es puesto a disposición de los

titulares de datos/cuentas o usuarios finales, directamente por la institución o por terceros por cuenta de ésta:

- a) Deben ser de acceso gratuito y remoto para el titular de datos/cuentas o usuario final.
- b) Deben contar con una interfaz usuaria fácil de utilizar, esto es, que permita al titular de datos/cuentas o usuario final conocer y revocar los consentimientos de manera simple e intuitiva. Además, deberán considerar los mecanismos dispuestos en el numeral 1.g), anterior.
- c) Para efectos de que el usuario final pueda modificar o revocar cualquiera de los consentimientos previamente otorgados, deberá efectuarse mediante el mismo mecanismo utilizado para su otorgamiento, debiendo el usuario final autenticarse conforme a lo dispuesto en la Sección III.C. N°2 de esta normativa.
- d) La interfaz usuaria debe permitir obtener el detalle de cada consentimiento otorgado, de manera que ese titular o usuario final pueda informarse respecto a:
 - i. La institución a la que otorgó el consentimiento para intercambiar, tratar o ceder sus datos para la prestación de un servicio en el marco del Sistema de Finanzas Abiertas, o iniciar y efectuar el pago. Para lo cual deberá indicarse el nombre comercial o de fantasía, así como razón social.
 - ii. La finalidad para la cual se otorgó dicho consentimiento. En caso de que la finalidad cambie durante la vigencia del consentimiento, se deberá mostrar la más actualizada.
 - iii. El tipo de información cuyo intercambio o tratamiento o cesión para la prestación de un servicio en el marco del Sistema de Finanzas Abiertas fue consentido.
 - iv. Fecha en la que se otorgó el consentimiento, incluida la hora en que se registró el mismo, permitiendo así identificar adecuadamente la existencia de múltiples consentimientos otorgados durante un mismo día.
 - v. Periodo o plazo y frecuencia cuando corresponda, para el cual el consentimiento fue otorgado.
 - vi. Estado actual del consentimiento respectivo, es decir, si está pendiente, rechazado, autorizado, expirado o revocado.

- vii. La identificación del usuario final o los representantes legales o mandatarios o apoderados que otorgaron o revocaron el consentimiento por esa persona, si corresponde y la identificación de la Persona Jurídica, en su caso.

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

- f) Permitir la visualización de todos los consentimientos que han sido rechazados, autorizados, expirados o revocados durante los últimos 5 años.

- g) Contar con un sistema destinado a prevenir y evitar que se continúe efectuando iniciaciones de pago, intercambio, tratamiento o cesión de datos para la prestación de un servicio en el marco del Sistema de Finanzas Abiertas una vez revocado el consentimiento. Para lo anterior, dicho sistema deberá contar con un mecanismo de comunicación asincrónica³ basada en eventos con los demás paneles de control de consentimiento implementados por los PSBI, PSIP, IPI e IPC que permita que los cambios en los estados de los consentimientos sean oportunamente comunicados entre dichas entidades, de manera que el titular de datos/cuentas o usuario final pueda gestionar sus consentimientos indistintamente en el PSBI, PSIP, IPI o IPC respectiva.

En caso de que el titular de los datos/cuentas o usuario final no acceda al panel de control de consentimientos habilitado por el PSBI o PSIP por un periodo de más de un año calendario y existan consentimientos vigentes, se deberá enviar una comunicación al lugar o medio que dicho titular de datos/cuentas o usuario final haya indicado para tales efectos, recordándole la existencia del panel de control de consentimientos a través del cual puede conocer, gestionar y revocar los consentimientos otorgados. Dicha comunicación se deberá remitir dentro de los cinco primeros días hábiles inmediatamente posteriores al cumplimiento de ese año de inactividad.

³ Especificaciones de este mecanismo en Anexo 3 y en el Portal de Desarrolladores.

Se reemplaza la sección III.E.1 por lo siguiente:

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.

Se reemplaza la sección IV letras A y B por lo siguiente:

SECCIÓN IV: INFORMACIÓN DEL SISTEMA

A. Datos para compartir en el SFA

La información para compartir en el SFA es la que se incluye en las siguientes categorías, con las características que a continuación se señala en materia de entrega, actualización, alcance histórico de los datos, sujetos obligados a proveer la información en el Sistema, y quienes pueden acceder a la misma.

Un detalle de las taxonomías de variables y datos a ser suministrados y compartidos se incluye en el Anexo N°1. En el Anexo N°2 se encuentra la codificación que permite distinguir los distintos productos a informar en el Sistema.

Tabla N°3: Tipos de datos a compartir en el SFA

CATEGORÍA	CONJUNTO DE INFORMACIÓN	DETALLE DE LA INFORMACIÓN
Términos, condiciones y canales de atención	Términos y condiciones	<ul style="list-style-type: none">• Descripción general: Listado de productos que ofrece la compañía y sus condiciones.• Actualización de la información: semanal• Tiempo para disponer la información en el SFA una vez cumplido el plazo de actualización: Hasta 5 minutos.• Historia del dato: No aplica.• Proveen la información: IPI.• Acceden a la información: PSBI.
	Canales de atención	<ul style="list-style-type: none">• Descripción general: Listado de los locales de atención, sitios web y ATM con sus respectivas ubicaciones.• Actualización de la información: Semanal.• Tiempo para disponer la información en el SFA una vez cumplido el plazo de actualización: Hasta 5 minutos.• Historia del dato: No aplica.• Proveen la información: IPI.• Acceden a la información: PSBI.

Identificación y registro	Enrolamiento	<ul style="list-style-type: none"> • Descripción general: Listado de datos e información que provee el cliente al momento de un enrolamiento. • Actualización de la información: Diaria. • Tiempo para disponer la información en el SFA una vez cumplido el plazo de actualización: Hasta 5 minutos. • Proveen la información: IPI. • Acceden a la información: PSBI. • Alcance del tipo de cliente del cual se comparten datos: Personas jurídicas y naturales.
Condiciones Comerciales Contratadas y el Uso o Historia de Transacciones	Posiciones financieras históricas	<ul style="list-style-type: none"> • Descripción general: Set de productos que tiene el cliente y sus características en el tiempo, tanto para activos y pasivos financieros. • Actualización de la información: Mensual • Tiempo para disponer la información en el SFA una vez cumplido el plazo de actualización: Hasta 5 minutos. • Unidad de tiempo de la información: Mensual (saldo a fin de mes). • Periodo histórico de la información: 24 meses. • La información tendrá, en su inicio operativo, 12 meses históricos, que se irán ampliando mensualmente hasta llegar a 24 meses de información. • Proveen la información: IPI según aplicabilidad indicada en el Anexo N°1. • Acceden a la información: PSBI. • Alcance del tipo de cliente del cual se comparten datos: Personas jurídicas y naturales.
Historia de uso y transacciones		<ul style="list-style-type: none"> • Descripción general: Información que da cuenta del uso de los instrumentos financieros y del acceso a éstos. • Actualización de la información: 5 minutos. • Los 5 minutos corresponden al máximo desfase que debe tener la información del cliente desde que

		<p>está presente en las interfaces propias del banco para su visualización, hasta cuando también queda disponible en el SFA para consultas del PSBI/PSIP.</p> <ul style="list-style-type: none"> • Tiempo para disponer la información en el SFA una vez cumplido el plazo de actualización: Hasta 5 minutos. • Unidad de tiempo de la información: No aplica. Se reporta en función a la fecha del uso o contratación. • Periodo histórico de la información: 24 meses. • Proveen la información: IPI según aplicabilidad indicada en el Anexo N°1. • Acceden a la información: PSBI y PSIP. • Alcance del tipo de cliente del cual se comparten datos: Personas jurídicas y naturales.
	Productos vigentes	<ul style="list-style-type: none"> • Descripción general: Información en línea del cliente vigente a la fecha de consulta. • Tiempo para disponer la información en el SFA: Hasta 5 minutos. • Unidad de tiempo de la información: No aplica. • Profundidad histórica de la información: No aplica. • Proveen la información: IPI según aplicabilidad indicada del Anexo N°1. • Acceden a la información: PSBI. • Alcance del tipo de cliente del cual se comparten datos: Personas jurídicas y naturales.
Iniciación de pagos	Iniciación de pagos	<ul style="list-style-type: none"> • Descripción general: Información mínima necesaria para la realización de ejecución de iniciaciones de pagos. • Actualización de la información: Tiempo real. • Unidad de tiempo de la información: No aplica. • Profundidad histórica de la información: No aplica. • Participantes en el intercambio de información: IPC y PSIP.

- Alcance del tipo de cliente del cual se realizan pagos: Personas jurídicas y naturales.

Los datos del SFA deberán cumplir con las siguientes condiciones:

- a) Estar disponibles al momento de la solicitud del cliente.
- b) Estar siempre vigentes y validados respecto a la situación del cliente según las condiciones determinadas en la presente normativa. En particular, deberán reflejar cualquier cambio en las condiciones, ajustes, rectificaciones que se hayan realizado o informado al IPI e IPC.
- c) Estar disponibles en las mismas condiciones antes señaladas, tanto para el mecanismo principal como para el alternativo.

Para el caso de información de saldos en línea, deben informarse todos los productos vigentes, independientemente si presentan saldo cero al momento de la consulta. Adicionalmente, para este mismo conjunto de información, en el caso de que los saldos se calculen considerando actualizaciones diarias o con una periodicidad mayor, debe reflejarse la fecha de la última información disponible.

B. Plazos para la disponibilidad de los conjuntos de datos

Las fechas en que los conjuntos de información identificados en la Tabla N°3 deben estar vigentes en el Sistema, son aquellas señaladas en la Sección V.D de esta Norma.

Se reemplaza la sección V en todas sus letras por lo siguiente:

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 se vean afectadas por algún tipo de incidente de ciberseguridad que comprometa los activos de información asociados al SFA o que involucre una vulneración de los datos personales de los clientes.
- c) Entidades que enfrenten algún incidente operacional que les impida la transferencia y/o el 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 incumplan los requisitos de participación en el Sistema que comprometan la integridad y la seguridad 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 en ninguna circunstancia deben afectar los activos de información asociados al SFA, entre ellos, los datos personales de los clientes. 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. Se consideran como riesgos relevantes al menos los considerados en las letras a, b y c previamente indicadas, entre otros evaluados por la misma institución en línea con los activos críticos considerados en su evaluación de riesgos. Acciones como auto desconexiones y denegaciones deben ser reportadas mediante RIO. Junto con lo anterior, deberá enviar a la brevedad un reporte a la CMF, mediante una actualización del RIO respectivo, informando las medidas implementadas 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 denegar el acceso a la información cuando reciba un volumen significativo de llamadas erróneas (4xx) o repetitivas por parte de un PSBI o PSIP que 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.

Previamente a cualquier medida restrictiva, el IPI/IPC deberá aplicar respecto del PSBI/PSIP un esquema de escalonamiento proporcional, que considere advertencias, notificaciones y la eventual denegación selectiva, manteniendo trazabilidad y evidencia que permitan sustentar su apelación.

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 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 RIO 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.

Medición de la disponibilidad durante las suspensiones o desconexiones

Para efectos de la evaluación del SLA, el cálculo de la disponibilidad considerará únicamente el periodo durante el cual el participante se encontraba obligado a efectuar el intercambio de información excluyendo el tiempo durante el cual estuvo desconectado o suspendido.

B. Desconexión por no vigencia de certificados

La vigencia de los certificados de identidad constituirá un requisito técnico mínimo para la participación en el Sistema y para el intercambio de información entre participantes.

En caso de caducidad de dichos certificados, la entidad correspondiente quedará automáticamente en estado de participación "Desconectado", condición que se mantendrá hasta que se disponibilice el certificado actualizado respectivo. Sin perjuicio de lo anterior, el Participante, en su calidad de primer responsable del cumplimiento asociado, deberá asignarse a sí mismo este estado, y reportarlo a través de un RIO.

C. Sanciones

De conformidad con el artículo 27 de la Ley Fintec, los Participantes del SFA que incurrieren en infracciones a las disposiciones de dicha ley o incumplieren las instrucciones de la presente normativa, serán sancionados conforme a las reglas establecidas en el Título III del DL N°3.538, de 1980, sin perjuicio de sanciones contenidas en otros cuerpos legales.

La Comisión, conforme a sus facultades, podrá sancionar con una suspensión definitiva o cancelación de registro, sin perjuicio de determinar la suspensión temporal mientras se recaban antecedentes, como parte de un proceso sancionatorio.

D. Plazos de implementación del Sistema

El SFA tendrá un periodo de implementación en dos etapas. La primera, que durará 36 meses, considera la preparación tecnológica y desarrollo de las tareas propias que corresponden a los participantes y a la Comisión. Este periodo de 36 meses comienza con la primera publicación de la NCG 514. Una vez terminado dicho periodo, la presente norma entrará en vigencia.

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

- Los bancos, los emisores de tarjetas de crédito y los emisores de tarjetas de pago con provisión de fondos, deberán cumplir con los siguientes plazos:
 - a) 5 meses para implementación de APIs sobre Términos y Condiciones Generales y de Canales de Atención.
 - b) 9 meses para implementación de APIs sobre Enrolamiento, Posiciones Financieras Históricas, Historial de usos y transacciones, y Productos vigentes; todo lo anterior referido a clientes personas naturales.
 - c) 12 meses para implementación de APIs sobre Enrolamiento, Posiciones Financieras Históricas, Historial de usos y transacciones, y Productos vigentes; todo lo anterior referido a clientes personas jurídicas.
 - d) 12 meses para implementación de APIs sobre Iniciación de Pagos en el caso de clientes personas naturales y pagos únicos.
 - e) 14 meses para implementación de APIs sobre Iniciación de Pagos en el caso de clientes personas naturales y pagos recurrentes.
 - f) 15 meses para implementación de APIs sobre Iniciación de Pagos en el caso de clientes personas jurídicas mandato simple y pagos únicos.
 - g) 16 meses para implementación de APIs sobre Iniciación de Pagos, en el caso de clientes personas jurídicas mandato simple y pagos recurrentes.
 - h) 17 meses para implementación de APIs sobre Iniciación de Pagos, en el caso de clientes personas jurídicas mandato múltiple y pagos únicos.
 - i) 18 meses para implementación de APIs sobre Iniciación de Pagos en el caso de clientes personas jurídicas mandato múltiple y pagos recurrentes.
- Para las entidades indicadas en el inciso segundo, letras (a) a la (h) del artículo 18 de la Ley Fintec, los plazos correspondientes para que deban tener disponibles sus APIs serán:
 - a) 20 meses para implementación de APIs sobre Términos y Condiciones Generales y Canales de Atención.
 - b) 24 meses para implementación de APIs sobre Enrolamiento, Posiciones Financieras Históricas, Historial de usos y transacciones y Productos vigentes, para clientes personas naturales. En el caso de compañías de seguros el alcance considera pólizas individuales.

- c) 28 meses para la implementación de APIs sobre Enrolamiento, Posiciones Financieras Históricas, Historial de usos y transacciones y Productos vigentes, en el caso de compañías de seguros para clientes que sean personas naturales con pólizas masivas.
- d) 30 meses para la implementación de APIs sobre Enrolamiento, Posiciones Financieras Históricas, Historial de usos y transacciones, y Productos vigentes, para clientes personas jurídicas.

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

- a) Hayan desarrollado las APIs de acuerdo con el calendario de implementación antes indicado.
- b) Hayan proporcionado la información pertinente al Directorio de Participantes.
- c) Hayan realizado las respectivas pruebas funcionales.
- d) Tengan la información efectiva de los clientes (no solo información de pruebas) ya disponible en el Sistema.
- e) Cuenten con el certificado de implementación de perfiles de seguridad de interfaces.
- f) Cuenten con los certificados digitales que acreditan la identidad provistos por un CA válido.

En el caso de entidades indicadas en la letra (b) del artículo 18 de la Ley Fintec, que emitan directamente tarjetas de pago o abran cuentas vistas, aplicarán para iniciación de pagos los plazos del Grupo 1.

E. Requerimientos de información

El detalle y el formato de la información requerida en esta normativa que debe ser enviada a la Comisión para efectos de supervisión será especificado en una o más normas que se dictarán en forma posterior a la publicación de esta NCG.

F. Entrada en vigencia

Las disposiciones incorporadas en esta Norma entrarán en vigencia 36 meses contados desde su primera dictación.

Se reemplaza la Sección VI en su Anexo 1 por lo siguiente:

SECCIÓN VI. ANEXOS NORMATIVOS

Anexo N°1: Variables para conjuntos de información del SFA

Las especificaciones de las variables aplicables en el SFA son aquellas disponibles en el Portal de Desarrolladores que tiene habilitado esta Comisión.

Se incorpora el siguiente contenido en el Anexo N°3:

ANEXO N°3: ANEXO TÉCNICO

I. INFRAESTRUCTURA Y FUNCIONAMIENTO: DIRECTORIO

A. ASPECTOS GENERALES DE FUNCIONAMIENTO DEL DIRECTORIO

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

Principios del directorio:

1. Este es bajamente acoplado (Directorio estará desacoplado de las transacciones), y sigue los principios *once-only* y de fuentes auténticas. Además, no debe afectar el flujo transaccional de intercambio de información entre los participantes.
2. El Directorio contará con servicios de verificación del estado de los participantes, pero que solo deberán ser utilizados en el proceso de DCR, y en ningún caso en el flujo transaccional de intercambio de información entre los participantes.
3. La API expone un segundo servicio liviano para obtener el *timestamp* de la última actualización del Directorio, que servirá al participante del SFA para saber si posee una copia actualizada. Este servicio debe ser consultado por los participantes al menos una vez cada 8 horas.
4. Cada participante debe implementar una interfaz, de manera que pueda recibir notificaciones cada vez que el Directorio se actualice. Para lo anterior, cada entidad deberá ingresar la dirección de su *webhook* para recibir esta notificación. Las especificaciones del *webhook* son las indicadas en el Portal de Desarrolladores.
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 o de iniciación de pagos.

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 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.

Se entenderá por marca, para efectos del Sistema de Finanzas Abiertas, la denominación comercial mediante la cual una entidad inscrita en el Directorio de Participantes ofrece o identifica ante el público los servicios asociados a uno o más roles dentro del Sistema, sin que ello implique la existencia de una persona jurídica distinta ni la alteración de la responsabilidad regulatoria de la entidad legal inscrita. La marca constituye un elemento de identificación comercial y de diferenciación operativa frente a usuarios y participantes, pero no configura por sí misma un sujeto regulado autónomo ni una categoría jurídica independiente de la entidad legal que actúa como participante del Sistema. Para todos los efectos, un Participante del Sistema y sus marcas tendrán estados de participación únicos en el Sistema, sin existir diferenciación en su calidad de activo o no en el Sistema.

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 deberá presentarse conjuntamente con la solicitud de inscripción y registro inicial, tratándose de marcas vigentes. No obstante, podrá generarse dicha solicitud en etapas posteriores para nuevas marcas. En todo caso el participante solo podrá activar una marca en el Directorio una vez que dicha solicitud 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
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 <i>endpoints</i> de producción del participante	Participante
URL de la API que contiene los <i>endpoints</i> 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"
  }
}
```

Los tipos de actualizaciones soportadas por el sistema son los siguientes:

- cl.sfa.participant.change.role
- cl.sfa.participant.change.cert
- cl.sfa.participant.left

- cl.sfa.participant.cs.inactive
- cl.sfa.participant.change.url

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 detalla en el Portal de Desarrolladores.

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* también se encuentra detallado en el Portal de Desarrolladores.

G. API DEL DIRECTORIO

Las APIs que tendrá el Directorio son aquellas que la CMF tenga habilitadas en su Portal de Desarrolladores 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.

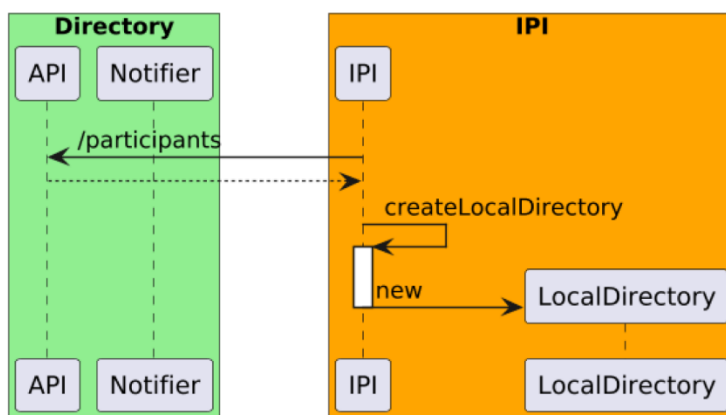
- Es responsabilidad del Directorio, administrado por la Comisión, enviar una notificación a los participantes del SFA informando los cambios que hayan ocurrido.
- Para ello, es responsabilidad de cada participante mantener un *endpoint* */notifyupdate* y */notify-incident*, ambos de tipo POST operativo.

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

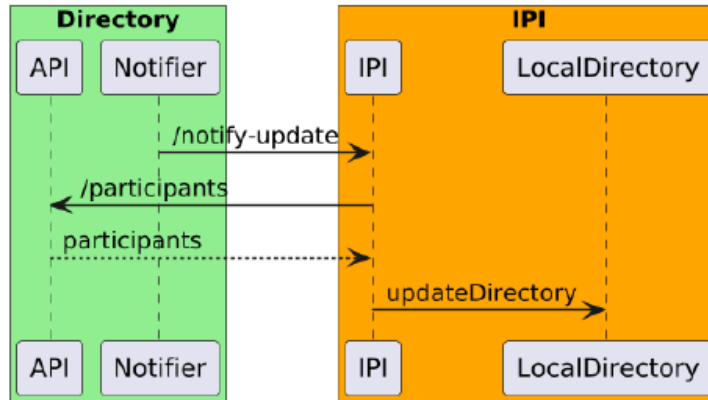


La Figura 1 muestra el proceso de creación del Directorio local. En este caso, una IPI/IPC/PSBI/PSIP está entrando por primera vez al sistema y consume el recurso de participantes desde el Directorio a través de un método GET sobre el *endpoint* */participants*. El Directorio responde a este REQUEST 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.

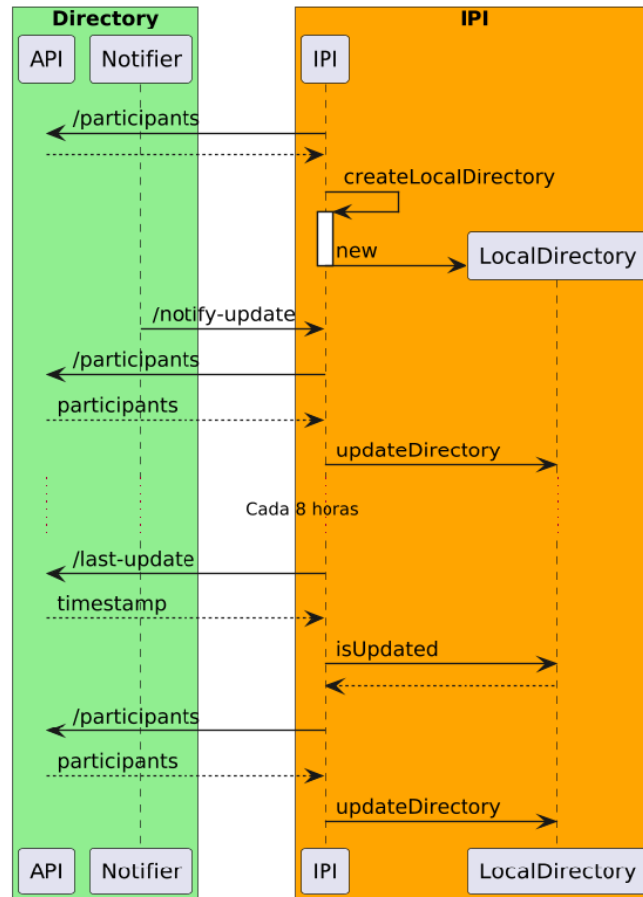
Figura 2: Actualización de la copia local del Directorio en un participante del SFA a través de una notificación del Directorio



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 a la página web del SFA donde deberá verificar si alguna entidad ha cambiado a un estado que inhabilite el intercambio de información.

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

Y de acuerdo con el *payload* indicado para estos efectos en el Portal de Desarrolladores.

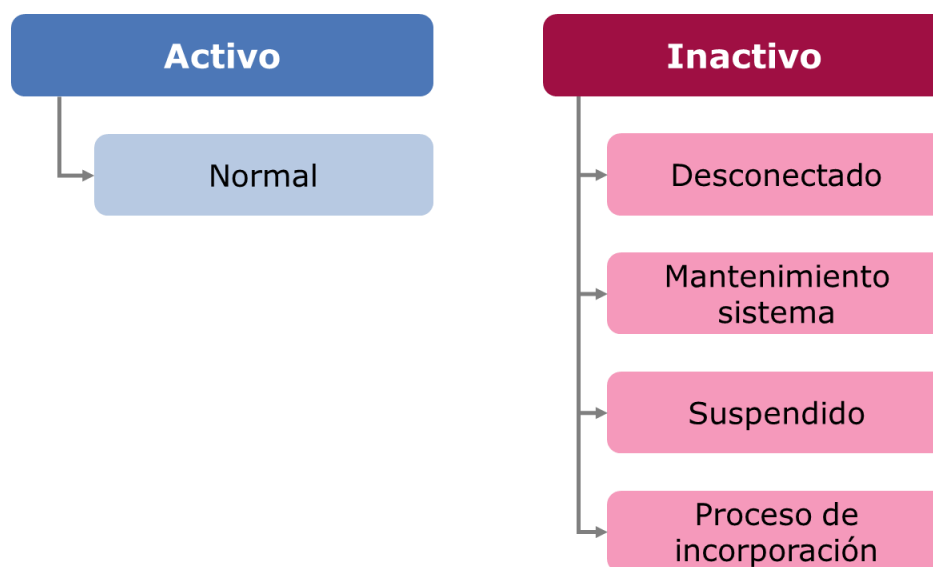
Cabe destacar que además hay canales de comunicación existentes en la CMF que se utilizan en el SFA:

- 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 5 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 5 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 en orden	CMF	No aplica	CMF de forma directa en el Directorio
Tipo: Inactivos				
Desconectado	Cuando la entidad se auto desconecta del Sistema por los motivos especificados en la normativa o cuando el Directorio desconecta a un participante por no tener certificados	Participante (IPI/IPC/PSBI/PSIP) o de forma automática para el caso de certificados de identidad vencidos.	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". En caso de vencimiento del certificado de identidad es el Directorio

	de identidad vigentes.			quien lo activa en caso de no haber sido activado por el propio participante.
Mantenimiento sistema	Cuando el mantenimiento programado afecta al mecanismo principal.	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 en el Directorio
Proceso de incorporación	Estado inicial de una entidad que entra al Directorio cuando es parte de un registro o nómina ⁴	CMF	CMF	CMF de forma directa en el Directorio

⁴ 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 CA⁵ o posterior o ETSI EN 319 411⁶) y cumplir con las características de funcionamiento en sus respectivas jurisdicciones.

Los participantes además deberán implementar RFC8659⁷ (*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.

⁵ Se debe contar con la versión 2.7 -SSL Baseline con seguridad de red o posterior.

⁶ 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)

⁷ <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 RFC7591⁸ (DCR) y RFC7592⁹ (DCRM), incluyendo el perfil de seguridad de *OpenID connect*.

El servidor de autenticación, como requisito de funcionamiento del DCR, expondrá sus metadatos según RFC8414¹⁰ (*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 de Desarrolladores.

E. CERTIFICACIÓN DE VIGENCIA Y AVISOS TEMPRANOS

Las entidades son responsables de verificar en todo momento que sus certificados estén vigentes¹¹ 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 esta deberá automáticamente autodesconectarse del Sistema hasta que tenga un certificado vigente en el Directorio.

⁸ <https://datatracker.ietf.org/doc/html/rfc7591>

⁹ <https://datatracker.ietf.org/doc/html/rfc7592>

¹⁰ <https://datatracker.ietf.org/doc/html/rfc8414>

¹¹ Esto implica que el certificado de identidad esté vigente en términos de los plazos de expiración y que no haya sido revocado por su respectiva CA.

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.

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

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 y diccionarios de datos asociados.
- 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 de Desarrolladores será el resultado de un proceso evolutivo e iterativo, y los ajustes, actualizaciones y/o aclaraciones a las especificaciones técnicas allí establecidas se comunicarán por oficio circular, en el que se indicará la fecha a partir de la cual dichas modificaciones serán exigibles.

El portal web de desarrolladores estará disponible en la siguiente URL:

<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 habilita un área de prueba para los procesos de certificación que deberán realizar los certificadores externos. 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 de Desarrolladores.

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.

Los datos sintéticos buscarán ser lo suficientemente representativos para detectar problemas de integración que podrían manifestarse solo con datos reales. En particular la información que proveerá la Comisión considerará:

- Diversidad de casos de uso;
- Volumen suficiente para detectar problemas de escala; y
- Escenarios de error que permitan verificar el comportamiento de las APIs ante condiciones adversas.

La información para estos efectos será provista por la Comisión, sin necesidad de entrega especial de información por parte de los Participantes para la construcción de esta base de datos. No es necesario que las entidades coordinen ningún tipo de entrega de información para estos efectos, ya que será provista para las pruebas del Sandbox por la Comisión de manera centralizada.

B. 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.

En relación a las IPI:

ID Paso	Fase	Componente / API	Descripción de la Acción / Prueba	Precondición / Datos Requeridos	Resultado Esperado	Evidencia Requerida
I-01	Preparación	Registro CMF	Completar formulario de registro institucional en el Directorio/Portal (datos de entidad, contactos, rol).	Formulario disponible; credenciales/canal CMF.	Solicitud recibida y registrada para revisión.	Captura del formulario enviado / acuse de recibo.
I-02	Preparación	Validación CMF	Validación de tipo de entidad y rol (IPI/IPC) y habilitación para pruebas.	Entidad registrada.	Entidad aprobada y habilitada en Sandbox/Directorio.	Captura de aprobación / notificación.
I-03	Preparación	Directorio Local	Exponer información del Directorio consumiendo las APIs expuestas por el directorio de CMF.	Entidad registrada.	Respuesta satisfactoria al consumo de los endpoints.	Captura de registros realizados al consumir las APIs
I-04	Preparación	Certificados	Generación (autofirmada) y registro/carga de certificados mTLS del participante (servidor) y certificados de firma, según perfil de seguridad.	Entidad aprobada; CA y CSR; acceso a repositorio/carga.	Certificado registrado en Directorio y asociado al participante/rol; handshake mTLS exitoso.	Captura/registro de carga en Directorio + detalle del certificado (subject/serial/fechas) + logs/captura de handshake TLS.
			Pruebas con externos:			

I-05	Preparación	Autenticación	Publicar metadata OAuth/OIDC (/well-known) y habilitar endpoints /authorize y /token conforme al perfil de seguridad.	Certificados cargados; configuración AS lista.	Metadata accesible; endpoints responden correctamente.	Respuesta metadata + logs de configuración.
I-06	Ejecución	DCR (AS)	Soportar registro dinámico de clientes (DCR): recibir solicitud POST /register y validar requisitos (mTLS + declaración/SSA).	AS expone registration_endpoint; claves/certificados disponibles; acceso a Directorio.	Registro exitoso y entrega de client_id/metadata; o rechazo con error estandarizado.	Logs DCR + payload request/response.
I-07	Ejecución	Consentimiento	Ejecutar flujo de consentimiento: autenticación de cliente, captura de consentimiento y creación de grant asociado.	Cliente demo disponible; PSBI/PSIP inicia flujo.	Consentimiento otorgado; grant creado y trazable.	Capturas del flujo + registro grant.
I-08	Ejecución	APIs de datos/pagos	Responder consumo de APIs sintéticas (ej. /accounts, /transactions o pagos) respetando autorizaciones y límites.	Token válido; consent/grant vigente.	Respuestas 200 OK con datos demo; errores estandarizados cuando aplique.	Response JSON + logs de request.
I-09	Ejecución	Revocación	Procesar revocación del consentimiento/grant y bloquear accesos posteriores.	Consentimiento o activo.	Llamadas posteriores retornan 401/403 según corresponda.	Captura de revocación + error esperado.
I-10	Ejecución	Rate limit	Aplicar límites operacionales (rate limit/burst) y responder 429	Script de carga / colección Postman.	429 al exceder; operación normal al aplicar back-off.	Logs + capturas de 429.

			con back-off cuando se excedan.			
I-11	Ejecución	Logs/Trazabilidad	Registrar eventos mínimos del ciclo de vida del grant (creación/uso/revocación) para auditoría y análisis.	Flujos ejecutados (consent + consumo + revocación).	Logs disponibles con correlación por grant/cliente/participantes.	Extracto de logs / evidencias si aplica.

En relación a las IPC:

ID Paso	Fase	Componente / API	Descripción de la Acción / Prueba	Precondición / Datos Requeridos	Resultado Esperado	Evidencia Requerida
I-01	Preparación	Registro CMF	Completar formulario de registro institucional en el Directorio/Portal (datos de entidad, contactos, rol).	Formulario disponible; credenciales/canal CMF.	Solicitud recibida y registrada para revisión.	Captura del formulario enviado / acuse de recibo.
I-02	Preparación	Validación CMF	Validación de tipo de entidad y rol (IPI/IPC) y habilitación para pruebas.	Entidad registrada.	Entidad aprobada y habilitada en Sandbox/Directorío.	Captura de aprobación / notificación.
I-03	Preparación	Directorio Local	Exponer información del Directorio consumiendo las APIs expuestas por el directorio de CMF.	Entidad registrada.	Respuesta satisfactoria al consumo de los endpoints.	Captura de registros realizados al consumir las APIs
I-04	Preparación	Certificados	Generación (autofirmada) y registro/carga de certificados mTLS del participante (servidor) y certificados de	Entidad aprobada; CA y CSR; acceso a repositorio/carga.	Certificado registrado en Directorio y asociado al participante/rol; handshake mTLS exitoso.	Captura/registro de carga en Directorio + detalle del certificado (subject/serial/fechas) + logs/captura de

			firma, según perfil de seguridad.			handshake TLS.
--	--	--	-----------------------------------	--	--	----------------

Pruebas con externos:

I-05	Preparación	Autenticación	Publicar metadata OAuth/OIDC (/well-known) y habilitar endpoints /authorize y /token conforme al perfil de seguridad.	Certificados cargados; configuración AS lista.	Metadata accesible; endpoints responden correctamente.	Respuesta metadata + logs de configuración.
I-06	Ejecución	DCR (AS)	Soportar registro dinámico de clientes (DCR): recibir solicitud POST /register y validar requisitos (mTLS + declaración/SSA).	AS expone registration_endpoint; claves/certificados disponibles; acceso a Directorio.	Registro exitoso y entrega de client_id/metadata; o rechazo con error estandarizado.	Logs DCR + payload request/respuesta.
I-07	Ejecución	Consentimiento	Ejecutar flujo de consentimiento: autenticación de cliente, captura de consentimiento y creación de grant asociado.	Cliente demo disponible; PSBI/PSIP inicia flujo.	Consentimiento otorgado; grant creado y trazable.	Capturas del flujo + registro grant.
I-08	Ejecución	APIs de datos/pagos	Responder consumo de APIs sintéticas (ej. /accounts, /transactions o pagos) respetando autorizaciones y límites.	Token válido; consent/grant vigente.	Respuestas 200 OK con datos demo; errores estandarizados cuando aplique.	Response JSON + logs de request.

I-09	Ejecución	Revocación	Procesar revocación del consentimiento/grant y bloquear accesos posteriores.	Consentimiento activo.	Llamadas posteriores retornan 401/403 según corresponda.	Captura de revocación + error esperado.
I-10	Ejecución	Rate limit	Aplicar límites operacionales (rate limit/burst) y responder 429 con back-off cuando se excedan.	Script de carga / colección Postman.	429 al exceder; operación normal al aplicar back-off.	Logs + capturas de 429.
I-11	Ejecución	Logs/Trazabilidad	Registrar eventos mínimos del ciclo de vida del grant (creación/uso/revocación) para auditoría y análisis.	Flujos ejecutados (consent + consumo + revocación).	Logs disponibles con correlación por grant/cliente/participantes.	Extracto de logs / evidencias WORM si aplica.

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

C. 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 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.

D. 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.I 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 este ambiente 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 del plan de pruebas a realizarse se presenta en la siguiente Tabla 4:

Tabla 4: Prueba de Integración

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 enlace 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 en 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 / algo 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 authorization_details.actions para el recurso. sin para	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	Alta de plan recurrente con	201/200 OK. recurringPaymentId, status.

			- creación parámetros (mock) válidos.		
Iniciación de pagos recurrentes de montos variables	15	Pagos	Plan recurrente variable - creación (mock)	Alta límites/reglas. Rechazo si inválido. con si	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 recursos/pagos fallen después.	Revocación 200/204; reintento 401/403.
Controles transversales (firma)	19	Firma aplica)	Firma (si 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.

E. 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.

F. 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), (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) y (n) indicadas en el punto "1.2 Antecedentes adjuntos".

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

G. ELEMENTOS TECNICOS QUE 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.

H. REQUISITOS DE LA ENTIDAD CERTIFICADORA DE LAS PRUEBAS FUNCIONALES

Las entidades certificadoras que podrán acreditar el requerimiento letras b y c de la sección I.E.1 en lo que respecta a las IPI/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 dar cuenta de 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.
- Competencia técnica y metodológica para la evaluación de la seguridad en interfaces de programación de aplicaciones (APIs). Experiencia en la aplicación de estándares técnicos reconocidos para la seguridad y el intercambio seguro de información mediante APIs, tales como OWASP API Security Top 10, OWASP ASVS y los perfiles financieros de OAuth 2.0 y OpenID Connect, incluidos los Financial-grade APIs (FAPI).

- La experiencia y competencia deben acreditarse con certificaciones internacionales reconocidas en el ámbito de la seguridad de la información y ciberseguridad (como certificación ISO 27001, estándar SOC2 u otros estándares asociados).

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

I. VALIDEZ DE LOS CERTIFICADOS FUNCIONALES

Los certificados de funcionamiento serán válidos hasta que:

1. Se incorporen nuevos datos o productos al Portal de Desarrolladores.
2. La entidad (IPI/IPC/PSBI/PSIP) realice una actualización tecnológica que pueda afectar la interoperabilidad del Sistema.
3. Haya un cambio en el listado de APIs que consumen en su modelo de negocio, en el caso de PSBI/PSIP.
4. Haya un cambio en los productos que ofrecen, en el caso de las IPI/IPC.
5. 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.

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.

Determinación del riesgo

Para efectos del numeral 5 precedente, la determinación de que una vulnerabilidad constituye un riesgo crítico y material, deberá fundarse en criterios técnicos objetivos y verificables, pudiendo considerarse estándares internacionales reconocidos de clasificación de severidad de vulnerabilidades, tales como el Common Vulnerability Scoring System (CVSS) u otros equivalentes. La entidad deberá documentar la evaluación efectuada.

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 de Desarrolladores del SFA, que para todos los efectos administra la Comisión. Estas especificaciones en caso de tener actualizaciones serán informadas por la Comisión según las formas y plazos indicados en el Portal de Desarrolladores.

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.

La API de confirmación de fondos es voluntaria en su uso para los PSIP, pero obligatoria respecto de su disponibilidad para los IPC.

B. CÓDIGOS DE ERROR

Se deben implementar los códigos de respuesta indicados en el Portal de Desarrolladores relativos a cada tipo de API.

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, 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.

D. TPM y TPS

En el caso de las IPI, se considerarán como *default* 10 Transacciones por Segundo (TPS) de una IPI a todos los PSBI y 60 Transacciones por Minuto (TPM) de una IPI a cada PSBI. 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 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 los requerimientos que recibe un 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 (entre 0 y 5) de segundos, para evitar que, en episodios de sobrecarga, muchos PSBI/PSIP reintenten en el mismo instante.

TPM:

- Se calcula para cada par *endpoint*/PSBI 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 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 (entre 0 y 15) de segundos para evitar que en episodio de sobrecarga muchos PSBI 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. 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 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 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 5: Matriz DAMA

Dimensión	Descripción	Métrica
Exactitud (<i>accuracy</i>)	Qué tan precisos son los datos en relación con otras instancias	% registros con errores y % de error de los datos
Compleitud (<i>completeness</i>)	Qué tan completos son los registros en relación con otras instancias	% registros completos
Integridad (<i>integrity</i>)	Qué tan correctas son las relaciones entre distintos datos y en el tiempo	% registros íntegros
Actualización (<i>timelines</i>)	Qué tan actualizados están las APIs relativas a otras fuentes	% registros actualizados
Validez (<i>validity</i>)	Cumplimiento de los formatos acordados	% registros con formatos correctos

Duplicación (<i>uniqueness</i>)	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.

Dentro del informe, la entidad deberá indicar cómo cumplirá con el requisito de disponibilizar la nueva información de la que dispongan los clientes en sus canales habituales y en las interfaces del SFA, con un atraso máximo de 5 minutos.

F. PERIODO DE EXIGIBILIDAD ATENUADA POST PERIODO PILOTO OBLIGATORIO

Las IPI/IPC verán reducida la exigibilidad de sus APIs por un periodo de 6 meses a contar del término del periodo piloto obligatorio. Los elementos que se verán atenuados en términos de exigibilidad son para el caso de las IPI:

- 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.

Por su lado, para el caso de las IPC los elementos atenuados serán:

- 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 1.000 milisegundos.

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

G. MANTENCIONES PROGRAMADAS

Las mantenciones programadas deben ser avisadas con anticipación 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 6: Tipos de mantenciones programadas y características

Tipo de Mantención	Tiempo de aviso a ejecución	Plazo máximo de extensión en la frecuencia	Frecuencia máxima permitida
Correctiva	48 horas	4 horas	Mensual
Preventiva	7 días	8 horas	Mensual
Evolutiva/ Actualización ¹²	14 días	12 horas	Mensual
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.

H. MECANISMOS DE MONITOREO

La siguiente tabla muestra las métricas, plazos e información que deberán enviar las IPI/IPC en un auto-reporte de entrega mensual:

¹² 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.

Tabla 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. 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
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 que implican consentimiento del cliente	Separado por PSBI/PSIP.	% de llamados de consentimiento con errores, separado por tipo de error	Semanal

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

I. IDEMPOTENCIA

Aplicará lo dispuesto para estos efectos en el Portal de Desarrolladores.

J. EJECUCIÓN DE LA INICIACIÓN DE PAGOS

La iniciación de pagos contempla el uso de la Transferencia Electrónica de Fondos para pagos únicos (instantáneos o no) y recurrentes (de montos variables o fijos), tanto por clientes personas naturales como por jurídicas.

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 2.0¹³ que se complementa con el Modelo de atacante¹⁴ (especificación final [19/02/2025]), ambos establecido por la Open ID Foundation (OIDF), basado en el marco de autorización OAuth 2.0 [RFC 6749]¹⁵. Respecto a los mensajes con objetivo de no repudio, se deberá implementar el protocolo de Firma de mensajes¹⁶ FAPI 2.0. El perfil de seguridad se complementa y detalla con lo indicado en el Portal de Desarrolladores.

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]¹⁷.
 - ii. Se implementará como control de seguridad en la capa de transporte el método de autenticación mutua TLS (mTLS) [RFC8705]¹⁸.
 - 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 autenticación 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. Informe de conformidad de seguridad de OIDF.
- VII. El token de acceso será en formato JWT (no opaco) para enviar o acceder a la información del campo *authorization details*.

¹³ https://openid.net/specs/fapi-security-profile-2_0-final.html

¹⁴ https://openid.net/specs/fapi-attacker-model-2_0-final.html

¹⁵ <https://www.rfc-editor.org/info/rfc6749>

¹⁶ https://openid.net/specs/fapi-2_0-message-signing-ID1.html

¹⁷ 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.

¹⁸ En *Security profile* de FAPI 2.0 se MTLs o DPoP para el uso de token de acceso restringido, esta implementación se decanta por el uso de MTLs, por sobre DPoP. Además, también define como valido el uso de MTLs o *private_key_jwt* para la autenticación de clientes, en este caso también se elige MTLs como método, ambas elecciones podrían ser revisadas en una etapa de implementación posterior considerando el avance de la implementación.

VII. CONSENTIMIENTO 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 de Desarrolladores.

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 denominado en inglés con el término "purpose", el cual consistirá en un campo libre de un largo máximo de 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 de Desarrolladores.

D. PANEL DE CONTROL DE CONSENTIMIENTOS

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

- **Pendiente:** Este estado indica que la solicitud de consentimiento se encuentra a la espera de autorización en el ambiente de la IPI/IPC, particularmente en los casos de actuación conjunta.
- **Rechazado:** Este estado indica que la solicitud de consentimiento ha sido rechazada por el usuario final o por uno o más de los firmantes en los casos de actuación conjunta, en el ambiente de la IPI/IPC.
- **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.
- **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.

Dado que el Panel de Control de Consentimientos se enfocará en el derecho de revocación que tiene el usuario final, la forma de comunicarse esta revocación entre las entidades y su reflejo en su Panel de Control de Consentimiento es la siguiente:

- **Si la revocación se realiza en la IPI/IPC:** La IPI/IPC deberá notificar mediante webhook en un plazo máximo de 5 minutos luego de la orden de

revocación del usuario final al PSBI/PSIP y actualizar su Panel de Control de Consentimientos instantáneamente. El PSBI/PSIP, en cuanto reciba la notificación por parte de la IPI/IPC, debe interrumpir el acceso a la información del usuario final o la iniciación de pago, borrar los datos del usuario final o titular de los datos/cuentas, y actualizar al instante su Panel de Control de Consentimientos.

- **Si la revocación se realiza en el PSBI/PSIP:** El PSBI/PSIP debe revocar el consentimiento en el Servidor de Autorización de la IPI/IPC, debiendo la IPI/IPC visualizar este cambio de forma instantánea en su Panel de Control de Consentimientos. El PSBI/PSIP debe interrumpir el acceso a la información del usuario final o la iniciación de pago, borrar los datos del usuario final o titular de los datos/cuentas, y actualizar al instante su Panel de Control de Consentimiento con su nuevo estado.

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 N°65 del manual de sistema de información y la región considerando la Tabla N°2 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.

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 contraparte¹⁹? (timestamp)

- Sí.
- No.

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

26. ¿Ejecutó la medida de desconexión²⁰? (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.

¹⁹ 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.

²⁰ 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.

28. Tiempo de resolución del incidente:

Este campo se incluirá cuando se cierra el incidente. Se debe completar el tiempo que demora 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.

REPORTE DE INCIDENTES MENSUAL

Las entidades, además de comunicar los incidentes del SFA a través de la plataforma Reporte de Incidentes Operacionales (RIO), 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 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 9: Reporte de Calidad de la Información:

Dimensión	Descripción	Métrica	Valor (Porcentaje)
Exactitud (<i>accuracy</i>)	Qué tan precisos son los datos en relación con otras instancias	Registros con errores	
		Error de los datos	
Compleitud (<i>completeness</i>)	Qué tan completos son los registros en relación con otras instancias	Registros completos	
Integridad (<i>integrity</i>)	Qué tan correctas son las relaciones entre distintos datos y en el tiempo	Registros íntegros	
Actualización (<i>timelines</i>)	Qué tan actualizados están las APIs relativas a otras fuentes	Registros actualizados	
Validez (<i>validity</i>)	Cumplimiento de los formatos acordados	Registros con formatos correctos	
Duplicación (<i>uniqueness</i>)	Ausencia de registros duplicados	Registros no duplicados	

D. REPORTE DE DISPONIBILIDAD Y RENDIMIENTO

Tabla 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 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 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 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.

F. REPORTE DE NÚMERO DE CLIENTES IPI

Las IPI deberán reportar mensualmente la siguiente información relativa al número de clientes vigentes que mantengan productos cuya información pueda ser compartida mediante el SFA. En el primer envío deberá incluirse además la información correspondiente a los últimos 12 meses.

Tabla 13: Información de número de clientes únicos con al menos un producto vigente que sea parte del set de instrumentos considerados a compartir en el Sistema de Finanzas Abiertas

Variable	Formato
Número de clientes personas naturales únicos que tienen al menos un producto vigente en la institución que esté incluido en el Anexo N°2: "Productos del SFA" de la Norma de Carácter General 514 que regula el Sistema de Finanzas Abiertas	Número
Número de clientes personas jurídicas únicos que tienen al menos un producto vigente en la institución que esté incluido en el Anexo N°2: "Productos del SFA" de la Norma de Carácter General 514 que regula el Sistema de Finanzas Abiertas	Número

Nota: La información tanto para clientes personas naturales y jurídicas es agregada para cada fila. Es decir, en cada fila solo debe reportarse el total de clientes únicos en cada categoría, sin necesidad de diferenciar por tipo de producto que esté presente en el Anexo 2 referenciado.

En el caso que su institución tenga alguna entidad relacionada dentro del grupo que también tendrá la condición de IPI, la información de número de clientes debe

ser reportada de forma independiente para cada institución que tendrá la calidad de IPI, no debiendo agregarse los clientes dentro del grupo.

CATHERINE TORNEL LEÓN
PRESIDENTA
COMISIÓN PARA EL MERCADO FINANCIERO