SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Lima, 16 de Octubre de 2026

RESOLUCIÓN SBS
N° 02519-2026

El Superintendente de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones se encarga de regular, supervisar y fiscalizar las entidades del sistema financiero, sistema de seguros y privado de pensiones, así como a otras entidades cuya supervisión haya sido encargada por otras leyes especiales, conforme a lo dispuesto en la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley Nº 26702, la Ley del Sistema Privado de Administración de Fondos de Pensiones, cuyo Texto Único Ordenando fue aprobado por el Decreto Supremo Nº 054-97-EF y otras leyes;

Que, mediante la Trigésima Segunda Disposición Final y Complementaria de la Ley Nº 26702, se establecen disposiciones aplicables a la publicación de proyectos normativos;

Que dicha disposición es concordante con el artículo IV del Título Preliminar de la Ley Nº 27444, Ley del Procedimiento Administrativo General, que establece el principio de participación de los administrados en el proceso de decisiones públicas, así como con el capítulo IV del Reglamento que establece disposiciones sobre publicación y difusión de normas jurídicas de carácter general, resoluciones y proyectos normativos, aprobado por Decreto Supremo N° 009-2024-JUS;

Que, considerando el desarrollo de los modelos de finanzas abiertas y los beneficios asociados a su implementación en términos de innovación, competencia e inclusión financiera, la Superintendencia considera necesario emitir disposiciones generales que regulen la implementación y funcionamiento del Sistema de Finanzas Abiertas, incluyendo los temas relacionados a la infraestructura digital común, el marco de confianza para la interacción entre participantes y los estándares técnicos, de seguridad y calidad de datos necesarios para garantizar la interoperabilidad y el adecuado funcionamiento del Sistema;

Que, en cumplimiento de lo antes referido, la Superintendencia dispone aprobar mediante resolución de Superintendencia sus proyectos normativos y publicarlos en su Sede Digital con el objetivo de asegurar la participación efectiva del público en general, y;

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

Contando con el visto bueno de la Superintendencia Adjunta de Regulación y Jurídica y el Departamento de Finanzas Abiertas;

RESUELVE:

Artículo Primero. - Autorizar la difusión en consulta pública del proyecto normativo que aprueba el Reglamento General del Sistema de Finanzas Abiertas, referente al Título V "Infraestructura Digital", Título VI "Marco de Confianza" y Título VII "Estándares, Seguridad y Calidad", en la Sede Digital de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (www.sbs.gob.pe).

Artículo Segundo. - El plazo para que el público en general pueda remitir a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones sus comentarios y observaciones sobre el proyecto señalado en el artículo anterior es de dieciocho (18) días calendario, contados desde el día siguiente de la fecha de publicación de la presente resolución en el Diario Oficial El Peruano.

Regístrese, comuníquese y publíquese

SERGIO JAVIER ESPINOSA CHIROQUE
SUPERINTENDENTE DE BANCA, SEGUROS Y AFP

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

PROYECTO NORMATIVO

Lima,

Resolución S.B.S. N° - 2026

El Superintendente de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que, de conformidad con lo dispuesto en el artículo 87 de la Constitución Política del Perú, así como en los artículos 347 y 349 de la Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros (en adelante, Ley General), corresponde a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (en adelante, la Superintendencia) regular y supervisar a las empresas del sistema financiero, del sistema de seguros y demás empresas sujetas a su supervisión y control por ley, cautelando la solidez, estabilidad y correcto funcionamiento de dichos sistemas, así como la protección de los intereses del público;

Que la Tercera Disposición Complementaria Final de la Ley N° 29985, Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera, establece que la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y el Banco Central de Reserva del Perú, en el ámbito de sus respectivas competencias, establecen a las entidades sujetas a su supervisión las condiciones y oportunidades para la interoperabilidad;

Que la transformación digital de los servicios financieros y el uso creciente de tecnologías y datos han impulsado el desarrollo de modelos como las finanzas abiertas, que permiten el acceso y suministro estandarizado y seguro de datos entre participantes habilitados, previo consentimiento del usuario, con el propósito de promover la innovación, la competencia y la inclusión financiera, bajo condiciones comunes de interoperabilidad, seguridad y funcionamiento;

Que, en el marco de las atribuciones conferidas por la Ley General, y de lo dispuesto en la citada Ley N° 29985, corresponde a esta Superintendencia establecer las disposiciones necesarias para la implementación del Sistema de Finanzas Abiertas (en adelante, SFA) respecto de las empresas bajo su ámbito de regulación y supervisión, incluyendo las condiciones de participación, interoperabilidad e implementación gradual necesarias para su adecuado funcionamiento;

Que, en febrero de 2026, la Superintendencia publicó la Hoja de Ruta de Finanzas Abiertas SBS, mediante la cual estableció un enfoque gradual para la implementación del Sistema de Finanzas Abiertas en el Perú, organizado en fases progresivas que comprenden el diagnóstico del mercado, el desarrollo del marco regulatorio y de las especificaciones

técnicas, la implementación gradual del sistema y la posterior consolidación del modelo de finanzas abiertas;

Que, como parte de la fase de diagnóstico, la Superintendencia desarrolló cuestionarios, reuniones bilaterales, mesas de trabajo y coordinaciones con empresas supervisadas, empresas de tecnología financiera, proveedores tecnológicos, autoridades públicas y otros actores relevantes, cuyos resultados permitieron identificar capacidades, riesgos, oportunidades y casos de uso, así como sustentar una implementación gradual del Sistema de Finanzas Abiertas bajo condiciones adecuadas de gobernanza, seguridad e interoperabilidad, sirviendo de insumo para el desarrollo de su marco regulatorio y técnico correspondiente;

Que, mediante Resolución SBS N° 01747-2026, se aprobó el Reglamento para la prestación de servicios bajo el modelo de *Banking as a Service* - BaaS, como parte del desarrollo progresivo del marco regulatorio asociado a la transformación digital y a los nuevos modelos de prestación de servicios financieros;

Que, posteriormente, la Superintendencia publicó para consulta pública los "Lineamientos para el Funcionamiento del Sistema de Finanzas Abiertas en el Perú", con el objeto de presentar los principales componentes del modelo propuesto y recoger comentarios y aportes de la industria y demás partes interesadas, los cuales han sido evaluados como parte del proceso de desarrollo del marco regulatorio;

Que, en atención al carácter progresivo de la implementación del Sistema de Finanzas Abiertas, resulta necesario establecer, de manera integrada, las disposiciones generales aplicables al Sistema, su forma de gobierno, el alcance de los datos y servicios comprendidos, las condiciones de participación, las reglas aplicables al acceso y control del usuario, así como las disposiciones relativas a la infraestructura digital común, el Marco de Confianza y los estándares técnicos, de seguridad y calidad de datos necesarios para su funcionamiento;

Que, con la finalidad de otorgar predictibilidad a los participantes respecto de los requerimientos técnicos y operativos aplicables al Sistema de Finanzas Abiertas, resulta necesario establecer disposiciones sobre la infraestructura digital común, el Directorio de Participantes, el Portal del Desarrollador, el ambiente de pruebas del SFA, la conformidad funcional, el Perfil de Seguridad, los niveles de servicio y la calidad de datos, así como prever su desarrollo mediante los anexos y las especificaciones técnicas correspondientes;

En uso de las atribuciones conferidas por los numerales 3, 7, 9, 13 y 19 del artículo 349 de la Ley General y por el artículo 57 del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones, aprobado por Decreto Supremo N° 054-97-EF;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento General del Sistema de Finanzas Abiertas, de acuerdo con el siguiente texto:

PROYECTO NORMATIVO

"REGLAMENTO GENERAL DEL SISTEMA DE FINANZAS ABIERTAS

ÍNDICE

[…]

PROYECTO NORMATIVO

REGLAMENTO GENERAL DEL SISTEMA DE FINANZAS ABIERTAS

Las disposiciones correspondientes a los Títulos I al IV fueron autorizadas para difusión pública el 5 de octubre de 2026 mediante la Resolución SBS N° 02433-2026, emitida el 2 de octubre de 2026, sin perjuicio de las modificaciones incorporadas a los referidos títulos contenidos en la presente Resolución.

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Alcance

[...]

Artículo 2. Definiciones

[...]

q) **Reglamento de Seguridad de la Información y Ciberseguridad**: Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N° 504-2021 y sus modificatorias.

r) **Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos:** Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado por Resolución SBS N° 272-2017 y sus modificatorias.

s) **Reglamento para la Gestión del Riesgo Operacional:** Reglamento para la Gestión del Riesgo Operacional, aprobado por Resolución SBS N° 2116-2009 y sus modificatorias

t) **Principio de mínimos privilegios**: principio conforme al cual cada usuario, aplicación, sistema o proceso debe contar únicamente con los permisos de acceso estrictamente necesarios para cumplir las funciones o tareas que le correspondan.

u) **Calidad de datos**: en el marco del SFA, es el grado en que los datos suministrados, recibidos, transformados o conservados cumplen las dimensiones establecidas en el presente Reglamento, de modo que resulten aptos para su intercambio y utilización conforme a las finalidades previstas en el Sistema.

v) **Fuente autoritativa**: sistema, registro o repositorio que el participante identifica como fuente oficial o prevalente de un dato para efectos de su suministro mediante el SFA Los datos suministrados mediante el SFA deben corresponder a la información que el participante proporciona a través de sus canales digitales propios comparables.

w) **Gobierno de datos**: en el marco del SFA, es el conjunto de principios, políticas, procedimientos, responsabilidades, estructuras de decisión y controles mediante los cuales se administran los datos suministrados, recibidos, transformados o conservados, con el fin de asegurar su integridad, disponibilidad, trazabilidad, seguridad y uso adecuado durante todo su ciclo de vida.

x) ***Endpoint***: ubicación digital específica provista por una Interfaz de Programación de Aplicaciones (API) hacia la cual se dirigen las peticiones electrónicas de un sistema cliente para acceder a un dato, recurso o servicio determinado alojado en un servidor.

[...]

TÍTULO II

ALCANCE, DATOS Y SERVICIOS

[...]

TÍTULO III

PARTICIPANTES, ROLES Y HABILITACIÓN

[...]

Artículo 11. Responsabilidades de las Entidades Proveedoras de Datos

[...]

k) Asegurar que los datos suministrados mediante las APIs del SFA correspondan a la información contenida en la fuente autoritativa, y que su alcance, actualización, oportunidad y disponibilidad no sean inferiores a los de la información proporcionada al usuario mediante sus canales digitales propios comparables.

[...]

Artículo 13. Responsabilidades de las Entidades Receptoras de Datos

[...]

k) Asegurar la calidad de las transformaciones, agregaciones, inferencias, enriquecimientos y demás tratamientos realizados sobre los datos recibidos, diferenciando sus resultados de los datos suministrados originalmente por la EPD y absteniéndose de presentarlos como originados o validados por esta.

TÍTULO IV
ACCESO Y CONTROL DEL USUARIO

[...]

TÍTULO V

INFRAESTRUCTURA DIGITAL COMÚN DEL SFA

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 41. Infraestructura digital común del SFA

41.1 La infraestructura digital común del SFA está constituida por el conjunto de los componentes y servicios destinados a identificar y coordinar a los participantes, gestionar la información técnica, ejecutar las pruebas y evaluaciones de conformidad, proveer soporte y comunicaciones operativas, así como recopilar la información técnica necesaria para el funcionamiento del Sistema.

41.2 La infraestructura digital común del SFA comprende los siguientes componentes y servicios:

a) Directorio de Participantes;
b) Portal del SFA;
c) Portal del Desarrollador;
d) Ambiente de pruebas del SFA;
e) Motor de conformidad funcional;
f) Mecanismos y herramientas de soporte técnico operativo;
g) Mecanismos comunes de comunicaciones operativas;
h) Herramientas de monitoreo y recopilación de métricas; y
i) Los demás componentes o servicios que la Superintendencia incorpore mediante sus disposiciones normativas para el adecuado funcionamiento y evolución del SFA.

41.3 Los componentes y servicios señalados en el párrafo 41.2 pueden implementarse mediante plataformas, servicios o módulos independientes o integrados, según determine la Superintendencia. Su clasificación en el presente Reglamento no prescribe una arquitectura tecnológica específica.

41.4 El acceso y suministro de los datos del usuario se realiza de forma directa entre las EPD y las ERD. La infraestructura digital común no intermedia ni constituye un punto obligatorio de tránsito para el intercambio de datos. Tampoco implica la centralización del contenido de las solicitudes, respuestas o datos intercambiados entre los participantes.

41.5 Los componentes y servicios únicamente pueden procesar o almacenar los datos técnicos, operativos, registrales o de otra naturaleza que resulten necesarios para el cumplimiento de sus respectivas funciones, de conformidad con el presente Reglamento y la normativa aplicable. No obstante, el tratamiento de datos técnicos o métricas operativas no autoriza el acceso al contenido de los datos del usuario intercambiados entre participantes.

Artículo 42. Gestión de la infraestructura digital común

42.1 La Superintendencia establece el diseño funcional, las condiciones de implementación y las reglas de funcionamiento de los componentes y servicios de la infraestructura digital común del SFA, de conformidad con lo dispuesto en el artículo 5 del presente Reglamento.

42.2 La implementación, operación, mantenimiento, evolución y soporte de los componentes y servicios de la infraestructura digital común del SFA puede realizarse directamente por la Superintendencia o mediante terceros especializados, conforme a las condiciones que se establezcan.

42.3 La intervención de terceros especializados no transfiere ni limita las competencias regulatorias, supervisoras, preventivas, correctivas o sancionadoras de la Superintendencia, ni las funciones que le corresponden respecto de la conducción del SFA.

42.4 Los terceros especializados que intervengan en la implementación, operación, mantenimiento o soporte de los componentes o servicios comunes deben cumplir las condiciones de seguridad, confidencialidad, protección de datos, continuidad, disponibilidad, resiliencia, trazabilidad, auditabilidad, gestión de incidentes y demás requisitos que establezca la Superintendencia.

42.5 Los terceros especializados deben identificar, comunicar, gestionar y mitigar los conflictos de intereses que puedan comprometer la confidencialidad de la información, la neutralidad de los servicios prestados o el adecuado funcionamiento del SFA. Cuando dichos conflictos no puedan ser gestionados o mitigados adecuadamente, deben abstenerse de realizar las actividades afectadas. La Superintendencia puede establecer las medidas y condiciones aplicables para la identificación, gestión y mitigación de dichas situaciones.

42.6 La intervención de los terceros a que se refiere los párrafos 42.2, 42.3 y 42.4 no les confiere, por ese solo hecho, la condición de participantes del SFA ni los habilita para acceder a los datos del usuario ni tratarlos para fines propios, salvo en la medida estrictamente necesaria para cumplir funciones que la Superintendencia le haya encomendado.

42.7 La utilización de terceros especializados para la operación o soporte de los componentes y servicios comunes no exime a los participantes del cumplimiento de las obligaciones que les corresponden conforme al presente Reglamento, sin perjuicio de la evaluación de las circunstancias particulares que pudieran afectar el cumplimiento de dichas obligaciones.

Artículo 43. Condiciones generales de funcionamiento

43.1 Los componentes y servicios de la infraestructura digital común se diseñan y operan de manera que permitan:

a) mantener niveles mínimos de disponibilidad, capacidad, desempeño, continuidad y recuperación;
b) permitir la interoperabilidad entre los participantes y el uso de componentes y servicios comunes;
c) segregar los ambientes de desarrollo, pruebas y producción, así como los ambientes operativos destinados a las pruebas de los participantes;
d) mantener registros suficientes de los accesos, actuaciones, eventos y modificaciones relevantes realizados en la infraestructura digital común;

e) gestionar de manera controlada las actualizaciones, configuraciones y cambios de versión;
f) contar con capacidades adecuadas y escalables para atender la incorporación de participantes, el incremento de operaciones y la evolución del SFA; y
g) aplicar controles de acceso diferenciados según el carácter público, reservado o restringido de la información.

43.2 El mantenimiento programado de los componentes y servicios de la infraestructura digital común debe encontrarse técnicamente justificado, reducir al mínimo su impacto sobre el SFA, ejecutarse, fuera de los periodos de mayor utilización razonablemente identificados por la Superintendencia sobre la base de métricas operativas disponibles y contar con procedimientos de ejecución, reversión y recuperación.

43.3 Los mantenimientos programados se comunican a los participantes mediante los mecanismos operativos del SFA con una anticipación no menor de cinco (5) días hábiles. La comunicación identifica, como mínimo, el componente o servicio y las funcionalidades afectados, la finalidad del mantenimiento, la fecha y hora previstas de inicio y finalización, su duración e impacto estimados, las medidas de contingencia y los canales de actualización aplicables, así como informar oportunamente su conclusión o ampliación.

43.4 Los mantenimientos urgentes pueden comunicarse con una anticipación menor cuando resulten necesarios para corregir vulnerabilidades, prevenir incidentes, responder a amenazas activas o restablecer condiciones seguras de operación.

43.5 Las ventanas de mantenimiento no deben programarse de manera que impidan la prestación regular y sostenida de los componentes y servicios de la infraestructura digital común.

43.6 Los componentes y servicios de la infraestructura digital común deben contar con mecanismos de continuidad y recuperación proporcionales a su criticidad, que permitan mantener o restablecer su operación ante incidentes, fallas o contingencias. Dichos mecanismos deben considerar, según corresponda, medidas de redundancia, respaldo, replicación de información, conmutación, recuperación, gestión de incidentes y pruebas periódicas.

43.7 Los niveles de disponibilidad, capacidad y desempeño, así como los tiempos y puntos objetivo de recuperación aplicables a los componentes y servicios de la infraestructura digital común, pueden establecerse en la documentación técnica correspondiente, conforme a las condiciones que determine la Superintendencia.

43.8 Los mecanismos de continuidad y recuperación deben probarse periódicamente y cuando se introduzcan cambios significativos o se produzcan incidentes que puedan afectar su efectividad. Los resultados deben documentarse y conservarse para fines de supervisión, auditoría y mejora continua.

43.9 Los participantes deben implementar los mecanismos técnicos y operativos que resulten necesarios para interactuar con los componentes y servicios de la infraestructura digital común, mantener actualizada la información bajo su responsabilidad y cumplir las condiciones técnicas y operativas aplicables.

43.10 Los requisitos aplicables al Directorio de Participantes se desarrollan en el Anexo N° 5; los correspondientes al Portal del Desarrollador, al diseño de las APIs y a la gestión de versiones, en el Anexo N° 6; los relativos al ambiente de pruebas y a la conformidad funcional, en el Anexo N° 7.

CAPÍTULO II

DIRECTORIO DE PARTICIPANTES

Artículo 44. Finalidad del Directorio de Participantes

44.1 El Directorio de Participantes a que se refiere el artículo 19 constituye el componente común del SFA destinado a identificar a las entidades registradas y a los participantes del SFA, y a mantener la información regulatoria, operativa y técnica necesaria para su interacción en el Sistema.

44.2 El Directorio de Participantes constituye la fuente oficial de información respecto del registro, los roles, la habilitación y los estados de los participantes, así como de las aplicaciones, servidores y demás componentes tecnológicos registrados para su operación en el SFA, permitiendo verificar las condiciones bajo las cuales dichos elementos se encuentran autorizados, habilitados o disponibles para operar, de conformidad con el presente Reglamento.

Artículo 45. Funciones del Directorio de Participantes

45.1 El Directorio de Participantes cumple las siguientes funciones:

a) Registrar la información de identificación de las entidades, los participantes y sus representantes autorizados.
b) Reflejar la situación de las entidades durante los procesos de registro y habilitación técnica, así como los roles y estados aplicables a los participantes habilitados.
c) Mantener la información de contacto de los responsables designados para la interacción técnica y operativa con el SFA.
d) Registrar las aplicaciones, servidores de autorización, servidores de recursos, metadatos, *endpoints* y demás componentes tecnológicos requeridos para la identificación, autenticación e interoperabilidad de los participantes.
e) Registrar las conformidades, certificaciones, validaciones técnicas, su vigencia y los componentes respecto de los cuales fueron emitidas.
f) Mantener el historial de los estados y de las modificaciones relevantes realizadas respecto de la información administrada por el Directorio de Participantes.
g) Facilitar el acceso a los ambientes, componentes y herramientas necesarios para los procesos de acceso anticipado y habilitación técnica previstos en los artículos 20 y 21.
h) Comunicar a los participantes las actualizaciones y la información registrada que resulten necesarias para su adecuada interacción en el SFA.
i) Proporcionar la información necesaria para la ejecución de las pruebas y verificaciones relacionadas a las conformidades y al mantenimiento de las condiciones técnicas exigibles.

Artículo 46. Información y niveles de acceso al Directorio de Participantes

46.1 La información administrada por el Directorio de Participantes se clasifica, según su nivel de acceso, en información de acceso público, información disponible para los participantes e información restringida.

46.2 La Superintendencia determina la clasificación de la información, así como las condiciones aplicables a su publicación, consulta, actualización y utilización, considerando su finalidad, sensibilidad y relevancia para el funcionamiento y seguridad del SFA.

46.3 Las categorías de información administradas por el Directorio de Participantes, los atributos registrados y los niveles de acceso aplicables se desarrollan en el Anexo N° 5.

Artículo 47. Estados registrados en el Directorio de Participantes

47.1 El Directorio de Participantes refleja de manera diferenciada el estado de las entidades durante su incorporación al SFA, los estados de participación respecto de cada rol y los estados operativos de las aplicaciones y demás componentes técnicos registrados.

47.2 Estado de incorporación al SFA.

47.2.1 La entidad que haya aprobado la etapa de registro prevista en el artículo 21 es incorporada por la Superintendencia en el Directorio de Participantes y recibe las credenciales y los accesos necesarios para continuar con la etapa de habilitación técnica. Durante dicha etapa, la entidad se encuentra en el estado "En habilitación técnica".

47.3 Estados de participación en el SFA

47.3.1 Los estados aplicables a los participantes respecto de cada uno de los roles para los cuales se encuentren habilitados son los siguientes:

a) Habilitado
b) Suspendido
c) Retirado
d) Cancelado
e) Mantenimiento

47.4 Estados operativos de los componentes tecnológicos

47.4.1 Los estados operativos aplicables a las aplicaciones, APIs, *endpoints*, servidores y demás componentes tecnológicos registrados son los siguientes:

a) Operativo
b) Operación degradada
c) Mantenimiento programado
d) Indisponibilidad no programada
e) Restringido técnicamente
f) Fuera de producción

47.5 El alcance, los efectos y las reglas aplicables al estado de incorporación, a los estados de participación y a los estados operativos de los componentes tecnológicos se desarrollan en el Anexo N° 5. Las especificaciones e instrucciones operativas para su registro, actualización, consulta y notificación se establecen en el Manual del Directorio de Participantes.

47.6 La Superintendencia registra el estado de incorporación y los estados de participación. Los participantes registran o actualizan directamente, mediante los mecanismos

habilitados en el Directorio de Participantes, los estados operativos de los componentes tecnológicos cuya gestión se encuentre bajo su responsabilidad. Los estados que correspondan a decisiones de la Superintendencia son registrados conforme a las reglas previstas en el Anexo N° 5.

47.7 El registro de un estado operativo distinto de "Operativo" no modifica por sí mismo el estado de participación. Mientras no exista una decisión de suspensión, retiro o cancelación por parte de la Superintendencia, el participante mantiene su estado de "Habilitado" respecto del rol correspondiente, sin perjuicio de las restricciones aplicables al componente afectado.

47.8 Los estados de participación se registran respecto de cada rol y los estados operativos respecto de las aplicaciones, APIs, *endpoints*, servidores y demás componentes tecnológicos. El Directorio de Participantes refleja adicionalmente los estados de los certificados, credenciales y demás elementos del Marco de Confianza, conforme al Título VI.

47.9 La cancelación o retiro de la totalidad de los roles habilitados determina que el registro del participante adquiera la condición de histórico, sin perjuicio de las obligaciones de conservación de información que resulten aplicables. La información se conserva para fines de trazabilidad, supervisión, auditoría, investigación de incidentes y resolución de disputas.

47.10 El catálogo de estados, transiciones permitidas, responsables, eventos desencadenantes, efectos técnicos y mecanismos de notificación se desarrolla en el Anexo N° 5. Las especificaciones e instrucciones operativas para su implementación se desarrollan en el Manual del Directorio de Participantes, disponible en el Portal del Desarrollador.

Artículo 48. Copia local y continuidad del Directorio de Participantes

48.1 Los participantes deben mantener una copia local de la información del Directorio de Participantes con el fin de asegurar la continuidad de sus interacciones en el SFA ante una indisponibilidad temporal del Directorio de Participantes.

48.2 La copia local debe actualizarse, como mínimo, una vez cada veinticuatro (24) horas, sin perjuicio de las actualizaciones extraordinarias que deban efectuarse inmediatamente cuando el participante reciba una comunicación sobre eventos críticos que afecten la validez o vigencia de la información.

48.3 La copia local constituye un mecanismo de contingencia y no sustituye al Directorio de Participantes como fuente oficial de información ni constituye el mecanismo ordinario para la actualización de los datos registrados. En caso de discrepancia entre la copia local y la información disponible en el Directorio de Participantes, prevalece esta última.

48.4 Durante una indisponibilidad temporal del Directorio de Participantes, los participantes pueden utilizar la última copia local vigente, dentro de los límites y condiciones establecidos en el Anexo N° 5 y hasta que se restablezca el servicio.

48.5 La comunicación de una suspensión, cancelación, restricción técnica o revocación, vencimiento o compromiso de certificados, credenciales u otros elementos del Marco de

Confianza determina la invalidación de la información correspondiente en la copia local, conforme a las reglas establecidas en el Anexo N° 5.

48.6 La indisponibilidad temporal del Directorio de Participantes no exime a los participantes de verificar el estado de participación de sus contrapartes, los estados operativos de los componentes tecnológicos y la vigencia de los elementos del Marco de Confianza utilizados en la interacción, mediante la copia local vigente habilitada para tal efecto.

48.7 Las condiciones de sincronización, actualización, vigencia, invalidación, uso en contingencia y restablecimiento se desarrollan en el Anexo N° 5 y en el Manual del Directorio de Participantes.

CAPÍTULO III

PORTALES DEL SFA

Artículo 49. Portal del Sistema de Finanzas Abiertas

49.1 El Portal del SFA constituye el medio digital oficial de difusión pública del Sistema y tiene por finalidad poner a disposición de los usuarios, participantes y demás interesados información clara, razonablemente actualizada y accesible sobre sus objetivos, funcionamiento, participantes, implementación y resultados. Asimismo, facilita el acceso a los canales que correspondan para formular consultas, reclamos y reportes, de acuerdo con las disposiciones aplicables a cada materia.

49.2 La información pública sobre los participantes, sus roles y estados debe mantenerse actualizada conforme a la información de acceso público registrada en el Directorio de Participantes.

49.3 La información publicada en el Portal del SFA debe presentarse de manera clara, comprensible, accesible y diferenciada según el público al que se encuentre dirigida. La Superintendencia puede habilitar espacios o mecanismos específicos para usuarios, participantes, desarrolladores y demás interesados.

49.4 El Portal del SFA no publica datos personales, información protegida por deberes de confidencialidad o reserva previstos en la normativa aplicable, ni información técnica cuya divulgación pueda comprometer la seguridad, integridad o adecuado funcionamiento del Sistema o de sus participantes.

49.5 La publicación de indicadores, información operativa o estados de los participantes debe efectuarse de manera que no permita acceder a datos del usuario ni reconstruir el contenido de los intercambios realizados entre las EPD y las ERD.

49.6 Los participantes del SFA deberán incluir en sus canales digitales un enlace al Portal del SFA y la información que permita al usuario identificar su condición de participante, según los lineamientos de la Superintendencia.

Artículo 50. Portal del Desarrollador

50.1 El Portal del Desarrollador constituye el repositorio técnico oficial del SFA y tiene por finalidad poner a disposición de los participantes, desarrolladores y demás público interesado la documentación necesaria para implementar, integrar, probar, obtener las

certificaciones aplicables, desplegar, operar y mantener los componentes tecnológicos requeridos para participar en el SFA.

50.2 Toda especificación, documento o recurso técnico publicado en el Portal del Desarrollador debe permitir identificar, como mínimo:
a) el título y código del documento o especificación;
b) su versión;
c) la fecha de publicación;
d) su estado;
e) la fecha a partir de la cual resulta aplicable o exigible, cuando corresponda;
f) el periodo de coexistencia con la versión anterior, de ser aplicable;
g) la fecha prevista para su modificación, deprecación o retiro, cuando corresponda; y
h) el historial de sus modificaciones relevantes.

50.3 La Superintendencia comunica a los participantes las nuevas publicaciones y las modificaciones relevantes realizadas en el Portal del Desarrollador mediante los mecanismos comunes de comunicaciones operativas previstos en el artículo 57.

50.4 La documentación publicada en el Portal del Desarrollador debe diferenciar claramente entre:
a) requisitos y especificaciones de cumplimiento obligatorio previstas en el presente Reglamento o sus anexos;
b) guías, ejemplos, implementaciones de referencia y materiales de carácter orientativo; y
c) comunicaciones, preguntas frecuentes y aclaraciones técnicas.

50.5 Las condiciones relativas a la organización del Portal del Desarrollador, la documentación técnica, el control de versiones, la clasificación de cambios, los periodos de coexistencia, la deprecación y el retiro de versiones se desarrollan en el Anexo N° 6. Las condiciones de conformidad funcional y Perfil de Seguridad se desarrollan en los Anexos N° 7 y 9, respectivamente.

CAPÍTULO IV

AMBIENTE DE PRUEBAS Y CONFORMIDAD FUNCIONAL

Artículo 51. Ambiente de pruebas del SFA

51.1 El ambiente de pruebas del SFA es el componente de la infraestructura digital común destinado a facilitar el desarrollo, integración, validación y prueba de las implementaciones requeridas para la participación en el Sistema antes de su utilización en el ambiente de producción.

51.2 Las pruebas realizadas en el ambiente de pruebas no producen efectos sobre cuentas, productos, consentimientos, datos u operaciones reales de los usuarios, ni habilitan por sí mismas a una entidad o participante para operar en el ambiente de producción.

51.3 Las pruebas se realizan exclusivamente con datos de prueba, de conformidad con lo dispuesto en el párrafo 20.6 del artículo 20. En ningún caso deben utilizarse datos personales, información real de los usuarios, credenciales de producción ni información sujeta a reserva o confidencialidad.

51.4 Los recursos, simuladores, implementaciones de referencia y demás herramientas que se habiliten en el ambiente de pruebas tienen por finalidad facilitar la integración y evaluación de las implementaciones y no eximen a las entidades o participantes del cumplimiento de sus obligaciones.

51.5 El ambiente de pruebas debe encontrarse segregado del ambiente de producción y contar con mecanismos que impidan el uso de credenciales, certificados, datos, configuraciones o componentes de prueba para acceder a los servicios de producción.

51.6 Las condiciones técnicas y operativas del ambiente de pruebas, los recursos disponibles, los datos de prueba, las implementaciones de referencia, las reglas de uso y los casos de prueba se desarrollan en el Anexo N° 7.

Artículo 52. Acceso al ambiente de pruebas

52.1 Toda entidad que solicite su habilitación para desempeñar uno o más roles en el SFA debe completar satisfactoriamente las pruebas que le resulten aplicables en el ambiente de pruebas, como parte de la etapa de habilitación técnica prevista en el artículo 21. El acceso anticipado regulado en el artículo 20 mantiene carácter voluntario.

52.2 El acceso al ambiente de pruebas se otorga bajo las siguientes modalidades:

a) Acceso anticipado: otorgado conforme al artículo 20 a las entidades interesadas en desarrollar, integrar o evaluar preliminarmente sus implementaciones antes de iniciar o culminar el proceso de registro.
b) Acceso para habilitación técnica: otorgado conforme al artículo 21 a las entidades que hayan superado la etapa de registro y deban completar las pruebas, conformidades, certificaciones y demás validaciones necesarias para obtener su habilitación.
c) Acceso para revalidación: otorgado a los participantes que deban ejecutar nuevas pruebas como consecuencia de cambios en sus implementaciones, nuevas versiones, vencimiento de certificaciones, deficiencias identificadas u otros supuestos previstos en el artículo 55.

52.3 La Superintendencia determina, para cada modalidad de acceso los ambientes, componentes, recursos, permisos, funcionalidades, vigencia y demás condiciones aplicables conforme a lo previsto en el presente Reglamento y en el Anexo N° 7.

52.4 El acceso anticipado es de carácter exploratorio y no otorga la condición de participante ni habilita para operar en producción. Los resultados obtenidos bajo esta modalidad no acreditan por sí mismos la conformidad funcional.

52.5 Las entidades y los participantes únicamente pueden utilizar el ambiente de pruebas para las actividades, componentes, roles y finalidades comprendidos en el acceso otorgado. En ese sentido, está prohibido:

a) utilizarlo para prestar servicios reales a usuarios;
b) introducir datos personales o información real de los usuarios;
c) emplear credenciales, certificados o llaves privadas del ambiente de producción;
d) afectar la disponibilidad, seguridad o funcionamiento del ambiente o de las implementaciones de otras entidades; y
e) utilizar los resultados, herramientas o información obtenidos para finalidades incompatibles con el proceso de integración, prueba, conformidad o habilitación.

52.6 La Superintendencia puede limitar o suspender el acceso al ambiente de pruebas cuando:
a) se incumplan las condiciones aplicables a su utilización;
b) se identifique un riesgo para la seguridad, disponibilidad o integridad del ambiente;
c) se utilicen datos, credenciales o componentes prohibidos;
d) se ejecuten actividades no comprendidas en el acceso otorgado; o,
e) venza el plazo aplicable.

52.7 La limitación o suspensión del acceso al ambiente de pruebas no constituye por sí misma la suspensión de la habilitación regulada en el artículo 22, sin perjuicio de las actuaciones supervisoras, correctivas o sancionadoras que correspondan.

52.8 La Superintendencia conserva y registra los resultados y evidencias de las pruebas oficiales efectuadas durante el plazo y bajo las condiciones establecidas en el Anexo N° 7. Las entidades y participantes deben conservar las evidencias que se encuentren bajo su responsabilidad.

Artículo 53. Conformidad Funcional

53.1 La conformidad funcional tiene por finalidad verificar el cumplimiento de los requisitos técnicos exigibles para la habilitación de la entidad en el SFA.

53.2 Para obtener la conformidad funcional, la entidad debe:
a) acreditar la certificación vigente correspondiente al Perfil de Seguridad previsto en el Título VII, que resulte aplicable al rol solicitado; y
b) superar satisfactoriamente, en el ambiente de pruebas del SFA, las pruebas obligatorias y demás validaciones técnicas previstas en el Anexo N° 7 que resulten aplicables al rol solicitado.

53.3 Las pruebas realizadas en el ambiente de pruebas comprenden únicamente los componentes, flujos y casos de prueba susceptibles de validación mediante dicho ambiente. El Anexo N° 7 establece el alcance de las pruebas aplicables a cada rol, así como los simuladores, implementaciones de referencia y demás mecanismos utilizados para su ejecución.

53.4 Cuando una implementación no supere las pruebas o validaciones técnicas aplicables, la entidad debe corregir las deficiencias identificadas y volver a ejecutar aquellas que resulten necesarias. La Superintendencia puede requerir la repetición del conjunto de pruebas y validaciones asociadas al componente evaluado cuando la naturaleza o el alcance de las deficiencias o de las correcciones realizadas no permitan delimitar sus efectos.

53.5 Los resultados deben permitir identificar el alcance evaluado, las versiones y casos de prueba aplicables, los resultados obtenidos, las observaciones y subsanaciones realizadas y la fecha de culminación de la evaluación. Asimismo, los resultados de la evaluación deben ser comunicados a la entidad evaluada a través de los mecanismos habilitados para tal efecto.

Artículo 54. Registro de la conformidad funcional

54.1 Completadas las condiciones previstas en el artículo 53, la conformidad funcional se registra en el Directorio de Participantes respecto del rol y de los componentes comprendidos en la evaluación.

54.2 La conformidad funcional constituye un requisito para la habilitación técnica prevista en el artículo 21, pero no sustituye la decisión de habilitación que corresponde a la Superintendencia.

54.3 La conformidad funcional no exime al participante de mantener las condiciones que sustentaron su obtención ni limita la facultad de la Superintendencia de requerir nuevas pruebas o verificaciones cuando corresponda.

Artículo 55. Revalidación de la conformidad funcional

55.1 Los participantes deben revalidar sus implementaciones y, cuando corresponda, obtener una nueva conformidad funcional en los siguientes supuestos:

a) cuando entre en vigencia una nueva versión obligatoria de una especificación, estándar o API que requiera la ejecución de nuevas pruebas de conformidad;
b) cuando implementen una nueva versión de una API o de un componente previamente evaluado;
c) cuando realicen cambios significativos que puedan afectar las funcionalidades, la interoperabilidad, la autenticación, la autorización, la gestión de consentimientos, los certificados, los *tokens*, los datos, los mensajes o la exposición de las APIs;
d) cuando modifiquen su infraestructura, configuración o arquitectura de manera que puedan afectar los resultados previamente obtenidos;
e) cuando la certificación de conformidad con el Perfil de Seguridad vinculada con el alcance evaluado sea sustituida, suspendida, retirada, pierda vigencia o sea renovada como consecuencia de cambios que puedan afectar las condiciones previamente evaluadas;
f) cuando se identifiquen deficiencias que puedan afectar las condiciones previamente evaluadas;
g) cuando ocurra un incidente que comprometa o pueda comprometer dichas condiciones;
h) cuando se identifique una vulnerabilidad u obsolescencia tecnológica con impacto material sobre la implementación; o
i) cuando la Superintendencia lo disponga de manera motivada.

55.2 La Superintendencia determina, atendiendo a la naturaleza y alcance del cambio o deficiencia, si la revalidación comprende:

a) pruebas específicas;
b) un conjunto parcial de pruebas;
c) la totalidad de las pruebas de conformidad funcional;
d) la renovación de la Certificación del Perfil de Seguridad; o
e) la obtención de una nueva conformidad funcional.

55.3 Los participantes deben asegurar que las implementaciones y componentes utilizados para operar en el SFA mantengan correspondencia con aquellos respecto de los cuales se obtuvo la conformidad funcional.

55.4 Las condiciones, eventos, alcances, procedimientos y evidencias aplicables a la revalidación se desarrollan en el Anexo N° 7.

CAPÍTULO V

SOPORTE Y COMUNICACIONES OPERATIVAS

Artículo 56. Soporte técnico operativo

56.1 El SFA cuenta con mecanismos comunes de soporte para la atención y seguimiento de consultas, requerimientos y problemas técnicos relacionados con los componentes y servicios de la infraestructura digital común.

56.2 Los mecanismos de soporte no sustituyen los procedimientos aplicables a la gestión de incidentes, atención de usuarios, resolución de disputas o supervisión. Sus condiciones operativas, criterios de atención, escalamiento y conservación de información se desarrollan en el Anexo N° 10.

Artículo 57. Comunicaciones operativas

57.1 La infraestructura digital común cuenta con mecanismos para comunicar de manera segura y oportuna la información operativa necesaria para el funcionamiento del SFA, incluyendo cambios relevantes en los estados de participantes y componentes, mantenimientos, indisponibilidades, cambios técnicos y alertas que requieran actuación de los participantes.

57.2 Los participantes deben mantener actualizados los canales y responsables necesarios para recibir dichas comunicaciones y atender aquellas que requieran su actuación. Las condiciones técnicas, categorías, prioridades, mecanismos de recepción, contingencia y conservación se desarrollan en el Anexo N° 10.

TÍTULO VI

MARCO DE CONFIANZA

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 58. Marco de Confianza del SFA

58.1 El Marco de Confianza del SFA es el conjunto de reglas, procedimientos, estándares, registros y mecanismos técnicos y operativos que establecen las condiciones comunes para la identificación, habilitación e interacción segura e interoperable de los participantes, sus aplicaciones y los demás componentes utilizados para operar en el Sistema.

58.2 El Marco de Confianza permite verificar, de manera estandarizada:

a) la identidad del participante con el que se interactúa;
b) los roles para los cuales se encuentra habilitado;
c) las aplicaciones y los componentes tecnológicos vinculados al participante;
d) los identificadores, certificados digitales, declaraciones de *software*, llaves públicas y demás elementos de confianza registrados;
e) las certificaciones, conformidades y validaciones aplicables; y
f) los estados, restricciones y demás condiciones que resulten relevantes para la interacción.

58.3 El Marco de Confianza tiene por finalidad establecer una base común de confianza regulatoria, operativa y técnica que permita la interacción directa entre los participantes, sin requerir acuerdos bilaterales para acreditar su identidad, habilitación o cumplimiento de los requisitos comunes del SFA, sin perjuicio de las relaciones contractuales que puedan corresponder por otros conceptos.

58.4 El Directorio de Participantes constituye la fuente oficial de información del Marco de Confianza respecto de la identidad, los roles, las aplicaciones, los elementos de confianza y los estados registrados. La información registrada produce efectos únicamente respecto del participante, rol, aplicación, componente y ambiente al que se encuentre vinculada.

58.5 La Superintendencia establece las condiciones de funcionamiento y evolución del Marco de Confianza y supervisa el cumplimiento de las obligaciones aplicables a los participantes.

Artículo 59. Responsabilidad de los participantes en el Marco de Confianza

59.1 Los participantes son responsables de verificar, antes de iniciar y durante cada interacción, que la contraparte, el rol, la aplicación, los componentes tecnológicos y los elementos de confianza utilizados se encuentren registrados, vigentes y en condiciones de ser utilizados para la interacción correspondiente.

59.2 Para efectuar las verificaciones señaladas en el párrafo 59.1, los participantes deben utilizar la información oficial del Directorio de Participantes y aplicar los mecanismos de autenticación, autorización, firma, cifrado y validación establecidos en el Perfil de Seguridad.

59.3 La inscripción o el registro de un participante, rol, aplicación, componente tecnológico o elemento de confianza en el Directorio de Participantes no sustituye la verificación técnica y criptográfica de su autenticidad, integridad, vigencia, estado, alcance y vinculación con la interacción correspondiente.

59.4 La confianza derivada de la información registrada en el Directorio de Participantes se limita al participante, rol, aplicación, componente tecnológico, elemento de confianza, ambiente y periodo de vigencia correspondientes. Dicha confianza no puede extenderse a otros roles, aplicaciones, componentes, elementos o ambientes que no se encuentren debidamente registrados y en condiciones de ser utilizados.

59.5 Los participantes deben rechazar o interrumpir la interacción cuando:

a) no resulte posible verificar la identidad o habilitación de la contraparte;
b) el participante no se encuentre habilitado para actuar bajo el rol correspondiente o la aplicación o el componente tecnológico no se encuentre registrado o en condiciones de ser utilizado para la interacción;
c) el certificado digital, la firma, el *token* u otro elemento de confianza se encuentre vencido, suspendido, revocado, comprometido o no pueda ser validado;
d) la solicitud exceda el alcance o la vigencia de la autorización o del consentimiento del usuario, cuando este resulte exigible; o
e) se presente otra condición que, conforme al Perfil de Seguridad, impida la interacción.

59.6 La indisponibilidad temporal del Directorio de Participantes no exime a los participantes de efectuar las verificaciones exigibles. Durante dicha indisponibilidad, pueden utilizar la última copia local vigente de su información, conforme a las condiciones establecidas en el Título V y el Anexo N° 5, siempre que la información correspondiente no haya sido previamente invalidada o modificada por el Directorio y puedan completarse las demás validaciones técnicas y criptográficas aplicables.

CAPÍTULO II

IDENTIDAD DIGITAL DE PARTICIPANTES Y APLICACIONES

Artículo 60. Identidad digital de los participantes

60.1 La identidad digital de un participante en el SFA está constituida por su identificador principal único y por el conjunto de información y atributos que permiten identificarlo de manera inequívoca y verificar su vinculación con los roles para los cuales se encuentra habilitado, así como con las aplicaciones, componentes tecnológicos, ambientes y elementos de confianza registrados a su nombre en el Directorio de Participantes.

60.2 La identidad digital del participante produce efectos únicamente respecto de los roles para los cuales se encuentre habilitado y de las aplicaciones, componentes tecnológicos, ambientes y elementos de confianza vinculados a dichos roles. Para cada interacción debe verificarse que el participante se encuentre habilitado para actuar bajo el rol correspondiente y que los elementos utilizados estén registrados, vigentes y vinculados con dicho rol y con el ambiente en el que se desarrolla la interacción.

60.3 La información y los atributos que conforman la identidad digital se registran durante el proceso de inscripción y habilitación de la entidad, se actualizan durante su permanencia en el SFA y se conservan después de su retiro o de la cancelación de su habilitación, para fines de trazabilidad, supervisión, auditoría, investigación de incidentes y resolución de disputas.

60.4 La identidad digital del participante se vincula con su estado de participación respecto de cada rol. La suspensión, el retiro o la cancelación de un rol impide utilizar las aplicaciones, componentes tecnológicos y elementos de confianza vinculados a dicho rol en las interacciones comprendidas en el alcance de la medida, sin extender sus efectos a otros roles que mantengan su habilitación, salvo que la naturaleza o el alcance de la medida determine lo contrario.

60.5 Los participantes son responsables de mantener actualizada la información y los atributos vinculados a su identidad digital y de comunicar o registrar oportunamente cualquier modificación que pueda afectar su identificación, habilitación o interacción con los demás participantes.

Artículo 61. Identidad y registro de aplicaciones

61.1 Las aplicaciones mediante las cuales los participantes interactúan en el SFA deben encontrarse registradas en el Directorio de Participantes y vinculadas, antes de su utilización, con el participante responsable, el rol y el ambiente correspondiente.

61.2 La identidad de una aplicación comprende la información y los atributos necesarios para identificarla de manera única y verificar su vinculación con el participante responsable, el rol y el ambiente aplicables, así como con los servidores, metadatos, certificados digitales, declaraciones de *software*, llaves públicas, información de descubrimiento y demás elementos de confianza que correspondan. La vinculación de la aplicación con el participante, el rol y el ambiente se acredita mediante la declaración de *software* obtenida a través de los mecanismos habilitados por el Directorio de Participantes, conforme al Perfil de Seguridad.

61.3 Solo pueden utilizarse en el SFA las aplicaciones que se encuentren registradas y cuyo estado permita su operación en el ambiente correspondiente. Las aplicaciones únicamente pueden utilizarse para los roles, ambientes e interacciones comprendidos en su registro y cuyo estado permita su utilización.

61.4 El participante es responsable de las aplicaciones registradas a su nombre y de las interacciones realizadas mediante estas. La contratación de terceros para su desarrollo, operación, alojamiento, mantenimiento o soporte no transfiere ni limita dicha responsabilidad.

61.5 Los participantes deben mantener actualizada la información y los atributos vinculados a sus aplicaciones y comunicar o registrar oportunamente ante el Directorio de Participantes su modificación, sustitución, suspensión, retiro, compromiso de seguridad o cualquier otro evento que pueda afectar su identificación, seguridad o utilización en el SFA.

61.6 El registro de una aplicación en el Directorio de Participantes constituye una condición previa para su registro dinámico ante los servidores de autorización con los que deba interactuar. El registro dinámico se realiza utilizando la declaración de *software* y los demás elementos de confianza aplicables, conforme al Perfil de Seguridad.

61.7 Las condiciones y procedimientos para el registro, actualización, consulta y conservación de la información de las aplicaciones se desarrollan en el Título V y en el Anexo N° 5. Los requisitos, protocolos y flujos técnicos aplicables a la emisión y validación de las declaraciones de *software*, al registro dinámico y a la autenticación y autorización de las aplicaciones se establecen en el Título VII y en el Anexo N° 9, que contiene el Perfil de Seguridad.

CAPÍTULO III

ELEMENTOS CENTRALES DE CONFIANZA Y AUTORIZACIÓN

Artículo 62. Certificados digitales

62.1 Los certificados digitales constituyen elementos del Marco de Confianza utilizados para autenticar a las aplicaciones y componentes tecnológicos, establecer comunicaciones seguras y verificar la autenticidad, integridad y procedencia de los mensajes, conforme al uso para el cual hayan sido emitidos.

62.2 Los certificados digitales deben encontrarse vigentes y vinculados con el participante, la aplicación, el componente tecnológico y el ambiente correspondientes. Las condiciones aplicables a su emisión, admisión, registro, utilización, validación, segregación por

ambiente, suspensión, revocación y uso en contingencia se establecen en el Título VII y en el Anexo N° 9.

Artículo 63. Ciclo de vida y custodia de certificados, credenciales y material criptográfico

63.1 Los participantes son responsables de gestionar el ciclo de vida y asegurar la custodia y utilización autorizada de los certificados digitales, credenciales, llaves y demás material criptográfico que se encuentren bajo su responsabilidad, incluso cuando su generación, administración, custodia u operación se encargue a terceros.

63.2 El vencimiento, la suspensión, la revocación, la pérdida o el compromiso de los certificados digitales, credenciales, llaves u otros materiales criptográficos impide su utilización para establecer nuevas interacciones y obliga a interrumpir aquellas cuya seguridad pueda resultar afectada. Las condiciones aplicables a su gestión, protección, renovación, rotación, sustitución, revocación y eliminación se establecen en el Título VII y en el Anexo N° 9.

Artículo 64. Autorización de aplicaciones y acceso a las APIs

64.1 El acceso de una aplicación a las APIs del SFA requiere que esta se encuentre registrada, autenticada y autorizada para actuar como aplicación de la ERD, bajo el rol y en el ambiente correspondientes. La autorización debe limitarse a los datos, recursos, acciones y periodo de vigencia que resulten aplicables y, cuando corresponda, al alcance del consentimiento del usuario.

64.2 Antes de permitir una interacción, la EPD que recibe la solicitud debe verificar la identidad de la ERD y su habilitación para desempeñar el rol correspondiente, el registro y estado de la aplicación, así como la vigencia y alcance de la autorización y de los elementos de confianza aplicables. Los requisitos, protocolos y flujos técnicos de registro dinámico, autenticación, autorización y acceso a las APIs se establecen en el Título VII y en el Anexo N° 9.

Artículo 65. *Tokens* y validación del acceso

65.1 Los *tokens* constituyen mecanismos técnicos mediante los cuales una aplicación acredita y ejerce una autorización válida para acceder a las APIs del SFA. Solo pueden emitirse a aplicaciones registradas y autenticadas, y no pueden conferir un alcance o periodo de vigencia superiores a los de la autorización y, cuando corresponda, del consentimiento que los sustenta.

65.2 Antes de permitir el acceso, la EPD debe verificar la autenticidad, integridad, vigencia, alcance y destinatario del *token*, así como su vinculación con la aplicación y la autorización correspondientes. Las condiciones técnicas aplicables a su emisión, vinculación, utilización, renovación, revocación y validación se establecen en el Título VII y en el Anexo N° 9.

CAPÍTULO IV

EVENTOS DE CONFIANZA Y TRAZABILIDAD

Artículo 66. Eventos relevantes para las condiciones de confianza

66.1 Constituyen eventos relevantes para las condiciones de confianza aquellos que modifiquen, restrinjan, suspendan, extingan o restablezcan la habilitación de un

participante respecto de un rol; el estado de una aplicación o componente tecnológico; o la vigencia, validez o utilización de un elemento de confianza, autorización, conformidad funcional o certificación requerido para interactuar en el SFA.

66.2 Los eventos que afecten condiciones registradas en el Directorio de Participantes deben reflejarse en dicho componente y comunicarse mediante los mecanismos operativos del SFA, cuando corresponda. Los eventos vinculados exclusivamente con una interacción, consentimiento, autorización o *token* se comunican entre los participantes involucrados. Cuando el evento constituya un incidente sujeto a reporte, que afecte o pueda afectar a más de un participante, o comprometa la seguridad, integridad, disponibilidad, continuidad o confianza en el SFA, debe comunicarse también a la Superintendencia y a los demás participantes afectados.

66.3 Los participantes deben gestionar de manera oportuna los eventos bajo su responsabilidad y adoptar las medidas necesarias para mitigar los riesgos derivados de estos, de acuerdo con su marco de gestión integral de riesgos y sin perjuicio de la aplicación de las medidas previstas en el artículo 59 cuando no puedan mantenerse las condiciones de confianza exigibles.

Artículo 67. Registros y evidencias del Marco de Confianza

67.1 Los participantes deben generar y conservar registros y evidencias suficientes de las actuaciones y validaciones del Marco de Confianza que se encuentren bajo su responsabilidad. Dichos registros deben permitir reconstruir las interacciones relevantes e identificar a los participantes, roles, aplicaciones, componentes tecnológicos y elementos de confianza intervinientes.

67.2 Los registros y evidencias deben permitir identificar, como mínimo y según corresponda:

a) la fecha y hora del evento o interacción;
b) el identificador único de la interacción;
c) la identidad de los participantes intervinientes, los roles bajo los cuales actuaron y sus respectivos estados de participación;
d) la identificación, el estado y el ambiente de las aplicaciones y componentes tecnológicos utilizados;
e) la actuación realizada, incluida la autenticación y autorización de la aplicación;
f) la validación de certificados digitales, firmas, credenciales, *tokens*, autorizaciones y demás elementos de confianza;
g) el alcance, la vigencia, el destinatario y el resultado de las validaciones efectuadas;
h) el elemento de confianza, autorización, estado o condición utilizado como sustento de la decisión técnica correspondiente;
i) la fuente de información o el mecanismo de validación utilizado, incluida, cuando corresponda, la copia local del Directorio de Participantes.;
j) los eventos que modifiquen restrinjan, extingan o restablezcan las condiciones de confianza y las medidas adoptadas como consecuencia de estos;
k) los rechazos o interrupciones de interacciones derivados de la imposibilidad de verificar o mantener las condiciones de confianza exigibles; y
l) el restablecimiento de las interacciones y las verificaciones efectuadas para tal fin.

67.3 Los registros y evidencias se conservan durante los plazos establecidos en el presente Reglamento y en las disposiciones que resulten aplicables, deben mantenerse a disposición de la Superintendencia y ser accesibles oportunamente para fines de

supervisión, auditoría, investigación de incidentes, aplicación de medidas correctivas y resolución de disputas. Los requisitos técnicos relativos a su contenido mínimo, generación, protección, conservación y acceso se establecen en el Título VII, en el Anexo N° 9 y en las especificaciones técnicas correspondientes.

TÍTULO VII

ESTÁNDARES, SEGURIDAD Y CALIDAD

CAPÍTULO I

ESTÁNDARES TÉCNICOS Y PERFIL DE SEGURIDAD

Artículo 68. Estándares técnicos aplicables al SFA

68.1 El acceso y suministro de los datos e información comprendidos en el SFA se realizan exclusivamente mediante APIs que cumplen los siguientes estándares técnicos:

a) Especificación y diseño: OpenAPI.
b) Arquitectura: estilo arquitectónico REST, con implementación RESTful.
c) Formato de mensajería: JSON.
d) Modelo y diccionario de datos: los definidos en el Anexo N° 3, tomando como referencia el estándar ISO 20022.
e) Perfil de Seguridad: el definido en el artículo 69.

68.2 Las especificaciones técnicas de las APIs son comunes y de cumplimiento obligatorio para los participantes. Son aprobadas por la Superintendencia y publicadas en el Portal del Desarrollador, con indicación de su versión y fecha de exigibilidad.

68.3 Los participantes no pueden emplear, para acceder a los datos e información comprendidos en el SFA o suministrarlos, mecanismos que requieran que el usuario proporcione a un participante distinto de la EPD las credenciales que esta le hubiera asignado, ni mecanismos que simulen la interacción del usuario con los canales digitales de la EPD.

68.4 Las EPD no pueden exigir parámetros, encabezados, pasos o condiciones adicionales a los previstos en las especificaciones técnicas aplicables, ni condicionar el acceso o suministro de los datos e información comprendidos en el SFA a la celebración de acuerdos bilaterales con las ERD. Las APIs que una EPD ofrezca fuera del SFA no forman parte de este ni pueden presentarse como sustitutas de las APIs reguladas, conforme al presente Reglamento.

68.5 Los requisitos de diseño y los niveles de servicio de las APIs, así como las reglas aplicables a la gestión de sus versiones, se desarrollan en el Anexo N° 6. La Superintendencia establece y publica en el Portal del Desarrollador las versiones exigibles de los estándares y especificaciones previstos en los párrafos 68.1 y 68.2, así como los periodos de transición y coexistencia correspondientes, conforme a las reglas establecidas en dicho Anexo. Las especificaciones técnicas y la gestión de versiones del Perfil de Seguridad se rigen por el artículo 70.

Artículo 69. Perfil de Seguridad

69.1 El Perfil de Seguridad establece los requisitos técnicos de cumplimiento obligatorio aplicables a la autenticación, autorización, firma, cifrado, registro dinámico de aplicaciones, emisión y validación de *tokens* y demás mecanismos de seguridad utilizados en las interacciones entre los participantes, sus aplicaciones y los componentes del SFA.

69.2 Para efectos del Perfil de Seguridad, la EPD opera el servidor de autorización y el servidor de recursos, y la ERD opera la aplicación cliente. Las obligaciones asignadas a dichos componentes recaen en el participante que los opera, aun cuando su desarrollo, operación, alojamiento, mantenimiento o soporte se encuentren a cargo de un tercero, conforme al artículo 80.

69.3 Los requisitos del Perfil de Seguridad se establecen en el Anexo N° 9. Las especificaciones técnicas que desarrollan dichos requisitos se aprueban y publican en el Portal del Desarrollador, conforme al artículo 70.

69.4 El acceso a la información señalada en el numeral 3 del párrafo 9.1 del artículo 9, que no requiere el consentimiento del usuario conforme al párrafo 9.2 del artículo 9, no se sujeta a los mecanismos de autenticación y autorización del usuario previstos en el Perfil de Seguridad. Dicho acceso se sujeta a los requisitos de seguridad, autenticación de aplicaciones, cifrado de las comunicaciones, disponibilidad y demás condiciones establecidas en el presente Reglamento y en las especificaciones técnicas aplicables.

Artículo 70. Especificaciones técnicas y gestión de versiones del Perfil de Seguridad

70.1 Las especificaciones técnicas que desarrollan el Perfil de Seguridad previsto en el Anexo N° 9 son aprobadas por la Superintendencia y publicadas en el Portal del Desarrollador. Estas comprenden, entre otros, los siguientes aspectos:

a) las versiones exigibles de las especificaciones de referencia;
b) los protocolos y flujos técnicos aplicables;
c) los algoritmos y las longitudes de clave admitidos;
d) las condiciones de vigencia, emisión, vinculación, renovación, revocación y validación de los elementos de seguridad;
e) los parámetros técnicos aplicables a certificados, firmas, autorizaciones y *tokens*; y
f) los catálogos técnicos requeridos para su implementación.

El cumplimiento de las especificaciones técnicas es obligatorio para los participantes a partir de la fecha de exigibilidad indicada en la publicación correspondiente.

70.2 La publicación, exigibilidad, modificación, coexistencia, deprecación y retiro de las versiones de las especificaciones técnicas se realizan a través del Portal del Desarrollador y se rigen por las disposiciones previstas en el Título V y en el Anexo N° 6.

70.3 La Superintendencia publica las nuevas versiones con una anticipación no menor de noventa (90) días calendario respecto de su fecha de exigibilidad.

70.4 Cuando la organización responsable de emitir, administrar o mantener una especificación de referencia utilizada en el SFA la declare obsoleta o la sustituya, o cuando se identifique una vulnerabilidad o amenaza que pueda comprometer la seguridad del SFA, la Superintendencia puede establecer plazos de adecuación menores a los previstos para las modificaciones ordinarias.

Artículo 71. Certificación de conformidad con el Perfil de Seguridad

71.1 Los participantes acreditan el cumplimiento del Perfil de Seguridad mediante una certificación emitida por la *OpenID Foundation* o por una entidad autorizada por dicha organización para ejecutar las pruebas y certificar implementaciones. La certificación se obtiene conforme a los planes de prueba del perfil de conformidad del SFA aplicables a cada rol desempeñado: las EPD como *OpenID Provider* y las ERD como *Relying Party*, de conformidad con el párrafo 21.3.2. La certificación tiene una vigencia de un (1) año calendario.

71.2 La certificación debe mantenerse vigente durante todo el periodo en que el participante se encuentre habilitado para operar el componente correspondiente. Asimismo, debe encontrarse publicada en el registro público de certificaciones de la OpenID Foundation o, cuando haya sido emitida por una entidad autorizada por dicha organización, en el registro público que esta mantenga.

71.3 El participante debe acreditar nuevamente la conformidad con el Perfil de Seguridad cuando:

a) entre en vigencia una nueva versión del Perfil de Seguridad que requiera una nueva evaluación;
b) implemente cambios que afecten los componentes de autenticación, autorización, emisión o validación de *tokens*, firma de mensajes o exposición de las APIs comprendidas en el SFA;
c) la certificación o acreditación sea suspendida, revocada, retirada o pierda vigencia;
d) se identifique una vulnerabilidad crítica o una deficiencia que pueda afectar materialmente las condiciones evaluadas; o,
e) se configure otro supuesto previsto en el Anexo N° 9.

71.4 La pérdida de vigencia de la certificación, su retiro del registro público correspondiente o la pérdida de la autorización otorgada por la *OpenID Foundation* a la entidad que la emitió impide utilizar la implementación certificada para nuevas interacciones en el SFA y da lugar a la aplicación de las medidas previstas en el artículo 22, según corresponda.

71.5 Los resultados y las evidencias de las pruebas deben conservarse y mantenerse a disposición de la Superintendencia. La certificación no exime al participante de su responsabilidad por el cumplimiento permanente del Perfil de Seguridad y de las demás obligaciones previstas en el presente Reglamento.

CAPÍTULO II

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Artículo 72. Marco de seguridad aplicable

72.1 Los participantes comprendidos en el ámbito de aplicación del Reglamento de Seguridad de la Información y Ciberseguridad deben incorporar en el alcance de su sistema de gestión de seguridad de la información y ciberseguridad los sistemas, componentes e infraestructura mediante los cuales participan en el SFA, así como los datos e información que reciban, almacenen o traten en el marco del Sistema.

72.2 Los participantes no comprendidos en el ámbito de aplicación del Reglamento de Seguridad de la Información y Ciberseguridad deben implementar y mantener, respecto

de los sistemas, componentes e infraestructura mediante los cuales participan en el SFA, así como de los datos e información que reciban, almacenen o traten en el marco del Sistema, las siguientes medidas previstas en dicho Reglamento:

a) las medidas mínimas de seguridad de la información establecidas en el artículo 12, incluidas las referidas al control de acceso físico y lógico, la seguridad en las operaciones, las copias de respaldo, la criptografía aplicada a la información almacenada y transmitida, y la gestión de los activos de información;
b) la identificación de los activos de información, el análisis de sus amenazas y vulnerabilidades, la adopción de las medidas de tratamiento correspondientes y la evaluación de su efectividad, con una periodicidad mínima anual, conforme a los literales a) y b) del artículo 13; y
c) un programa de ciberseguridad conforme al párrafo 14.2 del artículo 14.

72.3 Todos los participantes deben implementar, respecto de las APIs mediante las cuales acceden a los datos e información del SFA o los suministran, las medidas previstas en el artículo 21 del Reglamento de Seguridad de la Información y Ciberseguridad. El Perfil de Seguridad constituye el estándar de referencia para la autenticación mutua de los sistemas, la autorización del usuario y la limitación del acceso a la información comprendida en su autorización.

72.4 El análisis de riesgos requerido en el literal a) del párrafo 21.1 del Reglamento de Seguridad de la Información y Ciberseguridad debe usar como referencia el modelo de amenazas utilizado en el Perfil de Seguridad y considerar, además, los riesgos no comprendidos en dicho modelo. Estos riesgos deben ser gestionados conforme al marco de gestión aplicable al participante.

72.5 Cuando una misma materia se encuentre regulada por el presente Reglamento y por el Reglamento de Seguridad de la Información y Ciberseguridad, resulta aplicable el requisito específico previsto para el SFA. Los requisitos concurrentes que no resulten incompatibles son exigibles de manera conjunta. Cuando dichos requisitos tengan igual grado de especificidad, resulta aplicable el más exigente.

Artículo 73. Autenticación del usuario y confirmación

73.1 El otorgamiento, la modificación y la revocación del consentimiento requieren la autenticación reforzada del usuario, conforme al artículo 19 del Reglamento de Seguridad de la Información y Ciberseguridad.

73.2 La autenticación del usuario para el otorgamiento, modificación y revocación del consentimiento se realiza en el entorno de la EPD, conforme a los artículos 31 y 38 del presente Reglamento.

73.3 El control frente a ataques de intermediario previsto en el literal b) del artículo 19 del Reglamento de Seguridad de la Información y Ciberseguridad debe vincularse, durante la etapa de confirmación prevista en el artículo 32, con los detalles de autorización que el usuario confirma, de manera que cualquier alteración de su contenido invalide la confirmación.

73.4 El acceso posterior a los datos no requiere una nueva autenticación del usuario cuando se realice dentro del alcance y periodo de vigencia del consentimiento y de la autorización

correspondientes, sin perjuicio de los supuestos de renovación, modificación o nueva autenticación establecidos en el presente Reglamento y en el Perfil de Seguridad.

Artículo 74. Autenticación mutua entre participantes y certificados digitales

74.1 Los participantes deben utilizar certificados digitales emitidos por autoridades de certificación que cumplan los criterios de admisión establecidos en el Anexo N° 9 y en las especificaciones técnicas del Perfil de Seguridad. Los criterios de admisión y la información necesaria para verificar su cumplimiento se publican en el Portal del Desarrollador.

74.2 Los participantes deben custodiar las llaves privadas vinculadas con sus certificados y, ante su compromiso o sospecha de compromiso, solicitar inmediatamente la revocación del certificado correspondiente y comunicar el evento a la Superintendencia y al Directorio de Participantes, sin perjuicio de las notificaciones previstas en el artículo 76.

Artículo 75. Expresión, validación del alcance y ciclo de vida del consentimiento

75.1 El alcance de cada consentimiento se expresa mediante detalles de autorización estructurados que identifican de manera específica y verificable, entre otros elementos, los grupos y subconjuntos de datos, las acciones autorizadas y el periodo de vigencia, conforme a los catálogos técnicos publicados en el Portal del Desarrollador y en concordancia con el Anexo N° 3.

75.2 La ERD debe registrar la finalidad relacionada a cada consentimiento y a su identificador único, conforme al Anexo N° 1 y al catálogo de finalidades específicas publicado por la Superintendencia en el Portal del SFA.

75.3 La ERD es responsable de que el periodo de vigencia solicitado no exceda el máximo aplicable a la finalidad correspondiente, establecido conforme al Anexo N° 1 y publicado en el Portal del SFA.

75.4 La suspensión de la habilitación de una ERD impide la emisión y renovación de *tokens* a sus aplicaciones, sin extinguir por sí misma los consentimientos vigentes. La cancelación de la habilitación como ERD determina la revocación de las autorizaciones vinculadas a sus aplicaciones.

Artículo 76. Notificación de eventos de seguridad

76.1 Los participantes deben notificar, de acuerdo con los tiempos y forma establecidos en el Portal del Desarrollador, a los demás participantes involucrados, como mínimo, los siguientes eventos:

a) la revocación de una autorización o de los *tokens* asociados;
b) la rotación, suspensión, revocación o compromiso de los certificados digitales utilizados en el SFA; y
c) los demás eventos previstos en el Perfil de Seguridad y en las especificaciones técnicas publicadas en el Portal del Desarrollador.

Los eventos que afecten información o elementos registrados en el Directorio de Participantes deben comunicarse también mediante los mecanismos establecidos para su actualización.

76.2 Los cambios en los estados de participación se comunican mediante los mecanismos operativos del SFA y se reflejan en el Directorio de Participantes.

76.3 El emisor debe implementar reintentos y mecanismos que eviten el procesamiento duplicado de las notificaciones. El destinatario debe procesarlas de manera idempotente, sin asumir un orden de entrega. La falla en la entrega a un destinatario no impide su envío a los demás destinatarios.

76.4 Las notificaciones contienen únicamente la información necesaria para identificar y gestionar el evento y no deben incluir datos del usuario ni el contenido de la autorización. La información adicional se obtiene mediante una consulta autenticada a la fuente correspondiente.

Artículo 77. Trazabilidad y conservación de registros

77.1 Los participantes deben asignar y propagar un identificador único de interacción en cada solicitud y respuesta de las APIs del SFA, que permita reconstruir de extremo a extremo las interacciones entre la EPD, la ERD y, cuando corresponda, los componentes de la infraestructura digital común.

77.2 Los registros y evidencias asociados a las interacciones del SFA se conservan por un plazo mínimo de diez (10) años y se mantienen a disposición de la Superintendencia para fines de supervisión, auditoría, investigación de incidentes y atención de disputas, de conformidad con el artículo 67 y el Título IX.

Artículo 78. Desarrollo seguro y pruebas de seguridad

78.1 Los participantes deben realizar análisis de vulnerabilidades y pruebas de penetración sobre los componentes mediante los cuales participan en el SFA, de conformidad con el literal f) del párrafo 21.1 del artículo 21 del Reglamento de Seguridad de la Información y Ciberseguridad. Dichas evaluaciones se realizan:

a) antes de su habilitación técnica;
b) como mínimo una vez al año; y
c) cuando se introduzcan cambios que puedan afectar los componentes de autenticación, autorización, emisión o validación de *tokens*, firma de mensajes o exposición de las APIs.

Las pruebas deben ser realizadas por personal independiente de quienes desarrollan y operan los componentes evaluados.

78.2 Los hallazgos deben ser remediados en plazos proporcionales a su criticidad. Los resultados, planes de remediación y evidencias deben mantenerse a disposición de la Superintendencia.

Artículo 79. Monitoreo, gestión de incidentes y medidas de contención

79.1 El monitoreo de eventos de seguridad a que se refiere el literal j) del párrafo 21.1 del artículo 21 del Reglamento de Seguridad de la Información y Ciberseguridad comprende, respecto de los componentes del SFA, como mínimo, la detección de:

a) patrones anómalos de uso de *tokens* o de consumo de las APIs;
b) intentos fallidos de autenticación de participantes y firmas inválidas;
c) uso de certificados, credenciales o aplicaciones suspendidos, revocados o comprometidos;

d) las solicitudes que excedan el alcance consentido o se sustenten en autorizaciones revocadas o vencidas; y
e) volúmenes atípicos de otorgamiento o revocación de consentimientos.

79.2 Ante un incidente que afecte o pueda afectar la seguridad del SFA, el participante debe adoptar inmediatamente las medidas de contención necesarias, incluida la restricción o suspensión temporal del intercambio con una contraparte o aplicación determinada. Las medidas que afecten a otros participantes deben ser proporcionales, temporales, encontrarse sustentadas técnicamente y comunicarse de inmediato a la Superintendencia y a la contraparte afectada. Cuando la medida afecte una condición o elemento registrado, debe reflejarse también en el Directorio de Participantes conforme al Título V. Las medidas no pueden aplicarse de manera discriminatoria ni para fines distintos de la contención del incidente. La Superintendencia puede disponer la modificación o levantamiento de dichas medidas.

79.3 Los participantes deben clasificar y reportar los incidentes que afecten su participación en el SFA conforme a las disposiciones que les resulten aplicables y a los criterios establecidos en el presente Reglamento.

Artículo 80. Proveedores de servicios técnicos

80.1 Los participantes pueden contratar a terceros para el desarrollo, operación, alojamiento o soporte de los componentes tecnológicos mediante los cuales participan en el SFA. Dicha contratación no transfiere ni exime su responsabilidad por el cumplimiento del presente Reglamento, sus anexos y el Perfil de Seguridad. Los participantes deben asegurarse de que sus proveedores identifiquen, gestionen y mitiguen conflictos de interés que puedan afectar la seguridad, confidencialidad, neutralidad o adecuada prestación de los servicios vinculados al SFA.

80.2 Los participantes deben mantener un registro actualizado de los proveedores que operen el “servidor de autorización”, el “servidor de recursos”, la “aplicación cliente” o que gestionen llaves, certificados digitales, credenciales u otros elementos cuya indisponibilidad, alteración o compromiso pueda afectar la seguridad, interoperabilidad o continuidad de su participación en el SFA, así como de los componentes y servicios bajo su responsabilidad. Estos servicios se consideran significativos para efectos del SFA y se sujetan a los artículos 35 y 36 del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, y al artículo 14 del Reglamento para la Gestión del Riesgo Operacional, en lo que resulte compatible con la naturaleza del participante y con las actividades que realiza en el SFA.

80.3 Los certificados digitales y credenciales del participante se emiten a su nombre y no pueden compartirse con otros participantes, aun cuando un mismo proveedor opere los componentes de varios de ellos. El participante debe asegurar que el proveedor segregue los datos, certificados digitales, credenciales, llaves y demás material criptográfico de cada participante.

80.4 Los proveedores no adquieren la condición de participante ni pueden acceder a los datos del usuario por cuenta propia o utilizarlos para finalidades distintas de las autorizadas al participante que los contrata.

80.5 Los contratos correspondientes a servicios significativos deben contener cláusulas que permitan que el participante, la Superintendencia o las personas que esta designe, así como la función de auditoría interna y los auditores externos, cuando corresponda, accedan a la información, documentación, registros, sistemas, instalaciones y demás evidencias necesarias para revisar la prestación y verificar el cumplimiento de las obligaciones aplicables.

80.6 La contratación de proveedores de servicios técnicos se sujeta, adicionalmente, a los artículos 22 y 23 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, y a las demás disposiciones sobre servicios provistos por terceros que resulten aplicables. Cuando la contratación se encuentre comprendida en alguno de los supuestos establecidos en el artículo 37 del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, el participante debe obtener previamente la autorización correspondiente.

CAPÍTULO III

CALIDAD DE DATOS

SUBCAPÍTULO I

RESPONSABILIDADES Y GESTIÓN DE LA CALIDAD DE DATOS

Artículo 81. Responsabilidad general de los participantes

81.1 Los participantes deben incorporar los datos suministrados, recibidos o tratados mediante el SFA en sus políticas, responsabilidades y procesos de gobierno de datos, así como en su gestión de riesgos y sistema de control interno, según la normativa que les resulte aplicable.

81.2 Los participantes deben evaluar periódicamente la efectividad de las políticas, responsabilidades, procesos y controles implementados para gestionar la calidad de los datos objeto de suministro, recepción o tratamiento mediante el SFA, y adoptar las medidas necesarias para subsanar las deficiencias identificadas. Los resultados de dichas evaluaciones y las medidas adoptadas deben documentarse y mantenerse a disposición de la Superintendencia. Cuando la normativa aplicable exija una revisión independiente o la intervención de la función de auditoría interna, la evaluación debe realizarse conforme a dicha normativa.

Artículo 82. Responsabilidades de los participantes según el rol

82.1 Sin perjuicio de las responsabilidades previstas en los artículos 11 y 13, las EPD y las ERD deben cumplir las siguientes responsabilidades en materia de calidad de datos, según el rol que desempeñen:

a) Las EPD deben:
   i. validar los datos en origen mediante la aplicación de controles de calidad antes de su puesta a disposición a través de las APIs del SFA;
   ii. asegurar que los datos puestos a disposición mediante las APIs del SFA no presenten condiciones inferiores de alcance, exactitud, completitud, actualización y disponibilidad respecto de los proporcionados al usuario a través de sus canales digitales propios comparables;
   iii. cumplir las especificaciones técnicas aplicables, incluidos los formatos, estructuras, catálogos, reglas de validación y versiones vigentes; y
   iv. generar y conservar registros y evidencias sobre la validación, puesta a disposición y transmisión de los datos, así como sobre los incidentes de calidad relacionados con dichos datos.

b) Las ERD deben:
   i. validar los datos recibidos, verificando, según corresponda, su integridad, formato, consistencia, vigencia y correspondencia con la autorización otorgada por el usuario;
   ii. mantener la trazabilidad de los datos recibidos y de las transformaciones realizadas sobre estos;
   iii. reportar oportunamente a la EPD correspondiente las anomalías o incidentes de calidad identificados respecto de los datos recibidos; y
   iv. gestionar los datos almacenados temporalmente o en caché, evitando utilizar datos vencidos, desactualizados o no autorizados como si fueran vigentes.

Artículo 83. Gestión de riesgos asociados a la calidad de datos

83.1 Los participantes deben identificar, evaluar, gestionar y monitorear los riesgos asociados a la calidad de los datos suministrados, recibidos o tratados mediante el SFA, en el marco de su gobierno de datos y del sistema de gestión de riesgos que les resulte aplicable.

SUBCAPÍTULO II

TRAZABILIDAD, CONTROLES Y EVIDENCIAS

Artículo 84. Trazabilidad de los datos

84.1 Los participantes deben contar, de manera proporcional al rol que desempeñen, a la complejidad de sus operaciones y al volumen y criticidad de los datos, con capacidades, herramientas tecnológicas, procedimientos y registros que permitan mantener la trazabilidad de los datos suministrados, recibidos o tratados mediante el SFA.

84.2 La trazabilidad debe permitir identificar y reconstruir, según corresponda:

a) el recorrido del dato desde la fuente autoritativa o sistema de origen hasta su puesta a disposición a través de la API;
b) su recepción, almacenamiento y utilización por la ERD; y
c) las validaciones, transformaciones, transferencias y procesos de eliminación realizados durante dicho recorrido.

Artículo 85. Controles de calidad de datos

85.1 Los participantes deben implementar, de manera proporcional al rol que desempeñen, a la criticidad de los datos, el volumen de operaciones y los riesgos identificados, controles de calidad de datos en las siguientes etapas, cuando correspondan:

a) Captura u origen: validación de la exactitud, completitud, oportunidad y consistencia de los datos respecto de la fuente autoritativa o sistema de origen aplicable.
b) Transformación: control de las reglas de negocio, catálogos, formatos y demás condiciones establecidas en el gobierno de datos del participante.
c) Almacenamiento: controles de integridad, unicidad, consistencia y prevención de alteraciones no autorizadas.
d) Exposición mediante API: verificación de la conformidad con el esquema técnico, la oportunidad de actualización, la disponibilidad, la integridad y la consistencia de la respuesta.

Artículo 86. Registros y evidencias de calidad de datos

86.1 Los participantes deben generar y conservar registros y evidencias suficientes de la trazabilidad, los controles de calidad, las incidencias identificadas y las acciones correctivas aplicadas. Dichos registros y evidencias deben protegerse contra alteraciones no autorizadas y mantenerse íntegros, disponibles y accesibles oportunamente para fines de supervisión, auditoría, investigación de incidentes y resolución de disputas, durante los plazos establecidos en la normativa aplicable.

SUBCAPÍTULO III

MEDICIÓN, EVALUACIÓN Y REMEDIACIÓN

Artículo 87. Dimensiones de calidad de datos

87.1 La evaluación de la calidad de datos en el marco del SFA, prevista en el artículo 89 comprende, como mínimo, las siguientes dimensiones:

a) Exactitud: grado en que el dato representa correctamente la información contenida en la fuente autoritativa o sistema de origen correspondiente.
b) Completitud: grado en que se encuentran presentes los registros y campos obligatorios previstos en las especificaciones técnicas del SFA.
c) Consistencia: grado en que se preservan las relaciones, dependencias y restricciones aplicables a los datos durante su generación, almacenamiento, transformación y transmisión.
d) Integridad: grado en que un mismo dato mantiene valores coherentes entre sistemas, registros, canales y momentos de consulta, considerando las reglas de actualización aplicables.
e) Oportunidad: grado en que los datos se encuentran disponibles y actualizados de acuerdo con las condiciones aplicables.
f) Validez: grado en que los datos cumplen los formatos, catálogos, dominios, reglas de negocio y especificaciones técnicas aplicables.
g) Unicidad: grado en que cada registro o evento se encuentra representado una sola vez, salvo que su repetición se encuentre justificada por la naturaleza del dato o del servicio.

Artículo 88. Indicadores, métricas y umbrales

88.1 Los participantes deben calcular indicadores de calidad de datos respecto de las dimensiones previstas en el artículo 87, conforme a las métricas, fórmulas, reglas de cálculo y, cuando corresponda, umbrales mínimos establecidos por la Superintendencia mediante el Anexo N° 8.

88.2 Los resultados de la medición de indicadores deben permitir identificar, como mínimo, el universo o volumen total evaluado, el número y porcentaje de registros conformes y no conformes, las principales causas de no conformidad y la evolución respecto de periodos anteriores.

88.3 Los indicadores correspondientes a distintas dimensiones de calidad no deben compensarse entre sí. El cumplimiento o resultado favorable en una dimensión no subsana el incumplimiento, desviación o deficiencia en otra.

88.4 Los umbrales establecidos en el Anexo N° 8 constituyen niveles mínimos de cumplimiento. Los participantes pueden establecer niveles internos superiores, considerando la criticidad, finalidad y riesgos asociados a los datos.

88.5 La Superintendencia puede establecer periodos de adecuación, niveles diferenciados o esquemas de implementación gradual para el cumplimiento de las métricas y umbrales previstos en el Anexo N° 8, considerando las categorías de datos, los roles desempeñados, la materialidad y los riesgos asociados, la criticidad de la información y el avance de la implementación del SFA. La aplicación de dichos periodos, niveles o esquemas no exime a los participantes de adoptar, sin demora injustificada, las medidas necesarias cuando una deficiencia de calidad pueda ocasionar un perjuicio material al usuario, afectar la prestación del servicio o comprometer el adecuado funcionamiento del SFA.

Artículo 89. Evaluación, monitoreo y remediación de la calidad de datos

89.1 Los participantes deben evaluar y monitorear la calidad de los datos suministrados, recibidos o tratados mediante el SFA y remediar las deficiencias que afecten o tengan una probabilidad razonable de afectar de manera material las dimensiones previstas en el artículo 87.

89.2 Las EPD deben realizar pruebas de calidad de datos, como mínimo, con periodicidad semestral y, cuando corresponda, mediante criterios aleatorios, muestrales o basados en riesgos. Los resultados deben remitirse a la Superintendencia y ponerse a disposición de los participantes involucrados, en la forma, alcance y condiciones que establezca la Superintendencia.

89.3 Las EPD deben realizar, adicionalmente las pruebas señaladas en el párrafo 89.2:

h) cuando introduzcan cambios materiales en sus sistemas fuente, reglas de transformación, modelos de datos, infraestructura o mecanismos de exposición mediante API; y
i) después de incidentes significativos de calidad de datos.

89.4 Las ERD deben realizar, con periodicidad anual, pruebas de calidad respecto de los procesos bajo su responsabilidad, especialmente cuando efectúen transformaciones, agregaciones, inferencias, enriquecimientos, almacenamiento, integración con otras fuentes o generación de datos derivados.

89.5 Las evaluaciones y pruebas de calidad deben comprender, como mínimo, los indicadores previstos en el Anexo N° 8 que resulten aplicables y permitir evaluar, según corresponda, la exactitud y comparabilidad con la fuente autoritativa o sistema de origen, la consistencia entre fuentes, sistemas, canales y momentos de consulta, la conformidad técnica, la completitud, validez, oportunidad, unicidad e integridad de los datos, así como identificar los errores, su impacto, sus causas y las medidas correctivas aplicable.

89.6 Los resultados remitidos a la Superintendencia deben incluir, como mínimo, el universo evaluado, el periodo de referencia, el volumen de registros evaluados, el número y porcentaje de registros conformes y no conformes, las principales causas de no conformidad, las medidas correctivas adoptadas o previstas y la evolución respecto de periodos anteriores.

89.7 Cuando un indicador se ubique por debajo del umbral mínimo aplicable establecido en el Anexo N° 8, el participante debe adoptar las medidas necesarias para corregir la deficiencia y elaborar un plan de remediación. Cuando la deficiencia sea significativa conforme a los criterios previstos en dicho Anexo, el participante debe informar a la Superintendencia, sin demora injustificada, desde que determine o razonablemente deba determinar su existencia. El plan de remediación debe incluir, como mínimo, la descripción de la deficiencia, sus causas e impacto, los datos, APIs o servicios afectados, las medidas correctivas, los responsables, los plazos y los mecanismos para verificar su efectividad.

89.8 La Superintendencia puede disponer, en cualquier momento, evaluaciones extraordinarias, pruebas específicas, requerimientos de información, exámenes, auditorías, revisiones independientes o verificaciones técnicas. Para tal efecto, los participantes deben poner a su disposición la información, documentación, registros, evidencias, programas o códigos utilizados para efectuar las validaciones, reglas de validación, registros técnicos, reportes y demás elementos que les sean requeridos.

89.9 La Superintendencia puede disponer medidas preventivas, correctivas o de mitigación, incluidas la corrección de datos, la implementación de controles adicionales, la intensificación del monitoreo, la presentación de reportes especiales y la restricción o suspensión temporal de funcionalidades, APIs, *endpoints* o intercambios específicos, así como otras medidas proporcionales al riesgo identificado, conforme al marco normativo aplicable.

89.10 Los participantes deben generar y conservar evidencias de las evaluaciones, actividades de monitoreo, desviaciones, análisis de causas, comunicaciones, planes de remediación, acciones correctivas, verificaciones de efectividad y reportes remitidos, de conformidad con el artículo 86.

ANEXOS

Los anexos previstos en el presente Reglamento, distintos de los Anexos N° 1 al 4, publicados para consulta pública mediante Resolución SBS N° 02433-2026, y de los Anexos N° 5 al 9, comprendidos en la presente resolución, serán desarrollados y aprobados posteriormente mediante resolución de la Superintendencia.

ANEXO N° 1

[...]

ANEXO N° 2

[...]

ANEXO N° 3

[...]

ANEXO N° 4

[...]

ANEXO N° 5
DIRECTORIO DE PARTICIPANTES Y ESTADOS OPERATIVOS

I. INFORMACIÓN REGISTRADA EN EL DIRECTORIO DE PARTICIPANTES

1. Categorías de información

El Directorio de Participantes puede registrar, según corresponda, las siguientes categorías de información:

a) Información de identificación
   Comprende la información necesaria para identificar a las entidades solicitantes, participantes y representantes autorizados vinculados al SFA.

b) Información sobre roles y estados
   Comprende la información relativa a los roles para los cuales una entidad se encuentra registrada, habilitada, suspendida, retirada, cancelada o en mantenimiento, así como cualquier otra condición regulatoria relevante para su participación en el Sistema.

c) Información de contacto
   Comprende la información de los responsables regulatorios, técnicos, operativos y de seguridad, entre otros, designados para interactuar con la Superintendencia y con los demás participantes del SFA.

d) Información sobre componentes registrados
   Comprende la información referida a aplicaciones, servidores, interfaces, componentes tecnológicos y demás elementos necesarios para la participación dentro del SFA.

e) Información de descubrimiento e interoperabilidad
   Comprende los metadatos y demás información necesaria para la identificación, localización, autenticación, configuración e interoperabilidad entre participantes, aplicaciones y componentes registrados en el SFA.

f) Información sobre elementos de confianza
   Comprende la información relativa a certificados digitales, credenciales, identificadores, declaraciones de *software*, llaves públicas y demás elementos utilizados para la identificación y confianza entre participantes.

g) Información sobre conformidades y certificaciones
   Comprende la información relativa a conformidades funcionales, certificaciones, validaciones técnicas y demás requisitos exigibles para la incorporación, habilitación o permanencia de los participantes en el SFA.

h) Información sobre estados operativos
   Comprende la información relativa a mantenimientos, indisponibilidades, restricciones técnicas, degradaciones operativas y demás eventos relevantes para la operación del Sistema.

i) Información histórica y de trazabilidad
   Comprende la información necesaria para registrar los cambios efectuados sobre la información administrada por el Directorio de Participantes, los estados aplicables y demás eventos relevantes asociados a la participación en el SFA.

j) Otra información necesaria para el cumplimiento de las funciones del Directorio de Participantes.

2. Responsabilidad sobre la información registrada en el Directorio de Participantes

Los participantes son responsables de la exactitud, completitud, integridad y actualización de la información registrada en el Directorio de Participantes cuya administración, comunicación o mantenimiento se encuentre a su cargo. Las modificaciones que afecten la información registrada deben ser comunicadas o actualizadas conforme a las condiciones establecidas por la Superintendencia.

La información registrada en el Directorio de Participantes constituye la fuente oficial del SFA respecto de los participantes, sus roles, estados y demás elementos que resulten aplicables.

II. NIVELES DE ACCESO A LA INFORMACIÓN

La información administrada por el Directorio de Participantes se clasifica en las siguientes categorías de acceso:

a) Información de acceso público

Comprende la información cuya difusión resulta necesaria para promover la transparencia y el adecuado funcionamiento del SFA. La Superintendencia puede ponerla a disposición del público a través del Portal del SFA u otros medios que esta establezca.

Como mínimo, tiene carácter público la información relativa a la identificación de los participantes habilitados, los roles que desempeñan y sus estados vigentes.

b) Información disponible para los participantes

Comprende la información necesaria para la identificación, validación, autenticación, interoperabilidad e interacción operativa entre los participantes y los componentes habilitados del SFA.

c) Información restringida

Comprende la información disponible únicamente para la Superintendencia, para el participante al que corresponde o para las personas expresamente autorizadas, atendiendo a su naturaleza, finalidad, sensibilidad o requerimiento de seguridad.

III. ESTADOS REGISTRADOS

1. Estado aplicable durante la incorporación

a) En habilitación técnica

Corresponde a la entidad que ha culminado satisfactoriamente la etapa de registro y se encuentra ejecutando las pruebas, validaciones, conformidades, certificaciones y demás actuaciones necesarias para obtener la habilitación correspondiente.

Bajo este estado, la entidad puede realizar las actividades expresamente autorizadas para los procesos de habilitación técnica y utilizar los ambientes, componentes y herramientas necesarias para obtener su habilitación correspondiente. No obstante, no se encuentra habilitada para intercambiar datos o información en el ambiente de producción ni para desempeñar el rol respecto del cual se encuentra en proceso de habilitación.

La condición de *En habilitación técnica* concluye cuando la Superintendencia otorga la habilitación correspondiente o cuando determina la terminación del procedimiento aplicable.

2. Estados aplicables a los participantes

a) Habilitado

Corresponde al participante que cumple las condiciones regulatorias, técnicas y operativas aplicables al rol correspondiente y cuenta con autorización para operar en el ambiente de producción del SFA.

La condición de *Habilitado* permite al participante ejercer los derechos y asumir las obligaciones correspondientes al rol para el cual se encuentra habilitado, de conformidad con el Reglamento.

La habilitación se registra de manera independiente respecto de cada rol que desempeñe el participante.

b) Suspendido

Corresponde al participante respecto del cual la Superintendencia ha suspendido temporalmente la habilitación correspondiente a uno o más roles, de acuerdo a lo establecido en el artículo 22.

Mientras se mantenga la suspensión, el participante no puede ejercer las actividades comprendidas en el alcance del rol suspendido ni acceder a las funcionalidades cuya utilización requiera la habilitación afectada, sin perjuicio de las demás obligaciones que continúen siendo exigibles.

La suspensión se mantiene vigente hasta que la Superintendencia disponga su levantamiento o adopte otra decisión respecto de la habilitación correspondiente.

c) Retirado

Corresponde al participante respecto del cual la Superintendencia ha aprobado el retiro voluntario de uno o más roles desempeñados dentro del SFA, cuando resulte aplicable.

El estado de *Retirado* determina el cese de los derechos asociados al rol correspondiente, sin perjuicio de las obligaciones de conservación de información, colaboración, atención de requerimientos, resolución de disputas u otras obligaciones que continúen vigentes conforme a la normativa aplicable.

d) Cancelado

Corresponde al participante cuya habilitación respecto de uno o más roles ha sido cancelada por decisión de la Superintendencia.

La cancelación determina la pérdida de la habilitación correspondiente y la imposibilidad de continuar desempeñando el rol afectado dentro del SFA.

La información asociada al participante, al rol cancelado y a los eventos vinculados con su participación debe conservarse para fines de trazabilidad, supervisión, auditoría, investigación de incidentes y resolución de disputas.

e) En mantenimiento

Corresponde al participante que, respecto de uno o más roles, ha comunicado la ejecución de actividades de mantenimiento programado que afectan temporalmente su capacidad para intercambiar datos o prestar servicios en el SFA.

Mientras se mantenga este estado, el participante conserva su habilitación y continúa sujeto a las obligaciones previstas en el Reglamento, sin perjuicio de las limitaciones operativas derivadas del mantenimiento correspondiente.

El estado de *En mantenimiento* debe registrarse previamente a la ejecución de las actividades programadas y mantenerse únicamente durante el periodo informado para su realización.

La conclusión del mantenimiento determina el retorno al estado de *Habilitado*, salvo que durante su ejecución se configure alguna circunstancia que justifique la aplicación de otro estado conforme al Reglamento.

3. Estados aplicables a los componentes tecnológicos

Los estados operativos permiten reflejar la situación de las aplicaciones, servidores, APIs y demás componentes técnicos registrados en el Directorio de Participantes cuyo funcionamiento resulte relevante para la interacción entre participantes.

a) Operativo

Corresponde a la aplicación o componente tecnológico que se encuentra disponible para su utilización en el ambiente respectivo y que opera conforme a las condiciones técnicas declaradas por el participante o registradas en el Directorio de Participantes.

La condición de *Operativo* implica que el componente puede ser utilizado para las finalidades previstas en el SFA.

b) Operación degradada

Corresponde a la aplicación o componente tecnológico que mantiene disponibilidad para su utilización, pero presenta una reducción en su capacidad, desempeño, funcionalidad o calidad de servicio.

La condición de *Operación degradada* no impide necesariamente la utilización del componente, pero advierte la existencia de limitaciones que pueden afectar su funcionamiento normal o el cumplimiento de los niveles de servicio aplicables.

c) Mantenimiento programado

Corresponde a la aplicación o componente tecnológico que se encuentra temporalmente fuera de servicio debido a actividades de mantenimiento previamente planificadas y comunicadas.

La condición de *Mantenimiento programado* debe registrarse con anterioridad, como mínimo 5 días calendario, al inicio de la ventana de mantenimiento correspondiente y mantenerse hasta la finalización de las actividades programadas.

d) Indisponibilidad no programada

Corresponde a la aplicación o componente tecnológico que se encuentra fuera de servicio como consecuencia de una falla, incidente, contingencia o cualquier otro evento no planificado que afecte su disponibilidad.

La condición de *Indisponibilidad no programada* debe registrarse tan pronto como resulte razonablemente posible desde que el participante tome conocimiento de dicha situación.

e) Restringido técnicamente

Corresponde a la aplicación o componente tecnológico cuyo uso se encuentra limitado total o parcialmente como medida preventiva, correctiva, de contención o de gestión de riesgos, conforme a las reglas establecidas por la Superintendencia.

La condición de *Restringido técnicamente* puede aplicarse respecto de determinadas funcionalidades, interfaces, servicios, participantes, ambientes o categorías de intercambio, según corresponda.

f) Fuera de producción

Corresponde a la aplicación o componente tecnológico que ha dejado de encontrarse autorizado para su utilización en el ambiente de producción.

La condición de *Fuera de producción* no implica la eliminación de la información registrada en el Directorio de Participantes y permite conservar la información histórica asociada al componente para fines de trazabilidad, supervisión, auditoría, investigación de incidentes y resolución de disputas.

4. Consideraciones generales sobre los estados

Alcance de los estados

Los estados registrados en el Directorio de Participantes pueden aplicarse de manera independiente respecto de entidades solicitantes, participantes, roles, aplicaciones, servidores, APIs, certificados, credenciales, versiones o cualquier otro componente cuya gestión se encuentre comprendida dentro del SFA.

El registro de un estado produce efectos únicamente respecto del elemento al cual resulta aplicable, salvo que la naturaleza del evento o una disposición expresa determine un alcance diferente.

Los estados registrados en el Directorio de Participantes no sustituyen las decisiones, autorizaciones o medidas que correspondan a la Superintendencia conforme al Reglamento.

Información publicada respecto de los estados

El Directorio de Participantes debe registrar, como mínimo, el estado vigente, la fecha y hora de su registro, la fecha y hora a partir de la cual produce efectos y la información necesaria para identificar el elemento al que dicho estado corresponde.

La Superintendencia determina la información relacionada a cada estado que tiene carácter público, aquella disponible para los participantes y aquella considerada restringida, considerando la naturaleza de la información, las necesidades de interoperabilidad y los objetivos de seguridad y funcionamiento del SFA.

La publicación de un estado no debe revelar información cuya divulgación pueda comprometer la seguridad, integridad o adecuado funcionamiento del Sistema o de sus participantes.

Conservación de estados históricos

Todo cambio de estado se conserva como parte de la información histórica administrada por el Directorio de Participantes.

La información histórica permite identificar, como mínimo, los estados anteriores y vigentes, la fecha y hora de cada cambio y el elemento respecto del cual dicho cambio fue efectuado.

Los registros históricos se conservan para fines de supervisión, auditoría, monitoreo, investigación de incidentes, resolución de disputas y verificación del cumplimiento de las obligaciones aplicables a los participantes del SFA.

IV. TRANSICIONES Y EVENTOS

1. Transiciones de estados

Las transiciones de estado reflejan los cambios que experimentan las entidades solicitantes, participantes, roles, aplicaciones y demás componentes registrados en el Directorio de Participantes como consecuencia de actuaciones regulatorias, operativas o técnicas.

Las transiciones únicamente pueden realizarse entre los estados expresamente previstos para cada categoría de elemento registrado. No se permiten transiciones directas entre estados incompatibles ni la asignación simultánea de estados mutuamente excluyentes.

Corresponde a la Superintendencia efectuar las transiciones asociadas a los procesos de incorporación, habilitación, suspensión, retiro y cancelación de participantes, así como aquellas que deriven de decisiones adoptadas en el ejercicio de sus funciones.

Corresponde a los participantes registrar o comunicar los eventos operativos cuya declaración se encuentre bajo su responsabilidad, incluyendo aquellos relacionados con aplicaciones, componentes técnicos, mantenimientos programados, restricciones técnicas e indisponibilidades.

Toda transición debe encontrarse sustentada en un evento identificable y registrarse de manera que permita conocer, como mínimo:

a) el elemento afectado;
b) el nuevo estado;
c) la fecha y hora del cambio;
d) el responsable de la transición;
e) el evento que la originó; y
f) la fecha y hora a partir de la cual produce efectos.

2. Eventos sujetos a registro o notificación

Deben registrarse en el Directorio de Participantes o notificarse mediante los mecanismos establecidos por la Superintendencia, según corresponda, los eventos que puedan afectar la identificación, habilitación, interoperabilidad, seguridad, disponibilidad o funcionamiento de los participantes y componentes registrados en el SFA.

Como mínimo, se encuentran sujetos a registro o notificación los siguientes eventos:

a) Habilitación: Comprende el otorgamiento, modificación, ampliación o reactivación de habilitaciones aplicables a uno o más roles dentro del SFA.
b) Suspensión: Comprende toda suspensión temporal de la habilitación de un participante o de alguno de sus roles, así como el levantamiento de dicha medida.
c) Retiro: Comprende la aprobación y ejecución del retiro voluntario de uno o más roles desempeñados por un participante.
d) Cancelación: Comprende la cancelación de la habilitación correspondiente a uno o más roles y cualquier actuación asociada a dicho estado.
e) Modificaciones relevantes de aplicaciones o componentes técnicos: Comprende los cambios que afecten la identificación, configuración, funcionalidad, interoperabilidad,

certificación, seguridad o condiciones de operación de aplicaciones, servidores, APIs u otros componentes registrados.

f) Registro, sustitución, suspensión, vencimiento o revocación de certificados y demás elementos de confianza: Comprende los eventos relacionados con certificados digitales, credenciales, declaraciones de *software*, llaves públicas y demás elementos cuya utilización resulte necesaria para la operación del SFA.

g) Restricciones técnicas: Comprende la imposición, modificación o levantamiento de limitaciones que afecten total o parcialmente la utilización de aplicaciones, servicios o componentes registrados.

h) Mantenimiento programado: Comprende las actividades de mantenimiento previamente planificadas que puedan afectar la disponibilidad o funcionamiento de aplicaciones y componentes técnicos.

i) Indisponibilidades y operación degradada: Comprende las situaciones que afecten la disponibilidad, capacidad o desempeño normal de las aplicaciones o componentes registrados, así como su posterior restablecimiento.

j) Otros eventos relevantes: Comprende cualquier otro evento que pueda afectar las condiciones bajo las cuales un participante, rol, aplicación o componente se encuentra registrado, habilitado o disponible para operar en el SFA.

3. Matriz de transiciones de estados de incorporación y participación

Estado de origen	Evento desencadenante	Estado de destino	Responsable
Ninguno	Aprobación de la etapa de registro	En habilitación técnica	Superintendencia
En habilitación técnica	Otorgamiento de la habilitación correspondiente	Habilitado	Superintendencia
Habilitado	Inicio de mantenimiento programado del rol asociado	En mantenimiento	Participante
Habilitado	Suspensión de la habilitación	Suspendido	Superintendencia
Habilitado/ En mantenimiento / Suspendido	Aprobación del retiro voluntario, de acuerdo con el procedimiento correspondiente	Retirado	Superintendencia
Habilitado / En mantenimiento / Suspendido	Cancelación de la habilitación	Cancelado	Superintendencia
En mantenimiento	Finalización del mantenimiento programado	Habilitado	Participante
Suspendido	Levantamiento de la suspensión	Habilitado	Superintendencia
Retirado	Otorgamiento de la habilitación correspondiente	Habilitado	Superintendencia

4. Matriz de transiciones de estados operativos de componentes tecnológicos

Estado de origen	Evento desencadenante	Estado de destino	Responsable
Operativo	Inicio de mantenimiento programado	Mantenimiento programado	Participante
Operativo	Deterioro del servicio o reducción relevante de capacidad o funcionalidad	Operación degradada	Participante
Operativo	Falla, incidente o contingencia	Indisponibilidad no programada	Participante

Operativo	Aplicación de una limitación preventiva o correctiva	Restringido técnicamente	Participante o Superintendencia
Operativo	Retiro definitivo del componente del ambiente de producción	Fuera de producción	Participante
Mantenimiento programado	Finalización del mantenimiento	Operativo	Participante
Mantenimiento programado	Ocurrencia de una falla durante el mantenimiento	Indisponibilidad no programada	Participante
Operación degradada	Restablecimiento de las condiciones normales de funcionamiento	Operativo	Participante
Operación degradada	Agravamiento de la afectación que impida la prestación del servicio	Indisponibilidad no programada	Participante
Operación degradada	Aplicación de una limitación preventiva o correctiva	Restringido técnicamente	Participante o Superintendencia
Indisponibilidad no programada	Restablecimiento del servicio	Operativo	Participante
Indisponibilidad no programada	Aplicación de medidas de contención o limitación	Restringido técnicamente	Participante o Superintendencia
Restringido técnicamente	Levantamiento de la restricción	Operativo	Superintendencia
Restringido técnicamente	Retiro definitivo del componente	Fuera de producción	Superintendencia

V. COPIA LOCAL Y CONTINUIDAD DEL DIRECTORIO DE PARTICIPANTES

1. Utilización de la copia local durante una indisponibilidad del Directorio de Participantes

Durante una indisponibilidad temporal del Directorio de Participantes, la utilización de la copia local se encuentra sujeta a las siguientes condiciones:

a) Solo puede utilizarse la última versión de la información obtenida y actualizada conforme a las disposiciones del artículo 48.
b) La información utilizada debe corresponder únicamente a los participantes, roles, aplicaciones, componentes y elementos del Marco de Confianza que no hayan sido invalidados conforme a las reglas establecidas en el presente Anexo.
c) No puede utilizarse información respecto de la cual el participante haya recibido una comunicación posterior que modifique su estado, vigencia o condición de utilización.
d) La copia local no puede utilizarse para registrar, modificar o actualizar información en el Directorio de Participantes.
e) La copia local no puede utilizarse para omitir las verificaciones o controles exigidos por el Marco de Confianza o por el Perfil de Seguridad.
f) La copia local únicamente puede utilizarse hasta que el Directorio de Participantes recupere su disponibilidad y el participante pueda restablecer la consulta de la información oficial.

La Superintendencia establece el procedimiento para la copia local en el Manual del Directorio de Participantes, disponible en el Portal del Desarrollador.

2. Invalidación de información mantenida en la copia local

La invalidación de información implica que esta deja de ser apta para ser utilizada por los participantes para verificar la identidad, habilitación, estado, autorización o condiciones de

operación de participantes, roles, aplicaciones, componentes o elementos del Marco de Confianza.

La invalidación debe aplicarse respecto de la información directamente afectada por el evento comunicado, sin perjuicio de que también alcance a los elementos vinculados cuando ello resulte necesario para preservar la seguridad, integridad o funcionamiento del SFA.

Como mínimo, deben invalidarse:

a) La información relativa a los roles cuya habilitación haya sido suspendida o cancelada.
b) La información relativa a aplicaciones, APIs, servidores u otros componentes sujetos a restricciones técnicas que limiten su utilización.
c) La información relativa a certificados digitales suspendidos, revocados, vencidos o comprometidos.
d) La información relativa a credenciales, declaraciones de *software*, llaves públicas u otros elementos del Marco de Confianza que hayan perdido vigencia o hayan sido comprometidos.
e) La información cuya validez dependa de un elemento previamente invalidado.

La información invalidada no puede ser utilizada para establecer nuevas interacciones, validar participantes, autorizar accesos o verificar condiciones de operación dentro del SFA.

La información invalidada solo puede volver a ser utilizada cuando el Directorio de Participantes registre nuevamente una condición vigente que permita su utilización o cuando se encuentre asociada a un nuevo elemento debidamente registrado y habilitado.

3. Restablecimiento

Una vez restablecida la disponibilidad del Directorio de Participantes, los participantes deben actualizar su copia local utilizando la información vigente del Directorio de Participantes.

La información obtenida directamente del Directorio de Participantes prevalece sobre cualquier información previamente almacenada en la copia local.

Los participantes deben adoptar las medidas necesarias para asegurar que la información utilizada durante la contingencia sea reemplazada por la información actualizada del Directorio de Participantes tan pronto como resulte posible.

ANEXO N° 6

DISEÑO, NIVELES DE SERVICIO Y GESTIÓN DE VERSIONES DE LAS APIs DEL SFA

I. REQUISITOS DE DISEÑO DE APIs DEL SFA

1. Alcance y principios

Los requisitos de la presente sección desarrollan los estándares y las especificaciones técnicas previstos en el artículo 68 y son aplicables a todas las APIs utilizadas para acceder a los datos e información comprendidos en el artículo 9 del Reglamento o suministrarlos.

Las APIs del SFA se diseñan conforme a los siguientes principios:

a) Estándar común: las especificaciones de las APIs son únicas para todo el Sistema y son aprobadas por la Superintendencia y publicadas en el Portal del Desarrollador. Las EPD las implementan sin alterar su estructura, semántica ni comportamiento.
b) Mínima necesidad: las APIs exponen únicamente los datos comprendidos en el Anexo N° 3 que correspondan al alcance autorizado por el usuario.
c) Previsibilidad: un mismo recurso, error o situación se representa de la misma forma en todas las APIs y en todas las EPD.
d) Evolución controlada: los cambios se introducen conforme a las reglas de gestión de versiones de la sección III del presente Anexo, preservando la compatibilidad siempre que sea posible.

Las EPD deben implementar las especificaciones de las APIs conforme al párrafo 68.4 del Reglamento, sin incorporar requisitos técnicos adicionales a los previstos en dichas especificaciones.

2. Especificación de las APIs

Cada API del SFA cuenta con una especificación oficial elaborada conforme al estándar OpenAPI. La especificación oficial define, como mínimo, los recursos, operaciones, parámetros, esquemas de solicitud y respuesta, encabezados, códigos de respuesta, errores y ejemplos.

Los esquemas de datos contenidos en la especificación oficial deben corresponder al modelo y diccionario de datos del Anexo N° 3. Los campos se clasifican como obligatorios, condicionales u opcionales.

3. Recursos, rutas y operaciones

Las APIs se organizan en torno a recursos identificados mediante rutas estables y jerárquicas, que incluyen el grupo de la API y la versión mayor, conforme a la estructura publicada en el Portal del Desarrollador. Las rutas emplean sustantivos y no verbos.

Los métodos HTTP se utilizan conforme a su semántica estándar. Las operaciones de consulta emplean métodos seguros, que no modifican el estado de los recursos y pueden repetirse sin efectos adicionales.

Los identificadores de recursos que exponen las EPD son opacos, únicos y estables durante la vigencia de la autorización, y no deben corresponder a números de cuenta, tarjeta, documento de identidad ni a otros datos que identifiquen directamente al usuario o a sus productos.

4. Mensajes y representación de datos

Los mensajes emplean el formato JSON con codificación UTF-8 y siguen la estructura común de respuesta publicada en el Portal del Desarrollador.

Los datos se representan conforme a las siguientes reglas:

a) Fechas y horas: conforme a ISO 8601, con indicación de zona horaria.
b) Importes: como valores decimales exactos acompañados del código de moneda conforme a ISO 4217, sin redondeos ni representaciones en coma flotante.
c) Países, idiomas y demás códigos: conforme a los estándares ISO correspondientes o a los catálogos publicados en el Portal del Desarrollador.
d) Nombres de campos: conforme a la convención única de nomenclatura establecida en la especificación de cada API.

5. Encabezados

Las solicitudes y respuestas incluyen los encabezados establecidos en la especificación de cada API, entre ellos el identificador único de interacción y los encabezados de firma de mensajes exigidos por el Anexo N° 9. La EPD devuelve en la respuesta el identificador de interacción recibido o, en su defecto, el que genere.

6. Paginación, filtros y ordenamiento

Las operaciones que devuelven colecciones de recursos deben implementar paginación conforme al mecanismo establecido en la especificación de cada API, con enlaces de navegación hacia la página actual, siguiente y anterior, cuando existan. El número máximo de registros por página se publica en el Portal del Desarrollador, y la EPD no puede devolver páginas de un tamaño inferior al solicitado, salvo en la última página.

Las operaciones sobre movimientos y demás recursos con dimensión temporal admiten filtros por rango de fechas, conforme a la especificación oficial. El ordenamiento por defecto de cada colección es único y está definido en dicha especificación, de modo que consultas idénticas devuelvan resultados en el mismo orden.

7. Códigos de respuesta y errores

Las APIs emplean los códigos de estado HTTP conforme a su semántica estándar y a la tabla de uso publicada en el Portal del Desarrollador. Toda respuesta de error sigue la estructura común de error del SFA, que contiene un código del catálogo de errores, una descripción y, cuando corresponda, la referencia al campo o parámetro involucrado.

Los mensajes de error no deben revelar datos del usuario, la existencia de recursos fuera del alcance autorizado, información sobre la infraestructura de la EPD ni detalles que faciliten un

ataque. La solicitud de un recurso que no está comprendido en la autorización recibe la misma respuesta, sea que el recurso exista o no.

8. Idempotencia y reintentos

Las operaciones que modifiquen el estado de un recurso deben ser idempotentes o admitir una clave de idempotencia, conforme a la especificación de cada API, de modo que el reintento de una misma solicitud no produzca efectos duplicados. Las aplicaciones cliente deben aplicar estrategias de reintento con espera progresiva y no deben reintentar las solicitudes rechazadas por errores atribuibles a la propia solicitud.

9. Límites de consumo

Cuando un participante aplique límites de consumo, debe comunicar su superación mediante un código de estado HTTP e indicar el tiempo de espera aplicable. Los límites y las condiciones de su aplicación se rigen por la sección II del presente Anexo.

10. Descubrimiento y estado de las APIs

Las EPD deben registrar en el Directorio de Participantes, conforme al Anexo N° 5, las URL base de sus APIs y las versiones implementadas. Asimismo, deben exponer un *endpoint* de estado que informe la disponibilidad de cada API y las ventanas de mantenimiento programado, conforme a la especificación aplicable.

11. APIs de información sin consentimiento

Las APIs que exponen la información a que se refiere el párrafo 69.4 del artículo 69 deben cumplir los lineamientos de la presente sección, con excepción de aquellos relativos a la autenticación y autorización del usuario. El acceso a dichas APIs no requiere consentimiento, sin perjuicio de los requisitos de autenticación de aplicaciones, cifrado de las comunicaciones, disponibilidad y demás condiciones aplicables conforme al presente Reglamento.

II. NIVELES DE SERVICIO DE LAS APIS DE INTERCAMBIO DE DATOS

1. Alcance y categorías

La presente sección establece los niveles de servicio exigibles a los participantes respecto de las APIs mediante las cuales intercambian datos e información en el ambiente de producción del SFA. Su alcance comprende los servidores de autorización y de recursos operados por las EPD y los *endpoints* de recepción de eventos operados por los participantes.

Para efectos de medición, los *endpoints* se agrupan en las siguientes categorías:

a) Seguridad: solicitud de autorización enviada previamente, emisión de *tokens*, registro dinámico, revocación, introspección, gestión de consentimientos y publicación de llaves.
b) Autorización: presentación al usuario de las interfaces de autenticación y confirmación de la EPD.
c) Recursos de consulta simple.
d) Recursos de consulta con paginación.
e) Recepción de notificaciones de eventos.

f) la información a que se refiere el párrafo 69.4 del artículo 69.

La asignación de cada *endpoint* a una categoría consta en la especificación de cada API.

2. Disponibilidad

La disponibilidad se calcula como la proporción del tiempo del periodo en que cada *endpoint* se encuentra operativo, determinada mediante monitoreo activo con la frecuencia y el método publicados en el Portal del Desarrollador. Un *endpoint* se considera indisponible durante todo intervalo de medición en que no responde, responde fuera del tiempo máximo de espera previsto en el numeral 3 o responde con errores atribuibles al participante que recibe la solicitud. Se excluyen las ventanas de mantenimiento programado comunicadas conforme al numeral 6 y las suspensiones dispuestas por la Superintendencia. La medición diaria comprende las veinticuatro horas del día calendario, hora oficial del Perú.

Los participantes deben cumplir los siguientes niveles mínimos de disponibilidad, en cada categoría de *endpoint*:

Periodo	Disponibilidad mínima
Mensual	[99,5 %]
Diaria	[95,0 %]

La indisponibilidad de los *endpoints* de seguridad se computa como indisponibilidad de todos los *endpoints* que dependen de estos.

3. Tiempo de respuesta

El tiempo de respuesta se mide desde la recepción completa de la solicitud en el perímetro del participante hasta el envío del último byte de la respuesta, excluyendo la latencia de la red de la contraparte. En los *endpoints* con paginación se mide por página. Los participantes deben cumplir los siguientes tiempos máximos, medidos mensualmente sobre el percentil 95 de las solicitudes de cada categoría:

Categoría	Tiempo máximo (percentil 95)
Seguridad	[1 000 ms]
Autorización	[2 000 ms]
Recursos de consulta simple	[1 000 ms]
Recursos de consulta con paginación	[1 500 ms] por página
Recepción de notificaciones de eventos	[1 000 ms] hasta el acuse
Información a que se refiere el párrafo 69.4	[1 500 ms]

Las solicitudes que no sean atendidas dentro de diez (10) segundos se consideran no atendidas y se computan como error atribuible al participante que recibe la solicitud.

4. Tasa de error

La tasa de error se calcula como la proporción de solicitudes que reciben una respuesta con error atribuible al participante que recibe la solicitud, respecto del total de solicitudes recibidas durante el periodo, por categoría de *endpoint*. La tasa de error no debe exceder el uno por ciento (1 %) mensual.

Se consideran errores atribuibles los errores de servidor y las solicitudes no atendidas conforme al numeral 3. No lo son los rechazos que el Reglamento, el Anexo N° 9 o la especificación de cada API exigen ante solicitudes no conformes, ni los rechazos por superación de límites de consumo conforme al numeral 5.

La tasa de error se mide durante los periodos en que el *endpoint* se encuentra disponible conforme al numeral 2, de modo que un mismo intervalo no se compute a la vez como indisponibilidad y como error.

5. Capacidad y limitación de tasa de consumo

La especificación de cada API establece la capacidad mínima que la EPD debe atender sin degradar los tiempos de respuesta del numeral 3 del presente Anexo, expresada como:

a) Solicitudes por segundo, en conjunto para todas las ERD.
b) Solicitudes por minuto, por ERD, para cada endpoint.

Las solicitudes por segundo se computan por API y por segundo calendario; las solicitudes por minuto, por cada combinación de *endpoint* y ERD y por minuto calendario. Para ambos cómputos se consideran las solicitudes procesadas con éxito y las rechazadas por causas atribuibles a la ERD o a su aplicación cliente.

La Superintendencia revisa periódicamente las capacidades mínimas considerando la demanda observada conforme a los reportes previstos en el numeral 7 y publica sus actualizaciones conforme al artículo 70 y a la sección III del presente Anexo.

Los límites aplicables a las solicitudes que deben atender las EPD se publican en el Portal del Desarrollador y deben cumplir las siguientes condiciones:

aplicarse en condiciones equivalentes a todos los participantes habilitados para el mismo rol, sin discriminación;

a) no ser inferiores a las capacidades mínimas aplicables a cada *endpoint*; y
b) no aplicarse a las solicitudes de revocación ni a las consultas sobre el estado de las autorizaciones.

Al superar un límite, el participante responde conforme al numeral 9 de la sección I. Las solicitudes rechazadas por superar límites declarados no se computan como indisponibilidad ni como error.

6. Mantenimiento programado y operación degradada

Las ventanas de mantenimiento programado no deben exceder ocho (8) horas por mes calendario y deben ejecutarse entre las 00:00 y las 06:00 horas, hora oficial del Perú. Asimismo, deben registrarse en el Directorio de Participantes y comunicarse a las contrapartes con una anticipación no menor de cinco (5) días hábiles, a través del *endpoint* de estado y de los mecanismos de comunicaciones operativas previstos en el artículo 57. Las ventanas que no cumplan estas condiciones se computan como indisponibilidad.

Cuando un participante opere en condiciones degradadas, debe informarlo a través del *endpoint* de estado. La operación degradada no exime del cumplimiento de los niveles de servicio. La rotación de certificados y llaves debe planificarse de modo que no genere interrupción del servicio.

7. Medición, reporte y publicación

Los participantes deben medir los indicadores de la presente sección utilizando una fuente de tiempo sincronizada y conservar las mediciones conforme al artículo 77. Asimismo, deben remitir a la Superintendencia un reporte mensual sobre disponibilidad, tiempo de respuesta, tasa de error y volumen de solicitudes por categoría de *endpoint*, de acuerdo con el formato y plazo publicados en el Portal del SFA.

8. Incumplimiento

Sin perjuicio de las acciones administrativas que correspondan, el incumplimiento de un nivel de servicio durante dos periodos mensuales consecutivos o tres periodos dentro de doce (12) meses obliga al participante responsable a remitir a la Superintendencia un plan de remediación que identifique las acciones, los responsables y los plazos correspondientes. El incumplimiento sostenido de los niveles de servicio o del plan de remediación da lugar a la aplicación de las medidas previstas en el artículo 22.

III. GESTIÓN DE VERSIONES

1. Esquema de versionamiento

Las especificaciones de cada API se identifican con un número de versión compuesto por tres elementos (mayor.menor.corrección). La versión mayor forma parte de la ruta de las APIs; las versiones menores y de corrección se identifican en la especificación y no modifican la ruta.

2. Clasificación de cambios

Los cambios se clasifican de la siguiente manera:

a) Cambio mayor: el que no es compatible con la versión anterior, tal como la eliminación o el cambio de nombre de un recurso, operación o campo; el cambio de tipo, formato o significado de un campo; la incorporación de un parámetro o campo obligatorio en la solicitud; o la modificación del comportamiento esperado de una operación o de un error.
b) Cambio menor: el que es compatible con la versión anterior, tal como la incorporación de recursos, operaciones, campos opcionales o valores de catálogo.

c) Corrección: la que precisa o corrige la documentación sin alterar el comportamiento de las APIs.

3. Fechas de publicación y exigibilidad

Los cambios mayores y menores se publican con la anticipación prevista en el artículo 70 y se comunican a los participantes mediante los mecanismos operativos del SFA. Cuando corresponda, la Superintendencia puede someter los cambios a consulta de los participantes mediante los mecanismos de coordinación del SFA.

4. Coexistencia

Cuando se publica una nueva versión mayor, las EPD mantienen en producción la versión mayor anterior durante el periodo de coexistencia establecido en la publicación. Durante dicho periodo, ambas versiones deben cumplir los niveles de servicio establecidos en la sección II.

Las versiones menores no requieren coexistencia, dado que son compatibles con las anteriores.

5. Deprecación y retiro

Una versión se declara deprecada con la publicación de la versión mayor que la sustituye. Durante el periodo de coexistencia, las respuestas de la versión deprecada indican dicha condición y su fecha de retiro mediante los encabezados estándar previstos en la especificación de cada API.

Vencido el periodo de coexistencia, la versión se retira y las EPD dejan de atenderla. Las ERD son responsables de migrar sus aplicaciones antes de la fecha de retiro. La puesta en producción de una nueva versión por la EPD requiere la revalidación o conformidad funcional que corresponda conforme al artículo 55 y al Anexo N° 7

6. Historial

El Portal del Desarrollador conserva y mantiene accesible el historial completo de versiones de cada documento, con sus fechas, la clasificación y descripción de cada cambio, y las versiones retiradas.

7. Notificación de cambios

Toda nueva publicación, cambio de estado o modificación de fechas de exigibilidad, coexistencia o retiro se comunica a los participantes mediante los mecanismos de comunicaciones operativas previstos en el presente Reglamento.

8. Calendarios

La Superintendencia publica y mantiene actualizado en el Portal del Desarrollador el calendario consolidado de publicación, exigibilidad, coexistencia y retiro de las versiones vigentes y previstas.

ANEXO N° 7

AMBIENTE DE PRUEBAS Y CONFORMIDAD FUNCIONAL

El presente Anexo establece las condiciones técnicas y operativas aplicables al acceso y utilización del ambiente de pruebas del SFA, así como a la ejecución de las pruebas, la obtención y revalidación de la conformidad funcional y la verificación de los componentes desplegados en producción, conforme a los artículos 51 al 55 del Reglamento.

Las disposiciones del presente Anexo son aplicables a las entidades y participantes que deban desarrollar, integrar, probar o validar aplicaciones, servidores, APIs y demás componentes tecnológicos para desempeñar uno o más roles en el SFA.

Las pruebas, resultados, conformidades y validaciones se determinan de manera específica respecto de los siguientes elementos:

a) la entidad o participante;
b) el rol evaluado;
c) la aplicación, servidor, API o componente evaluado;
d) la versión de la implementación;
e) el ambiente correspondiente;
f) las especificaciones y casos de prueba vigentes; y
g) el alcance funcional comprendido en la evaluación.

La utilización del ambiente de pruebas, la superación de las evaluaciones y la obtención de la conformidad funcional no habilitan, por sí mismas, a una entidad o participante para operar en el ambiente de producción. La conformidad funcional es independiente de la certificación de conformidad con el Perfil de Seguridad regulada en el artículo 71. Las pruebas funcionales pueden verificar la integración de los mecanismos establecidos en dicho Perfil, pero no acreditan ni sustituyen la certificación correspondiente.

1. Tipos de acceso al ambiente de pruebas del SFA

1.1. Acceso anticipado

El acceso anticipado permite que una entidad interesada en incorporarse al SFA desarrolle, integre y evalúe preliminarmente sus implementaciones antes de iniciar el proceso de incorporación. El acceso debe solicitarse a la Superintendencia y se encuentra sujeto a las condiciones de uso aplicables. Su otorgamiento no garantiza la continuidad, permanencia o disponibilidad de la información, configuraciones, recursos, funcionalidades o versiones existentes en el ambiente de pruebas.

El acceso anticipado tiene carácter preparatorio y exploratorio y, según el rol que la entidad pretenda desempeñar, puede comprender las siguientes actividades:

a) consulta de la documentación técnica;
b) registrar y configurar aplicaciones, servidores, metadatos, certificados de prueba, *endpoints* y demás componentes técnicos exigibles;
c) integrarse con el Directorio de Participantes aplicable al ambiente de pruebas;
d) acceder a APIs simuladas y utilizar datos de prueba; y
e) realizar otras actividades de desarrollo, integración o evaluación que resulten necesarias para cumplir el objetivo para el cual se otorgó el acceso al ambiente de pruebas.

La disponibilidad del acceso anticipado se encuentra sujeta a la capacidad técnica y operativa del ambiente de pruebas.

1.2. Acceso durante habilitación

El acceso durante la habilitación técnica se otorga a la entidad que haya superado la etapa de registro. Bajo esta modalidad, y de acuerdo con el rol y el alcance para los cuales solicita su habilitación, la entidad debe realizar, según corresponda, las siguientes actividades:

a) registrar y configurar aplicaciones, servidores, metadatos, certificados de prueba, *endpoints* y demás componentes técnicos exigibles;
b) integrarse con el Directorio de Participantes aplicable al ambiente de pruebas;
c) acceder a las APIs simuladas, los datos de prueba y las implementaciones de referencia disponibles;
d) ejecutar los casos de prueba obligatorios y condicionales aplicables al rol, las funcionalidades y los componentes sometidos a evaluación;
e) utilizar el motor de conformidad funcional y las herramientas oficiales disponibles;
f) generar y presentar los resultados y evidencias requeridos;
g) identificar y subsanar los resultados no conformes; y
h) repetir los casos de prueba afectados y aquellos que puedan verse impactados por las modificaciones realizadas.

Las pruebas deben ejecutarse sobre la versión y configuración de la implementación que serán consideradas para la habilitación. Cuando la entidad introduzca modificaciones que puedan afectar los resultados obtenidos, debe repetir los casos de prueba que determine la Superintendencia de acuerdo con la naturaleza y el impacto del cambio.

1.3. Acceso para revalidación

El acceso para revalidación se otorga al participante que deba ejecutar nuevas pruebas en alguno de los supuestos previstos en el artículo 55. Bajo esta modalidad, el participante debe realizar, según corresponda, las siguientes actividades:

a) Registrar o actualizar, en el ambiente de pruebas, las aplicaciones, servidores, APIs, *endpoints*, certificados, metadatos y demás componentes afectados por el cambio.
b) Ejecutar los casos de prueba que resulten aplicables al cambio y al alcance afectado.
c) Utilizar el motor de conformidad, las implementaciones de referencia y las demás herramientas disponibles según corresponda.
d) Generar y presentar los resultados y evidencias requeridos.
e) Subsanar los resultados no conformes y repetir las pruebas correspondientes.
f) Ejecutar pruebas adicionales cuando el cambio pueda afectar componentes, funcionalidades o resultados previamente evaluados.

El alcance de la revalidación se determina considerando la naturaleza del cambio, los componentes afectados y su impacto sobre la interoperabilidad, seguridad y funcionamiento de la implementación. La revalidación puede comprender casos de prueba específicos, un conjunto parcial de pruebas o la totalidad de las pruebas aplicables.

2. Ambiente de pruebas del SFA

El ambiente de pruebas del SFA puede comprender uno o más ambientes, servicios o espacios diferenciados destinados a:

a) Desarrollo e integración preliminar.
b) Ejecución de pruebas funcionales y no funcionales.

c) Subsanación y repetición de pruebas.
d) Revalidación de implementaciones.
e) Validación de configuraciones previa al despliegue de cambios en producción.

El ambiente de pruebas del SFA ofrece, según la modalidad de acceso, el rol y las pruebas aplicables, un Directorio de Participantes para dicho ambiente, servidores y APIs simulados o de referencia, datos y escenarios de prueba, el motor de conformidad funcional, herramientas para ejecutar pruebas y recopilar evidencias, mecanismos de trazabilidad y documentación técnica de apoyo.

La relación de ambientes, servicios, herramientas, implementaciones de referencia y funcionalidades disponibles, así como las modalidades y condiciones aplicables a su utilización, se publica y mantiene actualizada en el Portal del Desarrollador.

3. Segregación del ambiente de pruebas del SFA

El ambiente de pruebas debe encontrarse segregado del ambiente de producción. La segregación debe impedir que:

a) Las credenciales o llaves privadas de prueba se utilicen en producción.
b) Los datos o configuraciones de prueba produzcan efectos en sistemas productivos.
c) Las aplicaciones, servidores o componentes no habilitados accedan a servicios de producción.
d) Una operación realizada en pruebas afecte cuentas, productos, consentimientos o datos reales.

Los participantes deben mantener segregados los componentes, credenciales, configuraciones e información utilizados en los ambientes de pruebas y producción.

La segregación entre el ambiente de pruebas del SFA y el ambiente de producción no sustituye la responsabilidad de cada participante de mantener separados sus ambientes internos de desarrollo, integración, pruebas, preproducción y producción, conforme a su arquitectura y marco de gestión de riesgos.

4. Datos de prueba

Las pruebas deben realizarse exclusivamente con datos generados para dicha finalidad, de conformidad con el párrafo 51.3.

Los datos de prueba deben permitir, según corresponda:
a) Representar distintos productos y categorías de datos.
b) Ejecutar escenarios funcionales positivos y negativos.
c) Evaluar reglas de obligatoriedad, formato, integridad y consistencia.
d) Probar volúmenes representativos.
e) Simular errores, excepciones y estados no habituales.
f) Probar diferentes estados del consentimiento, aplicaciones y componentes.

La provisión de datos de prueba por la Superintendencia no exime a las entidades y participantes de desarrollar sus propios datos y escenarios de prueba para asegurar la calidad de sus implementaciones.

5. Implementaciones de referencia

La Superintendencia pone a disposición implementaciones de referencia destinadas a facilitar el desarrollo, integración y evaluación de los componentes del SFA. Las implementaciones de referencia pueden comprender:

a) Aplicaciones cliente.
b) Servidores de autorización.
c) Servidores de recursos.
d) APIs simuladas.
e) Flujos de consentimiento y autorización.
f) Configuraciones y archivos de ejemplo.
g) Colecciones de solicitudes.
h) Ejemplos de mensajes, errores y respuestas.

Las implementaciones de referencia tienen carácter orientativo. En caso de discrepancia con una especificación obligatoria, prevalece esta última.

6. Motor de conformidad funcional

El Motor de conformidad funcional es la herramienta de la infraestructura digital común destinada a ejecutar, automatizar o asistir la ejecución de los casos de prueba oficiales aplicables a las implementaciones sometidas a evaluación.

El motor de conformidad funcional permite:

a) Seleccionar el rol, componente, API y versión que serán evaluados.
b) Ejecutar casos de prueba positivos y negativos.
c) Validar solicitudes, respuestas, mensajes y secuencias.
d) Verificar códigos de respuesta y estructuras de error.
e) Registrar los resultados obtenidos.
f) Generar reportes y evidencias.
g) Identificar observaciones y resultados no conformes.
h) Repetir las pruebas afectadas después de su subsanación.

El motor de conformidad funcional no sustituye:

a) la certificación de conformidad con el Perfil de Seguridad;
b) las pruebas internas del participante;
c) las pruebas de seguridad, continuidad o recuperación que correspondan;
d) la evaluación necesaria para la habilitación;
e) la supervisión posterior de la Superintendencia

Cuando una prueba no pueda automatizarse, su evaluación puede realizarse mediante revisión documental, inspección de evidencias, ejecución asistida u otro mecanismo que determine la Superintendencia.

7. Pruebas funcionales

Las pruebas funcionales verifican que la implementación se comporte de acuerdo con las funcionalidades, reglas de negocio, flujos y resultados definidos en las especificaciones aplicables.

Las pruebas funcionales pueden comprender, según el rol y el componente evaluados, los siguientes aspectos, así como otros que determine la Superintendencia:

a) Integración con el Directorio de Participantes aplicable al ambiente de pruebas.

b) Registro y actualización de aplicaciones y componentes.
c) Descubrimiento de *endpoints* y metadatos.
d) Flujos de autenticación y autorización.
e) Registro dinámico del cliente, cuando corresponda.
f) Creación, consulta, modificación y revocación de autorizaciones.
g) Consumo o exposición de las APIs aplicables.
h) Validación de recursos, operaciones, parámetros y mensajes.
i) Tratamiento de códigos de respuesta, errores y excepciones.
j) Paginación y filtros.
k) Aplicación de restricciones derivadas del consentimiento.
l) Rechazo de solicitudes inválidas, incompletas, vencidas, revocadas o no autorizadas.
m) Funcionamiento de los eventos o notificaciones exigibles.
n) Interacción con implementaciones de referencia.

Los casos de prueba obligatorios se determinan según:
a) El rol desempeñado.
b) Las APIs expuestas o consumidas.
c) Los dominios y grupos de datos habilitados.
d) Los servicios prestados.
e) La versión evaluada.
f) El componente sometido a evaluación.

8. Pruebas no funcionales

Las pruebas no funcionales verifican características de la implementación que no corresponden exclusivamente a una funcionalidad de negocio, pero que resultan necesarias para su adecuada operación e interoperabilidad.

Estas pruebas pueden comprender, según el rol y el componente evaluados, los siguientes aspectos, así como otros que determine la Superintendencia:
a) Rendimiento y tiempo de respuesta
b) Capacidad y comportamiento bajo carga
c) Límites de consumo
d) Tasa de errores
e) Disponibilidad y recuperación
f) Trazabilidad y propagación de identificadores de interacción
g) Manejo de concurrencia
h) Comportamiento ante indisponibilidad u operación degradada
i) Respuesta ante certificados, *tokens* o autorizaciones vencidos o revocados
j) Consistencia de configuraciones y metadatos

Las pruebas comprendidas en esta sección no sustituyen las pruebas independientes de seguridad, penetración, continuidad o recuperación que resulten exigibles conforme al Reglamento y a la normativa vigente.

Los umbrales de aprobación aplicables al rendimiento, capacidad, tasa de errores, disponibilidad y recuperación deben guardar correspondencia con los niveles de servicio previstos en los Anexos N° 6, según el componente evaluado.

9. Casos de prueba

Los casos de prueba constituyen la unidad verificable de evaluación y deben identificar, como mínimo:

a) Un código único
b) El objetivo
c) El rol y componente evaluado
d) La versión de la especificación aplicable
e) Las precondiciones
f) Los datos requeridos.
g) La solicitud, acción o secuencia que debe ejecutarse
h) El resultado esperado
i) Los criterios de aprobación
j) La evidencia que debe generarse
k) Su carácter obligatorio, condicional u orientativo

Los casos de prueba deben incluir:

a) Escenarios positivos.
b) Escenarios negativos.
c) Valores límite.
d) Datos inválidos o incompletos.
e) Estados vencidos, revocados, suspendidos o restringidos.
f) Errores técnicos y funcionales.
g) Reintentos y solicitudes duplicadas, cuando corresponda.
h) Escenarios de contingencia aplicables.

Los casos de prueba oficiales, sus versiones y sus fechas de exigibilidad se publican en el Portal del Desarrollador. Los cambios en los casos de prueba no se aplican retroactivamente a las evaluaciones concluidas, salvo cuando respondan a una vulnerabilidad, error crítico o riesgo que requiera actuación inmediata.

10. Criterios de aprobación

Una implementación obtiene un resultado conforme cuando:

a) Supera la totalidad de los casos de prueba obligatorios aplicables a su alcance
b) Cumple las condiciones y resultados esperados
c) No mantiene resultados no conformes pendientes de subsanación
d) Presenta las evidencias requeridas
e) Las pruebas han sido ejecutadas sobre la versión y configuración declaradas
f) No se identifican diferencias que invaliden los resultados obtenidos

La Superintendencia puede clasificar los resultados como:

a) Conforme
b) No conforme
c) No aplicable
d) No ejecutado
e) Inconcluso por una causa técnica debidamente identificada

La evaluación se considera aprobada cuando todos los casos de prueba obligatorios aplicables obtienen un resultado conforme. Los casos clasificados como no aplicables no afectan la aprobación, siempre que dicha clasificación se encuentre debidamente sustentada.

11. Resultados y evidencias

Los resultados deben permitir identificar:

a) La entidad o participante evaluado
b) El rol y componente evaluado
c) El ambiente
d) Las versiones aplicables
e) Los casos ejecutados
f) La fecha y hora de ejecución
g) Los resultados obtenidos
h) Las observaciones y resultados no conformes
i) Las subsanaciones efectuadas
j) La fecha de conclusión de la evaluación

Las evidencias deben comprender:

a) Solicitudes y respuestas
b) Mensajes y *payloads*
c) Registros técnicos
d) Resultados generados por el motor de conformidad
e) Capturas o constancias de ejecución
f) Identificadores de interacción
g) Versiones y huellas de los componentes evaluados
h) Informes de resultados
i) Evidencias adicionales expresamente requeridas

Las evidencias deben mantenerse íntegras, disponibles, trazables y protegidas contra modificaciones no autorizadas.

Las evidencias no deben contener llaves privadas, secretos, credenciales reales, factores de autenticación ni datos reales de usuarios.

12. Subsanaciones y repeticiones

Cuando una implementación no supere una o más pruebas obligatorias, la entidad o participante debe:

a) Identificar la causa del resultado no conforme.
b) Corregir la deficiencia.
c) Documentar el cambio efectuado.
d) Evaluar su impacto sobre otros componentes o resultados.
e) Repetir las pruebas que correspondan.

Cada repetición debe generar un nuevo resultado vinculado con el anterior, sin eliminar ni sustituir la evidencia histórica.

13. Conformidad funcional

La conformidad funcional se obtiene cuando:

a) Se han ejecutado todas las pruebas obligatorias aplicables
b) Se han superado los criterios de aprobación
c) Se han subsanado los resultados no conformes
d) Se han generado y conservado las evidencias requeridas
e) Se ha emitido el resultado final correspondiente

La conformidad funcional debe identificar:

a) La entidad o participante
   b) El rol
   c) La aplicación, servidor, API o componente
   d) La versión evaluada
   e) El ambiente
   f) Las especificaciones y casos de prueba aplicados
   g) La fecha de conclusión

La obtención de la conformidad funcional puede acreditarse mediante una constancia o credencial técnica emitida a través de los mecanismos habilitados por la Superintendencia. Dicha constancia o credencial únicamente acredita el resultado y alcance de la evaluación realizada y no sustituye la decisión de habilitación ni autoriza, por sí misma, la operación en producción.

14. Vigencia de la conformidad funcional

El participante debe mantener las condiciones que sustentaron la conformidad funcional. Cuando dichas condiciones sean modificadas o afectadas, resulta aplicable lo dispuesto en el artículo 55.

15. Revalidación

La revalidación se realiza en los supuestos y con el alcance previstos en el artículo 55. Cuando el participante determine que un cambio no afecta las condiciones previamente evaluadas, debe documentar y conservar el análisis técnico que sustente que no corresponde realizarla.

ANEXO N° 8

INDICADORES Y METODOLOGÍA DE CALIDAD DE DATOS

I. INDICADORES DE CALIDAD DE DATOS

Matriz consolidada de indicadores por Dimensiones

Dimensión	Detalle	Indicador	Umbral mínimo	Unidad
Exactitud	Un registro es exacto cuando todos sus campos coinciden con la fuente autoritativa de la EPD y con la información que esta misma muestra en sus propios canales digitales.	Número de registros sin diferencias respecto de la fuente autoritativa ÷ tamaño de la muestra representativa utilizada × 100%	≥ 95 %	Porcentaje
Completitud	Un registro está completo cuando todos sus campos tienen un valor informado, es decir, no están vacíos, nulos ni con valores de relleno como "N/A", "-", "0" o "sin dato", salvo que la regla lo permita.	Número de registros con todos los campos obligatorios completos ÷ tamaño de la muestra representativa utilizada × 100%	≥ 95 %	Porcentaje
Consistencia	Un registro es consistente cuando sus datos no se contradicen entre los distintos campos de un mismo endpoint o entre endpoints del API.	Número de registros que cumplen las reglas de compatibilidad aplicables ÷ tamaño de la muestra representativa utilizada × 100%	≥ 95 %	Porcentaje
Validez	Un registro es válido cuando todos sus campos cumplen las reglas técnicas; las cuales incluyen: el tipo de dato, el formato, la longitud, los rangos permitidos y los valores de los catálogos, entre otros.	Número de registros que cumplen todas las reglas técnicas y de negocio aplicables ÷ tamaño de la muestra representativa utilizada × 100%	≥ 95 % para reglas técnicas críticas	Porcentaje
Unicidad	Un registro es único cuando ningún otro registro del conjunto de datos representa al mismo registro. Esto se verifica con su llave primaria o con la combinación de campos primarios definida para ese tipo de registro.	Número de registros no duplicados ÷ tamaño de la muestra representativa utilizada × 100%	≥ 95 %	Porcentaje

(*) Las instrucciones para el cálculo de las métricas para cada grupo de datos habilitado se encontrarán en el Portal de Desarrollador

II. CONSIDERACIONES PARA EL CALCULO DE LOS INDICADORES DE CALIDAD DE DATOS

1. **<u>Alcance y frecuencia de evaluación:</u>**
   1.1. La EPD calcula las cinco dimensiones, dado que cuenta con la fuente autoritativa. La ERD solo calcula la completitud, la validez y la unicidad sobre los datos que recibe.

1.2. Los indicadores se calculan a nivel de cada endpoint y entre endpoints, cuando aplique.

1.3. La muestra utilizada para el cálculo de los indicadores debe considerar la materialidad, heterogeneidad, criticidad y volumen de los datos, y no debe excluir registros por contener errores, valores nulos, duplicidades, anomalías o estados excepcionales.

1.4. Los indicadores deben calcularse semestralmente, como mínimo. Sus resultados deben identificar el rol, el periodo evaluado y la versión de la API correspondiente.

2. <u>Conservación de evidencias:</u>

2.1. Los participantes deben conservar evidencia del cálculo del indicador, la muestra evaluada, las reglas aplicadas, los resultados, las diferencias detectadas, las causas identificadas y las medidas correctivas adoptadas para disposición de esta Superintendencia.

2.2. La conservación de la evidencia debe observar criterios de minimización de datos, seguridad, seudonimización y control de acceso, evitando duplicar innecesariamente datos personales o financieros.

ANEXO N° 9
PERFIL DE SEGURIDAD FAPI 2.0 PERÚ

Capítulo I: Introducción

1.1 El Perfil de Seguridad FAPI 2.0 Perú, en adelante Perfil de Seguridad, establece los requisitos técnicos de seguridad aplicables a los componentes mediante los cuales los participantes acceden a los datos e información comprendidos en el SFA que requieren consentimiento del usuario o los suministran.

1.2 El Perfil de Seguridad adapta al SFA las especificaciones FAPI 2.0 *Security Profile*, FAPI 2.0 *Attacker Model* y FAPI 2.0 *Message Signing* de la OpenID Foundation, complementadas con las especificaciones de OAuth 2.0 y OpenID Connect necesarias para su implementación.

1.3 Las especificaciones técnicas que desarrollan el Perfil de Seguridad, los catálogos técnicos, las versiones exigibles de las especificaciones de referencia y los parámetros técnicos aplicables, incluidos los algoritmos, vigencias, plazos y periodos de coexistencia, se publican en el Portal del Desarrollador conforme al artículo 70.

Capítulo II: Ámbito, Roles y Definiciones

2.1 Para efectos del Perfil de Seguridad, la EPD opera el servidor de autorización y el servidor de recursos, y la ERD opera la aplicación cliente. El acceso a la información a que se refiere el párrafo 69.4 no se sujeta a los mecanismos de autenticación y autorización del usuario, sin perjuicio de los demás requisitos de seguridad que resulten aplicables.

2.2 El Directorio de Participantes constituye la fuente oficial de la información registral necesaria para verificar la identidad, roles y estados de participación de las contrapartes, así como las aplicaciones, componentes tecnológicos y elementos de confianza registrados. Los participantes obtienen de dicho componente los *endpoints*, metadatos, llaves públicas y demás información necesaria para las interacciones, sin requerir acuerdos bilaterales. El servidor de autorización debe rechazar las solicitudes que excedan los roles habilitados o el alcance permitido a la aplicación solicitante.

Capítulo III: Modelo de Atacante y Principios de Seguridad

3.1 Los participantes deben adoptar como referencia el FAPI 2.0 *Attacker Model*. El Perfil de Seguridad tiene por objetivo impedir que un atacante pueda acceder a recursos ajenos, suplantar a un usuario o inducirlo a operar bajo una identidad o sobre recursos distintos de los que le corresponden.

3.2 Los riesgos no cubiertos por el modelo, como el compromiso del dispositivo del usuario, el compromiso interno de un participante o el uso indebido de datos obtenidos legítimamente, deben gestionarse conforme al artículo 72 y al marco de gestión de riesgos aplicable al participante. Los eventos de seguridad deben registrarse y conservarse conforme a los artículos 67 y 77.

Capítulo IV: Perfil de Implementación

4.1 Las conexiones deben emplear *TLS* 1.3. Se prohíben el algoritmo "*none*" y los algoritmos de firma simétrica.

4.2 Las respuestas de autorización se emiten firmadas mediante JARM y deben identificar al emisor.
4.3 Las solicitudes y respuestas de las APIs deben firmarse con el certificado de firma del emisor, conforme a la especificación FAPI 2.0 *Message Signing*. El receptor debe rechazar los mensajes cuya firma sea inválida o se encuentre ausente cuando resulte exigible.
4.4 Cada interacción debe contar con un identificador único que permita su trazabilidad de extremo a extremo, conforme al artículo 77.

Capítulo V: *Pushed Authorization Requests* (PAR)
5.1 Las solicitudes de autorización deben enviarse exclusivamente mediante PAR, a través de un canal autenticado de servidor a servidor. El navegador del usuario únicamente transporta una referencia de un solo uso, vinculada con la aplicación cliente y sujeta a un periodo de vigencia limitado.
5.2 Es obligatorio utilizar PKCE. No se admiten los flujos implícitos, híbridos ni aquellos basados en las credenciales asignadas al usuario por la EPD.

Capítulo VI: Autenticación de Clientes y *mTLS*
6.1 La aplicación cliente debe autenticarse mediante *mTLS*. Los *tokens* de acceso deben encontrarse vinculados al certificado de transporte de la aplicación, y el servidor de recursos debe verificar dicha vinculación en cada solicitud.
6.2 Se prohíben los secretos compartidos, las aserciones firmadas, los mecanismos *DPoP* y los *tokens* no vinculados. Un certificado revocado se rechaza en el establecimiento de la conexión.

Capítulo VII: *Scopes, Claims* y *Rich Authorization Requests* (RAR)
7.1 El alcance del consentimiento se expresa mediante detalles de autorización estructurados conforme a RAR. Dichos detalles identifican, entre otros elementos, el tipo de autorización, las acciones, los grupos y subconjuntos de datos y el periodo de vigencia, conforme a los catálogos publicados en el Portal del Desarrollador.
7.2 El servidor de autorización debe rechazar íntegramente las solicitudes que no cumplan los requisitos aplicables y presentar al usuario los detalles de autorización objeto de confirmación. El servidor de recursos debe verificar, en cada solicitud, que el acceso se encuentre comprendido en la autorización vigente.

Capítulo VIII: Consentimiento y *Grant Management*
8.1 Cada consentimiento se materializa técnicamente en una autorización con identificador único. La autorización puede encontrarse vigente, revocada o vencida. Los estados revocado y vencido son definitivos. La autorización puede ser consultada, ampliada, sustituida o revocada conforme a las condiciones establecidas en el Reglamento y en las especificaciones técnicas aplicables.
8.2 Ningún *token* puede conferir un alcance o una vigencia superiores a los de la autorización correspondiente. La revocación surte efectos inmediatos, invalida los *tokens* de renovación asociados y se notifica a los participantes involucrados conforme al artículo 76.

8.3 En los productos que requieran actuación conjunta, la autorización solo se genera una vez completadas las confirmaciones exigidas. Su revocación se rige por las disposiciones aplicables al tipo de producto y a las facultades de las personas intervinientes.

Capítulo IX: *Dynamic Client Registration* (DCR)

9.1 Las "aplicaciones cliente" deben registrarse ante cada servidor de autorización mediante registro dinámico, utilizando una declaración de *software* obtenida a través de los mecanismos habilitados por el Directorio de Participantes. No se admite una vía alternativa de registro manual.

9.2 Antes de completar el registro, el servidor de autorización debe verificar la declaración de *software*, la habilitación del participante, la vigencia de sus certificados y las direcciones de redirección registradas. La actualización y baja de las aplicaciones deben realizarse mediante los mecanismos técnicos establecidos en el Perfil de Seguridad.

Capítulo X: Certificados y Confianza

10.1 Cada participante debe contar con certificados digitales diferenciados para transporte y firma, segregados por ambiente y utilizados exclusivamente para la finalidad correspondiente. Los certificados deben ser emitidos por autoridades de certificación que cumplan los criterios de admisión establecidos en el presente Anexo y en las especificaciones técnicas aplicables. Antes de su utilización, deben encontrarse vigentes y registrados en el Directorio de Participantes.

10.2 Las autoridades de certificación deben contar con una auditoría o acreditación vigente bajo *WebTrust*, ETSI o un estándar nacional equivalente, y cumplir los demás criterios de admisión establecidos en las especificaciones técnicas aplicables.

10.3 Los certificados deben permitir verificar su estado mediante OCSP, CRL u otro mecanismo admitido en las especificaciones técnicas. El participante debe comunicar inmediatamente el compromiso o la sospecha de compromiso de las llaves privadas y solicitar la revocación del certificado correspondiente, conforme al artículo 74.

Capítulo XI: Eventos, Revocación y Notificación

11.1 Los participantes notifican activamente, mediante mensajes firmados y transmitidos por *mTLS*, la revocación de autorizaciones y los cambios en sus certificados. El Directorio de Participantes notifica los cambios de habilitación.

11.2 Las notificaciones deben contener únicamente la información necesaria para identificar y gestionar el evento y no deben incluir datos del usuario ni el contenido de la autorización. Las notificaciones y sus acuses deben registrarse y conservarse conforme a los artículos 67 y 77."

ANEXO N° 10
SOPORTE TÉCNICO Y COMUNICACIONES OPERATIVAS

Las disposiciones correspondientes al Anexo N° 10 serán desarrolladas y aprobadas posteriormente mediante resolución de la Superintendencia.

Artículo Segundo. - **Vigencia**

1. La presente Resolución entra en vigencia a partir del día siguiente de su publicación en el Diario Oficial *El Peruano*, salvo las disposiciones para las cuales el presente artículo establezca una fecha distinta.

2. Los Título V, VI y VII del Reglamento, referidos a la infraestructura digital común del SFA, el Marco de Confianza y los estándares técnicos, de seguridad y calidad, respectivamente, así como los Anexos N° 5 al 10, entran en vigencia el 1 de agosto de 2027, salvo lo dispuesto en el numeral 3.

3. El Capítulo IV del Título V del Reglamento y el Anexo N° 7 entran en vigencia el 1 de julio de 2027.

4. Las disposiciones del Reglamento vinculadas con, la recuperación de costos, la gestión de problemas, incidentes y disputas, el monitoreo, las medidas correctivas y las sanciones, así como las demás disposiciones complementaras para completar la funcionalidad del Sistema, entran en vigencia en los plazos que establezca la Superintendencia mediante las disposiciones que desarrollen dichas materias.

Regístrese, comuníquese, publíquese.