

Lima, 02 de octubre de 2026

Resolución SBS
N° 02433-2026

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 N° 26702, la Ley del Sistema Privado de Administración de Fondos de Pensiones, cuyo Texto Único Ordenando fue aprobado por el Decreto Supremo N° 054-97-EF y otras leyes;

Que, mediante la Trigésima Segunda Disposición Final y Complementaria de la Ley N° 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 N° 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 mecanismo de gobernanza, el alcance de los datos y servicios comprendidos, las condiciones de participación, y las disposiciones aplicables al acceso, intercambio y tratamiento de la información, así como al control de los usuarios sobre sus datos;

Que, en cumplimiento de lo antes referido, la Superintendencia dispone aprobar mediante resolución de Superintendencia sus proyectos



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

normativos y publicarlos en su Sede Digital con el objetivo de asegurar la participación efectiva del público en general, y;

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 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

Lima, «Dia» de «Mes» de «Año»

Resolución SBS
N° XXXX-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 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 inicialmente las disposiciones generales aplicables al Sistema, su forma de gobierno, el alcance de los datos y servicios comprendidos, así como las reglas relativas a sus participantes, roles y condiciones de participación, así como las disposiciones aplicables al acceso, tratamiento de la información y control del usuario, sin perjuicio del desarrollo progresivo de las demás disposiciones regulatorias y técnicas necesarias para su funcionamiento;

Que, con la finalidad de otorgar predictibilidad a los participantes respecto de las responsabilidades derivadas de su actuación en el Sistema de Finanzas Abiertas, resulta conveniente establecer escenarios referenciales y no limitativos de atribución inicial de responsabilidad, los cuales podrán ser complementados conforme avance el desarrollo regulatorio y operativo del Sistema;

Que, a efectos de recoger las opiniones del público en general respecto de la propuesta de norma, se dispuso la publicación del proyecto de resolución en el Portal Institucional de esta Superintendencia, al amparo de lo dispuesto en la Trigésima Segunda Disposición Final y Complementaria de la Ley General y el Decreto Supremo N° 009-2024-JUS y sus normas modificatorias, y;

En uso de las atribuciones conferidas por los numerales 3, 7, 9, 13 y 19 del artículo 349 de la Ley General, y 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:



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

PROYECTO NORMATIVO

“REGLAMENTO GENERAL DEL SISTEMA DE FINANZAS ABIERTAS

ÍNDICE

Título I

Disposiciones generales

Título II

Alcance, datos y servicios

Título III

Participantes, roles y habilitación

Título IV

Acceso y control del usuario

Título V

Infraestructura digital

Título VI

Marco de Confianza

Título VII

Estándares seguridad y calidad

Título VIII

Recuperación de Costos

Título IX

Problemas, incidentes y disputas

Título X

Monitoreo, medidas correctivas y sanciones

Disposiciones Finales y Complementarias

Anexos

REGLAMENTO GENERAL DEL SISTEMA DE FINANZAS ABIERTAS

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Alcance

- 1.1 El presente Reglamento es de aplicación a las empresas comprendidas en los artículos 16° y 17° y en la Vigésimo Cuarta Disposición Final y Complementaria de la Ley General, a las empresas bajo el ámbito de la Ley del Sistema Privado de Administración de Fondos de Pensiones, al Banco de la Nación, al Banco Agropecuario, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Fondo MIVIVIENDA S.A., a las Derramas y Cajas de Beneficios sujetas al control de la Superintendencia. Asimismo, es de aplicación a las personas jurídicas no supervisadas por la Superintendencia que soliciten su inscripción para participar voluntariamente en el Sistema de Finanzas Abiertas (en adelante, SFA), conforme a lo previsto en el Título III.
- 1.2 Las disposiciones contenidas en el Reglamento resultan aplicables a las entidades previamente señaladas, en tanto estén habilitadas a participar en el SFA, en cualquiera de los roles previstos en el Título III, conforme a los estándares establecidos por la Superintendencia.

Artículo 2. Definiciones

Para la aplicación del presente Reglamento deben considerarse las siguientes definiciones:

- a) **Usuario:** toda persona natural, persona jurídica o ente jurídico, cuyos datos e información son objeto del acceso o suministro que se ejecutan en el marco del SFA.
- b) **Consentimiento:** manifestación libre, expresa e inequívoca de la voluntad del usuario mediante la cual autoriza el acceso, suministro y tratamiento de sus datos, de acuerdo con las finalidades autorizadas y condiciones establecidas en la solicitud de acceso a sus datos, cumpliendo con las características previstas en la normativa vigente sobre protección de datos personales.
- c) **Autenticación:** proceso que permite verificar que una entidad es quien dice ser, para lo cual hace uso de las credenciales que se le asignan, en línea con lo establecido en la normativa de seguridad de la información y ciberseguridad.
- d) **Canal digital:** de acuerdo con la definición establecida en el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N° 504-2021 y sus normas modificatorias.
- e) **Confirmación:** validación final, expresa y verificable mediante la cual el usuario confirma el consentimiento para compartir sus datos a través de los canales digitales de la entidad proveedora de datos.
- f) **Directorio Centralizado:** infraestructura tecnológica centralizada que permite la identificación, autenticación y consulta de información de los participantes del SFA, así como de los recursos y servicios habilitados para el intercambio de datos.
- g) **Entidad Proveedora de Datos (EPD):** participante habilitado que brinda acceso y suministra los datos e información comprendidos en el SFA.
- h) **Entidad Receptora de Datos (ERD):** participante habilitado que solicita, accede y recibe datos e información comprendidos en el SFA y suministrados por las EPD.
- i) **Interfaz:** se entiende como la interfaz de usuario (UI), constituida por la pantalla o conjunto de pantallas y elementos visuales dispuestos a través de un canal digital, mediante los cuales se presenta información al usuario y se habilita su interacción con las funcionalidades disponibles.



- j) **Proveedor de servicios basados en datos (PSBD):** persona jurídica no supervisada por la Superintendencia, inscrita en el Registro de PSBD y habilitada para prestar servicios basados en datos mediante el acceso o recepción de datos a través del SFA y, cuando corresponda, para suministrar datos en calidad de EPD.
- k) **Servicios basados en datos:** servicios prestados al usuario mediante el análisis, consolidación, presentación o utilización de datos a los que se accede a través del SFA, conforme a la finalidad consentida.
- l) **Superintendencia:** Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones,
- m) **Participante:** persona jurídica, supervisada o no por la Superintendencia, que se encuentra inscrita en el Directorio Centralizado y habilitada para desempeñar uno o más roles en el SFA y sujetas a la supervisión de la Superintendencia respecto de las actividades que realiza en el sistema.
- n) **Estándares técnicos:** conjunto de especificaciones, requisitos y reglas técnicas de interoperabilidad, datos, seguridad y operación aplicables a las interfaces y los componentes de la infraestructura digital del SFA, conforme a lo establecido en el presente Reglamento.
- o) **Interfaz de programación de aplicaciones (API):** corresponde a la colección de métodos de invocación y parámetros asociados que puede utilizar un software para solicitar acciones de otro software, lo que define los términos en los que estos intercambian datos.
- p) **Datos del usuario:** datos relativos a la identificación del usuario, recabados por la EPD en el proceso de cumplimiento de las exigencias de debida diligencia de conocimiento de sus clientes, así como los datos relativos a las condiciones y transacciones de los productos y servicios financieros que el usuario mantiene o ha mantenido contratados, cuyo acceso y suministro requieren su consentimiento.

Artículo 3. Objetivo

- 3.1 El presente Reglamento tiene por objeto establecer el alcance del Sistema de Finanzas Abiertas, las obligaciones de sus participantes, los mecanismos de habilitación y supervisión, y las reglas aplicables a su operación, con el propósito de permitir el acceso y suministro estandarizado y seguro de datos y servicios comprendidos en el SFA, conforme a los principios previstos en el artículo 7 y promoviendo la protección de los usuarios y la estabilidad financiera.

Artículo 4. Sistema de Finanzas Abiertas

- 4.1 El Sistema de Finanzas Abiertas es el conjunto de normas, estándares, infraestructura digital y participantes habilitados que interoperan mediante interfaces de programación de aplicaciones para acceder, suministrar e intercambiar, de manera estandarizada y segura, los datos y servicios comprendidos en artículo 9 del Reglamento. Estas actividades se realizan con el consentimiento previo y expreso del usuario, cuando corresponda, y con sujeción a las exigencias y condiciones establecidas en el Título IV.

Artículo 5. Gobierno del SFA

- 5.1 La Superintendencia conduce el gobierno del SFA y establece los lineamientos necesarios para su adecuada implementación, funcionamiento y evolución. El gobierno se orienta a asegurar que el Sistema opere de manera segura, interoperable, eficiente, transparente y sostenible, proteja a los usuarios, cumpla sus objetivos y observe los principios establecidos en el presente Reglamento. Para estos efectos, la Superintendencia ejerce las siguientes funciones:
 - a) Establecer el marco normativo y operativo aplicable al SFA.
 - b) Establecer y actualizar los estándares técnicos necesarios para su funcionamiento.



- c) Definir los cronogramas, condiciones y criterios para la implementación progresiva del Sistema.
- d) Establecer las condiciones de participación y determinar los roles que pueden desempeñar los participantes en el SFA, conforme a lo dispuesto en el Título III.
- e) Administrar el Directorio del SFA y los demás componentes comunes que se encuentren bajo su responsabilidad.
- f) Conducir los mecanismos de coordinación y consulta con los participantes y, cuando corresponda, con otras autoridades y entidades.
- g) Supervisar el cumplimiento de las obligaciones de los participantes y el adecuado funcionamiento del SFA, así como adoptar las medidas preventivas y correctivas que correspondan e imponer las sanciones aplicables, de conformidad con el marco normativo vigente.
- h) Aprobar la incorporación o actualización de los componentes, funcionalidades, estándares y mecanismos comunes necesarios para el funcionamiento del Sistema.
- i) Adoptar las actuaciones complementarias expresamente previstas en el marco normativo aplicable y aquellas necesarias para el ejercicio de las funciones señaladas en el presente artículo, dentro del ámbito de sus competencias.

5.2 La Superintendencia puede adecuar progresivamente la forma de gobierno del SFA, considerando el nivel de adopción y la complejidad operativa del Sistema, sus requerimientos de sostenibilidad, su evolución y las mejores prácticas aplicables.

Artículo 6. Objetivos del Sistema de Finanzas Abiertas

6.1 Son objetivos del SFA:

- 1. Fomentar la competencia y la innovación en el sistema financiero peruano, promoviendo el desarrollo de nuevos productos y servicios financieros, en condiciones de acceso equitativo, no discriminatorias y de interoperabilidad.
- 2. Promover la inclusión financiera, facilitando que los usuarios accedan a una oferta más amplia y diversa de productos y servicios financieros adecuados a sus necesidades, perfil y comportamiento financiero mediante criterios objetivos, transparentes y no discriminatorios.
- 3. Empoderar al usuario en el uso y gestión de sus datos, garantizando su capacidad de decidir sobre el acceso y suministro de su información permitiendo que consentimiento sea informado, libre, específico y comprensible, así como de revocar su consentimiento en cualquier momento y acceder a servicios financieros desarrollados a partir del tratamiento autorizado de sus datos, en el ejercicio de sus derechos, conforme a lo dispuesto en el marco normativo que regula la protección de datos personales y en el presente Reglamento.

Artículo 7. Principios del Sistema de Finanzas Abiertas

Son principios del SFA:

- 1. **Reciprocidad:** Todo participante del Sistema que accede o recibe información tiene la obligación de compartir la información comprendida dentro de las categorías y condiciones previstas en el SFA, sin que ello implique un intercambio equivalente.
- 2. **No discriminación:** Ningún participante o usuario debe ser objeto de trato desigual en el acceso, uso o provisión de datos y servicios del SFA. Las condiciones de participación se sustentan en criterios objetivos, evitando cualquier sesgo, exclusión o preferencia injustificada entre participantes o usuarios sin perjuicio de la aplicación de medidas diferenciadas sustentadas en obligaciones legales, regulatorias, prudenciales, de seguridad o de gestión de riesgos.



3. **Proporcionalidad:** lo establecido por este Reglamento, sus anexos y, en lo que corresponda, por otras disposiciones normativas de esta Superintendencia, consideran el tamaño, perfil de riesgo y complejidad operativa del rol que los participantes desempeñan en el SFA, sin reducir los estándares de seguridad y control del usuario, permitiendo que la regulación acompañe y habilite la innovación y la competencia.
4. **Seguridad y protección de datos:** Los datos deben ser protegidos mediante mecanismos eficaces de seguridad de la información y ciberseguridad, garantizando su confidencialidad, integridad, disponibilidad y trazabilidad, y evitando su uso no autorizado.
5. **Control del usuario:** El usuario mantiene el control efectivo sobre sus datos a través de un consentimiento previo, libre, informado, específico y revocable, y debe contar con información clara, accesible y oportuna sobre el uso de sus datos y los servicios ofrecidos respecto del intercambio de información, sin perjuicio de los tratamientos de datos exigidos por disposiciones legales o regulatorias.
6. **Interoperabilidad:** Los protocolos de intercambio de información que implementen los participantes se rigen por estándares comunes que permitan una interacción eficiente, segura y transparente.
7. **Calidad de los datos:** Los datos compartidos deben ser precisos, íntegros y actualizados, permitiendo que sean utilizados de manera efectiva para ofrecer servicios y productos de mayor valor. Para ello, los participantes deben adoptar las medidas razonables para garantizarlo.
8. **Transparencia:** En el SFA la información debe ser comprensible, clara, accesible, suficiente y oportuna sobre su funcionamiento y sus componentes, de modo que los usuarios, participantes y demás interesados puedan conocer las condiciones bajo las cuales opera el Sistema.

TÍTULO II **ALCANCE, DATOS Y SERVICIOS**

Artículo 8. Alcance de los datos y servicios del SFA

- 8.1 El SFA comprende el acceso y suministro estandarizado y seguro de los datos del usuario y de la información general sobre los productos y servicios financieros, previsionales, cooperativos y de pagos ofrecidos al público por los participantes, así como la prestación de los servicios comprendidos dentro de las categorías de información habilitadas por el presente Reglamento. Para estos efectos, los participantes deben encontrarse habilitados de acuerdo con los roles que desempeñen, con la finalidad de facilitar a los usuarios el acceso a información y la oferta de productos y servicios.
- 8.2 El intercambio de información en el marco del SFA se realiza sin perjuicio de las restricciones, obligaciones de reserva y deberes de confidencialidad establecidos en la normativa vigente.
- 8.3 Los participantes deben implementar y mantener las medidas y/o mecanismos necesarios para cumplir los estándares técnicos y los demás requisitos establecidos en el presente Reglamento.

Artículo 9. Datos y servicios comprendidos en el SFA

- 9.1 El SFA comprende el acceso y suministro de las siguientes categorías de datos e información:
 1. Información de identificación y registro del usuario, incluida la de sus representantes o apoderados legales cuando corresponda, recabada por las EPD durante el proceso de



- enrolamiento, contratación de productos y servicios, ejecución de operaciones o para el cumplimiento de las exigencias regulatorias de debido conocimiento del cliente.
2. Información sobre los productos y servicios financieros, cooperativos y previsionales que el usuario mantenga contratados, incluyendo la identificación y el estado del producto o servicio, sus condiciones comerciales y operativas vigentes, los saldos y el historial de transacciones, según corresponda. Esta categoría comprende la información relacionada con cuentas de pago o de depósito, operaciones de crédito, operaciones de cambio de divisas, productos de seguros, productos previsionales y las demás relaciones contractuales o de servicio comprendidas en el SFA.
 3. Información sobre las características y condiciones generales de carácter público de los productos y servicios financieros y previsionales ofrecidos al público por los participantes, incluyendo, según corresponda, los requisitos de acceso y contratación, tasas de interés, comisiones, gastos, beneficios, plazos, monedas, límites, canales de contratación y atención, y demás elementos que permitan a los usuarios conocer y comparar dichos productos y servicios.
- 9.2 La información correspondiente al numeral 3 del párrafo 9.1 debe mantenerse actualizada y encontrarse disponible mediante las interfaces del SFA que se establezcan para tal efecto. Su acceso no requiere el consentimiento del usuario cuando no comprenda datos personales ni información asociada a un usuario determinado, conforme a la normativa aplicable.
- 9.3 El historial de transacciones a que se refiere el numeral 2 del párrafo 9.1 debe comprender los treinta y seis (36) meses anteriores a la fecha en que la EPD recibe la solicitud de acceso. Cuando la relación contractual o de servicio del usuario con la EPD tenga una antigüedad menor, se suministra la totalidad del historial disponible. La profundidad histórica exigible se implementa conforme a la primera disposición complementaria transitoria.
- 9.4 El acceso y suministro de datos y servicios a través de canales digitales deberán observar los mecanismos de autenticación reforzada, así como mecanismos de monitoreo, trazabilidad y gestión de incidentes de seguridad y las demás exigencias aplicables en materia de seguridad de la información y ciberseguridad.
- 9.5 La información generada a partir del análisis, procesamiento o transformación de los datos comprendidos en las categorías señaladas en el presente artículo no se encuentra sujeta al intercambio obligatorio en el marco del SFA. No obstante, la EPD podrá compartir dicha información de manera voluntaria, conforme a los acuerdos que celebre con la ERD. Esta disposición no exime a la EPD de suministrar los datos base comprendidos en el SFA sobre los cuales hubiera efectuado dicho análisis, previo consentimiento del usuario cuando corresponda.
- 9.6 No forman parte de las categorías de información objeto de intercambio obligatorio las evaluaciones internas de riesgo, clasificaciones, perfiles de riesgo, alertas, reportes regulatorios, análisis de prevención del lavado de activos y financiamiento del terrorismo, ni cualquier otra información generada para el cumplimiento de obligaciones legales o regulatorias cuya divulgación se encuentre restringida por el ordenamiento jurídico.
- 9.7 Los datos específicos, variables, atributos, formatos, reglas de actualización y demás especificaciones técnicas correspondientes a cada categoría de datos e información indicados en el presente artículo serán definidos y estandarizados en el Anexo N° 3 del presente Reglamento.



- 9.8 La Superintendencia puede incorporar otras categorías de datos, información o servicios al SFA mediante norma de carácter general.

TÍTULO III **PARTICIPANTES, ROLES Y HABILITACIÓN**

Artículo 10. Entidades Proveedoras de Datos

10.1 Desempeñan el rol de EPD las entidades comprendidas en el párrafo 1.1 del artículo 1 que custodien, administren o sean responsables del suministro de los datos e información comprendidos en el SFA, se encuentren habilitadas para desempeñar dicho rol y que cumplan los requisitos técnicos, operativos, de seguridad y de gestión de riesgos que resulten aplicables, ya sea en virtud de su incorporación obligatoria conforme al cronograma establecido en el Anexo N° 2 o de su incorporación voluntaria. Una vez habilitadas, las EPD se sujetan a las obligaciones previstas para dicho rol en el presente Reglamento.

10.2 Las EPD deben dar acceso y suministrar a las ERD los datos e información expresamente comprendidos en el SFA que se encuentren bajo su custodia, administración o responsabilidad, conforme a las condiciones, finalidades y mecanismos previstos en el presente Reglamento y, cuando corresponda, previo consentimiento del usuario y para las finalidades autorizadas por este. Dicho suministro debe efectuarse observando la normativa sobre protección de datos personales, seguridad de la información, ciberseguridad, prevención del lavado de activos y financiamiento del terrorismo, conducta de mercado y demás disposiciones aplicables.

Artículo 11. Responsabilidades de las Entidades Proveedores de Datos

11.1 Son responsabilidades de las EPD:

- a) Desarrollar, implementar, documentar, actualizar y mantener disponibles las APIs mediante las cuales se realiza la solicitud de acceso a los datos del usuario, de conformidad con las especificaciones técnicas y los niveles mínimos de disponibilidad, rendimiento, interoperabilidad y seguridad establecidos en el presente Reglamento.
- b) Verificar, antes del suministro de datos, la identidad de la ERD, la vigencia de sus credenciales y su habilitación en el Directorio para desempeñar dicho rol, así como autenticar al usuario y verificar la existencia, vigencia y alcance de su consentimiento, conforme a lo establecido en el presente Reglamento.
- c) Dar acceso y suministrar a la ERD, de manera oportuna y segura, los datos e información comprendidos en el SFA que se encuentren bajo su custodia o administración y le resulten exigibles, conforme al consentimiento del usuario, cuando corresponda y a las finalidades para las cuales dicho acceso hubiera sido autorizado.
- d) Brindar a las ERD condiciones objetivas, equitativas y no discriminatorias para solicitudes equivalentes, incluidas las condiciones de acceso a las APIs, disponibilidad, rendimiento y calidad del servicio.
- e) Respetar el alcance del consentimiento del usuario y limitar el suministro a los datos, periodo de vigencia y demás condiciones autorizadas.
- f) Registrar y mantener actualizado el estado de los consentimientos asociados a los datos que custodia o administra, poner a disposición del usuario mecanismos accesibles para su consulta, modificación y revocación, y comunicar oportunamente los cambios de estado a los demás participantes involucrados, conforme a los estándares establecidos en el presente Reglamento.
- g) Asegurar que los datos suministrados sean precisos, íntegros, consistentes y actualizados, e implementar controles para identificar y corregir oportunamente los errores materiales que afecte dicha integridad y/o actualización.



- h) Informar las contingencias, incidentes operativos y eventos de seguridad o ciberseguridad que afecten o puedan afectar el acceso o suministro de datos, y coordinar su atención con los participantes involucrados y la Superintendencia, así como con los usuarios afectados, cuando corresponda.
- i) Mantener registros, metadatos y evidencias que permitan demostrar la trazabilidad de las acciones relacionadas con el acceso y suministro de datos, incluyendo, como mínimo, las solicitudes de acceso, la identificación y autenticación de los participantes, los consentimientos, las autenticaciones y confirmaciones del usuario, el suministro de datos, las modificaciones y revocaciones de los consentimientos y los resultados de las solicitudes, por un plazo mínimo de diez (10) años.
- j) Adoptar y mantener políticas, procedimientos y controles para la gestión de los riesgos asociados al desempeño del rol de EPD, incluyendo los relacionados con la seguridad de la información, ciberseguridad, continuidad operativa, prevención del LAFT, conducta de mercado y protección de datos del usuario, de conformidad con el presente Reglamento y las demás disposiciones emitidas por la Superintendencia que le resulten aplicables.

Artículo 12. Entidades Receptores de Datos

- 12.1 Pueden desempeñar el rol de ERD las entidades comprendidas en el párrafo 1.1 del artículo 1 que se encuentren habilitadas para desempeñar dicho rol, de conformidad con el presente Reglamento y que cumplan los requisitos técnicos, operativos, de seguridad y de gestión de riesgos que resulten aplicables.
- 12.2 Asimismo, pueden desempeñar el rol de ERD los PSBD a que se refiere el artículo 14, siempre que se encuentren inscritos en el Registro de Proveedores de Servicios Basados en Datos y habilitados para dicho rol, de conformidad con el presente Reglamento.
- 12.3 Las entidades supervisadas por la Superintendencia que se encuentren habilitadas como ERD pueden prestar servicios basados en datos sin inscribirse en el Registro de Proveedores de Servicios Basados en Datos, siempre que tales servicios se encuentren comprendidos en las actividades que pueden realizar y cumplan la normativa que les resulte aplicable. La exoneración de inscripción no las libera del cumplimiento de las obligaciones previstas para los servicios basados en datos regulados en el presente Reglamento.

Artículo 13. Responsabilidades de las Entidades Receptoras de Datos

Son responsabilidades de las ERD:

- a) Adoptar y mantener los estándares de seguridad, autenticación, control de acceso y monitoreo que permitan proteger la confidencialidad, integridad y disponibilidad de los datos durante su recepción, transmisión, almacenamiento y tratamiento, así como detectar usos no autorizados o actividades potencialmente fraudulentas, de conformidad con el presente Reglamento y las demás disposiciones emitidas por la Superintendencia que resulten aplicables al desempeño del rol de ERD.
- b) Cumplir los estándares de experiencia del usuario aplicables a las solicitudes de acceso, la obtención y gestión del consentimiento y la prestación de servicios basados en datos, de conformidad con el presente Reglamento.
- c) Recibir, almacenar y tratar únicamente los datos necesarios para las finalidades autorizadas por el usuario y abstenerse de utilizarlos para finalidades distintas o adicionales, así como de comunicarlos, cederlos o transferirlos a terceros no comprendidos en el consentimiento.
- d) Identificarse y autenticarse ante la EPD en cada solicitud de acceso, haciendo uso de sus credenciales vigentes como participante del SFA correspondientes al rol de ERD.
- e) Mantener registros, metadatos y evidencias que permitan demostrar la trazabilidad de las acciones relacionadas con la solicitud, acceso, recepción y tratamiento de los datos, así



- como con la obtención, modificación y revocación de los consentimientos, y conservarlos a disposición de la Superintendencia por un plazo mínimo de diez (10) años.
- f) Obtener y gestionar el consentimiento del usuario, garantizando que este sea previo, informado, libre, específico, inequívoco y fácilmente comprensible; poner a su disposición mecanismos accesibles para su consulta, modificación y revocación, y comunicar oportunamente a la EPD la información y los cambios de estado necesarios para verificar su existencia, vigencia y alcance, conforme a los estándares establecidos en el presente Reglamento.
 - g) Gestionar y atender las consultas, solicitudes y reclamos del usuario relacionados con el acceso, recepción y tratamiento de sus datos en el marco del SFA.
 - h) Informar las contingencias y los incidentes operacionales significativos, que incluyen los eventos de interrupción significativa de operaciones y los incidentes de seguridad significativos que afecten o puedan afectar el acceso, recepción o tratamiento de los datos, y coordinar su atención con los participantes involucrados y la Superintendencia, así como con los usuarios afectados, cuando corresponda.
 - i) Suprimir o bloquear, según corresponda, los datos del usuario cuando cese la finalidad que justificó su tratamiento o venza o se revoque el consentimiento que lo sustenta, salvo exista una obligación que justifique su conservación.
 - j) Adoptar y mantener políticas, procedimientos y controles para la gestión de los riesgos asociados al desempeño del rol de ERD, incluyendo los relacionados con la seguridad de la información, ciberseguridad, continuidad operativa, conducta de mercado y protección de datos del usuario, así como con la prevención del LAFT, cuando resulte aplicable, de conformidad con el presente Reglamento y las demás disposiciones emitidas por la Superintendencia.

Artículo 14. Proveedores de Servicios Basados en Datos

- 14.1 Las personas jurídicas no supervisadas por la Superintendencia pueden incorporarse voluntariamente al SFA como PSBD y desempeñar el rol de ERD, para lo cual deben inscribirse en el Registro de Proveedores de Servicios Basados en Datos y encontrarse habilitadas para dicho rol, de conformidad con los requisitos y condiciones establecidos en el presente Reglamento.
- 14.2 Durante su participación en el SFA, los PSBD quedan sujetos al cumplimiento de las disposiciones contenidas en el presente Reglamento y de las demás disposiciones emitidas por la Superintendencia que resulten aplicables al desempeño de sus roles.
- 14.3 Los PSBD deben desempeñar el rol de EPD cuando generen, custodien o administren datos e información comprendidos en el SFA que les resulten exigibles, para lo cual deben obtener previamente la habilitación correspondiente.

Artículo 15. Sobre el servicio de agregación de información

- 15.1 El servicio de agregación de información consiste en recibir, organizar y presentar al usuario, de manera consolidada y a través de una única plataforma o aplicación, información sobre las cuentas, productos y servicios comprendidos en el SFA que mantenga o haya contratado con una o más EPD, incluyendo sus saldos, movimientos y demás datos disponibles, según corresponda.
- 15.2 Pueden prestar el servicio de agregación de información las entidades habilitadas como ERD. Tratándose de entidades supervisadas por la Superintendencia, dicho servicio debe guardar relación con las actividades y operaciones que se encuentren autorizadas a realizar, de conformidad con la normativa que les resulte aplicable. Los PSBD deben haber informado la prestación de dicho servicio como parte de su inscripción y habilitación.



- 15.3 La prestación del servicio se realiza conforme al consentimiento otorgado por el usuario y únicamente respecto de las EPD, productos, servicios, categorías de datos, finalidades, periodo de vigencia y demás condiciones autorizadas.
- 15.4 La información agregada debe presentarse de manera clara, actualizada e identificando la EPD de origen y el producto o servicio al que corresponde. La información elaborada, inferida o calculada por la ERD debe diferenciarse de la información suministrada por las EPD.

Artículo 16. Responsabilidades del PSBD

- 16.1 El PSBD asume las responsabilidades correspondientes a los roles de ERD y/o EPD según se encuentre habilitado. Adicionalmente, debe cumplir las siguientes responsabilidades:
- a) Mantener las condiciones técnicas, operativas, de seguridad, patrimoniales y las demás condiciones que sustentaron su inscripción en el Registro de PSBD y su habilitación para desempeñar los roles correspondientes.
 - b) Informar a la Superintendencia cualquier modificación significativa en su estructura societaria, modelo de negocio, servicios prestados o condiciones que sustentaron su inscripción o habilitación, dentro del plazo y conforme a las condiciones establecidas en el presente Reglamento.
 - c) Proporcionar a la Superintendencia la información, documentación, registros y evidencias que esta le requiera para verificar el cumplimiento de las obligaciones aplicables al PSBD en el marco de su participación en el SFA.
 - d) Designar a un responsable para la coordinación con la Superintendencia sobre aspectos relacionados con el cumplimiento de las obligaciones derivadas de su participación en el SFA, y mantener actualizados los mecanismos de contacto con la Superintendencia.
 - e) Adoptar y mantener políticas, procedimientos y controles internos que aseguren el cumplimiento de las obligaciones aplicables a su inscripción, habilitación y participación en el SFA, de conformidad con el presente Reglamento y las demás disposiciones emitidas por la Superintendencia.

Artículo 17. Registro de Proveedores de Servicios Basados en Datos

- 17.1 La Superintendencia administra el Registro de Proveedores de Servicios Basados en Datos, en el cual deben inscribirse las personas jurídicas no supervisadas por la Superintendencia que soliciten participar voluntariamente en el SFA como PSBD.
- 17.2 Para su inscripción en el Registro de PSBD, la solicitante debe presentar la siguiente información y documentación:
- a) Número de la partida registral de la persona jurídica.
 - b) Número del Registro Único de Contribuyentes (RUC).
 - c) Relación actualizada de accionistas y beneficiarios finales, así como de sus directores, gerentes y principales funcionarios, acompañada de la información y documentación permita evaluar y acreditar su idoneidad moral. Las empresas solicitantes deberán completar el cuestionario del Anexo I de la Resolución SBS N° 211-2021, en lo que les sea aplicable.
 - d) Descripción de la estructura organizacional, las funciones y responsabilidades internas y los mecanismos de gobierno aplicables a las actividades que la solicitante proyecta desarrollar en el marco del SFA.
 - e) Plan de negocio que describa los servicios que proyecta prestar en el SFA, las actividades asociadas, los tipos de usuarios a los que se dirige, las categorías de datos a las que solicita acceder, el modelo de generación de ingresos y las proyecciones financieras y operativas que sustenten su viabilidad.
 - f) Procedimientos para la atención de consultas, solicitudes y reclamos de los usuarios relacionados con los servicios prestados en el marco del SFA.



- g) Políticas, procedimientos y controles para la gestión de riesgos, seguridad de la información, ciberseguridad, protección de datos, prevención de LAFT y de atención a solicitudes del usuario en el marco del SFA.
 - h) Acreditar un patrimonio neto no menor de S/ 678 000. Para tal efecto, la solicitante presenta sus estados financieros auditados correspondientes a los dos (02) últimos ejercicios anuales. Si cuenta con menos de dos ejercicios anuales cerrados, presenta los estados financieros auditados del último ejercicio anual, cuando corresponda, y los estados financieros más recientes del ejercicio en curso. Tratándose de solicitantes recientemente constituidos o que no cuenten con estados financieros auditados, presentar el estado de situación financiera de apertura, la documentación que sustente el patrimonio aportado y el origen de los recursos, así como la información financiera y patrimonial de sus accionistas significativos o controladores que permita acreditar la solvencia económica de dichos accionistas y su capacidad para sostener financieramente las operaciones de la solicitante. En cualquiera de los supuestos anteriores, la Superintendencia puede requerir información adicional para evaluar la solvencia económica de la solicitante.
 - i) Declaración jurada de cumplimiento del presente Reglamento, de la normativa y de someterse a las instrucciones y mandatos emitidos por la Superintendencia que resulten aplicables a su inscripción, habilitación y participación en el SFA.
- 17.3 La solicitante deberá completar satisfactoriamente el proceso de registro y habilitación previsto en el artículo 21 y encontrarse inscrito en el Directorio como ERD y, cuando corresponda, como EPD, como condición necesaria para finalizar su inscripción en el Registro de PSBD.

Artículo 18. Participación obligatoria y voluntaria en el SFA

18.1. Participación obligatoria:

- 18.1.1 Las entidades comprendidas en el párrafo 1.1 del artículo 1 que sean incluidas en la relación publicada por la Superintendencia en su Portal Institucional participan obligatoriamente en el SFA como EPD, conforme a los plazos de incorporación que les resulten aplicables. Para tal efecto, deben completar el proceso de inscripción y habilitación e implementar las APIs y demás componentes técnicos y operativos necesarios para suministrar las categorías de datos que les resulten exigibles.
- 18.1.2 La Superintendencia puede actualizar la relación de entidades obligadas, los plazos de incorporación y las categorías de datos, APIs u otros componentes técnicos y operativos que les resulten exigibles, conforme a los mecanismos previstos en el presente Reglamento y considerando el avance de la implementación y las condiciones necesarias para el adecuado funcionamiento del SFA.

18.2 Participación voluntaria:

- 18.2.1 Las entidades incluidas en la relación de incorporación obligatoria a que se refiere el párrafo 18.1 pueden incorporarse anticipadamente al SFA, antes del vencimiento del plazo de incorporación que les corresponda, previo cumplimiento del proceso de inscripción y habilitación previsto en el presente Título.
- 18.2.2 Las demás entidades comprendidas en el párrafo 1.1 del artículo 1 que no se encuentren incluidas en la relación de incorporación obligatoria pueden solicitar su habilitación para desempeñar voluntariamente el rol de ERD. Cuando generen, custodien o administren datos e información comprendidos en el SFA que les resulten exigibles, deben obtener también la habilitación como EPD.

18.3 Condiciones de permanencia:

- 18.3.1 Los participantes deben mantener los requisitos y condiciones correspondientes a los roles para los que se encuentran habilitados. La Superintendencia puede suspender la habilitación limitar el ejercicio de uno o más roles o excluirlos del Directorio de Participantes cuando



incumplan los requisitos, obligaciones o estándares que resulten aplicables, conforme a lo establecido en el Artículo 22.

Artículo 19. Sobre el Directorio de Participantes

19.1 La inscripción en el Directorio acredita la condición de participante habilitado para desempeñar uno o más de los roles previstos en el presente Título. Dicha inscripción es necesaria para acceder, suministrar o recibir datos e información en el SFA, según el rol reconocido. El Directorio se sujeta a las siguientes disposiciones:

- a) Las entidades pueden inscribirse en el Directorio como EPD, ERD o en ambos roles.
- b) El Directorio es único y permanente, es administrado por la Superintendencia y contiene la información necesaria para identificar a las entidades registradas y a los participantes habilitados, los roles que desempeñan y su estado operativo en el SFA.
- c) Las entidades incluidas en la relación de incorporación obligatoria publicada por la Superintendencia deben inscribirse en el Directorio como EPD. La inscripción como ERD es voluntaria y puede tramitarse conjuntamente con la inscripción como EPD. Las entidades que soliciten su inscripción en ambos roles deben acreditar el cumplimiento de los requisitos correspondientes a cada uno de ellos.
- d) Los participantes deben mantener actualizada la información registrada en el Directorio e informar a la Superintendencia cualquier modificación significativa de la información presentada durante el proceso de registro y habilitación, dentro del plazo y conforme a las condiciones establecidas en el Título V.
- e) El Directorio refleja el estado de las entidades durante el proceso de registro y habilitación a que se refiere el artículo 21, así como el estado operativo de los participantes respecto de cada rol. Solo los estados identificados como habilitado permiten operar en el SFA, conforme a lo previsto en el Título V.

Artículo 20. Acceso anticipado al ambiente de pruebas del Directorio

20.1 La Superintendencia puede otorgar acceso anticipado al ambiente de pruebas del Directorio a las entidades interesadas, antes de iniciar o culminar el proceso de registro y habilitación previsto en el presente Título. Este acceso es voluntario, no otorga la condición de participante ni habilita para operar en el SFA, y no sustituye el cumplimiento de los requisitos exigidos para la inscripción y habilitación correspondientes.

20.2 Las empresas supervisadas por la Superintendencia y los PSBD inscritos en el Registro de PSBD deben presentar:

- a) Solicitud de acceso, indicando los componentes y pruebas que proyectan realizar.
- b) Identificación del funcionario responsable que actúa como punto de contacto ante la Superintendencia.

20.3 Las personas jurídicas no supervisadas que no se encuentren inscritas en el Registro de PSBD deben presentar:

- a) Solicitud de acceso, indicando los componentes y pruebas que proyectan realizar.
- b) Descripción de las actividades que realizan y de su relación con el SFA.
- c) Número de la partida registral de la persona jurídica.
- d) Número del Registro Único de Contribuyentes (RUC).
- e) Identificación de sus directores, gerentes y representantes legales.
- f) Documentación que acredite la idoneidad moral de las personas que integran los órganos de dirección y administración de la empresa. Las empresas deberán aplicar el cuestionario del Anexo I de la Resolución SBS N° 211-2021, en lo que les sea aplicable.
- g) Identificación del responsable que actúa como punto de contacto ante la Superintendencia.

20.4 La Superintendencia aprueba o deniega la solicitud de acceso dentro de los cinco (5) días hábiles siguientes a la presentación de la solicitud completa, en el caso de las entidades a que se refiere



el párrafo 20.2, y dentro de los treinta (30) días hábiles siguientes, en el caso de las personas jurídicas a que se refiere el párrafo 20.3.

20.5 El acceso anticipado se otorga por un plazo máximo de noventa (90) días calendarios, contado desde su habilitación. El otorgamiento y mantenimiento del acceso anticipado están sujetos a la disponibilidad de recursos y capacidades técnicas y operativas de la Superintendencia. Cuando concurren solicitudes o existan limitaciones de capacidad, la Superintendencia puede aplicar criterios de priorización.

20.6 Las pruebas se realizan exclusivamente con datos sintéticos o ficticios y no pueden comprender datos personales ni información real de los usuarios.

Artículo 21. Proceso de inscripción para participar en el SFA

21.1. La inscripción de una entidad en el Directorio como EPD, ERD o en ambos roles comprende dos etapas: registro y habilitación técnica. La aprobación de la etapa de registro no otorga la condición de participante ni habilita a la entidad para operar en el SFA.

21.2. Etapa de registro en el Directorio del SFA

21.2.1 La entidad solicitante debe presentar la siguiente información y documentación:

- a) Formato de solicitud de participación, que incluya la identificación de la entidad, sus representantes y los responsables designados para la interacción con el SFA, así como el rol o los roles para los que solicita su habilitación.
- b) Informe de riesgos por nuevos productos o cambios importantes, conforme a los lineamientos de la Circular N° G-165-2012 o la norma que la sustituya.
- c) Informe de Cumplimiento de la regulación del SFA, aprobado por el Directorio u órgano equivalente, que describa el estado de implementación de los requisitos aplicables a los roles solicitados y contenga, como mínimo, lo siguiente:
 - i. La estructura de gobierno, la asignación de responsabilidades y los mecanismos de gestión de riesgos y control interno aplicables a su participación en el SFA.
 - ii. La infraestructura tecnológica, los recursos y capacidades técnicas y operativas, y las APIs y demás componentes implementados o en proceso de implementación para suministrar o recibir datos, según el rol solicitado.
 - iii. Las medidas implementadas en materia de seguridad de la información, ciberseguridad, protección de datos, monitoreo y trazabilidad.
 - iv. Los mecanismos implementados para la obtención y gestión del consentimiento, la autenticación y confirmación del usuario, y la comunicación de los cambios en el estado del consentimiento entre los participantes involucrados.
 - v. Los flujos, interfaces y controles implementados para cumplir los estándares de experiencia del usuario, así como los procedimientos para atender sus consultas, solicitudes y reclamos.
 - vi. El plan de trabajo para completar las pruebas, validaciones y certificaciones exigibles durante la etapa de habilitación técnica, indicando las actividades realizadas, las actividades pendientes y los plazos previstos para su culminación.
- d) Cuando la participación sea voluntaria, la entidad debe presentar, adicionalmente, el sustento de la aprobación de su directorio u órgano equivalente para participar en el SFA.

21.2.2 La Superintendencia evalúa la documentación presentada dentro del plazo de treinta (30) días hábiles, contado desde la recepción de la solicitud completa.

21.2.3 Concluida la evaluación, la Superintendencia aprueba o deniega la etapa de inscripción. Cuando la aprueba, incorpora a la entidad en el Directorio y le asigna las credenciales y accesos necesarios para continuar con la etapa de habilitación técnica.

21.3 Etapa de habilitación técnica en el Directorio del SFA:

21.3.1 La etapa de habilitación técnica tiene por finalidad verificar que la entidad solicitante dispone de las capacidades técnicas, operativas, de seguridad, interoperabilidad, gestión de datos y



experiencia del usuario exigibles para desempeñar los roles solicitados. Para tal efecto, la Superintendencia brinda a la entidad incorporada al Directorio en la etapa anterior acceso al ambiente de pruebas y a las demás herramientas necesarias para completar esta etapa.

21.3.2 Para obtener la habilitación técnica, la entidad debe:

- a) Cuando solicite desempeñar el rol de EPD, registrar y configurar los servidores de autorización, APIs, metadatos, certificados digitales, endpoints, mecanismos de contingencia y demás componentes técnicos exigibles para dicho rol.
- b) Cuando solicite desempeñar el rol de ERD, registrar y configurar las aplicaciones cliente, metadatos, certificados digitales, endpoints y demás componentes técnicos exigibles para dicho rol.
- c) Superar satisfactoriamente las pruebas de integración, interoperabilidad y seguridad, así como las validaciones funcionales y de experiencia del usuario, de conformidad con los estándares técnicos y casos de prueba definidos por la Superintendencia, a través del ambiente de pruebas (sandbox tecnológico) y de los demás mecanismos de validación establecidos en el Directorio.
- d) Presentar evidencia de la obtención de la certificación FAPI 2.0 Perú que corresponda al rol solicitado:
 - i. En el caso de las EPD, como OpenID Provider.
 - ii. En el caso de las ERD, como Relying Party.

21.3.3 La Superintendencia puede realizar visitas de comprobación y requerir las demostraciones, documentos o evidencias adicionales necesarias para verificar el cumplimiento de los requisitos de habilitación.

21.3.4 Aprobada esta etapa, la Superintendencia habilita a la entidad en el Directorio respecto de cada rol aprobado. Desde ese momento, la entidad adquiere la condición de participante y puede operar en el SFA conforme a dichos roles.

21.3.5 La entidad dispone de un plazo de noventa (90) días calendario, contado desde la aprobación de la etapa de registro, para culminar satisfactoriamente la etapa de habilitación técnica. Si transcorre el plazo máximo para obtener la habilitación sin que la entidad la haya obtenido por causas imputables a ella, la SBS declara la pérdida de vigencia de su inscripción en el Directorio mediante resolución debidamente motivada. En tal supuesto, la entidad podrá presentar una nueva solicitud de participación en el SFA conforme al procedimiento establecido en el presente Reglamento.

21.4 Los requisitos previstos en el presente artículo se aplican según el rol o los roles para los que la entidad solicita su inscripción en el Directorio. El participante habilitado para un solo rol, que posteriormente solicite su habilitación para un rol distinto, debe presentar una nueva solicitud de inscripción y cumplir con los requisitos aplicables a dicho rol.

Artículo 22. Suspensión, retiro y cancelación de la inscripción en el SFA

22.1 La Superintendencia puede suspender la habilitación de un participante respecto de uno o más roles cuando:

- a) Incumpla los requisitos, obligaciones o estándares aplicables a su participación en el SFA, cuando dicho incumplimiento genere riesgos significativos para la seguridad, continuidad operativa, integridad de los datos, protección de los usuarios, eficiencia del Sistema o su estabilidad, o en el caso que no se subsane dichos incumplimientos dentro del plazo otorgado por la Superintendencia.
- b) Presente deficiencias operativas, de seguridad, ciberseguridad, continuidad, calidad de datos o gestión de riesgos que generen un riesgo relevante, actual o inminente para la confidencialidad, integridad, disponibilidad de los datos o continuidad de los servicios del SFA.



- c) La Superintendencia podrá suspender temporalmente la habilitación cuando identifique incidentes graves, vulneraciones de seguridad, riesgos operativos significativos o cualquier situación excepcional debidamente acreditada que pueda producir un perjuicio relevante a los usuarios o a la integridad del SFA. La suspensión de la habilitación se mantendrá mientras persista el incumplimiento que dio lugar a su imposición, sin perjuicio de las responsabilidades administrativas, civiles o penales que correspondan.

La suspensión de la habilitación se mantendrá mientras persista el incumplimiento que dio lugar a su imposición hasta un plazo máximo de ciento veinte (120) días calendarios, sin perjuicio de las responsabilidades administrativas, civiles o penales que correspondan.

- 22.2 La Superintendencia puede cancelar la habilitación de un participante respecto de uno o más roles cuando:

- a) Pierda la autorización, inscripción o condición legal necesaria para desarrollar las actividades vinculadas con su participación en el SFA, sea sometido a un régimen de intervención, disolución o liquidación, o se configure una situación jurídica o material debidamente acreditada que determine la imposibilidad legal o técnica permanente de continuar ejerciendo el rol para el cual fue habilitado.
- b) El incumplimiento que motivó la suspensión no sea subsanado dentro del plazo otorgado por la Superintendencia, el cual no podrá ser mayor de ciento veinte (120) días calendarios.
- c) El incumplimiento sea insubsanable o genere una afectación grave o un riesgo inminente para la confidencialidad, integridad, disponibilidad de la información, continuidad de los servicios o protección de los usuarios del SFA.
- d) Se apruebe la solicitud de retiro respecto de un rol cuya participación tenga carácter voluntario.

Cuando la cancelación comprenda todos los roles para los que el participante se encuentra habilitado, la Superintendencia cancela su inscripción y lo excluye del Directorio. La cancelación produce efectos desde la fecha que determine la resolución correspondiente, sin perjuicio del cumplimiento de las obligaciones pendientes derivadas de su participación en el SFA.

- 22.3 El participante puede solicitar su retiro voluntario respecto de uno o más roles cuya participación no tenga carácter obligatorio. Para tal efecto, debe presentar un plan de salida ordenada que contemple, como mínimo, el tratamiento de las solicitudes y operaciones pendientes, el cese de nuevos accesos o suministros correspondientes a los roles objeto del retiro, la gestión de los consentimientos vigentes y la comunicación a los usuarios y demás participantes involucrados. Durante la ejecución del plan, la Superintendencia puede suspender la habilitación respecto de uno o más roles objeto del retiro o limitar la realización de nuevos intercambios bajo dichos roles. El retiro produce efectos cuando la Superintendencia lo aprueba y actualiza el estado correspondiente en el Directorio.

- 22.4 La suspensión, retiro o cancelación de la habilitación como ERD no afecta la obligación de la entidad de mantener su participación y continuar suministrando los datos e información que le resulten exigibles como EPD, cuando dicha participación tenga carácter obligatorio. La entidad no puede interrumpir unilateralmente el cumplimiento de dicha obligación. Su incumplimiento da lugar a la adopción de las medidas correctivas y a la aplicación de las sanciones administrativas que correspondan, incluida la suspensión temporal de la habilitación como EPD cuando se configure alguna de las causales previstas en el párrafo 22.1.

TÍTULO IV

ACCESO Y CONTROL DEL USUARIO

CAPÍTULO I

DISPOSICIONES GENERALES DEL CONTROL DEL USUARIO



Artículo 23. Tratamiento de la información del usuario en el SFA

- 23.1 Los participantes deben acceder, suministrar y tratar los datos e información conforme a la finalidad establecida en el consentimiento otorgado por el usuario y sujetarse a los principios establecidos en la normativa aplicable sobre protección de datos personales, sin perjuicio de los tratamientos permitidos o exigidos por la normativa vigente.
- 23.2 Los datos del usuario no pueden ser utilizados, almacenados, cedidos o tratados para finalidades distintas de aquellas expresamente autorizadas por el usuario, salvo que exista una habilitación legal para ello. Los participantes deben adoptar las medidas que correspondan para garantizar que los datos tratados en el marco del SFA sean adecuados, pertinentes y limitados a lo necesario para la finalidad autorizada.
- 23.3 Las personas jurídicas no supervisadas por la Superintendencia, inscritas en el Registro de PSBD y habilitadas en el Directorio para desempeñar el rol de ERD, que presten el servicio de agregación de información previsto en el artículo 15, no pueden conservar los datos e información a los que accedan más allá del plazo necesario para la prestación del servicio de agregación conforme a la finalidad autorizada por el usuario, salvo que exista una obligación legal que justifique su conservación.

Artículo 24. Condiciones generales de la experiencia de usuario

- 24.1 Los participantes deben diseñar, implementar y mantener las interfaces, comunicaciones, mecanismos de interacción y demás elementos vinculados a la solicitud de acceso a los datos del usuario y a la gestión de sus consentimientos, de manera que garanticen una experiencia uniforme, transparente, eficiente y centrada en el usuario. Para ello, estas deben cumplir las siguientes características:
- a) Simplicidad: implica que las interfaces, comunicaciones y mecanismos de interacción deben diseñarse de manera sencilla e intuitiva, de modo que el usuario pueda comprender fácilmente la información que se le presenta y las decisiones que debe adoptar.
 - b) Transparencia: busca que el usuario disponga de información suficiente, precisa y oportuna que le permita comprender las características, el alcance y las consecuencias del acceso a sus datos. Los participantes deben adoptar medidas que permitan al usuario identificar claramente el entorno en el que se encuentra y reconocer las acciones que realiza y autoriza durante el proceso.
 - c) Agilidad: procura que el flujo para otorgar acceso a los datos del usuario se desarrolle de manera continua y eficiente, evitando demoras, interrupciones o pasos innecesarios que puedan afectar la adecuada finalización del proceso. Para ello, los participantes deben reducir las acciones innecesarias requeridas al usuario y facilitar la conclusión del proceso.
 - d) Neutralidad: asegura que las interfaces, comunicaciones y demás mecanismos de interacción no influyan indebidamente en las decisiones del usuario respecto del otorgamiento, gestión o revocación de un consentimiento. Los participantes deben abstenerse de utilizar mensajes, configuraciones, tratamientos diferenciados de la información, elementos visuales u otros mecanismos que favorezcan injustificadamente una determinada decisión del usuario o desincentiven el ejercicio de los derechos del usuario respecto de sus datos.
 - e) Accesibilidad: implica que las interfaces, comunicaciones y mecanismos de interacción consideren las necesidades de los distintos tipos de usuarios y faciliten el acceso, la comprensión y la utilización de los servicios vinculados al SFA. Para ello, la información debe presentarse de forma legible y comprensible, y deben implementarse mecanismos que faciliten la interacción del usuario y reduzcan las barreras de acceso derivadas de limitaciones físicas, sensoriales o cognitivas.
- 24.2 Está prohibido incorporar interfaces, procedimientos, validaciones o elementos redundantes o que generen complejidad innecesaria para el usuario, ni utilizar mecanismos que dificulten el



proceso o induzcan injustificadamente al usuario a abandonar la solicitud de acceso a sus datos. Esta prohibición no comprende las medidas de autenticación, verificación, seguridad, prevención del fraude o cumplimiento regulatorio que resulten necesarias y proporcionales para gestionar los riesgos asociados al SFA.

Artículo 25. Indicadores de la experiencia del usuario

Los participantes deben medir anualmente los indicadores de experiencia del usuario relacionados con las solicitudes de acceso a sus datos y la gestión de sus consentimientos. Las mediciones deben permitir identificar oportunidades de mejora en el diseño e implementación de las interfaces, comunicaciones, mecanismos de interacción y demás elementos que formen parte de la experiencia del usuario. Los resultados y el sustento de las mediciones deben conservarse en formato digital y mantenerse a disposición de la Superintendencia.

Cuando las mediciones evidencien deficiencias o riesgos que puedan afectar la adecuada toma de decisiones por parte de los usuarios, los participantes deben adoptar las medidas correctivas que correspondan.

Artículo 26. Manual de experiencia del usuario

26.1 La Superintendencia publica el Manual de Experiencia del Usuario del Sistema de Finanzas Abiertas en el Portal del SFA, con la finalidad de desarrollar y facilitar la aplicación de las disposiciones sobre experiencia del usuario en la solicitud de acceso a los datos del usuario y la gestión del consentimiento previstas en el presente Título, así como orientar el diseño e implementación de las interfaces, comunicaciones y mecanismos de interacción requeridos para su cumplimiento. El contenido del Manual es de cumplimiento obligatorio para los participantes y están orientadas a garantizar una experiencia uniforme, clara, eficiente y centrada en el usuario.

26.2 El Manual desarrolla requisitos aplicables a:

- a) El flujo de consentimiento para el acceso a los datos del usuario que sean personas naturales.
- b) El flujo de consentimiento para el acceso a los datos del usuario que sean personas jurídicas.
- c) El flujo de consentimiento para el acceso a datos vinculados a productos o servicios respecto de los cuales su otorgamiento requiera la participación o autorización de más de un titular, representante o persona facultada.
- d) El diseño e implementación del panel de gestión de consentimientos de personas naturales y jurídicas.

CAPÍTULO II

ACCESO A LOS DATOS DEL USUARIO Y GESTIÓN DEL CONSENTIMIENTO

Artículo 27. Solicitud de acceso a los datos del usuario

27.1 La solicitud de acceso a los datos del usuario en el marco del SFA comprende las etapas sucesivas de consentimiento, autenticación y confirmación definidas en el Artículo 2 del presente Reglamento.

27.2 Los participantes deben proporcionar al usuario información empleando lenguaje sencillo y fácilmente accesible para el usuario y adecuada sobre el funcionamiento y alcance de las etapas de consentimiento, autenticación y confirmación implementados en el SFA. Dichas etapas deben cumplir con las siguientes características:

- a) Ejecutarse de forma segura y eficiente



- b) Realizarse por canales digitales.
 - c) Desarrollarse de manera sucesiva y sin interrupciones injustificadas. Las interrupciones justificadas pueden ser aquellas necesarias por razones operativas, de seguridad o prevención de fraude.
- 27.3 Los participantes deben asegurar que la solicitud de acceso a los datos del usuario permita a este comprender, antes de otorgar su consentimiento, el alcance de la solicitud, la identidad de los participantes involucrados, la finalidad, las categorías o grupos de datos y el plazo de vigencia del consentimiento.
- 27.4 La finalidad para el acceso a los datos del usuario debe ser específica y corresponder a alguno de los supuestos previstos en el Anexo N° 1 del presente Reglamento. El acceso a los datos del usuario no constituye, por sí mismo, una finalidad.
- 27.5 El usuario debe poder rechazar la solicitud de acceso a los datos o abandonar el proceso en cualquier momento antes de la confirmación, de forma sencilla, clara y accesible, mediante mecanismos simples y equivalentes a los utilizados para otorgar el consentimiento.

Artículo 28. Sobre la etapa de consentimiento del usuario

- 28.1 El otorgamiento del consentimiento para acceder a los datos del usuario constituye un proceso independiente de la oferta o contratación de los productos o servicios ofrecidos por los participantes. En consecuencia, la decisión del usuario de otorgar, denegar o revocar su consentimiento no debe afectar el acceso o provisión de estos productos o servicios, salvo para la prestación del servicio de agregación de información referido en el Artículo 15 u otros supuestos expresamente previstos en el presente Reglamento.
- 28.2 El consentimiento debe ser granular y proporcionar un nivel de detalle suficiente que permita al usuario conocer con claridad los elementos que comprende, incluidas las finalidades específicas y las categorías o grupos de datos asociadas a estas. Las categorías o grupos de datos vinculadas con cada finalidad deben presentarse de forma agrupada, clara, objetiva y comprensible para el usuario, permitiéndole conocer los datos que las integran y su correspondencia con la finalidad respectiva.
- 28.3 Las interfaces deben permitir al usuario otorgar el consentimiento de manera independiente para cada finalidad. Cada finalidad debe estar asociada a las categorías o grupos de datos necesarias y proporcionales para su cumplimiento.

Artículo 29. Contenido mínimo del consentimiento

- 29.1 El consentimiento debe permitir al usuario conocer, de manera clara y comprensible la siguiente información:
- a) Identificación del usuario
 - b) La identidad de la ERD que solicita el acceso a sus datos.
 - c) La identidad de la EPD que suministrará los datos.
 - d) El rol que desempeña cada participante.
 - e) Los productos o servicios financieros, cooperativos o previsionales del usuario respecto de los cuales se solicita el acceso a los datos objeto del consentimiento, cuando corresponda.
 - f) Las categorías o grupos de datos comprendidas en el consentimiento
 - g) La descripción clara y específica de la finalidad para la que se utilizarán los datos del usuario, conforme a las finalidades establecidas en el Anexo N° 1 del presente Reglamento. Cuando el consentimiento comprenda más de una finalidad, estas deben presentarse de manera separada, de modo que el usuario pueda identificar claramente cada una de ellas.
 - h) El plazo de vigencia del consentimiento y su fecha de vencimiento, así como la posibilidad de que la nueva información, asociada a las categorías o grupos de datos referidas en el literal f) del presente artículo que se genere hasta el término de la vigencia del consentimiento también será compartida.



- i) La información sobre el derecho del usuario a revocar su consentimiento en cualquier momento.

29.2 La modificación de cualquiera de los elementos señalados en el párrafo 29.1 que altere el alcance del consentimiento requiere la obtención de un nuevo consentimiento del usuario.

Artículo 30. Prohibiciones aplicables en el proceso de obtención del consentimiento del usuario

30.1 Las ERD tienen prohibido solicitar, obtener o mantener consentimientos:

- a) Que contengan finalidades genéricas, indeterminadas o que no permitan identificar de manera específica el uso que se dará a los datos.
- b) Que comprendan categorías o grupos de datos que no resulten pertinentes, necesarias y proporcionales para la finalidad informada al usuario.
- c) Obtenidos sin cumplir con las disposiciones de experiencia del usuario establecidas en el presente Título.
- d) Que comprendan la misma finalidad y las mismas categorías o grupos de datos que otro consentimiento vigente otorgado por el usuario respecto de la misma EPD.
- e) Que condicionen el otorgamiento de productos o servicios al consentimiento para finalidades distintas de aquellas estrictamente necesarias para su prestación.

Artículo 31. Sobre la etapa de autenticación del usuario

La autenticación del usuario debe ser realizada por la EPD mediante mecanismos que observen estándares de seguridad equivalentes o superiores a los exigidos para acceder a sus canales digitales, de conformidad con las disposiciones previstas en el Título VII del presente Reglamento. La autenticación es obligatoria para otorgar, modificar o revocar el consentimiento en el marco del SFA y debe efectuarse mediante mecanismos que impidan que la ERD tenga acceso a las credenciales utilizadas por el usuario ante la EPD.

Artículo 32. Sobre la etapa de confirmación

- 32.1 Las EPD deben solicitar la confirmación expresa del usuario para compartir sus datos antes de suministrarlos a las ERD. Dicha confirmación debe realizarse con el uso de un factor de autenticación que cumpla con las disposiciones aplicables en materia de seguridad de la información y ciberseguridad y con lo establecido en el presente Reglamento.
- 32.2 El procedimiento de confirmación debe permitir al usuario visualizar, de forma clara y mediante un lenguaje sencillo, el detalle del consentimiento, el cual debe corresponder a la información autorizada por el usuario en la ERD. Cuando los datos cuyo acceso se autoriza se encuentren vinculados a un producto con más de un titular y se requiera la confirmación de los demás titulares para su suministro, la EPD debe informar esta situación al usuario y notificar a dichos titulares, a fin de que otorguen la confirmación correspondiente.
- 32.3 Las ERD deben comunicar de forma inmediata al usuario la ejecución satisfactoria de la solicitud de acceso a sus datos y proporcionarle información que le permita conocer las principales características del consentimiento otorgado y los mecanismos disponibles para su gestión.
- 32.4 Las notificaciones y comunicaciones señaladas en los párrafos precedentes deben realizarse a través de medios que permitan dejar constancia de su envío y contenido, tales como correos electrónicos o notificaciones mediante aplicaciones móviles que permitan su trazabilidad.

Artículo 33. Información mínima para el usuario durante la etapa de confirmación de la solicitud de acceso a sus datos

- 33.1 Para el suministro de los datos del usuario, la confirmación debe mostrar, como mínimo la información señalada en los literales a), b), c), d), f), h) e i) del numeral 29.1 del Artículo 29. Adicionalmente, se debe presentar al usuario la posibilidad de seleccionar el origen de los datos,



que podría incluir la selección de cuentas, productos o servicios financieros que cumplan con la información requerida en el literal e) del numeral 29.1 del Artículo 29.

Artículo 34. Panel de gestión del consentimiento

- 34.1 Los participantes deben poner a disposición del usuario un panel de gestión de consentimientos que le permita consultar, gestionar o revocar los consentimientos otorgados en el marco del SFA.
- 34.2 El panel de gestión de consentimientos debe ser de acceso gratuito, remoto, seguro, accesible, intuitivo, estar disponible mediante los canales electrónicos de los participantes y cumplir con los lineamientos para su implementación.
- 34.3 El panel de gestión de consentimientos debe permitir al usuario consultar, gestionar o revocar sus consentimientos desde la ERD o la EPD involucradas.
- 34.4 Los participantes deben mantener actualizado el estado de los consentimientos y evitar accesos o tratamientos luego de su vencimiento o revocación.

Artículo 35. Información disponible en el panel de gestión de consentimientos

- 35.1 El panel de gestión de consentimientos debe mostrar al usuario, respecto de cada consentimiento vigente, revocado o vencido, su identificador único y, como mínimo, la información que, según corresponda, le hubiera sido presentada por la ERD o la EPD durante el proceso de otorgamiento del consentimiento, así como las modificaciones realizadas respecto de cada uno.
- 35.2 La información correspondiente a los consentimientos vigentes debe mantenerse disponible para consulta y visualización del usuario en el panel durante su vigencia. Tratándose de consentimientos vencidos o revocados, dicha información debe mantenerse disponible por un plazo mínimo de diez (10) años, contado desde la fecha de su vencimiento o revocación, según corresponda.

Artículo 36. Sobre la revocación del consentimiento

- 36.1 Los participantes deben garantizar que el consentimiento pueda ser revocado por el usuario en cualquier momento, de forma inmediata y sin expresión de causa a través del panel de gestión de consentimientos.
- 36.2 La revocación del consentimiento impedirá a los participantes continuar accediendo, suministrando o tratando los datos del usuario; salvo respecto de la conservación de información exigida por ley o por requerimientos regulatorios, sin que ello habilite nuevos tratamientos incompatibles con la finalidad que justificó dicha conservación.
- 36.3 Se prohíbe a las EPD incentivar, inducir o sugerir a los usuarios la revocación de los consentimientos otorgados a otros participantes del SFA, así como desplegar acciones comerciales o de comunicación orientadas a tal fin.

CAPÍTULO III

EXPERIENCIA DEL USUARIO EN EL FLUJO PARA ACCEDER A LOS DATOS DEL USUARIO

Artículo 37. Experiencia del usuario durante la etapa de consentimiento

- 37.1 Al iniciar la solicitud de acceso a los datos del usuario, las ERD deben:
 - a) Poner a disposición del usuario un entorno de bienvenida que le permita reconocer que está iniciando una solicitud de acceso a sus datos en el marco del SFA, incorporando elementos que faciliten la identificación de dicho entorno.
 - b) Proporcionar información que permita al usuario comprender que el acceso a sus datos se realiza mediante mecanismos seguros y conforme a las disposiciones establecidas en el Reglamento.



- c) Presentar un resumen de las principales etapas que conforman la jornada de consentimiento y de las acciones que el usuario debe realizar para completar cada etapa.
- 37.2 Para la identificación del usuario, la ERD debe solicitar únicamente la información necesaria para identificar a aquel respecto del cual se efectuará la solicitud de acceso a los datos.
- 37.3 Para la selección de la EPD, las ERD deben:
- a) Poner a disposición del usuario mecanismos que faciliten la búsqueda, identificación y selección de la EPD.
 - b) Mostrar únicamente las EPD registradas en el Directorio de Participantes referido en el Título V del presente Reglamento, incorporando mecanismos que permitan al usuario identificar de manera clara su estado de disponibilidad, tales como elementos visuales diferenciados o restricciones que impidan iniciar el intercambio de datos cuando la EPD no se encuentre en estado activo.
 - c) Mostrar la denominación y el logotipo de cada EPD disponible para su selección.
 - d) Permitir al usuario identificar de manera clara e inequívoca la EPD seleccionada, distinguiéndola visualmente de las demás alternativas disponibles antes de continuar con la jornada.
- 37.4 Para que el usuario pueda conocer el alcance del consentimiento, las ERD deben considerar la información mínima establecida en el numeral 29.1 del Artículo 29 de manera clara, visible y comprensible. La información debe organizarse y presentarse de forma que facilite su lectura, identificación y comprensión por parte del usuario, evitando elementos que dificulten, confundan o interfieran con su entendimiento.
- 37.5 Las ERD deben permitir al usuario definir el plazo durante el cual se mantendrá vigente el consentimiento. Para tal efecto, deben:
- a) Fijar un plazo predeterminado para cada solicitud de acceso a los datos, siempre que este corresponda al plazo mínimo necesario para la finalidad para la cual se solicita el consentimiento. El usuario debe poder modificar fácilmente dicho plazo antes de otorgar su consentimiento, y el establecimiento predeterminado de dicha condición para la finalidad respectiva no debe desincentivar la selección de otras alternativas disponibles.
 - b) Permitir que el usuario seleccione el plazo dentro de los límites previstos en el Reglamento y de acuerdo con la finalidad correspondiente.
 - c) Presentar las alternativas de plazo de manera clara y debe ser consistente con la finalidad.
 - d) Informar al usuario la fecha de vencimiento del consentimiento correspondiente al plazo seleccionado.
 - e) Informar al usuario que, mientras el consentimiento permanezca vigente, los datos generados con posterioridad a su otorgamiento también podrán ser objeto de acceso, hasta que el consentimiento sea revocado o expire por vencimiento del plazo seleccionado, según corresponda.
- 37.6 Antes de redireccionar al usuario al entorno de la EPD para continuar con la solicitud de acceso a los datos del usuario, la ERD debe:
- a) Informarle que será redireccionado al entorno de la EPD y que dicho redireccionamiento se realiza mediante mecanismos seguros.
 - b) Permitirle identificar claramente la ERD desde la cual se realiza el redireccionamiento y la EPD al que será redireccionado.
- 37.7 Durante el redireccionamiento, en la interfaz de redireccionamiento la ERD debe:
- a) Presentar el proceso de redireccionamiento mediante elementos visuales que permitan al usuario comprender la transición entre la ERD y la EPD.
 - b) Ejecutar el redireccionamiento, sin requerir acciones adicionales innecesarias o ajenas al proceso de autenticación y seguridad.

Artículo 38. Experiencia del usuario durante la etapa de autenticación



38.1 Durante el proceso de autenticación, la EPD debe:

- a) Permitir que el usuario identifique de manera clara que se encuentra en el entorno de la EPD.
- b) Aplicar los mecanismos de autenticación de manera que el usuario pueda completar el proceso sin pasos, validaciones o requerimientos adicionales a aquellos que formen parte de los mecanismos habituales de autenticación utilizados por la EPD.
- c) Garantizar que las credenciales no sean visibles, almacenadas, capturadas, procesadas ni compartidas con la ERD.
- d) Adoptar medidas técnicas y organizativas destinadas a impedir que la ERD tenga acceso directo o indirecto a las credenciales utilizadas por el usuario.

Artículo 39. Experiencia del usuario durante la etapa de confirmación

39.1 Para obtener la confirmación del usuario respecto de la solicitud de acceso a sus datos, la EPD debe presentar la información referida en el Artículo 33. Además, debe informarse al usuario que, mientras el consentimiento permanezca vigente, los datos generados con posterioridad a su otorgamiento también podrán ser objeto de suministro, hasta que este sea revocado o expire por vencimiento del plazo correspondiente, de ser aplicable.

39.2 La EPD debe permitir al usuario seleccionar los productos respecto de los cuales autorizará el suministro de los datos. Para tal efecto, debe:

- a) Mostrar únicamente los productos respecto de los cuales pueda efectuarse el suministro de los datos solicitados por la ERD, presentándolos de manera estructurada y comprensible y agrupándolos según su naturaleza o categoría.
- b) Abstenerse de presentar productos preseleccionados o utilizar configuraciones predeterminadas que impliquen una manifestación anticipada de la voluntad del usuario.
- c) Proporcionar información suficiente que permita al usuario identificar claramente cada producto respecto del cual puede autorizar el suministro de sus datos.
- d) Permitir al usuario seleccionar uno o más productos cuando existan múltiples alternativas disponibles y ello resulte compatible con la finalidad correspondiente.

39.3 La EPD debe obtener la manifestación expresa de la voluntad del usuario para confirmar el suministro de los datos solicitados, utilizando para ello un factor de autenticación que cumpla con las disposiciones de la normativa vigente aplicables a la ejecución de operaciones.

39.4 Una vez realizada la confirmación y antes de redireccionar al usuario al entorno de la ERD, la EPD debe:

- a) Informar al usuario que será redireccionado a la ERD y que dicho redireccionamiento se realiza mediante mecanismos seguros.
- b) Permitir que el usuario identifique claramente la EPD desde la cual se realiza el redireccionamiento y la ERD hacia la cual será dirigido.
- c) Presentar el proceso de redireccionamiento mediante elementos visuales que permitan al usuario comprender la transición entre la EPD y la ERD.
- d) Realizar el redireccionamiento sin requerir acciones adicionales innecesarias o ajenas a los controles de seguridad y gestión de riesgos

39.5 Una vez ejecutada satisfactoriamente la solicitud de acceso a los datos, la ERD debe comunicarlo al usuario de manera inmediata y proporcionarle información establecida en el artículo 29, incluyendo:

- a) Información acerca que la solicitud de acceso a sus datos ha sido ejecutada satisfactoriamente.



- b) Los mecanismos disponibles para consultar, gestionar, modificar o revocar el consentimiento.
- c) Que puede revocar el consentimiento en cualquier momento durante su vigencia.

Artículo 40. Experiencia del usuario en la gestión de sus consentimientos a través del panel de gestión de consentimientos

- 40.1 Los participantes deben poner a disposición del usuario, a través de sus canales digitales, el panel de gestión de consentimientos al que se refiere el artículo 34 del presente Reglamento. El panel debe ser de fácil acceso y, para tal efecto, el mecanismo dispuesto para acceder a este debe encontrarse de forma destacada y visible en la interfaz que se muestra al usuario una vez autenticado en dichos canales, sin que requiera realizar acciones adicionales de navegación o desplazamiento para identificarlo.
- 40.2 El panel de gestión de consentimientos debe disponer de mecanismos de acceso diferenciados y claramente identificables que permitan al usuario acceder a las siguientes opciones:
 - a) Consulta de consentimientos: interfaz que permita visualizar los consentimientos otorgados y acceder a la información asociada a cada uno de ellos. Esta opción debe contar con herramientas de búsqueda de fácil acceso y uso intuitivo que faciliten al usuario la identificación y localización de sus consentimientos.
 - b) Revocación de consentimientos: interfaz que permita dejar sin efecto los consentimientos previamente otorgados.
 - c) Modificación de consentimientos: interfaz que permita modificar el alcance o extender el plazo de vigencia de los consentimientos previamente otorgados, previendo lo establecido en el artículo 29.
- 40.3 La información puesta a disposición del usuario a través del panel de gestión de consentimientos debe ser consistente con el rol que desempeñe cada participante en la solicitud de acceso a los datos del usuario y con la información que le corresponda gestionar, incluyendo el estado del consentimiento, de acuerdo con lo establecido en el Título VII del presente Reglamento.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

PROYECTO NORMATIVO

TÍTULO V
INFRAESTRUCTURA DIGITAL

Las disposiciones correspondientes al presente Título serán desarrolladas y aprobadas mediante resolución posterior de la Superintendencia. Hasta su entrada en vigencia, resultan aplicables las disposiciones vigentes que correspondan según la materia.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

PROYECTO NORMATIVO

TÍTULO VI
MARCO DE CONFIANZA

Las disposiciones correspondientes al presente Título serán desarrolladas y aprobadas mediante resolución posterior de la Superintendencia. Hasta su entrada en vigencia, resultan aplicables las disposiciones vigentes que correspondan según la materia.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

PROYECTO NORMATIVO

TÍTULO VII
ESTÁNDARES, SEGURIDAD Y CALIDAD

Las disposiciones correspondientes al presente Título serán desarrolladas y aprobadas mediante resolución posterior de la Superintendencia. Hasta su entrada en vigencia, resultan aplicables las disposiciones vigentes que correspondan según la materia.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

PROYECTO NORMATIVO

TÍTULO VIII
RECUPERACIÓN DE COSTOS

Las disposiciones correspondientes al presente Título serán desarrolladas y aprobadas mediante resolución posterior de la Superintendencia. Hasta su entrada en vigencia, resultan aplicables las disposiciones vigentes que correspondan según la materia.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

PROYECTO NORMATIVO

TÍTULO IX
PROBLEMAS, INCIDENTES Y DISPUTAS

Las disposiciones correspondientes al presente Título serán desarrolladas y aprobadas mediante resolución posterior de la Superintendencia. Hasta su entrada en vigencia, resultan aplicables las disposiciones vigentes que correspondan según la materia.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

PROYECTO NORMATIVO

TÍTULO X
MONITOREO, MEDIDAS CORRECTIVAS Y SANCIONES

Las disposiciones correspondientes al presente Título serán desarrolladas y aprobadas mediante resolución posterior de la Superintendencia. Hasta su entrada en vigencia, resultan aplicables las disposiciones vigentes que correspondan según la materia.

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

Primera.- Implementación progresiva de la profundidad histórica

Para la implementación de la profundidad histórica prevista en el párrafo 9.3, las EPD deben habilitar el historial de la información transaccional correspondiente a cada grupo de datos conforme al siguiente cronograma:

Grupo de Datos	Información transaccional	01/01/2028	01/07/2028	01/01/2029	01/07/2029	01/01/2030	01/07/2030
Grupo de datos 1	Cuentas de ahorro	12 meses	18 meses	24 meses	30 meses	36 meses	36 meses
Grupo de datos 2	Tarjetas de crédito	No exigible	12 meses	18 meses	24 meses	30 meses	36 meses

La profundidad histórica exigible se incrementa en un mes por cada mes calendario transcurrido entre los hitos señalados en el cuadro, hasta alcanzar un máximo de treinta y seis (36) meses. Alcanzado dicho máximo, las EPD deben mantener disponible el historial correspondiente a los treinta y seis (36) meses inmediatamente anteriores a la fecha en que reciban cada solicitud de acceso.

Cuando la relación contractual o de servicio del usuario con la EPD tenga una antigüedad menor a la profundidad histórica exigible, se suministra la totalidad del historial disponible.

Segunda.- Implementación progresiva de las subcategorías de datos

Para la implementación de las subcategorías de datos prevista en el párrafo 9.1, las EPD deben habilitar los grupos de datos, según corresponda a sus operaciones, conforme al siguiente cronograma:

N°	Tipo de datos	Plazo
1	Información de Cuentas Ahorro y Cuentas Corrientes	01/01/2028
2	Información de Tarjetas de Crédito	01/07/2028
3	Información de Cuentas a Plazo y Dinero Electrónico	Por definir
4	Información de Identificación del cliente	Por definir
5	Canales y Términos y Condiciones de Productos Financieros	Por definir
6	Información de Créditos de Consumo y PYME	Por definir
7	Información de Créditos Hipotecarios	Por definir
8	Portabilidad financiera de créditos	Por definir
9	Información de las pólizas de seguro contratadas	Por definir
10	Información de los aportes provisionales administrados	Por definir

(...las demás disposiciones finales y complementarias se encuentran en desarrollo y serán definidas como parte de las Resoluciones que posteriormente emita la Superintendencia...)

ANEXOS

Los demás anexos previstos en el presente Reglamento, distintos a los Anexos N° 1, 2, 3 y 4, serán desarrollados y aprobados posteriormente mediante resolución de la Superintendencia.

ANEXO N° 1 **LISTADO DE FINALIDADES**

Las ERD, en cumplimiento con lo dispuesto en el artículo 27, deben solicitar el consentimiento de los usuarios utilizando las finalidades previstas en el presente Anexo.

La Superintendencia publica en el Portal del SFA las finalidades específicas que pueden ser utilizadas por las ERD, así como los lineamientos para su presentación al usuario, sus descripciones, los grupos de datos que pueden ser asociados a cada una de ellas y demás especificaciones que resulten aplicables.

Las finalidades específicas publicadas por la Superintendencia deben encontrarse asociadas a alguna de las siguientes finalidades previstas:

1. **Gestión financiera personal:** Comprende el tratamiento de datos destinado a permitir al usuario acceder, visualizar, consolidar, organizar o monitorear información relacionada con sus productos, servicios, operaciones o situación financiera, incluyendo sus pólizas de seguro y sus aportes y fondos previsionales, así como el uso de dicha información por el propio titular para fines personales.
2. **Gestión financiera empresarial:** Comprende el tratamiento de datos destinado a facilitar la administración, monitoreo o análisis de información financiera vinculada a actividades empresariales o profesionales.
3. **Comparación de productos o servicios financieros y previsionales:** Comprende el tratamiento de datos destinado a facilitar al usuario la comparación de características, condiciones o beneficios de productos o servicios financieros o previsionales, contratados o por contratar, así como la presentación de ofertas o cotizaciones acordes con su perfil.
4. **Evaluación para el acceso a productos o servicios:** Comprende el tratamiento de datos destinado a determinar la elegibilidad del usuario para acceder a productos o servicios ofrecidos por los participantes, incluyendo la evaluación de su capacidad de pago, sus ingresos o su riesgo crediticio.
5. **Contratación, traslado y cierre de productos o servicios:** Comprende el tratamiento de datos destinado a facilitar o ejecutar los procesos asociados a la contratación, apertura, vinculación, traslado, portabilidad o cierre de productos o servicios por parte del usuario, incluyendo el proceso de registro y conocimiento del cliente.
6. **Administración y seguimiento de productos contratados:** Comprende el tratamiento de datos destinado a la administración y seguimiento de productos o servicios previamente contratados por el usuario, incluyendo el seguimiento crediticio y la gestión de cobranzas.
7. **Asesoramiento y apoyo a la toma de decisiones financieras:** Comprende el tratamiento de datos destinado a proporcionar análisis, recomendaciones, orientación o herramientas de apoyo para la toma de decisiones financieras por parte del usuario, incluyendo la asesoría en inversiones o gestión patrimonial, la asesoría de corredores de seguros y la proyección de pensiones.



8. Prestación de servicios de seguros: Comprende el tratamiento de datos destinado a la cotización, evaluación, suscripción, contratación, administración, endoso, renovación, traslado, ejecución o seguimiento de productos y servicios relacionados con seguros, incluyendo la atención de siniestros.
9. Prestación de servicios previsionales: Comprende el tratamiento de datos destinado a la gestión de operaciones vinculadas al Sistema Privado de Pensiones, tales como el traspaso entre administradoras, la elección de modalidades de pensión, el retiro de fondos, su uso para fines de vivienda y el ahorro previsional voluntario.
10. Verificación y prevención del fraude: Comprende el tratamiento de datos destinado a verificar la identidad del usuario, la titularidad de sus cuentas o la veracidad de la información que declara, así como a prevenir, detectar o mitigar operaciones fraudulentas.
11. Otras finalidades autorizadas por la Superintendencia: Comprende aquellas finalidades que la Superintendencia incorpore mediante su publicación en el Portal del Sistema de Finanzas Abiertas, así como aquellas que, no estando comprendidas en las anteriores, sean declaradas de forma específica por el participante conforme a las disposiciones que establezca la Superintendencia.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

PROYECTO NORMATIVO

ANEXO N° 2

CRONOGRAMA DE INCORPORACIÓN OBLIGATORIA DE ENTIDADES AL SFA

La Superintendencia establece los plazos máximos para que las entidades cuya participación sea determinada como obligatoria completen su inscripción y habilitación en el Directorio como EPD e inicien el suministro de los datos que les resulten exigibles, de conformidad con el presente Reglamento y la Segunda Disposición Complementaria Transitoria.

Para tal efecto, la Superintendencia publica en su Portal Institucional la relación de entidades obligadas y los plazos de incorporación aplicables a cada una (<https://www.sbs.gob.pe/Portals/0/Cronograma-FA-SBS.pdf>). Dicha relación se actualiza, cuando corresponda, con el nombre de las entidades y los plazos aplicables a las etapas posteriores.

ANEXO N° 3
CATÁLOGO DE DATOS

1. Distribución de endpoints por grupo de datos

1.1. Grupo de Datos: Cuentas

N°	Endpoint (preliminar)	Descripción
1	GET /accounts	Listado de las cuentas asociadas al usuario
2	GET /accounts/{accountId}	Datos generales de una cuenta específica del usuario
3	GET /accounts/{accountId}/balances	Saldos actualizados de una cuenta específica del usuario
4	GET /accounts/{accountId}/transactions	Historial de transacciones de una cuenta específica del usuario
5	GET/accounts/accountID/current-overdraft-limit	Límites de sobregiros vigentes de la cuenta específica del usuario
6	GET/ /accounts/{accountID}/overdraft	Movimientos de sobregiros de la cuenta específica del usuario

1.2. Grupo de Datos: Tarjetas de Crédito

N°	Endpoint (preliminar)	Descripción
1	GET/accounts	Lista todas las cuentas de tarjeta de crédito del cliente.
2	GET/accounts/{creditCardAccountID}	Devuelve el detalle asociado de una tarjeta específica.
3	GET/accounts/{creditCardAccountID}/balance	Entrega el balance de cierre (estado de cuenta) de una tarjeta específica.
4	GET/accounts/{creditCardAccountID}/current-balance	Saldo actualizado a la fecha/hora actual.
5	GET/accounts/{creditCardAccountID}/limit	Muestra los límites de crédito aprobados y disponibles.
6	GET/accounts/{creditCardAccountID}/transactions	Devuelve las transacciones realizadas con la tarjeta de crédito

2. Campos para endpoints transaccional

2.1. Grupo de Datos: Cuentas Información Transaccional

N°	ENDPOINT (PRELIMINAR)	DESCRIPCIÓN
4	GET /accounts/{accountId}/transactions	Historial de transacciones de una cuenta específica del usuario

N°	CAMPOS	DETALLE
1	Código de Entidad Financiera	Identificador de la entidad que custodia la cuenta. (Puede ser código SWIFT o Código SBS).
2	Nombre Entidad Financiera	Nombre de la entidad que custodia la cuenta.
3	Tipo de Identificador de cliente	Señalar el número de acuerdo con la casuística de la nota ¹ .

¹ En caso se trate de una persona natural: (01) DNI, (02) Carnet de Extranjería, (05) Pasaporte, (07) Carnet de Identidad emitido por el Ministerio de Relaciones Exteriores, (08) Carnet de Permiso Temporal de Permanencia, (09) Permiso Temporal de Permanencia. En caso se trate de personas jurídicas, entes jurídicos, dependencias, organismos, entidades u otros: (06) RUC, (20) Personas jurídicas locales sin RUC, (21) Empresas Extranjeras sin RUC. En caso se trate de bancos del exterior: (61) Código SWIFT (Society for Worldwide Interbank Financial Telecommunication), (62) Código Fiscal de País de Origen, (63) Código IBAN (International Bank Account Number), (64) Código ABA (American Bankers Association). En caso de que el documento no esté identificado o se trate de otro documento: (98) No Identificado, (99) Otros



N°	CAMPOS	DETALLE
4	Número de Identificación del Cliente	Número de identificación asociado al tipo de identificador del cliente
5	Número de la Cuenta asociada	ID de la cuenta o producto financiero. Conforme al mecanismo de anonimización que establezca la SBS.
6	Subtipo de cuenta	Individual, mancomunada simple, mancomunada solidaria.
7	Tipo de Producto asociado	Tipo de producto: cuentas de ahorro, cuenta corriente, cuentas a plazo, etc.
8	Tasa de Interés	Tasa de Interés aplicada al producto al momento del reporte
9	ID de la transacción	Identificador Único de la Transacción
10	Fecha de la transacción	Fecha y hora de ocurrencia, autorización o generación de la transacción. Formato (DD-MM-AA-hora)
11	Fecha contable de la transacción	Fecha y hora en que la operación se registra en los sistemas contables. Formato (DD-MM-AA-hora)
12	Tipo de Transacción	Indica si se trata de un abono o un cargo.
13	Monto de la Transacción	Importe monetario original de la transacción.
14	Moneda de la Transacción	Moneda en la que se realizó la transacción (abono o cargo).
15	Categoría de la Transacción	Categoría o Naturaleza de la transacción: transferencias, compras con débito, operación en cajeros automáticos, retiros/depósitos en cajeros corresponsales.
16	Glosa Original de la Transacción	Texto breve que explica el detalle de la transacción tal y como se muestra en el Estado de Cuenta.
17	Glosa Regulatoria SBS	Se proponen 13 agrupaciones: <ol style="list-style-type: none">1. Transferencia interbancaria o a Terceros (CCI)2. Transferencia intrabancaria (entre cuentas del mismo banco y usuario)3. Pago de boleta / factura / recibo de servicios4. Pago con tarjeta de débito en comercios5. Retiro en cajero automático6. Depósito en efectivo / cajero7. Abono de nómina / planilla8. Débito automático9. Rendimiento / intereses devengados10. Cargo por comisión / tarifa bancaria11. Operación de crédito (desembolso o pago de cuota)12. Pago de impuestos / tributos (SUNAT, aduanas)13. Otros / no clasificado



N°	CAMPOS	DETALLE
18	Código de Categoría del Comercio (MCC)	Indicar el Merchant Category Code (MCC) asociado a la transacción, en caso aplique.
19	Nombre del Comercio	El texto crudo del comercio registrado
20	Tipo de Persona	En el caso de cargos, indicar si el cargo es contra un comercio o no. Variable Dicotómica: 1. Si / 2 No
21	Tipo de Identificador de la contraparte	Señalar el número de acuerdo con la casuística de la nota. En el caso de personas naturales, conforme al mecanismo de anonimización que establezca la SBS ² .
22	Número de Identificador de contraparte	Número de identificación asociado al tipo de identificador de la contraparte. En el caso de personas naturales, conforme al mecanismo de anonimización que establezca la SBS
23	Nombre contraparte	Nombre de la contraparte. En el caso de personas naturales, conforme al mecanismo de anonimización que establezca la SBS
24	Canal de la Transacción	Canal por el cual se realizó la transacción: ventanilla, cajeros, corresponsales, banca móvil, banca por internet, aplicaciones bancarias, billeteras digitales, entre otros.

2.2. Grupo de Datos: Tarjetas de Crédito - Información Transaccional

N°	ENDPOINT (PRELIMINAR)	DESCRIPCIÓN
6	GET/accounts/{creditCardAccountID}/transactions	Devuelve las transacciones realizadas con la tarjeta de crédito.

N°	VARIABLES	DETALLE
1	Código de Entidad Financiera	Identificador de la entidad emisora de la tarjeta. (Puede ser código SWIFT o Código SBS).
2	Nombre Entidad Financiera	Nombre de la entidad que es emisora de la tarjeta de crédito.
3	Identificador de cliente	RUC o DNI asociado al cliente que posee la tarjeta ³ .

² En caso se trate de una persona natural: (01) DNI, (02) Carnet de Extranjería, (05) Pasaporte, (07) Carnet de Identidad emitido por el Ministerio de Relaciones Exteriores, (08) Carnet de Permiso Temporal de Permanencia, (09) Permiso Temporal de Permanencia. En caso se trate de personas jurídicas, entes jurídicos, dependencias, organismos, entidades u otros: (06) RUC, (20) Personas jurídicas locales sin RUC, (21) Empresas Extranjeras sin RUC. En caso se trate de bancos del exterior: (61) Código SWIFT (Society for Worldwide Interbank Financial Telecommunication), (62) Código Fiscal de País de Origen, (63) Código IBAN (International Bank Account Number), (64) Código ABA (American Bankers Association). En caso de que el documento no esté identificado o se trate de otro documento: (98) No Identificado, (99) Otros. En caso de que el documento no esté identificado o se trate de otro documento: (98) No Identificado, (99) Otros.

³ En caso se trate de una persona natural: (01) DNI, (02) Carnet de Extranjería, (05) Pasaporte, (07) Carnet de Identidad emitido por el Ministerio de Relaciones Exteriores, (08) Carnet de Permiso Temporal de Permanencia, (09) Permiso Temporal de Permanencia. En caso se trate de personas jurídicas, entes jurídicos, dependencias, organismos, entidades u otros: (06) RUC, (20) Personas jurídicas locales sin RUC, (21) Empresas Extranjeras sin RUC. En caso se trate de bancos del exterior: (61) Código SWIFT (Society for Worldwide Interbank Financial Telecommunication), (62) Código Fiscal de País de Origen, (63) Código IBAN (International Bank Account Number), (64) Código ABA (American Bankers Association). En caso de que el documento no esté identificado o se trate de otro documento: (98) No Identificado, (99) Otros. En caso de que el documento no esté identificado o se trate de otro documento: (98) No Identificado, (99) Otros.



4	Número de la Tarjeta asociada	ID de la tarjeta de crédito asociada. Conforme al mecanismo de anonimización que establezca la SBS
5	Tipo de Tarjeta	Indicar si la Tarjeta corresponde a: Titular, adicional, empresarial, corporativa
6	ID de la transacción	Identificador Único de la Transacción
7	Fecha de la transacción	Fecha y hora de ocurrencia, autorización o generación de la transacción. Formato (DD-MM-AA-hora)
8	Fecha contable de la transacción	Fecha y hora en que la operación se registra en los sistemas contables. Formato (DD-MM-AA-hora)
9	Tipo de Transacción	Indica si se trata de un abono o un cargo.
10	Monto de la Transacción	Importe monetario original de la transacción.
11	Moneda de la Transacción	Moneda en la que se realizó la transacción (abono o cargo).
12	Categoría de Transacción	Indica si se trata de una compra, avance, pago, interés, comisión, impuesto, ajuste, devolución, etc.
13	Glosa Original de la Transacción	Texto breve que explica el detalle de la transacción tal y como se muestra en el Estado de Cuenta de la Tarjeta.
14	Código de Categoría del Comercio (MCC)	Indicar el Merchant Category Code (MCC) asociado a la transacción, en caso aplique.
15	Nombre del Comercio	El texto crudo del comercio registrado
16	Tipo de Persona	En el caso de cargos, indicar si el cargo es contra un comercio o no.

(...los demás campos asociados a los otros endpoints se encuentran en desarrollo y serán definidos conjuntamente con las especificaciones técnicas y las API correspondientes...)

ANEXO N° 4
ESCENARIOS REFERENCIALES Y ATRIBUCIÓN INICIAL DE RESPONSABILIDAD

1. Reglas Generales

- 1.1. Los escenarios previstos en el presente Anexo tienen carácter referencial y no limitativo y establecen una atribución inicial de responsabilidad sobre la base de las obligaciones aplicables y del ámbito de control que corresponda a los participantes previstos en el Título III del presente Reglamento.
- 1.2. La atribución inicial señalada para cada escenario puede modificarse cuando, de la evaluación de los hechos y de la evidencia disponible, se determine que el evento fue causado por otro participante, por más de un participante, por un tercero o por una circunstancia no imputable.
- 1.3. Las atribuciones previstas en el presente Anexo no constituyen una declaración definitiva de responsabilidad administrativa, civil o penal; no establecen una presunción legal ni invierten la carga de la prueba prevista en otras normas; y no generan por sí mismas una obligación de indemnización o compensación.
- 1.4. Los escenarios contenidos en el presente Anexo no excluyen otros supuestos de responsabilidad derivados del incumplimiento de las obligaciones previstas en el Reglamento y demás normativa aplicable.

2. Matriz de escenarios y atribución inicial de responsabilidad

Categoría	Escenario	Atribución inicial
Calidad de datos	La EPD suministra datos incorrectos como consecuencia de una falla atribuible a sus sistemas o procesos	EPD
	La EPD no preserva adecuadamente la integridad o consistencia de los datos suministrados	EPD
	La información es incorrecta porque originalmente fue proporcionada de manera incorrecta o desactualizada por el usuario	Sin atribución automática; la EPD responderá cuando haya incumplido obligaciones aplicables de actualización, verificación o mantenimiento
	La ERD altera, interpreta, transforma o presenta incorrectamente datos recibidos correctamente	ERD
Acceso a datos	La EPD no suministra injustificadamente información válidamente solicitada por una ERD	EPD
	La ERD formula una solicitud sin encontrarse habilitada o utilizando credenciales que no correspondan	ERD
Consentimiento	La ERD solicita información sin consentimiento, con consentimiento inválido, vencido o excediendo su alcance	ERD
	La EPD suministra datos que exceden el alcance autorizado pese a haberse recibido una solicitud conforme al consentimiento	EPD
	El usuario revoca el consentimiento ante la ERD y esta no comunica o procesa adecuadamente la revocación	ERD
	La revocación ha sido válidamente recibida por la EPD y esta continúa suministrando información	EPD
	La ERD continúa formulando solicitudes después de vencido el consentimiento	ERD



	La EPD continúa suministrando datos después del vencimiento del consentimiento pese a encontrarse en condiciones de verificarlo	EPD
	Existe concurrencia de incumplimientos de EPD y ERD respecto de un consentimiento	Compartida, según contribución causal
Autenticación	Autenticación defectuosa o fraudulenta del usuario en el entorno de la EPD por incumplimiento de controles que se encuentran bajo su responsabilidad	EPD
Uso de datos	La ERD utiliza información para una finalidad distinta de la autorizada	ERD
	La ERD permite acceso o comunica información a terceros fuera de los supuestos autorizados	ERD
Conservación	La ERD conserva o trata información luego de extinguirse la finalidad o revocarse el consentimiento, fuera de los supuestos permitidos por ley	ERD
Seguridad	Se produce acceso no autorizado, pérdida o divulgación en sistemas bajo control de la EPD	EPD
	Se produce acceso no autorizado, pérdida o divulgación en sistemas bajo control de la ERD	ERD
	Se produce compromiso durante la transmisión	EPD o ERD según causa; compartida cuando exista concurrencia causal
Credenciales	Compromiso de certificado, clave, token u otra credencial por incumplimiento de deberes de custodia	Participante responsable de la credencial
APIs	Indisponibilidad o degradación de API por incumplimiento atribuible a la EPD	EPD
	Consumo de API fuera de límites o condiciones técnicas aplicables que genere afectación atribuible a la ERD	ERD
Gestión de cambios	Cambio de endpoint, certificado, versión o componente no comunicado o implementado conforme a las reglas aplicables	Participante obligado a gestionar o comunicar el cambio
Interoperabilidad	Error originado por configuración o implementación técnica no conforme al estándar	Participante responsable de la implementación defectuosa
Evidencia	Falta de conservación de logs, registros o evidencia obligatoria	Participante obligado a conservarla, respecto de dicho incumplimiento
	Alteración, destrucción u ocultamiento de evidencia relevante	Participante bajo cuyo control se encontraba la evidencia, sujeto a evaluación
Costos	Incumplimiento de pago de un costo válidamente exigible conforme al Reglamento	Participante obligado al pago
	Aplicación de un cobro no permitido por el Reglamento	Participante que efectúa el cobro



	Divergencia razonable sobre volumen, medición o monto de costos recuperables	Sin atribución inicial; sujeto a evidencia
Terceros tecnológicos	Incidente causado por proveedor contratado para cumplir una obligación del participante	Participante contratante frente al SFA, sin perjuicio de las acciones contra el proveedor
Otros	Escenario no previsto expresamente	Sin atribución inicial; se determina conforme a las obligaciones aplicables, ámbito de control, causalidad y evidencia disponible

Artículo Segundo. - Aprobar el procedimiento N° 223 “Autorización de inscripción para participar en el Sistema de Finanzas Abiertas”, N° 224 “Autorización de acceso anticipado al ambiente de pruebas del Directorio Centralizado del Sistema Finanzas Abiertas” y N° 225 “Solicitud de retiro de la Inscripción del Sistema de Finanzas Abiertas aplicable a participantes voluntarios” el Texto Único de Procedimientos Administrativos - TUPA de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, aprobado por Resolución SBS N° 01581-2023 y sus normas modificatorias, conforme al texto se adjunta a la presente resolución y se publica en el portal institucional (www.sbs.gob.pe).

Artículo Tercero. - 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 que el presente artículo establezca un plazo distinto.
2. El Reglamento General del Sistema de Finanzas Abiertas, aprobado por el artículo Primero de la presente Resolución, entra en vigencia el 1 de enero de 2028, salvo aquellas disposiciones para las cuales se establezca expresamente un plazo distinto.
3. Los artículos 19 al 22 del Reglamento, referidos al Directorio de Participantes, al acceso al ambiente de pruebas y a la inscripción y habilitación de los participantes, así como las disposiciones y anexos necesarios para la ejecución de dichos procesos, entran en vigencia el 1 de agosto de 2027.
4. El artículo Segundo de la presente Resolución entra en vigencia el 1 de enero de 2028.
5. Las disposiciones del Reglamento vinculadas con la infraestructura digital, el marco de confianza, los estándares de seguridad y calidad, la recuperación de costos, la gestión de problemas, incidentes y disputas, el monitoreo, las medidas correctivas y las sanciones, así como las demás disposiciones necesarias para que los participantes se encuentren en capacidad de operar en el SFA, entran en vigencia en los plazos que establezca la Superintendencia mediante las disposiciones que desarrollen dichas materias.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

PROYECTO NORMATIVO

6. La incorporación del TUPA N° 223, N° 224 y N° 225, a que se refiere el Artículo Segundo de la presente Resolución, entra en vigencia el 01 de agosto de 2027.

Regístrese, comuníquese, publíquese.