

ALERTA LEGISLATIVA | PROTECCIÓN DE DATOS PERSONALES Y SEGURIDAD DE LA INFORMACIÓN



La SBS publica proyecto de Reglamento de Finanzas Abiertas: claves sobre consentimiento y seguridad en materia de protección de datos personales

La Superintendencia de Banca, Seguros y AFP (SBS) ha puesto a difusión pública la propuesta del Reglamento General del Sistema de Finanzas Abiertas (SFA). Se pueden remitir observaciones y comentarios a dicho proyecto hasta el 23 de octubre.

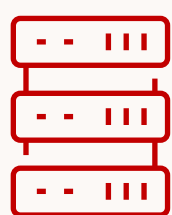
Al respecto, el proyecto prioriza el control del usuario (titular de datos) sobre su información financiera y establece exigencias de seguridad para la interoperabilidad entre entidades. A continuación, analizamos los aspectos principales del proyecto y su interacción con la normativa de protección de datos personales (Ley N.º 29733 y su Reglamento, D.S. N.º 016-2024-JUS).

¿Cuáles son las partes intervinientes en los Sistemas de Finanzas Abiertas?



Usuario

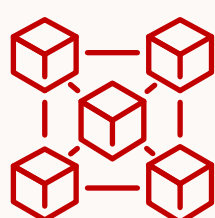
Persona natural (titular de datos personales) o jurídica cuyos datos o productos financieros son objeto de tratamiento o intercambio.



EPD (Entidad Proveedora de Datos)

Quien custodia y entrega

Entidad supervisada (ej. banco, aseguradora, AFP) que almacena la información financiera del usuario y la transmite únicamente previa verificación del consentimiento y confirmación del titular.



ERD (Entidad Receptora de Datos)

Quien solicita y recibe

Entidad (ej. fintech, app de gestión financiera u otra entidad supervisada) que solicita y recibe los datos del usuario para prestarle un servicio específico, previo consentimiento libre, expreso e informado.

¿Qué propone el proyecto respecto al procesamiento de datos de los usuarios en los Sistemas de Finanzas Abiertas?

01 Consentimiento



Lo pide la ERD

- Debe ser libre, expreso, informado y específico, cumpliendo los estándares de la Ley N.º 29733.
- Requiere una finalidad concreta por cada autorización (sin fórmulas genéricas ni casillas preseleccionadas).
- Debe detallar con claridad: quién solicita (ERD), quién suministra (EPD), qué datos específicos se tratarán, el propósito exacto y la vigencia/plazo.

02 Autenticación



La hace la EPD

- El usuario es redirigido al entorno seguro de su propia entidad (banco, AFP, etc.).
- Se autentica con sus credenciales habituales sin que la ERD tenga acceso, visibilidad o almacenamiento de dichas claves (cero captura de credenciales).
- Aplica el mismo nivel de seguridad reforzada para modificar o revocar el consentimiento.

03 Confirmación



A cargo del usuario

- El usuario revisa el alcance exacto del intercambio y selecciona expresamente los productos o cuentas a compartir.
- Confirma mediante un factor de autenticación robusto (ej. token o biometría).
- La ERD notifica de inmediato al usuario una vez ejecutado el acceso de forma exitosa.

¿Qué medidas de seguridad exige el proyecto y cómo se articula con el marco normativo de protección de datos personales?

1. Exigencias del Proyecto de Reglamento SFA (SBS):

- Principios de Seguridad: Obliga a garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de los datos financieros, previniendo usos no autorizados.
- Canales Digitales: Requiere autenticación reforzada, monitoreo continuo, registros de trazabilidad y gestión de incidentes.
- Deberes de la EPD: Debe verificar la identidad y habilitación de la ERD, así como la vigencia y alcance exacto del consentimiento antes de transferir la información.
- Deberes de la ERD: Debe implementar controles estrictos de acceso, autenticación, cifrado y monitoreo durante la recepción, transmisión y almacenamiento del dato.

2. Complementariedad con la normativa vigente de datos personales:

- Ley N.º 29733 (LPDP): Exige medidas de seguridad organizativas, legales y técnicas adecuadas al nivel de riesgo y categoría de datos (Arts. 9 y 16).
- Reglamento de la LPDP (D.S. N.º 016-2024-JUS): Impone contar con un Documento de Seguridad actualizado, procedimientos formales de gestión de accesos/privilegios y políticas de respaldos e integridad de la información (Arts. 47.1 y 48.1).

¿Por qué es relevante este proyecto?

- > **Autonomía de etapas:** El consentimiento, la autenticación y la confirmación son procesos diferenciados e independientes; el cumplimiento de uno no exime del otro.
- > **Conservación de evidencias vs. Conservación de datos:** El plazo de 10 años previsto en el proyecto aplica exclusivamente para registros de trazabilidad y evidencias de consentimientos otorgados, revocados o vencidos; en ese sentido, no constituye una autorización para conservar la información financiera del usuario, por lo tanto, vencida la finalidad, la entidad debe proceder al bloqueo o supresión de los datos.

Conclusión y perspectivas:

Cabe señalar que la propuesta publicada por la SBS corresponde a un proyecto normativo actualmente sujeto a la recepción de comentarios y aportes del público y del sector, **por lo que se deberá dar seguimiento a la versión final que sea aprobada.**

Sin perjuicio de ello, este nuevo marco regulatorio conllevará de manera inminente a que tanto las EPD como las ERD analicen y adecuen la gobernanza de sus datos personales. Para ello, resultará clave ir evaluando desde ya:

- 01 **El diseño transparente** de las cláusulas de consentimiento para evitar autorizaciones genéricas
- 02 **La auditoría de los sistemas** de gestión de accesos, trazabilidad y seguridad vigentes.
- 03 **La actualización de los protocolos** de respuesta y notificación de incidentes ante la Autoridad dentro de las 48 horas fijadas por el Reglamento de datos personales.

Para mayor información, puede contactarse a los siguientes correos electrónicos:



- carolquiroz@esola.com.pe
- danielachavez@esola.com.pe
- andreachumpitazi@esola.com.pe



Carol Quiroz
Socia



Daniela Chávez
Asociada



Andrea Chumpitazi
Asistente



Juana Buleje
Asistente