Carta N° 216-2026/DE/COMEXPERU

Lima, 16 de junio de 2026

Señor
SERGIO ESPINOSA CHIROQUE
Superintendente
Superintendencia de Banca, Seguros y AFP
Presente. -

Ref.: Resolución SBS N° 01371-2026

De nuestra consideración:

Es grato saludarlo y dirigirnos a usted a nombre de la Sociedad de Comercio Exterior del Perú –ComexPerú, una organización privada que busca contribuir en la implementación de políticas públicas, con una visión de defensa de principios por sobre intereses particulares, teniendo como objetivo mejorar la calidad de vida del ciudadano. Nuestro trabajo se basa en análisis objetivos, rigurosos y sólida evidencia técnica.

En esta oportunidad, compartimos nuestros comentarios con relación al proyecto normativo del reglamento para la prestación de servicios bajo el modelo de Banking as a Service (en adelante, BaaS), contenida en la Resolución SBS N° 01371-2026 (en adelante, Reglamento):

1. Artículos 5, 6 y 11. Costos operativos y demora en escalamiento

De acuerdo con lo previsto en el artículo 5 del proyecto de reglamento, se exige la aprobación del Directorio, o del órgano en quien este delegue dicha facultad, para la incorporación de cada nuevo receptor BaaS y de cada nuevo servicio asociado. Si bien se comprende la finalidad de asegurar una adecuada supervisión de estas actividades, la exigencia de una aprobación individual para cada receptor o servicio podría generar cuellos de botella incrementando las cargas administrativas y ralentizando el lanzamiento de nuevos productos o servicios al mercado. Ello resulta particularmente relevante en un entorno caracterizado por la innovación constante y la necesidad de responder con agilidad a las demandas de los usuarios y a los cambios tecnológicos.

En ese sentido, podría evaluarse un esquema regulatorio más flexible y basado en riesgos, en el cual el Directorio mantenga la responsabilidad de aprobar las políticas generales, los límites de exposición, los criterios de elegibilidad y los lineamientos de control aplicables a las operaciones BaaS. Bajo este enfoque, la aprobación de receptores o servicios específicos podría delegarse a instancias ejecutivas o comités especializados, en función de su materialidad, complejidad y nivel de riesgo, permitiendo una gestión más eficiente sin menoscabar los estándares de gobierno corporativo y control interno.

Por último, consideramos que el proyecto podría orientarse a exigir la adopción de políticas y procedimientos obligatorios sobre aspectos críticos de la operación, en lugar de establecer un listado excesivamente detallado de cláusulas contractuales que deban incorporarse en cada acuerdo entre el proveedor y el receptor BaaS. Se debería plantearla implementación de manuales y protocolos, que luego de consensuarlos con el sector privado, puedan regular estándares avanzados de ciberseguridad, gestión de incidentes operacionales y de seguridad

de la información, continuidad del negocio, protección de datos personales, mecanismos de monitoreo y supervisión, así como lineamientos claros sobre la identificación de usuarios, la obtención de consentimientos y la asignación de responsabilidades entre las partes.

2. Artículo 7.- Responsabilidades del proveedor de servicios BaaS

En el numeral 7.2, el proyecto normativo establece las responsabilidades del proveedor de servicios BaaS para la prestación de los servicios incluyendo el cumplimiento de la normativa aplicable a determinadas materias. Entre ellas, en los puntos ii) y iii) del apartado 3, señala las responsabilidades vinculadas con gestión de la seguridad de la información y ciberseguridad, que comprende:

> *"[...] 3. Gestión de la seguridad de la información y ciberseguridad, asegurando: i) que los contratos de seguridad implementados… ii) ejercer supervisión continua sobre los receptores de servicios BaaS y los proveedores tecnológicos críticos que intervengan en su provisión, adoptando las medidas correctivas necesarias ante el incumplimiento de los estándares de seguridad establecidos, incluyendo de ser el caso la suspensión del acceso a la plataforma BaaS, y iii) reportar a la Superintendencia los eventos o incidentes de seguridad que afecten la confidencialidad, integridad o disponibilidad de la información o que limiten el ofrecimiento de los servicios financieros permitidos, con independencia del actor en cuya plataforma se haya originado el incidente. [...]"*

Al respecto, consideramos que las responsabilidades de supervisión continua por parte de proveedores de servicios BaaS deben delimitarse a las partes involucradas en el servicio. Así, sugerimos que la supervisión debe enfocarse en proveedores que participan directamente en la lógica del servicio financiero BaaS tal como procesadores de pagos o proveedores de core bancario. Ello permite distinguir dichos proveedores de aquellos de infraestructura tecnológica de propósito general utilizada transversalmente por múltiples industrias.

Por otro lado, consideramos que la obligación de "supervisión continua" individualizada podría duplicar mecanismos de aseguramiento ya ampliamente aceptados en la industria cloud tal como los estándares cumplimiento y seguridad de la información SOC 2 (System and Organization Controls 2), ISO 27001, PCI DSS (Payment Card Industry Data Security Standard), entre otros. Frente a ello, sugerimos que el Reglamento reconozca expresamente como mecanismos válidos de cumplimiento las certificaciones internacionales y reportes de auditoría independiente, evitando esquemas de auditorías de supervisión individual que no resultan escalables.

Respecto a la facultad de suspensión del acceso a la plataforma BaaS, consideramos que existe ambigüedad respecto de si esta aplica al receptor de servicios BaaS o al proveedor tecnológico crítico. En caso de aplicación al proveedor tecnológico, la suspensión de acceso a la plataforma BaaS podría afectar la continuidad operativa de múltiples clientes simultáneamente. En esta línea, sugerimos explicitar que la medida se dirige al receptor de servicios BaaS y establecer que cualquier medida relacionada con proveedores tecnológicos siga procedimientos graduales y proporcionales.

Finalmente, respecto a los servicios tecnológicos de nube, consideramos que la propuesta no reconoce expresamente el modelo de responsabilidad compartida en servicios cloud, distinguiendo de manera clara entre seguridad de la nube y seguridad en la nube. Recomendamos incorporar este principio de manera explícita, alineándose con estándares y referencias internacionales como los de MAS (Monetary Authority of Singapore), NIST (National Institute of Standards and Technology - EE.UU.) y CSA (Cloud Security Alliance).

3. Artículo 9.- Receptores de BaaS con quienes no se puede celebrar contratos de BaaS

El artículo 9 del proyecto normativo señala dos supuestos en los cuales los receptores no pueden establecer contratos de BaaS. Así, se señalan dos grandes supuestos: la regla de exclusividad por servicio (Art. 9.1.1) y la prohibición de redistribución (Art. 9.2).

Estas dos prohibiciones podrían afectar modelos de negocio legítimos ampliamente adoptados en mercados más maduros, tales como comparadores financieros con terminación completa del servicio (full journey) y agregadores PFM que integran funcionalidades transaccionales.

En ese sentido, sugerimos que la norma incorpore criterios objetivos para distinguir entre un receptor BaaS que actúa como canal de distribución (sujeto a exclusividad) y una plataforma tecnológica que facilita la comparación o agregación, sin asumir riesgo financiero ni operar bajo licencia delegada.

En ese mismo sentido, la norma exige exclusividad por servicio entre receptor y proveedor BaaS, pero no establece un mecanismo de consulta centralizado que permita a los proveedores BaaS verificar en tiempo real si un potencial receptor ya mantiene un contrato con otro proveedor para el mismo servicio. El Anexo N°1 (reporte semestral a la SBS) presenta latencia significativa, y la publicación consolidada del Art. 12.3 es potestativa.

En ese sentido, sugerimos que la SBS establezca un registro público de acceso en línea, actualizado con periodicidad razonable, que permita a los participantes del ecosistema verificar el cumplimiento de la exclusividad antes de formalizar una relación contractual.

4. Artículo 11.- Contenido del contrato

En el apartado 6 del numeral 11.2, el proyecto de Reglamento enumera las cláusulas expresas que debe contener el contrato que suscriba el proveedor de servicios BaaS estableciendo las responsabilidades del proveedor y del receptor de servicios BaaS.

Entre las cláusulas, se incluye:

> *"[...] 6. Las obligaciones del receptor de servicios BaaS de:*
> *a. Reportar oportunamente al proveedor de servicios BaaS sobre cualquier evento o incidente que limite el ofrecimiento de los servicios permitidos y/o el cumplimiento de la normativa aplicable, incluyendo lo dispuesto en el presente Reglamento; y*
> *b. Notificar la contratación de un proveedor tecnológico, con carácter previo a su contratación o, de forma inmediata en caso de contratación urgente, cuando este procese o almacene datos, así como cuando se trate de servicios que el proveedor de servicios BaaS considere relevante para la prestación de servicios BaaS. [...]"*

Al respecto, consideramos importante que se defina que la obligación de notificar la contratación de un proveedor tecnológico por parte del receptor se refiera únicamente a la notificación y no a un mecanismo de aprobación previa. En la misma línea, sugerimos explicitar que la referencia al proveedor tecnológico que "procese o almacene datos" se limita a los datos de clientes finales del servicio financiero y no a cualquier dato operativo. Esto se fundamenta en que una interpretación amplia podría implicar que cualquier servicio de almacenamiento en nube esté sujeto a la obligación, generando fricción innecesaria en los procesos de contratación.

Por otro lado, en el apartado 9 del numeral 11.2 del proyecto normativo señala que el contrato debe contener una cláusula sobre acceso oportuno a la información y auditorías de los receptores. Específicamente, se señala:

> *"[…] 9. Cláusula que asegure el acceso oportuno y adecuado a la información, así como la realización de revisiones y auditorías de los receptores de servicios BaaS respecto de la prestación de los servicios. por parte del personal del proveedor de servicios BaaS, sociedades de auditoría externa, la Superintendencia o las personas que ésta designe, en condiciones normales de operación y regímenes especiales […]".*

Al respecto, sugerimos que la norma precise que el derecho de acceso y auditoría de la SBS (o sus delegados) sobre proveedores tecnológicos se ejerza de manera proporcional y reconozca mecanismos equivalentes ya existentes, tales como reportes de auditoría independiente (SOC 1/2/3), certificaciones internacionales y programas de cumplimiento sectorial. Una interpretación amplia que exija auditorías individuales on-site a proveedores de infraestructura de propósito general no resultaría escalable y podría generar conflictos contractuales con modelos de servicio estandarizados que atienden a miles de clientes simultáneamente.

5. Ampliación del alcance subjetivo: Inclusión de empresas de seguros

El proyecto normativo limita su ámbito de aplicación a las empresas comprendidas en el literal A del Art. 16 y el numeral 4 del Art. 17 de la Ley 26702, excluyendo a las empresas de seguros (literales B y D del Art. 16).

Sin embargo, el modelo de distribución de productos de seguros por terceros mediante APIs (Insurance-as-a-Service) presenta características operativas y riesgos análogos al modelo BaaS. Es por ello por lo que, sugerimos que la SBS evalúe la extensión del marco normativo — o la emisión de una norma complementaria — que aborde los modelos de distribución digital de seguros, evitando un vacío regulatorio que podría generar asimetrías competitivas y riesgos no supervisados.

Por lo expuesto, agradecemos de antemano su atención y colaboración, y aprovechamos la ocasión para reiterarle nuestra especial consideración y estima personal.

Atentamente,

Jaime Dupuy Ortiz de Zevallos
Director Ejecutivo

Firmado digitalmente por:
JAIME RICARDO DUPUY ORTIZ DE ZEVALLOS
Motivo: Soy el autor del documento
Fecha: 16/06/2026 10:52:25-0500