REQUISITOS
PARA LA VINCULACIÓN
DE PARTICIPANTES
DEL SISTEMA
DE PAGO DE BAJO VALOR INMEDIATO

credibanco

REQUISITOS PARA LA VINCULACIÓN DE PARTICIPANTES

Podrán ser participantes del Sistema de Pagos Inmediato administrado por Credibanco:

1. Entidades vigiladas y no vigiladas por la Superintendencia Financiera de Colombia

2. Cooperativas multiactivas con Sección de Ahorro y Crédito o cooperativas de ahorro y crédito vigiladas por la Superintendencia de la Economía Solidaria, inscritas en el Fondo de Garantías de Entidades Cooperativas Fogacoop,

3. Entidades no vigiladas inscritas en el Registro de Adquirentes no Vigilados por la Superintendencia Financiera de Colombia (RANV).

4. Entidades indirectas que participen mediante un Modelo Sponsor y las demás permitidas por la reglamentación local.

5. Pasarelas, Agregadores, e Iniciadores de Pago serán considerados como un participante no vigilado, siempre y cuando no ostente la calidad de vigilado.

A. En el caso de los **ADQUIRENTES NO VIGILADOS**:

1. Previamente a su solicitud de ingreso, deberán realizar el trámite del RANV cuyo objeto es permitir que se evalúe por dicha entidad la solvencia de la sociedad no vigilada que pretende desarrollar la actividad de adquirencia, de manera previa a que sea aceptada como participante del SPBV. Dicho procedimiento se circunscribe a validar el cumplimiento de los requisitos de carácter general que establece el artículo 2.17.3.1.2 del Decreto 2555 de 2010 y demás normas que lo regulen, e informar acerca de su acreditación o no las sociedades postulantes.

2. Es aceptado que el RANV opera como un mecanismo habilitante para ejercer las actividades de adquirencia, pero en ningún caso otorga a quienes lo conforman la calidad de entidad vigilada por la SFC, ni constituye un proceso de licenciamiento ante el Estado, ni garantiza el ingreso como participante dentro del sistema de pagos. En consecuencia, la inscripción en el RANV no exime a la sociedad no vigilada que pretende desarrollar la actividad de adquirencia del cumplimiento de los requisitos definidos en el presente reglamento para obtener su acceso como participante.

3. El Adquirente no vigilado, al solicitar su ingreso al sistema de pagos se compromete a mantener y actualizar la vigencia de su inscripción en el RANV, procediendo para el efecto de la forma y dentro de los términos previstos en la Circular Básica Jurídica para el efecto. En todo caso, la operación y permanencia

del Adquirente no Vigilado dentro del sistema de pago se encuentra sujeta a la condición de que dicha inscripción se encuentre vigente.

4. El Adquirente no vigilado está en la obligación de colaborar con la Superintendencia Financiera en los requerimientos de información, atención de visitas y actividades de control en cumplimiento de su atribución de poder verificar, en cualquier momento, el cumplimiento de los requisitos definidos para el RANV por parte del Adquirente. En todo caso, dicho ente de control podrá cancelar la inscripción de la sociedad no vigilada que desarrolla la actividad de adquirencia cuando: (i) Deje de acreditar el cumplimiento de los requisitos establecidos en el art. 2.17.3.1.2. del Decreto 2555 de 2010; (ii) No remita la información completa a que se refiere el subnumeral 2.4.1 dentro de los plazos establecidos; (iii) No atienda algún requerimiento de información efectuado por esta Superintendencia o, (iv) El representante legal de la sociedad no vigilada que desarrolla la actividad de adquirencia solicite la cancelación voluntaria del RANV.

5. Conforme al ordenamiento, en caso de que la inscripción en el registro sea cancelada y la sociedad no vigilada que desarrolla la actividad de adquirencia queda inhabilitada, esta deberá: (i) Ordenar inmediatamente la dispersión de los recursos que tuviere por cuenta de los comercios a las cuentas habilitadas por dichos comercios y/o trasladar dichos fondos a la cuenta puente definida por Credibanco para que culmine el procedimiento; (ii) trasladar los recursos producto de la compensación que no hubiesen sido trasladados a la sociedad no vigilada a la cuenta puente designada por Credibanco para ser dispersados directamente en favor de los comercios. La sociedad no vigilada deberá informar a la SFC, dentro de los 3 días hábiles siguientes, sobre lo definido para el efecto y su cumplimiento.

Adicional a lo mencionado anteriormente:

1. Deberán entregar a Credibanco la solicitud de entrada al SPBVI, la cual debe ser suscrita por su representante legal.

2. Deberán entregar el Certificado de Representación Legal expedido por la Superintendencia Financiera o la Cámara de comercio según sea el caso, con fecha de expedición no mayor a 30 días.

3. Deberán entregar diligenciado el Formato de Vinculación o Actualización LA/FT con los campos mínimos requeridos, el cual debe estar suscrito por su Representante Legal.

4.Deberán presentar diligenciado el Formato de KYC que soporte que cuenta con políticas y procedimientos relacionados con la prevención de riesgos SARLAFT.

5. Deberá describir la arquitectura de su infraestructura o plataforma tecnológica con énfasis en los mecanismos de redundancia y ciberseguridad y las reglas estándares operativos, técnicos y de seguridad de la entidad.

6. Acreditación y certificación por el líder de riesgos o en su lugar por el representante legal o quien haga sus veces de contar con estándares para la prevención, control, monitoreo y mitigación de los riesgos operativos, previendo a su vez situaciones originadas por errores humanos o fallas en los equipos, tendientes a mantener la continuidad de la operación, así como posibles riesgos visualizados por lo mismo dentro del Sistema de Pago.

7. En relación con su exposición a los riesgos operacionales (SARO) y prevención del riesgo de fraude (No transaccional), deberá acreditar que cuenta con estándares adecuados a través de lo siguiente:

8. Riesgo Operacional (SARO:) Suministro, extracto o descripción del manual SARO o esquema equivalente con el que cuenta la entidad. En el caso de no ser vigilada, acompañados de la certificación del Líder de riesgos o Representante Legal sobre su aplicación efectiva. Debe incluir la administración de riesgos operacionales de terceros u Outsourcing.

9. En materia de prevención del riesgo de fraude. Manual o documento explicativo acorde con las exigencias legales y los programas de cumplimiento de los sistemas de marca internacionales o locales. (Indicar si está contenido dentro del manual SARO o se contiene dentro del manual de buen gobierno, Antifraude y soborno, etc.) Opcional: Copia de las certificaciones (ISO 9001, ISO 37001, etc.) pertinentes con las que cuente y apoyen la acreditación de la administración de estos riesgos. En el caso de no ser vigilada, acompañar los puntos anteriores de certificación del Líder de riesgos o Representante Legal sobre su aplicación efectiva. Incluir la administración de riesgos con terceros (Proveedores).

10.En relación con su exposición a los riesgos de Continuidad de Negocio: Deberá acreditar que cuenta con estándares adecuados a través de lo siguiente:

10.1. Suministro, extracto o descripción del manual de continuidad de negocio o documento explicativo acerca de la administración de Riesgos de Continuidad de Negocio.

10.2. Suministro, extracto o descripción de planes de continuidad (tecnológica y operativa), sistemas de contingencia que permitan tener la tranquilidad frente a la disponibilidad de los servicios.

10.3. Opcional: Copia de certificación ISO 22301 o equivalentes que apoye con la acreditación de la implementación de los estándares.

11.En el caso de no ser vigilada, acompañar los puntos anteriores de certificación del Líder de riesgos o Representante Legal sobre su aplicación efectiva. Incluir la administración de riesgos con terceros críticos.

12. Frente a seguridad de la información y ciberseguridad, deberá entregar un documento explicativo de las reglas estándares de Seguridad de la Información y Ciberseguridad o Certificación de implementación y cumplimiento del SGSI Sistema

de Seguridad de la Información y Ciberseguridad, emitida por la entidad y/o representante legal.

13.Adicionalmente, un documento explicativo donde se detalle la metodología de riesgos de Seguridad de la Información y Ciberseguridad, la frecuencia de actualización y una acreditación en la cual se indique que cuentan con una matriz de riesgos de Seguridad de la Información y Ciberseguridad donde se identifican los riesgos asociados a la confidencialidad, integridad y/o disponibilidad de los datos que se intercambian con CredibanCo y que dichos riesgos se encuentran en el apetito de riesgo aceptado por el Participante.

14. Frente la prevención del riesgo de fraude deberá entregar la acreditación de la prevención del riesgo de fraude adquirente, según el caso, acordes con las exigencias legales y los programas de cumplimiento de los sistemas de marca internacionales o locales.

B. En el caso de los **PARTICIPANTES PATROCINADOS (INDIRECTOS):**

Las entidades que aspiren a vincularse al Sistema de Pagos Inmediato de Credibanco en condición de Participante Indirectos, deben cumplir con las condiciones previstas en el ordenamiento legal para ello. Además, deberán acreditar las condiciones aquí descritas y entregar la siguiente documentación:

1. Deberán entregar a Credibanco la solicitud de entrada al SPBVI, la cual debe ser suscrita por su representante legal.

2. Deberá entregar el Convenio de relación con Banco Sponsor según lo mencionado en la Circular DSP-471 del Banco de la República

3. Deberán entregar el Certificado de Representación Legal expedido por la Superintendencia Financiera o la Cámara de comercio según sea el caso, con fecha de expedición no mayor a 30 días.

4. Deberán entregar diligenciado el Formato de Vinculación o Actualización LA/FT con los campos mínimos requeridos, el cual debe estar suscrito por su Representante Legal.

5. Deberán presentar diligenciado el Formato de KYC que soporte que cuenta con políticas y procedimientos relacionados con la prevención de riesgos SARLAFT.

6. Deberá describir la arquitectura de su infraestructura o plataforma tecnológica con énfasis en los mecanismos de redundancia y ciberseguridad y las reglas estándares operativos, técnicos y de seguridad de la entidad.

7. Acreditación y certificación por el líder de riesgos o en su lugar por el representante legal o quien haga sus veces de contar con estándares para la prevención, control, monitoreo y mitigación de los riesgos operativos, previendo a su vez situaciones originadas por errores humanos o fallas en los equipos, tendientes

a mantener la continuidad de la operación, así como posibles riesgos visualizados por lo mismo dentro del Sistema de Pago.

8. En relación con su exposición a los riesgos operacionales (SARO) y prevención del riesgo de fraude (No transaccional), deberá acreditar que cuenta con estándares adecuados a través de lo siguiente:

9. Riesgo Operacional (SARO:) Suministro, extracto o descripción del manual SARO o esquema equivalente con el que cuenta la entidad. En el caso de no ser vigilada, acompañados de la certificación del Líder de riesgos o Representante Legal sobre su aplicación efectiva. Debe incluir la administración de riesgos operacionales de terceros u Outsourcing

10.En materia de prevención del riesgo de fraude. Manual o documento explicativo acorde con las exigencias legales y los programas de cumplimiento de los sistemas de marca internacionales o locales. (Indicar si está contenido dentro del manual SARO o se contiene dentro del manual de buen gobierno, Antifraude y soborno, etc.) Opcional: Copia de las certificaciones (ISO 9001, ISO 37001, etc.) pertinentes con las que cuente y apoyen la acreditación de la administración de estos riesgos.

En el caso de no ser vigilada, acompañar los puntos anteriores de certificación del Líder de riesgos o Representante Legal sobre su aplicación efectiva. Incluir la administración de riesgos con terceros (Proveedores).

11.En relación con su exposición a los riesgos de Continuidad de Negocio: Deberá acreditar que cuenta con estándares adecuados a través de lo siguiente:

11.1. Suministro, extracto o descripción del manual de continuidad de negocio o documento explicativo acerca de la administración de Riesgos de Continuidad de Negocio.

11.2. Suministro, extracto o descripción de planes de continuidad (tecnológica y operativa), sistemas de contingencia que permitan tener la tranquilidad frente a la disponibilidad de los servicios.

11.3. Opcional: Copia de certificación ISO 22301 o equivalentes que apoye con la acreditación de la implementación de los estándares.

12.En el caso de no ser vigilada, acompañar los puntos anteriores de certificación del Líder de riesgos o Representante Legal sobre su aplicación efectiva. Incluir la administración de riesgos con terceros críticos.

13. Frente a seguridad de la información y ciberseguridad, deberá entregar un documento explicativo de las reglas estándares de Seguridad de la Información y Ciberseguridad o Certificación de implementación y cumplimiento del SGSI Sistema de Seguridad de la Información y Ciberseguridad, emitida por la entidad y/o representante legal.

14.Adicionalmente, un documento explicativo donde se detalle la metodología de riesgos de Seguridad de la Información y Ciberseguridad, la frecuencia de actualización y una acreditación en la cual se indique que cuentan con una matriz de riesgos de Seguridad de la Información y Ciberseguridad donde se identifican los riesgos asociados a la confidencialidad, integridad y/o disponibilidad de los datos que se intercambian con CredibanCo y que dichos riesgos se encuentran en el apetito de riesgo aceptado por el Participante.

C. En el caso de los **PARTICIPANTES DIRECTOS VIGILADOS POR SFC**

Las entidades que aspiren a vincularse al Sistema de Pagos Inmediato de Credibanco en condición de Participante, deben cumplir con las condiciones previstas en el ordenamiento legal para ello. Además, deberán acreditar las condiciones aquí descritas y entregar la siguiente documentación:

1. Deberán cumplir, en el caso de las entidades vigiladas, con los requisitos de capital, solvencia y mecanismos de separación de fondos previstos en el Estatuto Orgánico del Sistema de Financiera y regulaciones complementarias y, en el caso de los Adquirentes no vigilados con los requisitos de capital, solvencia o mecanismos de separación de fondos provenientes de órdenes de pago o transferencias de fondos previstos en el artículo 2.17.3.1.2 del Decreto 2555 de 2010.

2. Deberán entregar a Credibanco la solicitud de entrada al SPBVI, la cual debe ser suscrita por su representante legal junto con las declaraciones de origen de fondos y autorizaciones para el cotejo, procesamiento y actualización de la información y documentación de ingreso.

3. Deberán entregar el Certificado de Representación Legal expedido por la Superintendencia Financiera o la Cámara de comercio según sea el caso, con fecha de expedición no mayor a 30 días.

4. En lo que respecta al riesgo de lavado de activos, financiación del terrorismo y de la proliferación de armas de destrucción masiva, la Entidad Vigilada por la SFC, deberá acreditar que cuenta con un SARLAFT que soportará en certificación firmada por su Oficial de Cumplimiento Principal o Suplente.

5. Deberá describir la arquitectura de su infraestructura o plataforma tecnológica con énfasis en los mecanismos de redundancia y ciberseguridad y las reglas estándares operativos, técnicos y de seguridad de la entidad.

6. Acreditación y certificación por el líder de riesgos o en su lugar por el representante legal o quien haga sus veces de contar con estándares para la prevención, control, monitoreo y mitigación de los riesgos operativos, previendo a su vez situaciones originadas por errores humanos o fallas en los equipos, tendientes a mantener la continuidad de la operación, así como posibles riesgos visualizados por lo mismo dentro del Sistema de Pago.

7. En relación con su exposición a los riesgos operacionales (SARO) y prevención del riesgo de fraude (No transaccional), deberá acreditar que cuenta con estándares adecuados a través de lo siguiente:

8. Riesgo Operacional (SARO:) Suministro, extracto o descripción del manual SARO o esquema equivalente con el que cuenta la entidad. En el caso de no ser vigilada, acompañados de la certificación del Líder de riesgos o Representante Legal sobre su aplicación efectiva. Debe incluir la administración de riesgos operacionales de terceros u Outsourcing.

9. En materia de prevención del riesgo de fraude. Manual o documento explicativo acorde con las exigencias legales y los programas de cumplimiento de los sistemas de marca internacionales o locales. (Indicar si está contenido dentro del manual SARO o se contiene dentro del manual de buen gobierno, Antifraude y soborno, etc.) Opcional: Copia de las certificaciones (ISO 9001, ISO 37001, etc.) pertinentes con las que cuente y apoyen la acreditación de la administración de estos riesgos.

10. En relación con su exposición a los riesgos de Continuidad de Negocio: Deberá acreditar que cuenta con estándares adecuados a través de lo siguiente: a. Suministro, extracto o descripción del manual de continuidad de negocio o documento explicativo acerca de la administración de Riesgos de Continuidad de Negocio. b. Suministro, extracto o descripción de planes de continuidad (tecnológica y operativa), sistemas de contingencia que permitan tener la tranquilidad frente a la disponibilidad de los servicios. c. Opcional: Copia de certificación ISO 22301 o equivalentes que apoye con la acreditación de la implementación de los estándares.

11. Frente a seguridad de la información y ciberseguridad, deberá entregar un documento explicativo de las reglas estándares de Seguridad de la Información y Ciberseguridad o Certificación de implementación y cumplimiento del SGSI Sistema de Seguridad de la Información y Ciberseguridad, emitida por la entidad y/o representante legal.

12. Adicionalmente, un documento explicativo donde se detalle la metodología de riesgos de Seguridad de la Información y Ciberseguridad, la frecuencia de actualización y una acreditación en la cual se indique que cuentan con una matriz de riesgos de Seguridad de la Información y Ciberseguridad donde se identifican los riesgos asociados a la confidencialidad, integridad y/o disponibilidad de los datos que se intercambian con CredibanCo y que dichos riesgos se encuentran en el apetito de riesgo aceptado por el Participante Frente la prevención del riesgo de fraude deberá entregar la acreditación de la prevención del riesgo de fraude adquirente y/o emisor, según el caso, acordes con las exigencias legales y los programas de cumplimiento de los sistemas de marca internacionales o locales.

D. En el caso de las PASARELAS, AGREGADORES E INICIADORES DE PAGO

Las entidades que aspiren a vincularse al Sistema de Pagos Inmediato de Credibanco en condición de Pasarelas, Agregadores e Iniciadores de Pago, deben cumplir con las condiciones previstas en el ordenamiento legal para ello. Además, deberán acreditar las condiciones aquí descritas y entregar la siguiente documentación:

1. Deberán entregar a Credibanco la solicitud de entrada al SPBVI, la cual debe ser suscrita por su representante legal.

2. Cuando la vinculación se realice para el agregador con tecnología propia, se debe anexar la certificación de su relacionamiento contractual con la entidad adquirente.

3. Deberá entregar la Carátula PSP firmada.

4. Deberán entregar el Certificado de Representación Legal expedido por la Superintendencia Financiera o la Cámara de comercio según sea el caso, con fecha de expedición no mayor a 30 días.

5. Deberán entregar diligenciado el Formato de Vinculación o Actualización LA/FT con los campos mínimos requeridos, el cual debe estar suscrito por su Representante Legal.

6. Deberán presentar diligenciado el Formato de KYC que soporte que cuenta con políticas y procedimientos relacionados con la prevención de riesgos SARLAFT.

7. Deberá describir la arquitectura de su infraestructura o plataforma tecnológica con énfasis en los mecanismos de redundancia y ciberseguridad y las reglas estándares operativos, técnicos y de seguridad de la entidad.

8. Acreditación y certificación por el líder de riesgos o en su lugar por el representante legal o quien haga sus veces de contar con estándares para la prevención, control, monitoreo y mitigación de los riesgos operativos, previendo a su vez situaciones originadas por errores humanos o fallas en los equipos, tendientes a mantener la continuidad de la operación, así como posibles riesgos visualizados por lo mismo dentro del Sistema de Pago.

9. En relación con su exposición a los riesgos operacionales (SARO) y prevención del riesgo de fraude (No transaccional), deberá acreditar que cuenta con estándares adecuados a través de lo siguiente

10.Riesgo Operacional (SARO:) Suministro, extracto o descripción del manual SARO o esquema equivalente con el que cuenta la entidad. En el caso de no ser vigilada, acompañados de la certificación del Líder de riesgos o Representante Legal sobre su aplicación efectiva. Debe incluir la administración de riesgos operacionales de terceros u Outsourcing

11.En materia de prevención del riesgo de fraude. Manual o documento explicativo acorde con las exigencias legales y los programas de cumplimiento de

los sistemas de marca internacionales o locales. (Indicar si está contenido dentro del manual SARO o se contiene dentro del manual de buen gobierno, Antifraude y soborno, etc.) Opcional: Copia de las certificaciones (ISO 9001, ISO 37001, etc.) pertinentes con las que cuente y apoyen la acreditación de la administración de estos riesgos. En el caso de no ser vigilada, acompañar los puntos anteriores de certificación del Líder de riesgos o Representante Legal sobre su aplicación efectiva. Incluir la administración de riesgos con terceros (Proveedores).

12. Frente a seguridad de la información y ciberseguridad, deberá entregar un documento explicativo de las reglas estándares de Seguridad de la Información y Ciberseguridad o Certificación de implementación y cumplimiento del SGSI Sistema de Seguridad de la Información y Ciberseguridad, emitida por la entidad y/o representante legal

13.Adicionalmente, un documento explicativo donde se detalle la metodología de riesgos de Seguridad de la Información y Ciberseguridad, la frecuencia de actualización y una acreditación en la cual se indique que cuentan con una matriz de riesgos de Seguridad de la Información y Ciberseguridad donde se identifican los riesgos asociados a la confidencialidad, integridad y/o disponibilidad de los datos que se intercambian con CredibanCo y que dichos riesgos se encuentran en el apetito de riesgo aceptado por el Participante.

Para el caso de aquellos participantes ya vinculados a otros Sistema de Pagos administrado por Credibanco S.A., solo se deberán acreditarse los requisitos y documentación que no se hubiese acreditado al momento de postularse como participante en dicho Sistema, o en caso tal que se requiera actualizar el cumplimiento de los requisitos listados en este reglamento, deberán acreditar toda la documentación que les sea solicitada.