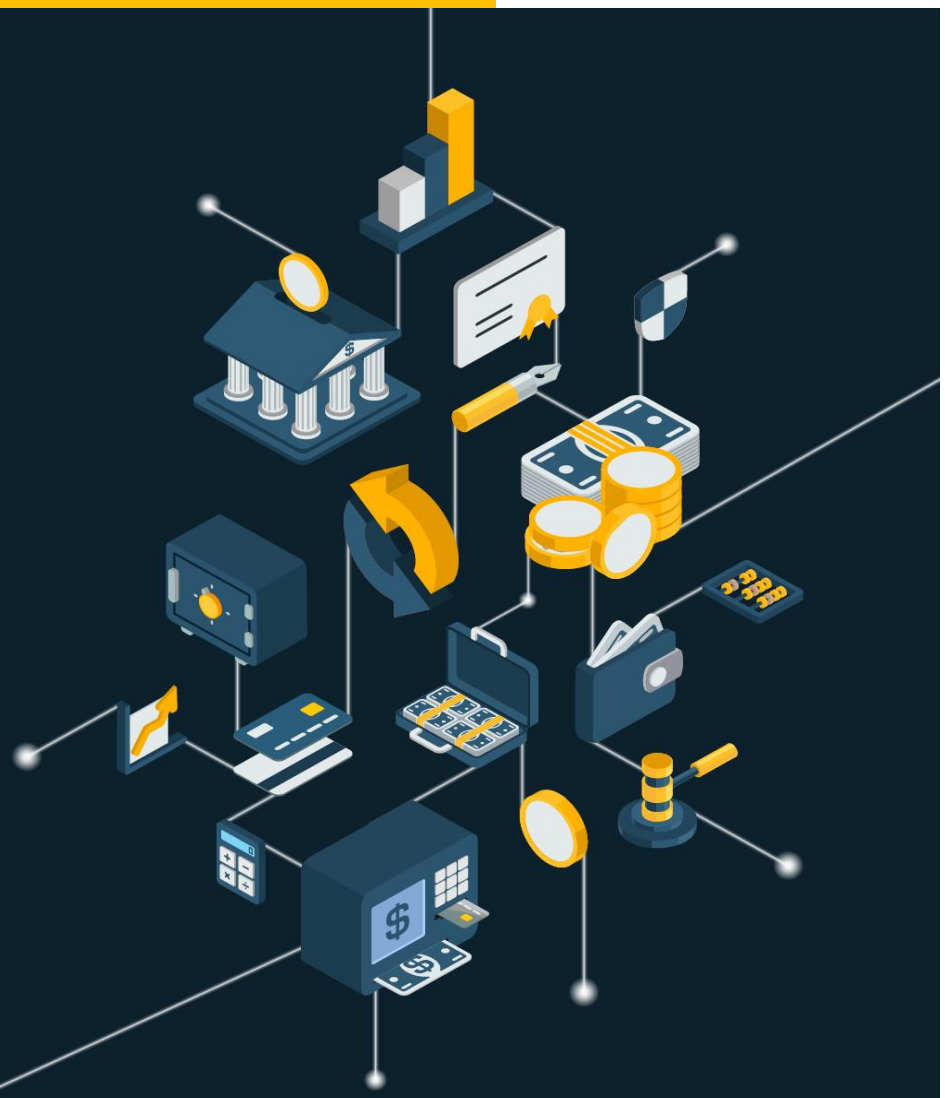
FORO

Sistemas de Pago de Colombia

Seguridad

Reglas y Estándares

23 de mayo de 2023



Contenido

1. Introducción
2. Seguridad en el ecosistema de pagos inmediatos
3. Prevención de fraude en los pagos inmediatos
4. Continuidad de la operación
5. Preguntas
6. Consideraciones del Supervisor en materia de seguridad: Presentación a cargo de la Superintendencia Financiera de Colombia

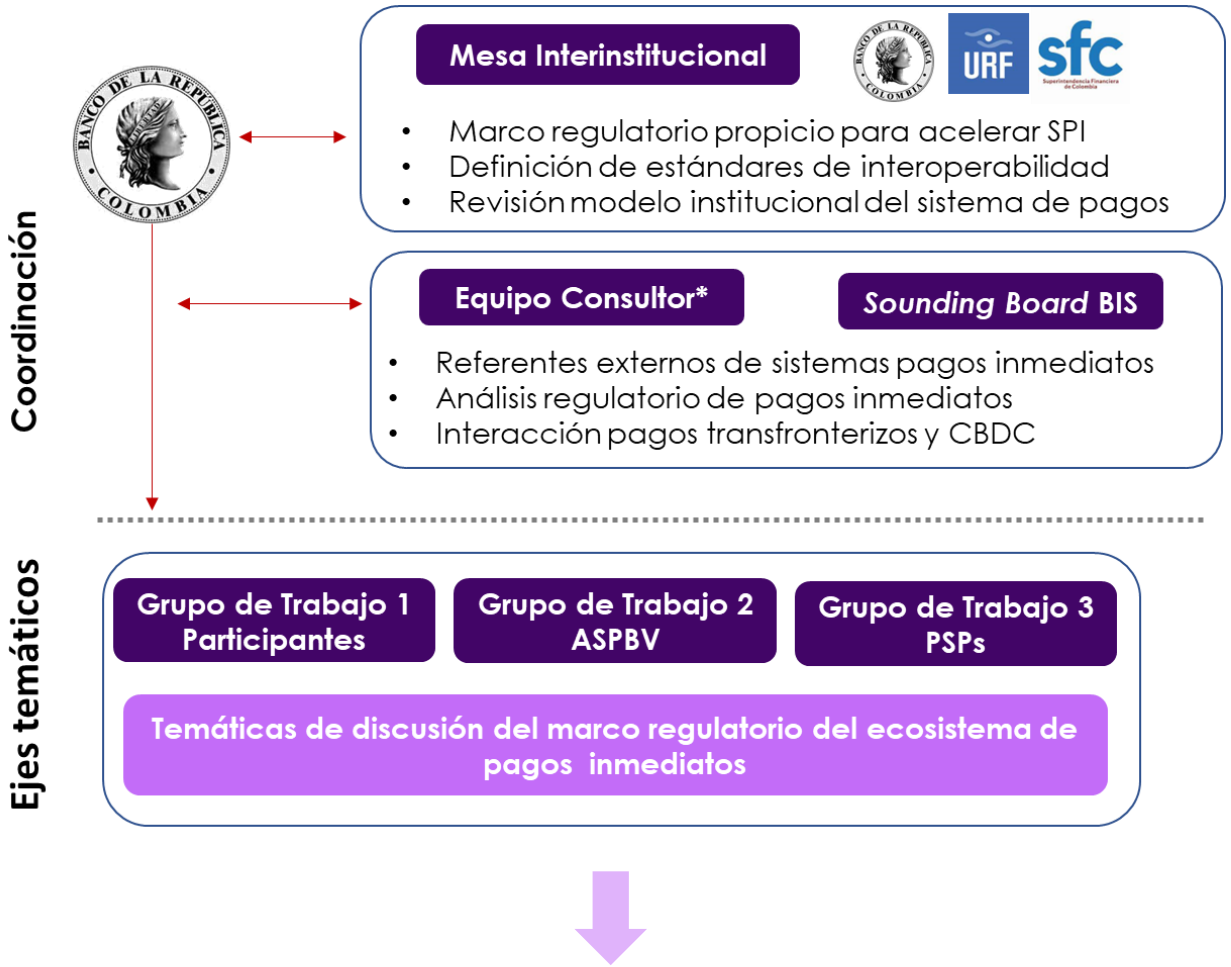
Contenido

¿CUÁL ES EL OBJETIVO DE LA SEGUNDA ETAPA?

Analizar y discutir las reglas y estándares necesarios para facilitar el funcionamiento del Ecosistema de Pagos Inmediatos en Colombia y la promoción de la interoperabilidad al interior del mismo.

¿CÓMO ES SU ESTRUCTURA?

La industria será convocada a participar en sesiones magistrales en las cuales se presentarán las propuestas de regulación. En sesiones sucesivas se llevará acabo la discusión y retroalimentación. La industria podrá, además, remitir comentarios escritos al correo pagosinmediatos@banrep.gov.co.



*La firma Marulanda Consultores apoya técnicamente al Banco de la República en el diseño y ejecución del Foro de Sistemas de Pago.

Cronograma

SEGUNDA ETAPA FORO DE SISTEMAS DE PAGO

	MARTES Sesiones Magistrales	Recepción de comentarios adicionales	JUEVES Sesiones de Discusión G1 y G3	VIERNES Sesiones de Discusión G2
A. Ámbito de los pagos inmediatos y Tecnologías de Acceso	**Abril 25** 2:30 p.m. - 4:30 p.m.	**Mayo 2**	**Mayo 4** 10:00 a.m. - 12:00 p.m G1	**Mayo 5** SPBV 8:00 - 10:00 a.m. PSPs 3:30 - 5:30 p.m.
B. Directorio y Llaves	**Mayo 2** 2:30 p.m. - 4:30 p.m.	**Mayo 9**	**Mayo 11** 10:00 a.m. - 12:00 p.m G1	**Mayo 12** SPBV 8:00 - 10:00 a.m. PSPs 2:30 - 4:30 p.m.
C. Marca, UX homogénea y Tarifas	**Mayo 9** **Presencial** 8:00 a.m. - 12:00 p.m.	**Mayo 16**	**Mayo 18** 10:00 a.m. - 12:00 p.m **G1, G2 y G3**	
D. Compensación y Liquidación e Interconexión	**Mayo 16** 2:30 p.m. - 4:30 p.m.	**Mayo 24**	**Mayo 25** 10:00 a.m. - 12:00 p.m **G1 y G3**	**Mayo 26** SPBV 8:00 - 10:00 a.m. **G2**
E. Seguridad	**Mayo 23** 2:30 p.m. - 4:30 p.m.	**Mayo 31**	**Junio 1** 10:00 a.m. - 12:00 p.m **G1 y G3**	**Junio 2** SPBV 8:00 - 10:00 a.m. **G2**
F. Siguientes casos de uso y servicios superpuestos	**Mayo 30** **Presencial** 8:00 a.m. - 12:00 p.m.	**Junio 7**	**Junio 8** 10:00 a.m. - 12:00 p.m **G1 y G3**	**Junio 9** SPBV 8:00 - 10:00 a.m. **G2**
G. Indicadores de seguimiento y monitoreo	**Junio 6** 2:30 p.m. - 4:30 p.m.	**Junio 14**		

SIGUIENTES CASOS DE USO Y SERVICIOS SUPERPUESTOS – Sesión Presencial

30 de mayo de 2023, Biblioteca Luis Ángel Arango

8:00 a.m. **Bienvenida**

8:15 a.m. **Escalabilidad del ecosistema de pagos inmediatos: la experiencia internacional**
Dylan Lennox, Consultor CGAP - Banco Mundial

9:00 a.m. **Nuevos casos de uso en el Sistema PIX: lecciones y retos**
Mayara Yano, Senior Advisor - Banco Central de Brasil

9:45 a.m. **Actividad de iniciación de pagos en Colombia**
Ana Maria Zuluaga, Directora Innova SFC - Superintendencia Financiera de Colombia

10:15 a.m. **Café**

10:45 am **Panel Necesidades y retos de los pagos digitales en la economía**
Moderadora: Bibiana Taboada, Codirectora Banco de la República
Orlando Santiago Cely, Gerente General de Transmilenio S.A. ***(TBC)***
Maria Fernanda Quiñones, Presidente Cámara CCE
Alexandra Rodriguez, Tesorera Empresa de Acueducto y Alcantarillado de Bogotá
Jorge Jaller, Vicepresidente Retail Grupo Éxito ***(TBC)***

11:30 a.m. **Panel Expansión del ecosistema de pagos en Colombia**
Moderador: Camilo Hernandez, Subdirector de Desarrollo de Mercados URF
Andres Duque, Presidente Redeban
Gustavo Vega, Presidente ACH Colombia
Ricardo Zambrano, Presidente (e) Credibanco
Federico Martinez, Country Manager MasterCard Colombia
Adriana Cárdenas, Gerente General Visa Colombia

12:15 p.m. **Cierre** – *Ana Maria Prieto, Banco de la República*

SESIONES VIRTUALES

El día anterior de cada sesión, el equipo Banco República compartirá el link de conexión a la plataforma Teams.

SESIONES PRESENCIALES

Tendrán lugar en la Biblioteca Luis Angel Arango. La agenda de las jornadas serán remitidas vía correo a los inscritos.

El Banco de la República invita a la industria de pagos a participar en la **Segunda Etapa del Foro de Sistemas de Pagos.**

Si requiere actualizar su inscripción o tiene alguna pregunta frente a la misma favor contactarnos al correo pagosinmediatos@banrep.gov.co.

PREGUNTAS DE DISCUSIÓN

En las sesiones magistrales se presentarán las preguntas que serán discutidas en las sesiones siguientes. Quienes deseen remitir sus comentarios escritos podrán hacerlo en las fechas que se indicarán en cada sesión al correo pagosinmediatos@banrep.gov.co

MEMORIAS

Consulte las memoras del Foro de Sistemas de Pago en la página del Banco de la República: www.banrep.gov.co/es/sistemas-pago/foro-sistemas-pago-colombiav.co)

Contenido

¿Aumenta el riesgo de fraude en los pagos inmediatos?

CARACTERÍSTICAS DE INMEDIATEZ E IRREVOCABILIDAD EN EL PAGO INMEDIATO DEMANDAN MAYOR ATENCIÓN A LA PREVENCIÓN Y GESTIÓN DE RIESGOS

- Menor tiempo de monitoreo y detección oportuna de intentos de fraude por parte de participantes.
- La inmediate del procesamiento y liquidación impiden que usuario originador pueda suspender una orden de pago, p.ej. por error en datos enviados, una vez se ha iniciado el procesamiento, como si ocurre en otros pagos digitales.
- Disponibilidad inmediata de los recursos en los depósitos receptores, sumado a procesos simplificados de KYC en depósitos de bajo monto, genera incentivos adicionales para el fraude.

En Estados Unidos un encuesta a principales entidades financieras encontró que 32% de los encuestados afirma que hay patrones de fraude específicos en los pagos Inmediatos.

"El abuso de la inmediatez y la irrevocabilidad están presentes. También ocurre el robo / conocimiento masivo de PII y el robo de OTP y otras autenticación escalonada. Es más rápido que antes".

Alrededor del 50% de los encuestados reportaron que han adoptado tecnologías y mecanismos de control para pagos inmediatos (Ej. sistemas de monitoreo en tiempo real); 40% han implementado IA y 30% han mejorado técnicas de autenticación.

Mejores prácticas de prevención a nivel internacional

1. Visión holística del fraude. Analizar tipologías aplicables especialmente en los pagos inmediatos y adecuar modelos de prevención actuales al ecosistema.

2. Herramientas en los participantes. Incorporar tecnologías y protocolos para fortalecer la autenticación y validación de identidad, definir límites según patrones y uso de IA para detección de fraude en tiempo real, entre otros.

3. Demora en el procesamiento. En México, Suiza y Corea del Sur implementaron mecanismos de procesamiento lento ante sospecha de fraude alertada por participantes, incluida opción de retención de recursos.

4. Información compartida. En India, Estados Unidos y Australia, entre otros, se obliga a los participantes a reportar cuentas y Llaves sospechosas de fraude en registros creados con ese fin. Participantes consultan información para fortalecer su monitoreo y detección temprana.

5. Campañas masivas. Sensibilización a los usuarios sobre las características de los pagos, los riesgos y sugerencias para prevenirlos. Ej: no entregar información personal, revisar estado de QR del comercio, etc.

pix powered by Banco Central

Ante modalidad de Secuestro Express el Banco Central de Brasil fijó tope máximo a los pagos de 8 pm a 6 am y autorizó a que participantes fijen límites diferenciales día y noche.

Campaña Consejo de Pagos Inmediatos Reino Unido

1) Nunca revele detalles de seguridad como PIN, 2) no asuma que las solicitudes de correo electrónico o las personas que llaman son genuinas, 3) no se apresure, 4) escuche sus instintos y 5) mantenga el control.

Fuente: US Faster Payments Council (2021) *Faster Payments Fraud Survey and Report* y FedNow.

En algunos sistemas de pagos inmediatos, como PIX, **los Directorios incluyen información para apoyar la prevención de fraude que deben adelantar los participantes.**

En el caso de PIX el Directorio dispone de una estadística de suspensiones de cada Llave. Esta y otras marcas similares pueden ser consultadas por los participantes como parte de sus monitoreos de riesgo.

GT de Segurança | Fluxo de uso da informação de disputa

Contexto

Após posicionamento do BCB sobre informações de disputa na DICT, análises foram aprofundadas com objetivo de manter compartilhamento de informações de fraude, garantindo os seus benefícios, mas sem trazer prejuízos ao usuário recebedor

Proposta Inicial (binária)

10. Chave em processo de análise de disputa (S/N)
11. Data da análise da disputa

Nova Proposta (estatística)

% Transações Disputadas (0-1 dia)
% Transações Disputadas (0-7 dias)
% Transações Disputadas (0-30 dias)

Sugestão de regras aplicadas à Proposta Atual:

I. A variável **"% Transações Disputadas"** será calculada através da quantidade de transações com suspeita de fraudes, sobre a quantidade total de transações realizadas pela chave nos períodos de 0 a 1 dia, 0 a 7 dias e 0 a 30 dias; Ex.: a chave aaa@gmail.com abaixo realizou 2 transações em d-1, sendo que houve uma suspeita de fraude (1/2=50%), contudo, o cliente realizou 20 transações na semana (1/20=5%) e 100 no mês (1/100=1%). A chave de celular do mesmo CPF no BANCO2, onde não há fraude, não é prejudicada.

II. A marcação de suspeita de fraude no DICT será feita à toda requisição de devolução feita pelo PSP pagador por motivo de fraude (CP76 - art. 39 - §1º - Inciso III)

III. O BCB fará o processamento de cálculo desses campos apenas uma vez ao dia, não onerando o DICT.

IV. PSP Recebedor tem acesso rápido às informações de fraude da chave, realizando as análises e excluindo a chave quando necessário, minimizando fraudes futuras

Exemplos:

DICT							
CHAVE	CPF	CONTA	PSP Origem	...	% Transações Disputadas (0-1 dia)	% Transações Disputadas (0-7 dias)	% Transações Disputadas (0-30 dias)
aaa@gmail.com	111.222.333-04	554488965	BANCO1	...	50%	5%	2%
(11)945426688	111.222.333-04	21566871	BANCO2	...	-	-	-
123.456.789-09	123.456.789-09	1001265469	BANCO3	...	100%	100%	100%
321.654.987-12	321.654.987-12	226598756	BANCO4	...	-	-	-

Contenido

La seguridad en el ecosistema **requiere definir mecanismos y procesos en cada fase del flujo** de pagos inmediatos orientados a la prevención de fraude.

1. Previo a la operación

2. Gestión de Llaves y QR

3. Operación

Mecanismos de seguridad

Previo a la operación

AUTENTICACIÓN

- Participante deberá realizar el proceso de autenticación y validación de identidad del cliente originador en sus canales, siguiendo políticas de seguridad y la normatividad aplicable.

LÍMITES AL VALOR DE LAS TRANSACCIONES DISCRECIONALES DEL PARTICIPANTE

- Participante podrá definir el valor máximo de las operaciones que permite originar como pago inmediato acorde con sus modelos de riesgo.

- El límite deberá ser aplicable de forma transversal tanto a los pagos intra-SPBV e inter-SPBV como *on-us* inmediatos.

- Dentro de dicho límite los usuarios podrán establecer montos inferiores.

- Adicionalmente, participante podrá, establecer límite al número de operaciones, sin discriminar por tipo de operación inmediata.

VERIFICACIÓN

- En cada operación el participante deberá, al resolver la Llave, disponer al usuario originador el mecanismo de confirmación del nombre del receptor antes de iniciar un pago o transferencia.

Mecanismos de seguridad

Gestión de Llaves

Procesos de registro y ciclo de vida de Llave(s) requiere autenticación previa, siguiendo las políticas de seguridad del participante.

Como medida de seguridad adicional, se propone restringir horarios a nivel del ecosistema para surtir estos procesos, excepto consulta y cancelación de Llave.

OPERACIÓN	HORARIOS
Consulta Llave	Habilitado 24/7
Registro	6 am – 8 pm
Modificación	
Portabilidad	
Cancelación	Habilitado 24/7

REGISTRO

- Para la Llave de ID, celular y correo, como mecanismo de seguridad y de mejor UX, el proceso debe hacerse usando la información del usuario que tiene el participante y utilizando el mecanismo de "autollenado".

- En caso que el usuario dese usar correo o celular diferente al que está registro en la entidad, deberá actualizar los datos de forma previa.

- Para la Llave alfanumérica, se recuerda que la misma debe incluir una combinación de letras, números y símbolos. En todo caso se propone como reglas de control las siguientes:
  1. No se podrá utilizar el signo @
  2. No puede consignarse ningún dato de ID personal

- En cualquier caso, para finalizar solicitud de registro se requiere confirmación con doble factor de autenticación.

- Periodo de activación de 24 horas, contado a partir del registro exitoso de Llave, para que el usuario pueda recibir una pago.

MODIFICACIÓN, CANCELACIÓN o PORTABILIDAD

- Doble factor de autenticación para solicitar procesos.

- Para portabilidad se prevé un periodo de "suspensión" de Llave para permitir al usuario finalizar proceso en nueva entidad.

Mecanismos de seguridad

Gestión de Llaves

SUSPENSIÓN DE LA LLAVE POR SOLICITUD DEL USUARIO

- Usuario podrá solicitar a su entidad bloquear la Llave ante sospecha de fraude.
- Participante deberá solicitar al SPBV respectivo cambiar el estado de la Llave en el Directorio a "suspendida". A los 15 días hábiles máximo el participante deberá confirmar con el usuario si la Llave debe ser actividad o cancelada.
- El Directorio deberá mantener la marca del estado suspendido durante el periodo de suspensión y a disposición de ser consultado por cualquier otro participante durante ese lapso.

SUSPENSIÓN DE LA LLAVE POR EL PARTICIPANTE

- Los participantes podrán suspender la(s) Llave(s) ante sospecha de fraude.
- Participante deberá informar al usuario y solicitar al SPBV respectivo cambiar el estado de la Llave en el Directorio a "suspendida". A los 15 días hábiles máximo el Participante deberá confirmar si la Llave debe ser actividad o cancelada.
- El Directorio deberá mantener la marca del estado suspendido durante el periodo de suspensión y a disposición de ser consultado por cualquier otro participante durante ese lapso.

Mecanismos de seguridad

Gestión de QR

- Los fraudes asociados a operaciones con QR se pueden originar en:
  - Insertar vínculos a URL maliciosas (malware o ataques de phishing)
  - Reemplazo de los códigos para desviar un pago a la cuenta del defraudador

- La operación fraudulenta es exitosa solo si existe un depósito activo a nombre del defraudador. La literatura resalta que estos fraudes implican fallas en la validación de identidad, así como en la suplantación del Código QR, y resalta algunos mitigantes:

  - Información clara a los comercios invitándoles a confirmar periódicamente su QR y la vinculación del mismo a sus cuentas.

  - Disponer mecanismo de validación de identidad del comercio al cliente originador antes de iniciar el pago.

MECANISMOS DE SEGURIDAD PROPUESTOS

- Adopción de estándares acordados por la industria para la generación de QR estático y dinámico.

- Originación de QR solo en la aplicación/pagina web de un participante o mediante los PSP autorizados por el mismo.

- Confirmación al usuario originador sobre identidad del comercio asociado al QR antes de iniciar el pago.

- Valor del pago debe ser introducido por parte del usuario originador. Si el QR incorpora el valor, se requiere validación del originador sobre el valor a pagar.

Mecanismos de seguridad

Durante la operación

SUSPENSIÓN DE LA OPERACIÓN POR PARTE DEL PARTICIPANTE ORIGINADOR

- Participante originador podrá suspender o rechazar una transacción ante operaciones inusuales o sospecha de fraude (Ejemplo por posible suplantación de identidad del usuario originador).

- Esta posibilidad se entiende como un control preventivo que debe ser tramitado previo al momento de aceptación de la orden de pago o transferencia en el SPBV. Lo anterior, debido a que una vez aceptada la operación, el principio de finalidad aplica y por tanto la operación es irrevocable.

- Para validar o descartar la alarma, el participante debe enviar al usuario una solicitud de confirmación de la operación por OTP al correo electrónico o vía SMS:

    - Si el usuario confirma OTP, el participante originador continua el procesamiento de la operación.

    - Si el usuario desconoce la operación, el participante originador debe rechazar la operación, activar proceso de suspensión de Llave ante el SPBV respectivo e informar al usuario.

    - Si el usuario no responde la OTP. La operación puede quedar suspendida por un máximo de 5 minutos. Si la operación no es confirmada por el usuario en dicho plazo, el participante podrá rechazar la operación para lo cual deberá informar al usuario. También podrá de manera preventiva suspender la Llave siguiendo el proceso descrito.

Mecanismos de seguridad

Durante la operación

SUSPENSIÓN DE LA OPERACIÓN POR PARTE DEL PARTICIPANTE RECEPTOR

- Participante receptor podrá suspender o rechazar una transacción ante operaciones inusuales o sospecha de fraude (Ejemplo: posible lavado de activos o creación de una cuenta y su Llave para extraer recursos enviados desde cuenta originadora comprometida).

- Esta posibilidad se entiende como un control preventivo que debe ser tramitado previo al momento de aceptación de la orden de pago o transferencia en el SPBV. Lo anterior, debido a que una vez aceptada la operación, el principio de finalidad aplica y por tanto la operación es irrevocable.

- Para validar o descartar la alarma, el participante receptor debe enviar al usuario receptor una solicitud de confirmación de la operación por OTP al correo electrónico o vía SMS:

    - Si el usuario confirma OTP, el participante receptor continua el procesamiento de la operación.

    - Si el usuario desconoce la operación, el participante receptor debe rechazar la operación, activar proceso de suspensión de Llave ante el SPBV respectivo e informar al usuario receptor. El SPBV debe informar al participante originador del rechazo y el motivo del mismo para que éste evalúe necesidad de realizar suspensión de la Llave originadora.

    - Si el usuario no responde la OTP. La operación puede quedar suspendida por un máximo de 5 minutos. Si la operación no es confirmada por el usuario en dicho plazo, el participante podrá rechazar la operación para lo cual deberá informar al usuario y al participante originador. También podrá de manera preventiva suspender la Llave siguiendo el proceso descrito.

Contenido

Contingencia operativa: experiencia internacional

Banco Central de Australia NPP – FSS

1. FSS puede ser operado desde dos ubicaciones alternas y remotas en caso de reportarse una falla operativa.

2. En caso de falla grave del FSS, NPP cuenta con un plan de contingencia en el cual mantiene los procesos de compensación de pagos inmediatos hasta un máximo de 12 horas y encola las solicitudes de liquidación hasta que FSS esté disponible nuevamente.

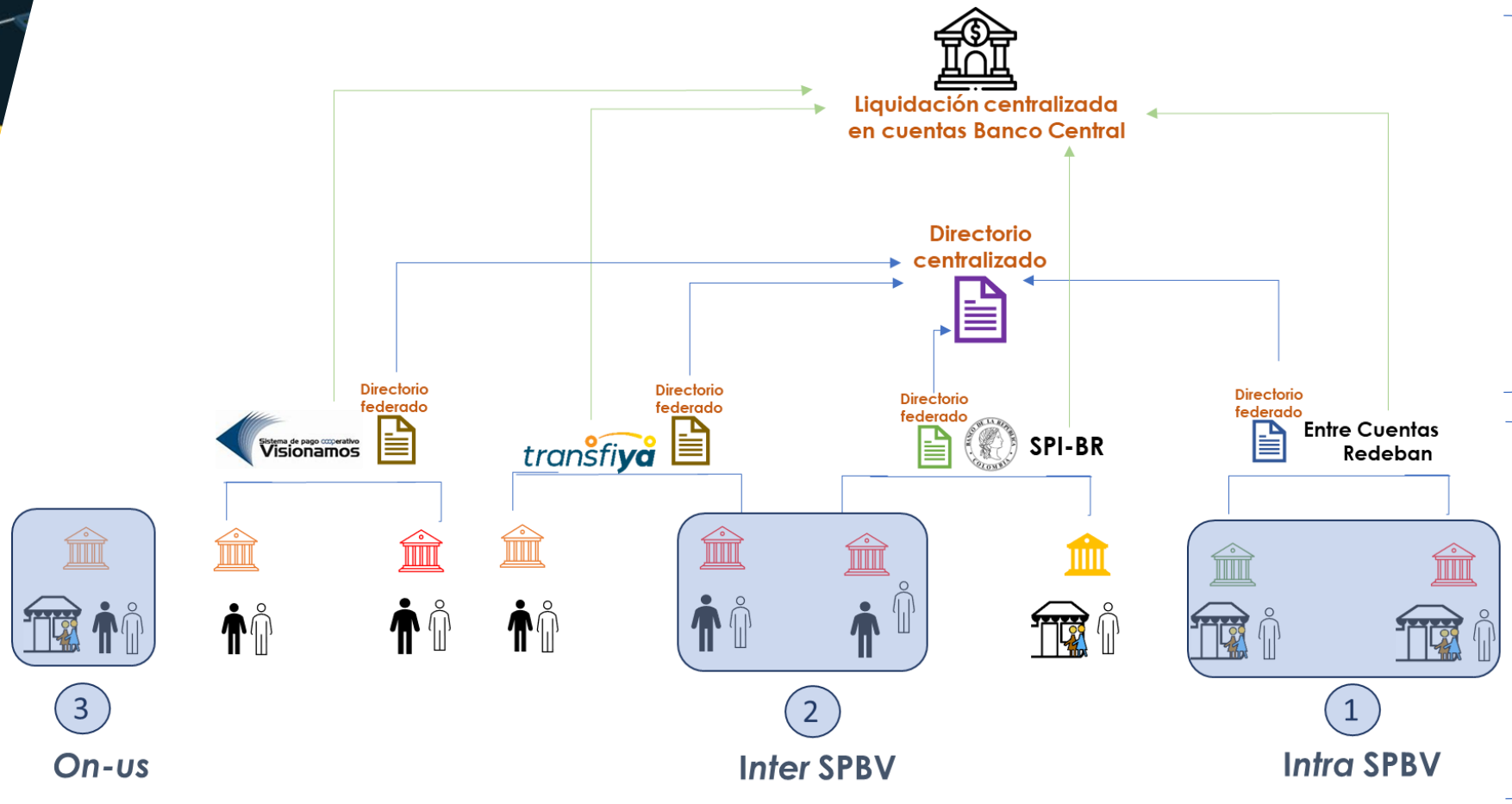
Reserva Federal de Estados Unidos – FEDNOW

1. Los mensajes de pago pueden ser retrasados/encolados hasta que la falla sea resuelta.

2. Los participantes deben disponer de políticas y procedimientos para reconciliar sus posiciones hasta el momento de la falla, bajo las instrucciones dadas por la FED.

Fuente: Banco Central de Australia. Reporte del Incidente RITS and FSS del 12 October 2022. https://www.rba.gov.au/media-releases/2022/pdf/mr-22-40-final-incident-report-rits-and-fss-incident-12-october-2022.pdf

Componentes Ecosistema de Pagos Inmediatos



1

Operación Banco República Liquidación Centralizada y Directorio Centralizado

2

Operación SPBV y sus participantes, incluido el SPI-BR y sus participante, así como las entidades vigiladas que ofrezcan pagos inmediatos *on-us*

Los SPBV y sus participantes deberán contar con **elevados estándares para que permitan el desarrollo de los pagos inmediatos en condiciones de seguridad, transparencia y eficiencia** según previsto en el D. 1692 de 2020.

2

Operación SPBV y sus participantes, incluido el SPI-BR y sus participante, así como las entidades vigiladas que ofrezcan pagos inmediatos *on-us*

ARTÍCULO 2.17.2.1.5. Deberes EASPBV
(…)
6. Contar con reglas y elevados estándares operativos, técnicos y de seguridad que permitan el desarrollo de sus operaciones, y las de sus participantes, en condiciones de seguridad, transparencia y eficiencia.

7. Exigir a sus participantes contar con reglas y elevados estándares operativos, técnicos y de seguridad que permitan el desarrollo de sus operaciones y su participación dentro del sistema de pago de bajo valor en condiciones de seguridad, transparencia y eficiencia, y el mantenimiento de sistemas adecuados de administración de los riesgos inherentes a su actividad….

8. Exigir a sus participantes contar con una política de tratamiento y protección de datos personales, políticas y procedimientos relacionados con la prevención y el control del riesgo de lavado de activos y financiación del terrorismo y deberes de información a los beneficiarios respecto a sus tarifas, comisiones y procedimientos de pago.

9. Poner a disposición de las autoridades competentes la información que conozca, relacionada con posibles actuaciones o situaciones que puedan llegar a configurar conductas fraudulentas, ilegales o anticompetitivas.

ARTÍCULO 2.17.2.1.12. Reglamento. Las EASPBV deberán incorporar en su reglamento lo siguiente:
(…)
12. El modelo y los procedimientos definidos para la gestión de los riesgos del sistema de pago, incluidos los riesgos de crédito, legal, de liquidez, operativo y sistémico….

Contenido

Preguntas (1/2)

A. RESPECTO A LA PREVENCIÓN DE FRAUDES EN LOS PAGOS INMEDIATOS

1. ¿Considera necesario precisar reglas o estándares adicionales a los propuestos en relación con la mitigación de fraudes en los pagos inmediatos?

2. ¿Considera que existen otras circunstancias en las cuales una transacción puede ser suspendida o rechazada por parte del participante?

3. En la experiencia internacional existen mecanismos para que los participantes compartan información relativa a los fraudes. Considera que esta práctica es necesario en Colombia? Y qué reglas, estándares y mecanismos se requerirían para ese fin?

4. Algunos sistemas en el mundo han permitido suspender operaciones posterior a su aceptación. Allí el participante congela los fondos en la cuenta receptora y valida veracidad de la operación. Considera que esta práctica es necesaria en Colombia? Y qué reglas, estándares y mecanismos se requerirían para ese fin?

5. Una práctica internacional ha sido la de fijar límites máximos como mecanismo de seguridad aplicable a todos el esquema de pagos inmediatos, ¿encuentra necesario definir a nivel del ecosistema un valor máximo para un pago o transferencia inmediata?

6. Ante la materialización de un fraude, ¿considera que es necesario definir reglas o estándares adicionales a los previstos en la normatividad aplicable? Por ejemplo, procesos para facilitar disputas y reclamos entre participantes, o políticas para resarcir perdidas de los usuarios, entre otras.

Preguntas (2/2)

B. RESPECTO A LA CONTINUIDAD DE LA OPERACIÓN

1. Siguiendo la experiencia internacional, en caso de una falla técnica que afecte la prestación del servicio en el ecosistema de pagos inmediatos:

   a) ¿Cuanto sería el tiempo máximo de la suspensión de la operación?

   b) ¿Encuentra necesario que se definan reglas y estándares uniformes en el ecosistema para el manejo de los incidentes. Por ejemplo, proceso de encolamiento de los pagos, reconciliación de los pagos en el restablecimiento del servicio.

2. La experiencia australiana plantea la posibilidad de un plan de contingencia para la liquidación en caso de fallas en la disponibilidad del sistema. Considera que esta práctica es necesaria en Colombia? Y qué reglas, estándares y mecanismos se requerirían para ese fin, tanto para las operaciones intra-SPBV como las inter-SPBV? Ejemplo: prefondeos o mecanismos de gestión de riesgo de crédito.

3. En otras industrias, ejemplo valores, se han definido protocolos para el manejo de desastres y crisis sistémicas. Considera que esta práctica es necesaria para el ecosistema de pagos inmediatos? Y qué reglas, estándares y mecanismos se requerirían para ese fin?

Favor remitir sus respuestas **antes del 31 de Mayo** al correo pagosinmediatos@banrep.gov.co.

Contenido

1. Introducción
2. Seguridad en el ecosistema de pagos inmediatos
3. Prevención de fraude en los pagos inmediatos
4. Continuidad de la operación
5. Preguntas
6. **Consideraciones del Supervisor en materia de seguridad: Presentación a cargo de la Superintendencia Financiera de Colombia**

FORO

Sistemas de Pago de Colombia

Seguridad

Reglas y Estándares

23 de mayo de 2023