



# Guía para la supervisión de emisores de dinero electrónico

Denise Dias y Stefan Staschen

Guía técnica

# Guía para la supervisión de emisores de dinero electrónico

Guía técnica

Diciembre de 2018

Denise Dias y Stefan Staschen



Grupo Consultivo de Ayuda a los Pobres  
1818 H Street NW, MSN IS7-700  
Washington DC 20433  
Sitio web: [www.cgap.org](http://www.cgap.org)  
Correo electrónico: [cgap@worldbank.org](mailto:cgap@worldbank.org)  
Tel.: +1 (202) 473 9594

#### **Derechos y autorizaciones**

Esta publicación está disponible bajo la Licencia Creative Commons de Reconocimiento 4.0 Internacional (<https://creativecommons.org/licenses/by/4.0/deed.es>). Bajo la licencia Creative Commons de Reconocimiento, queda permitido copiar, distribuir, transmitir y adaptar esta obra para fines comerciales en las siguientes condiciones:

Cita de la fuente: La obra debe citarse de la siguiente manera: Dias, Denise y Stefan Staschen (2018), *Guía para la supervisión de emisores de dinero electrónico: Guía técnica*, Washington, DC, CGAP.

Traducciones: En caso de traducirse la presente obra, la cita de la fuente deberá ir acompañada de la siguiente nota de exención de responsabilidad: “La presente traducción no es obra del CGAP y no deberá considerarse traducción oficial de dicho grupo. El no responderá por el contenido ni los errores de la traducción”.

Adaptaciones: En caso de que se haga una adaptación de la presente obra, la cita de la fuente deberá ir acompañada de la siguiente nota de exención de responsabilidad: “La presente obra es una adaptación de una publicación original del CGAP y el Banco Mundial. Las opiniones y los puntos de vista expresados en ella son exclusiva responsabilidad de su autor o sus autores y no han sido avalados por el CGAP ni el Banco Mundial”.

Cualquier consulta sobre derechos y licencias deberá enviarse a la siguiente dirección: CGAP Publications, 1818 H Street, NW, MSN P3-300, Washington, DC 20433, EE. UU.; correo electrónico: [cgap@worldbank.org](mailto:cgap@worldbank.org).

<b>1</b>	<b>Presentación</b>	<b>1</b>
<b>2</b>	<b>Un enfoque proporcional para la supervisión de emisores de EDE</b>	<b>4</b>
2.1	Proporcionalidad en la supervisión de EDE	4
2.2	Bancos y EDE: Diferentes ámbitos de actividad y diferentes perfiles de riesgo	4
2.3	¿Los EDE plantean riesgos sistémicos?	6
2.4	Aumentar la eficiencia de las visitas <i>in situ</i> mediante una mejor preparación externa	9
2.5	Implementar la supervisión de los EDE basada en los riesgos	10
2.6	Disposiciones organizacionales para la supervisión de EDE	11
<b>3</b>	<b>Concesión de licencias a los EDE: Análisis del plan de desarrollo</b>	<b>14</b>
<b>4</b>	<b>Seguimiento externo (vigilancia) de EDE</b>	<b>17</b>
<b>5</b>	<b>Exámenes de los EDE (procedimientos externos e internos)</b>	<b>21</b>
5.1	Presentación	21
5.2	Salvaguardia de los fondos	22
5.2.1	Requisitos reglamentarios clave	22
5.2.2	Alcance de los exámenes	24
5.2.3	Procedimientos de los exámenes	24
5.3	Riesgo operacional	31
5.3.1	Requisitos reglamentarios clave	31
5.3.2	Alcance de los exámenes	31
5.3.3	Procedimientos de los exámenes	32
5.4	Lucha contra el lavado de activos y el financiamiento del terrorismo	40
5.4.1	Requisitos reglamentarios clave	40
5.4.2	Alcance de los exámenes	41
5.4.3	Procedimientos de los exámenes	41
<b>6</b>	<b>Conclusiones</b>	<b>46</b>

<b>Anexo 1. Instituciones entrevistadas</b>	<b>48</b>
<b>Anexo 2. Referencias bibliográficas</b>	<b>49</b>
<b>Anexo 3. Material de referencia para supervisores</b>	<b>53</b>
Cuadro 1. Riesgos que presentan los EDE	7
Cuadro 2. Estructura posible para el plan de desarrollo de un EDE	15
Cuadro 3. Ejemplos de objetivos que se persiguen con el seguimiento externo y los datos relacionados	18
Cuadro 4. Ejemplos de indicadores comerciales y financieros para la supervisión de EDE	20
Recuadro 1. Enfoques para la supervisión de EDE	5
Recuadro 2. Supervisión basada en los riesgos	11
Recuadro 3. Revisión de las políticas y los manuales de procedimiento: Una técnica clave para el examen	22
Recuadro 4. Ejemplos de medidas de seguridad de los datos que pueden adoptar los EDE	38

## 1. *Presentación*

---

Una ventanilla especializada en reglamentación para emisores de dinero electrónico (EDE) no bancarios es uno de los cuatro mecanismos básicos que permite reglamentar servicios financieros digitales inclusivos en los mercados emergentes y las economías en desarrollo (Staschen y Meagher, 2018). A los efectos de esta guía, por “emisor de dinero electrónico” se entiende toda entidad regulada, ya sea bancaria o no bancaria, que se dedica a emitir dinero electrónico o cuentas similares para depósito de valores, aun cuando comercie bajo otra denominación, como un banco de objeto limitado o banco de pago<sup>1</sup>.

Una ventanilla especial de reglamentación para los EDE puede resultar eficaz solo cuando se combina con los cambios de supervisión necesarios. La tarea de supervisión tiene tres finalidades: i) garantizar que los riesgos sean identificados, gestionados de manera adecuada y mitigados por los EDE; ii) imponer el cumplimiento de los requisitos reglamentarios, y iii) crear procedimientos para gestionar crisis de EDE. La supervisión eficaz ayuda a los supervisores a identificar y gestionar los riesgos antes de que estos alcancen una magnitud considerable y brinda aportes basados en evidencias para los cambios reglamentarios. La pregunta es: ¿cómo se supervisa eficazmente a los EDE?

La proporcionalidad en la supervisión puede optimizar el uso eficiente de recursos limitados y evitar que la innovación y el crecimiento de los EDE se vean sofocados. No existe una receta única para elaborar un enfoque proporcional aplicable a los EDE, y lo que resulta proporcional en un país puede no serlo en otro. Para definir un enfoque es necesario comprender el perfil de riesgo inherente de los EDE, en consonancia con lo que la normativa vigente les permite hacer. Al igual que los bancos, los EDE recaudan

---

<sup>1</sup> Por consiguiente, un EDE puede ser una entidad no bancaria (que no intermedia depósitos recaudados del público) o una entidad bancaria especializada en la emisión de dinero electrónico sin autorización para emitir préstamos, como los bancos de pago en India, los bancos de nicho en México y los bancos de servicios de pago en Nigeria. No incluye modelos donde los depósitos de clientes se encuentran en cuentas de depósito tradicionales, aun cuando a dichas cuentas se acceda a través de agentes o canales digitales como los teléfonos móviles (por ejemplo, la banca electrónica en Pakistán). Salvo indicación en contrario, el término “banco” en esta publicación hace referencia a las entidades bancarias tradicionales que están autorizadas para intermediar y apalancar depósitos de clientes.

fondos de clientes y prometen reembolsar dichos fondos, pero no extienden facilidades de crédito ni participan en operaciones de riesgo. En efecto, por lo general están obligados a respaldar todo el dinero electrónico emitido (el dinero adeudado a los clientes) con fondos líquidos. Debido a esta diferencia fundamental, tienen un perfil de riesgo más bajo y, por lo tanto, requieren menos atención supervisora que los bancos.

En un enfoque proporcional también se considera si un EDE reviste importancia sistémica debido a su tamaño, actividad interjurisdiccional u otros aspectos<sup>2</sup>. En consecuencia, el grado de atención recibida en materia de supervisión variará de un EDE a otro. Por ejemplo, un enfoque superficial centrado en el seguimiento externo y el cumplimiento de las normas de salvaguardia de los fondos podría ser suficiente para algunos EDE, en particular para los de menor tamaño que operan en un determinado país. Para otros (de mayor tamaño, de importancia sistémica o problemáticos) del mismo país, un enfoque proporcional podría consistir en inspecciones que den cobertura a todos los temas abordados en esta y otras publicaciones. Asimismo, el enfoque de cada país depende de una variedad de factores específicos al contexto, como las prioridades de supervisión simultáneas, los conocimientos especializados disponibles y la tecnología de supervisión<sup>3</sup>, así como etapa de implementación de la supervisión basada en los riesgos.

El presente documento tiene como objetivo i) proporcionar orientación general a los supervisores de mercados emergentes y economías en desarrollo que diseñan enfoques proporcionales para la supervisión de los EDE, y ii) servir como referencia para preparar o mejorar manuales de supervisión de EDE en algunas áreas específicas. Luego de presentar brevemente el concepto de proporcionalidad y explicar cómo se aplica a la supervisión de los EDE, se describen los procedimientos de supervisión que se adoptarán durante la concesión de licencias, el seguimiento externo (vigilancia) y los exámenes de los EDE. Se toman como base las propias experiencias de los autores, entrevistas con una muestra de supervisores<sup>4</sup> y la literatura disponible, incluidas las normas internacionales y orientaciones en materia de supervisión abiertas al público.

---

<sup>2</sup> De acuerdo con BCBS (2016a, p. 2): “[E]n algunos países, las instituciones financieras no bancarias, aunque no sean sistémicas por el importe de los fondos que intermedian, pueden presentar una dimensión sistémica en virtud del número y del tipo de clientes a los que atienden”.

<sup>3</sup> La tecnología de supervisión consiste en el uso de tecnologías innovadoras por parte de las entidades de supervisión como apoyo para su labor. Véase Broeders y Prenio (2018) y Dias (2018).

<sup>4</sup> En 2017 se realizaron entrevistas presenciales, telefónicas o por escrito con autoridades de supervisión financiera responsables de la actuación de los emisores de dinero electrónico de Austria, Colombia, Filipinas, Francia, Ghana, Hong Kong, India, Luxemburgo, Malasia, México, Myanmar, Nigeria, Perú, Singapur, Tanzania, Uganda y Reino Unido.

Asimismo, se pone el foco en la protección de los fondos de los clientes y se abordan los riesgos operacionales, los riesgos de lavado de activos y financiamiento del terrorismo, y los planes de operaciones de los EDE y el seguimiento externo. Desde luego, existen otras áreas pertinentes para la supervisión de los EDE, pero dichas áreas exceden el alcance del presente documento. Por ejemplo, no se abordan las medidas correctivas o de cumplimiento, la resolución de los EDE, los análisis de solvencia y probidad, los aspectos transfronterizos de la supervisión de los EDE, o el rol de la interoperabilidad, la computación en la nube, y las interfaces para programas de aplicación en la supervisión de los EDE. Tampoco se aborda cada una de las áreas importantes de riesgo, en parte debido a que algunas de ellas están tratadas en otros documentos. (Para consultar las definiciones de los riesgos más importantes asociados a los EDE, algunos de los cuales se analizan en este documento, véase el cuadro 1)<sup>5</sup>.

Mientras que algunos supervisores opinan que la combinación de todos los procedimientos descritos en el presente documento resulta excesiva o compleja, otros la consideran insuficiente y poco profunda. El objetivo no consiste en proponer una lista definitiva de temas y procedimientos, sino más bien en ilustrar de qué manera se podrían llevar adelante los análisis en las áreas abarcadas. En consonancia con el enfoque de supervisión general, los supervisores pueden incorporar de forma total o parcial los procedimientos que figuran en sus manuales de supervisión y aplicarlos en exámenes integrales o específicos, el seguimiento externo u otras revisiones temáticas.

Por último, los procedimientos están descritos en una “versión” manual exhaustiva, que es lo único que se puede lograr en varios mercados emergentes y economías en desarrollo donde la tecnología de supervisión es aún incipiente. En este documento se destacan algunos ejemplos donde este tipo de tecnología podría aliviar la carga de trabajo del supervisor. El grado en que esta se aproveche afectará la eficacia y proporcionalidad de la supervisión de los EDE.

La presente publicación está destinada principalmente a supervisores de EDE de mercados emergentes y economías en desarrollo. Asimismo, puede resultar de interés para organismos reguladores, responsables de la formulación de políticas y organizaciones internacionales que promueven la supervisión eficaz de los EDE para fomentar una inclusión financiera saludable en los mercados emergentes y las economías en desarrollo.

---

<sup>5</sup> Los temas referidos a la protección del cliente, la recopilación de datos para la supervisión de los EDE y las implicaciones de la operación de los EDE a través de agentes se encuentran tratados en Dias (2013); Dias y Staschen (2017), y Dias, Noor, y Staschen (2015), respectivamente.



## 2. *Un enfoque proporcional para la supervisión de EDE*

### 2.1 Proporcionalidad en la supervisión de EDE

En un enfoque proporcional de supervisión, las expectativas del supervisor deben adecuarse al perfil de riesgo de los EDE (los riesgos inherentes a sus actividades) y a la importancia sistémica de estos. Dichas expectativas determinan la intensidad de la supervisión que habrá de aplicarse y el consecuente empleo de los recursos de supervisión. En general, los EDE requieren un menor grado de escrutinio en comparación con la banca tradicional. Todos ellos exigen diferentes grados de intensidad: los EDE de mayor tamaño, de importancia sistémica o problemáticos pueden requerir la supervisión de todos los temas incluidos en este u otros documentos, mientras que un enfoque más superficial (por ejemplo, limitado a un seguimiento externo o a una evaluación de la salvaguardia de los fondos) puede resultar apropiado para pequeños EDE que no supongan problemas especiales.

No existe una única receta para elaborar un enfoque proporcional de supervisión aplicable a los EDE. Lo que un supervisor considera proporcional puede resultar desproporcionado para otro. Los supervisores tienen distintas opiniones sobre el uso de las herramientas de supervisión (seguimiento del mercado, exámenes externos e internos, y revisiones temáticas), el alcance de la supervisión (los temas abarcados) y la profundidad de la supervisión (el grado de detalle de los exámenes, las técnicas empleadas—procedimientos analíticos y de auditoría—y su frecuencia).

### 2.2 Bancos y EDE: Diferentes ámbitos de actividad y diferentes perfiles de riesgo

En otros tiempos, los bancos recaudaban dinero en efectivo y otros activos (oro, por ejemplo) de los clientes para ponerlos a resguardo (*función fiduciaria*). Tras advertir que no todos los clientes (depositantes) solicitaban todos sus activos al mismo tiempo, los bancos comenzaron prestar parte de esos activos a otros clientes (*función de intermediación*). Esto dio nacimiento a la banca moderna, con sus riesgos inherentes fundamentales (crédito, discordancia de los plazos de vencimientos, liquidez y capital). Al asumir estos riesgos, los bancos desempeñan un papel crucial en la asignación de fondos en la economía. La intermediación y el apalancamiento financieros crean riesgos básicos, pero los bancos también participan en muchas otras operaciones de riesgo, incluso entre ellos y más allá de

### Recuadro 1. Enfoques para la supervisión de EDE

Todos los supervisores entrevistados para esta investigación realizan algún tipo de actividad de supervisión de EDE, incluso en jurisdicciones donde la legislación permite eximir a los pequeños EDE de la concesión de licencias y de la supervisión (por ejemplo, Francia, Luxemburgo y Reino Unido). Como mínimo, todos recopilan estadísticas periódicas con el fin de hacer el seguimiento a los mercados, y algunos (por ejemplo, Luxemburgo) incluyen exámenes de seguridad y solvencia—verifican si un EDE goza de buena salud financiera—y exámenes enfocados en cada institución. La mayoría de los supervisores entrevistados han establecido procedimientos de supervisión que incluyen algunos riesgos a nivel institucional y de mercado, los cuales varían ampliamente en alcance y profundidad, al abarcar desde un pequeño número de asuntos relacionados con el sistema, tales como la eficiencia y la competencia a través del análisis de estadísticas bianuales (por ejemplo, el Banco Central del Brasil), hasta recopilar un acervo de datos frecuentes y realizar inspecciones internas periódicas sobre riesgos clave, incluida la protección del consumidor y la salvaguardia de los fondos (por ejemplo, la mayoría de los supervisores de África al sur del Sahara), así como el uso de una metodología basada en los riesgos que aborda todo tipo de riesgos (por ejemplo, la Comisión de Vigilancia del Sector Financiero de Luxemburgo).

las fronteras nacionales, y ofrecen servicios de pago. Debido a la complejidad y los riesgos (que los pequeños depositantes no pueden estimar a un costo razonable) y su importancia para la economía, los bancos han estado fuertemente regulados durante generaciones.

Los EDE son mucho menos complejos, pues su rol no consiste en la intermediación ni el apalancamiento de los fondos de los clientes. Sin embargo, comparten con los bancos la función fiduciaria: recaudan fondos de clientes bajo la promesa de reintegrarlos en el futuro, en una fecha indeterminada<sup>6</sup>. Al igual que los bancos, necesitan gestionar los riesgos para cumplir esa promesa. La diferencia fundamental es que, mientras que los bancos gestionan una compleja variedad de riesgos interconectados y cuentan con apalancamiento (no disponen de fondos suficientes para reembolsar todos los depósitos al mismo tiempo), los EDE, por reglamentación, están obligados a disponer siempre de fondos suficientes para reembolsarlos íntegramente a todos los clientes. Los requisitos

<sup>6</sup> La función fiduciaria existe con independencia de la definición que cada país establezca para el dinero electrónico, al contrario de lo que sucede con los depósitos bancarios.

de salvaguardia de los fondos están orientados a proteger a los clientes y permitir un enfoque de supervisión más ligero. Los EDE deben mantener una reserva de fondos líquidos diferenciados equivalente a la suma de fondos recaudados de los clientes y tienen prohibido actuar como intermediarios de dichos fondos. Asimismo, las reglamentaciones a menudo restringen las transacciones y cuentas de dinero electrónico para limitar los riesgos operacionales, relacionados con los clientes y de lavado de activos<sup>7</sup>. Los EDE no presentan la mayoría de los riesgos financieros que enfrentan los bancos.

No obstante, sí enfrentan riesgos. Lo que es más importante, ofrecen servicios de pagos (retiros, transferencias y compras) a través de una variedad de canales, mediante sistemas informáticos, de telecomunicaciones, asociaciones comerciales, acuerdos de tercerización, personal y agentes distribuidos de manera muy dispersa, conexión con comercios, e infraestructuras de pago, como plataformas y otros sistemas de pago. Estos elementos crean riesgos operacionales, de lavado de activos y financiamiento del terrorismo, y asociados a los clientes, entre otros. En el cuadro 1 se enumera la mayoría de los riesgos institucionales que presentan los EDE, algunos de los cuales se incluyen en este documento.

### 2.3 ¿Los EDE plantean riesgos sistémicos?

Los bancos pueden ser objeto de un escrutinio intenso debido a su importancia sistémica. Las consideraciones básicas incluyen: i) la pertinencia del financiamiento bancario para la economía; ii) el tamaño del banco o grupo bancario; iii) el riesgo de corrida bancaria (incluido el contagio de un banco en problemas a un banco saludable), y iv) la interrelación entre bancos. Por ejemplo, un banco puede tener grandes clientes corporativos que cumplen una función crucial en la economía; si de forma repentina el banco interrumpe el financiamiento de dichos clientes, el país podría verse perjudicado. Asimismo, un banco puede tener millones de clientes que corren a retirar sus depósitos porque escucharon que la institución está en problemas. Esto podría provocar corridas en otras entidades bancarias. Finalmente, debido a que los bancos se otorgan préstamos entre sí en una red dinámica de operaciones interbancarias, cuanto más dependen de un banco en particular (por ejemplo, para liquidez diaria), mayor es la importancia sistémica de este último. Y si este quiebra, otros podrían correr la misma suerte.

*Todos los supervisores entrevistados—incluidos los de países en que los EDE han alcanzado un tamaño considerable—coinciden en que los EDE de sus países plantean un riesgo sistémico limitado o nulo.*

<sup>7</sup> Véanse Staschen y Meagher (2018) y CPMI (2016, pp. 26 y 27).

**Cuadro 1. Riesgos que presentan los EDE**

Riesgo	Descripción
Riesgo de pérdida o de uso indebido de los fondos de los clientes (tema tratado en este documento)	Este riesgo consiste en i) que empleados del EDE, agentes o terceros accedan y hagan uso indebido de los fondos de los clientes, incluidos los destinados a préstamos o inversiones; ii) que el EDE no controle los saldos de cuenta de los clientes, y iii) que los fondos de los clientes no se encuentren disponibles debido a la quiebra del EDE o del banco donde se encuentren depositados los fondos de los clientes. Si bien puede parecer que este riesgo forma parte de los demás riesgos que figuran en este cuadro, se lo enfatiza aquí debido a que constituye el eje del examen de supervisión.
Riesgos operacionales e informáticos (tema tratado parcialmente en este documento)	Gestión y controles internos: la falta de una buena gestión de los riesgos, de fiscalización por parte del directorio y de un entorno de control corporativo eficaz puede llevar a que los riesgos se materialicen.
	Riesgo relativo a los datos y la seguridad cibernética: el riesgo de que los activos físicos y digitales, como datos de clientes, equipos informáticos y redes, se vean comprometidos. Este tipo de riesgo guarda estrecha relación con el riesgo de fraude y el riesgo asociado a la confidencialidad de los datos <sup>a</sup> .
	Riesgo de liquidación: el riesgo de que la liquidación no se realice según lo esperado. Comprende el riesgo vinculado al crédito y la liquidez de las contrapartes. Los fallos operacionales en los EDE o en las contrapartes pueden ser una fuente de riesgo de liquidación.
	Riesgo de fraude: fraudes internos (por ejemplo, cometidos por empleados) y externos (por ejemplo, perpetrados por clientes y ciberdelincuentes). El número de casos de fraude informados en los EDE a nivel mundial sigue en aumento, especialmente el número de fraudes internos cometidos por personal de los EDE, en ocasiones en colusión con agentes.
	Riesgos asociados a la continuidad de las operaciones: deficiencia en la gestión, el mantenimiento o la solidez del equipamiento, las redes, las conexiones o las instalaciones físicas; incapacidad de prepararse para desastres o actuar en caso de que estos se produzcan (por ejemplo, inundación e incendio), y falta de personal esencial. Este riesgo puede ocasionar la interrupción de las operaciones.
	Riesgos relacionados con los agentes: un componente clave de los riesgos operacionales de los EDE que puede aumentar los riesgos de lavado de activos y financiamiento del terrorismo, los asociados a los clientes y de otro tipo. No todos los riesgos operacionales son atribuibles a la tecnología. Muchos obedecen al comportamiento de las personas, como el incumplimiento de las políticas debido a la ausencia de capacitación o de medidas destinadas a exigir el cumplimiento. Para los EDE existe el riesgo de la falta de efectivo (a menudo conocido como “liquidez de los agentes”) en los sitios de los agentes y el riesgo de deficiencias en el proceso de debida diligencia aplicable a los clientes.
Riesgos de terceros: además de los riesgos asociados a los agentes, los EDE enfrentan otros riesgos derivados de sus relaciones comerciales (por ejemplo, operadores de sistemas de pago, empresas de tarjetas, compañías de telecomunicaciones, proveedores de servicios en la nube y entidades vinculadas a través de interfaces para programas de aplicación).	
Riesgo de liquidez (no tratado en este documento)	El riesgo de no contar con fondos suficientes para que los EDE cumplan sus obligaciones (por ejemplo, proveedores, personal tercerizado y empleados) al vencimiento de estas. Ello difiere del riesgo relacionado con la falta de efectivo de los agentes de los EDE para atender a los clientes.
Riesgo de lavado de activos y financiamiento del terrorismo (tratado en este documento)	Riesgo de que las cuentas y transacciones de dinero electrónico puedan emplearse para financiar actividades terroristas o lavar ganancias producto del delito. Para limitar este riesgo, las transacciones de dinero electrónico y el saldo de las cuentas de dinero electrónico de los clientes en general están restringidos por alguna reglamentación.
Riesgo asociado a los clientes (no tratado en este documento)	Falta de divulgación o divulgación ineficaz de información clave, cláusulas y condiciones contractuales injustas, inadecuación de los productos, prácticas comerciales y de venta indebidas, falta de mecanismos de reparación extrajudiciales (incluidos los canales internos de gestión de reclamos). También despiertan preocupación los riesgos relacionados con la confidencialidad, el riesgo de pérdida de fondos y las demoras en la finalización de las transacciones.
Riesgo estratégico (tratado parcialmente en este documento) <sup>b</sup>	El riesgo de grandes pérdidas derivadas de malas decisiones estratégicas (por ejemplo, expansión a nuevos mercados) que podrían llevar al cese de las operaciones de los EDE.
Riesgo jurídico (no tratado en este documento)	Situaciones donde los derechos y obligaciones de las partes en un contrato (por ejemplo, la responsabilidad ante los clientes cuando la transacción fracasa) son imprecisos. Pueden incluir también la falta de protección legal de los fondos de clientes reunidos en cuentas fiduciarias y los posibles costos de las demandas legales contra el EDE por incumplimiento de la ley (por ejemplo, el derecho laboral).

Fuente: Comité de Pago e Infraestructuras del Mercado (CPMI) (2016, 2014, 2000).

<sup>a</sup>Véase CGAP (2018).

<sup>b</sup>Una parte del análisis del riesgo estratégico se realiza a través del estudio de los planes de desarrollo, tema que se aborda en la sección 3.

Si bien los EDE no otorgan financiamiento, pueden prestar a los clientes servicios de pago y de depósito de fondos. Los supervisores de los mercados emergentes y las economías en desarrollo deben determinar si un EDE presenta un riesgo sistémico y comprender que algunos pueden crecer de forma considerable a gran velocidad. Para establecer la importancia sistémica de los EDE, los supervisores pueden plantearse las siguientes preguntas:

- ¿Un EDE puede crecer de tal modo (en términos de la cantidad y tipos de clientes) que el bienestar de un gran número de personas podría verse afectado considerablemente si dicho EDE quebrara y, por lo tanto, ya no pudiera brindar un servicio crucial o muy valorado?
- ¿Podría el fracaso de un EDE deteriorar la confianza pública en el sector y, de ese modo, desencadenar un efecto de contagio?
- ¿Podría el fracaso de un EDE debilitar la confianza pública en los bancos u otras instituciones financieras reguladas?
- ¿Qué tipo de actividades (por ejemplo, servicios estatales y empresas del sector privado) dependen considerablemente de los EDE? ¿De qué manera estas actividades se verían afectadas por una interrupción en las operaciones de un EDE? ¿Se prevén pérdidas importantes?
- ¿Un EDE se ha convertido en un sistema de pago importante desde el punto de vista sistémico?<sup>8</sup>
- ¿Un EDE puede generar riesgos en el sistema nacional de pagos?<sup>9</sup>
- ¿Un EDE puede afectar a los bancos aumentando la exposición de estos a grandes depositantes (grandes saldos en las cuentas flotantes de dinero electrónico)?<sup>10</sup>
- ¿Un EDE puede afectar la rentabilidad de los bancos compitiendo por clientes, limitando el acceso a las redes de agentes, etc.?
- ¿Un EDE puede ser un vehículo para el lavado de grandes sumas de dinero ilícito?

---

<sup>8</sup> En CPMI (2001, p. 14) se proporciona una serie de directrices acerca de cómo identificar sistemas de pago importantes desde el punto de vista sistémico. La guía se centra en la estabilidad del sector financiero y no abarca la protección al cliente, la competencia y la prevención de delitos, temas que también podrían resultar importantes para los EDE.

<sup>9</sup> Solo en un pequeño número de países (por ejemplo, el Reino Unido), los EDE pueden participar en el sistema nacional de pagos, más específicamente a través de la vinculación directa con el sistema de liquidación bruta en tiempo real.

<sup>10</sup> Para obtener más información sobre los riesgos de concentración, véase Kerse y Staschen (2018).

#### 2.4 Aumentar la eficiencia de las visitas *in situ* mediante una mejor preparación externa

La proporcionalidad requiere buscar la eficiencia en el seguimiento externo y los procedimientos internos o externos durante un examen<sup>11</sup>. Por ejemplo, la distribución anticipada del trabajo externo de preparación (lo que implica hacer un seguimiento externo continuo de alta calidad y, durante los exámenes, solicitar y analizar documentos y datos antes de visitar el lugar) puede optimizar el tiempo de la labor interna. Para preparar una visita *in situ*, puede ser necesario solicitar información al EDE (por ejemplo, políticas y procedimientos y un conjunto de datos pormenorizados) para luego realizar un seguimiento con pedidos específicos (por ejemplo, una muestra de transacciones).

*Algunos supervisores de mercados emergentes y economías en desarrollo envían una única solicitud de documentación antes de la visita in situ.*

La flexibilidad en la preparación de un examen que incluye visitas *in situ* permite a los supervisores realizar varias solicitudes a los EDE y organizar las conclusiones preliminares para el seguimiento interno. Esto aumenta la eficiencia y ahorra tiempo tanto para el supervisor como para el emisor.

Asimismo, la tecnología de supervisión podría ayudar a incrementar, entre otras cosas, la eficiencia y eficacia del análisis de datos, las auditorías de sistemas y las pruebas de penetración. Las aplicaciones de aprendizaje automático, que se encuentran ampliamente disponibles, pueden identificar patrones y correlaciones que podrían indicar, por ejemplo, cambios no autorizados de registros de clientes, intentos de intrusión y transacciones sospechosas<sup>12</sup>. Sin embargo, la calidad de los productos de la tecnología de supervisión depende de la calidad de los datos empleados, de modo que los supervisores pueden necesitar, como primera medida, mejorar sus datos<sup>13</sup>.

Los datos incluyen los datos estandarizados que periódicamente informan los EDE y los no estandarizados (no estructurados), como los informes previos a la inspección, solicitudes de concesión de licencias, informes de gestión de los EDE, revisiones temáticas, acuerdos con agentes, contratos con clientes, etc. La supervisión resulta más eficaz cuando se utilizan este tipo de datos, aunque no siempre sea fácil reunirlos.

<sup>11</sup> En el presente documento, el término “examen” se utiliza para hacer referencia a una evaluación centrada en un único EDE. Un examen a menudo incluye tanto procedimientos externos como internos y su alcance puede variar sustancialmente. Distintos países emplean otros términos para referirse a las evaluaciones de instituciones puntuales.

<sup>12</sup> Para consultar más ejemplos, véanse Dias (2018) y FSI (2018).

<sup>13</sup> Para obtener más información sobre datos de supervisión de los servicios financieros digitales y sobre mecanismos de recopilación de datos, véase Dias y Staschen (2017).

*Los supervisores de los mercados emergentes y las economías en desarrollo enfrentan algunos desafíos a la hora de usar datos no estructurados o no estandarizados. Dedicar largas horas a leer documentos donde la información se presenta de forma de narración o datos numéricos no estructurados, en formatos como PDF o incluso en versiones impresas.*

Las soluciones de la tecnología de supervisión incluyen el uso de programas informáticos que permiten incorporar una variedad de formatos de datos y lograr que sean utilizables<sup>14</sup>. Por ejemplo, los programas analíticos permiten a los usuarios buscar y revisar de forma automática una gran variedad de documentos digitalizados y realizar un análisis comparativo de datos estructurados y no estructurados extraídos de diversas fuentes para generar conocimientos destinados a la labor de supervisión. La tecnología de supervisión puede facilitar considerablemente la tarea de seleccionar y analizar documentos con abundante texto, como las políticas y los manuales de procedimiento.

## 2.5 Implementar la supervisión de los EDE basada en los riesgos

Los supervisores pueden emplear una metodología basada en los riesgos para formular un enfoque proporcional aplicable a los EDE. Este tipo de metodología ofrece un panorama sistematizado de los riesgos y su importancia relativa en el seno de los EDE y entre ellos, y puede ayudar a estandarizar los procedimientos de supervisión. Asimismo, ayuda a los supervisores a aumentar o disminuir la intensidad de la supervisión de distintos EDE en el transcurso del tiempo, de manera estructurada y de acuerdo con las evaluaciones anteriores de dichos EDE. En un enfoque basado en los riesgos, los procedimientos de supervisión, como los descritos en este documento, se aplican de acuerdo con una evaluación inicial de los riesgos fundada en un análisis integral de los datos. Por lo general, perfil de riesgo de una institución regulada se resume empleando una matriz de riesgos.

No existe una única metodología basada en los riesgos ni un único modelo de matriz de riesgos que resulte eficaz para todos los supervisores de EDE. Estos suelen definir los riesgos de distinta forma y eligen distintas categorías de riesgo, factores de riesgo y ponderaciones relativas para sus matrices de riesgo. Además, crean diferentes métodos de calificación de riesgos y de evaluación de tendencias. Una matriz de riesgos que en general está diseñada para los bancos no se adecuará al perfil de riesgo de los EDE, por lo que será necesario adaptarla.

<sup>14</sup> Para obtener más información sobre datos electrónicos de supervisión (datos en un formato idóneo para programas analíticos), véase Bauguess (2018).

## Recuadro 2. Supervisión basada en los riesgos

En un enfoque basado en los riesgos, la tarea de supervisión se centra en los principales riesgos de los mercados regulados<sup>a</sup>. Este enfoque ofrece una orientación formal sobre cuáles son las prioridades, cómo se llevará a cabo la supervisión y cómo se adoptarán las decisiones del caso.

Las metodologías basadas en los riesgos a menudo se resumen en matrices de riesgo, en la que se presentan todos los riesgos inherentes a un modelo de negocios—según las actividades permitidas por reglamentación para el tipo de institución de que se trate—y los factores de riesgo para cada categoría de riesgo. Se asignan ponderaciones a los factores y categorías de riesgo según su importancia relativa para el tipo de actividad. A partir de evaluaciones de los riesgos reales de instituciones puntuales, los supervisores indican con cuánta eficacia una institución mitiga los riesgos inherentes a través de la gestión institucional, la gestión de los riesgos y los controles internos. Por último, se genera una calificación de los riesgos que se asigna a cada institución y que permite compararlas entre sí. Esta matriz permite planificar mejor la supervisión y utilizar mejor los recursos. Cuantas más áreas de riesgo existen en un tipo de institución regulada, más útil resulta la matriz para identificar las prioridades de supervisión y resumir los resultados de los exámenes.

<sup>a</sup> Para obtener una orientación más exhaustiva sobre la supervisión basada en los riesgos, véase Wright (2018).

*Si bien todos los supervisores entrevistados informan que utilizan un enfoque basado en los riesgos para supervisar bancos, solo algunos de ellos han adaptado su metodología a los EDE.*

## 2.6 Disposiciones organizacionales para la supervisión de EDE

Pese a que no existe un único enfoque acerca de dónde debe ubicarse la supervisión de los EDE, el dinero electrónico de un servicio financiero y, como tal, debería ser responsabilidad de las autoridades del sector financiero (por ejemplo, el banco central), y no de las autoridades de telecomunicaciones, aun cuando los EDE sean propiedad de operadores de redes de telefonía móvil<sup>15</sup>. Dentro de una autoridad del sector financiero, las disposiciones internas para la supervisión de los EDE pueden variar.

<sup>15</sup> Al menos en un país, Kenya, el Banco Central puede autorizar a los operadores de redes móviles a convertirse en EDE, en cuyo caso la línea de negocios correspondiente al dinero electrónico del operador queda regulada por el Banco Central y sujeta a supervisión. Sin embargo, en la mayoría de los países, el EDE debe constituirse como una entidad jurídica independiente dedicada a la emisión de dinero electrónico.



*Las autoridades del sector financiero de todos los países estudiados asignan la responsabilidad de la supervisión de los EDE a una autoridad de supervisión financiera—generalmente el banco central—y no en las autoridades del sector financiero, como el ministerio de Finanzas. En unos pocos países, una autoridad de supervisión independiente (por ejemplo, una superintendencia bancaria) asume esta responsabilidad. En la mayoría de esos casos, el banco central sigue teniendo a su cargo la regulación de los pagos y la fiscalización del sistema de pagos (con la atención puesta en la infraestructura, la seguridad y la eficiencia).*

*En 2015 se creó en el Reino Unido una entidad reguladora independiente, el Regulador de Servicios de Pago, que regula a los proveedores de servicios de pago y a los proveedores de sistemas de pago, mientras que la Autoridad de Conducta Financiera supervisa a los proveedores de servicios de pago, incluidos los EDE. La fiscalización del sistema nacional de pagos a los efectos de la estabilidad y la operación de los sistemas de pago clave recaen en el Banco de Inglaterra.*

*Internamente, las autoridades de supervisión también aplican diferentes enfoques. En la mayoría de los países africanos estudiados (por ejemplo, Ghana, Kenya, Rwanda y Tanzania), el departamento de pagos del banco central—enfocado principalmente en la fiscalización del sistema de pagos—se ha convertido en el supervisor de los EDE. En la mayoría de los casos, la fiscalización y la supervisión están desvinculadas de las operaciones del banco central (por ejemplo, los sistemas de liquidación bruta en tiempo real, la compensación de cheques y las operaciones de mercado). En Hong Kong y Singapur, donde el banco central es también el supervisor de los EDE, la supervisión de los EDE recae sobre el departamento de supervisión de dicha entidad. En países con una entidad de supervisión financiera independiente del banco central (por ejemplo, Austria, Francia, Luxemburgo, México y Reino Unido), esta a menudo incluye un equipo especializado en proveedores de servicios de pago.*

*La experiencia entre los supervisores entrevistados indica que resulta positivo crear un equipo especializado para los riesgos operacionales e informáticos que se aboque a todo tipo de entidades reguladas, incluidos los EDE. Ejemplos de esto pueden encontrarse en Austria, Brasil, Filipinas, Francia, Hong Kong, Luxemburgo, Malasia, México, Perú y Singapur. Algunos de estos países también cuentan con equipos especializados en lavado de activos y financiamiento del terrorismo y en conducta del mercado, y otros, con equipos especializados en ciberseguridad (por ejemplo, la Autoridad de Conducta Financiera del Reino Unido).*

Todos los mecanismos organizacionales exigen algún grado de coordinación. La coordinación interinstitucional resulta útil tanto para la reglamentación (por ejemplo, la reglamentación de los operadores de redes de telefonía móvil sobre el acceso a canales como el servicio suplementario de datos no estructurados) como para la supervisión (por ejemplo, el seguimiento realizado por las autoridades de protección de los datos,

la evaluación de los efectos de las actividades de dinero electrónico en la actividad de los operadores de redes de telefonía móvil y viceversa, el seguimiento de los seguros para redes móviles por parte del supervisor de seguros, etc.). Es necesario que exista coordinación interdepartamental, por ejemplo, entre la fiscalización de los pagos y la supervisión de los EDE, entre la supervisión de los EDE y la supervisión bancaria (por ejemplo, para aprender de la experiencia con los exámenes bancarios, controlar el cumplimiento de los límites impuestos a un banco para el dinero electrónico en circulación, y coordinar en caso de resolución de los EDE), y entre la supervisión de los EDE y los equipos especializados (por ejemplo, riesgos operacionales).

### 3. Concesión de licencias a los EDE: Análisis del plan de desarrollo

---

En muchos países se exige a los EDE una licencia para operar<sup>16</sup>. Las autoridades de supervisión realizan una serie de análisis de las solicitudes de licencias para garantizar que los EDE, sus titulares y su órgano directivo reúnan los criterios mínimos, como los requisitos de capital y de solvencia y probidad. Algunos supervisores también realizan una inspección de los EDE antes de que estos comiencen a operar y una verificación de antecedentes de los accionistas principales, miembros del directorio, la gerencia general y otros cargos clave.

En esta sección no se incluyen todos los temas abordados durante la concesión de licencias, sino que se proporciona una orientación básica para el análisis de los planes de desarrollo de los EDE.

*Todos los supervisores entrevistados solicitan un plan de desarrollo (y de proyecciones financieras) a los EDE cuando estos se encuentran sujetos a la concesión de licencias, mientras que algunos (por ejemplo, la Comisión de Vigilancia del Sector Financiero de Luxemburgo y el Banco de Indonesia) también exigen actualizaciones periódicas del plan de desarrollo una vez concedida la licencia.*

Los planes de desarrollo pueden analizarse desde dos perspectivas: su calidad como herramienta de planificación y la solidez del plan propiamente dicho.

Un plan de desarrollo de baja calidad podría ser señal de escasas aptitudes de planificación o renuencia a compartir información con el supervisor. Un plan deficiente en términos de contenido podría indicar riesgos estratégicos producto de una escasa perspicacia empresarial. Estas perspectivas se aplican a los planes de desarrollo de los EDE tanto nuevos como establecidos. Los EDE pueden actualizar su plan de desarrollo periódicamente para adaptar las estrategias y proyecciones a los cambios en las condiciones de mercado y el desempeño anterior.

Al evaluar la calidad de un plan de desarrollo, los supervisores deben contemplar los siguientes aspectos:

- El plan debe ser completo e integral.
- La suma de las partes de un plan debe ser convincente y mostrar pocas incongruencias.

---

<sup>16</sup> La expresión “concesión de licencias” se emplea de forma amplia para aludir al proceso de autorización obligatoria al que están sujetos los EDE antes de que se les permita comenzar a operar o continuar operando tras la adopción de una nueva reglamentación que rige su actividad. En algunos países se suelen utilizar otros términos como “inscripción” y “permiso”.

Si bien no existe un enfoque estándar para organizar y clasificar las secciones de un plan de desarrollo, en un plan completo (de cualquier tipo de organización) por lo general se describen la estrategia general, las operaciones y las proyecciones financieras. En el cuadro 2 se incluye, a título ilustrativo, la estructura del plan de desarrollo de un emisor de dinero electrónico.

En un plan de desarrollo deficiente, suele suceder que no se aborden componentes importantes o que estos no se formulen de manera adecuada. Sin embargo, aun cuando dichos componentes consten en el plan y estén plenamente desarrollados, pueden existir incongruencias. Por ejemplo, un EDE puede proyectar un crecimiento poco realista del número de clientes y transacciones sin una estrategia de apoyo para enfrentar la competencia, un plan sólido para aumentar la red de agentes ni recursos suficientes para cubrir los gastos de comercialización. Otras posibles incongruencias incluyen el desajuste entre los ingresos previstos y un segmento de mercado pequeño (por ejemplo, solo agricultores de zonas rurales), gastos de capital elevados (por ejemplo, mobiliario, infraestructura informática y programas informáticos para la gestión de riesgos) con respecto a un presupuesto bajo, y discrepancias entre la sección descriptiva del plan y las proyecciones financieras.

**Cuadro 2. Estructura posible para el plan de desarrollo de un EDE**

Riesgo	Descripción
Plan estratégico	<ul style="list-style-type: none"> <li>i. Misión, visión, objetivo</li> <li>ii. Análisis de mercado               <ul style="list-style-type: none"> <li>a. Panorama del mercado, tamaño total y potencial de crecimiento</li> <li>b. Tendencias de mercado, entorno competitivo</li> <li>c. Segmentos de mercado y segmentos objetivo</li> <li>d. Posicionamiento (qué necesidades de los segmentos objetivo se atenderán)</li> <li>e. Productos y servicios para ofrecer</li> <li>f. Cuota de mercado prevista</li> <li>g. Factores de éxito (por ejemplo, red de agentes, diseño de productos, compromiso de los accionistas, reglamentación, asociaciones, tecnología, infraestructura)</li> </ul> </li> <li>iii. Análisis de las fortalezas, debilidades, oportunidades y amenazas</li> <li>iv. Resumen de la estrategia de desarrollo</li> </ul>
Plan de operaciones	<ul style="list-style-type: none"> <li>i. Productos y servicios</li> <li>ii. Modelo de negocios y asociaciones</li> <li>iii. Estrategia de crecimiento e inversión</li> <li>iv. Estrategia de comercialización</li> <li>v. Gestión de gobierno, estructura organizacional y dotación de personal</li> <li>vi. Sistemas, controles y gestión de riesgos</li> <li>vii. Hoja de ruta para la implementación (cronograma)</li> </ul>
Plan financiero (también denominado proyecciones financieras o plan de viabilidad)	<ul style="list-style-type: none"> <li>i. Supuestos básicos (por ejemplo, índice de inflación, costo de los fondos y crecimiento del producto interno bruto [PIB])</li> <li>ii. Capital inicial, inversión y plan de inyección de capital, fuente de fondos</li> <li>iii. Ingresos previstos, gastos de capital, gastos operativos, ganancias y pérdidas</li> <li>iv. Principales indicadores de desempeño financiero</li> <li>v. Estados financieros previstos</li> </ul>

Para determinar si los supuestos en que se basan las proyecciones financieras son razonables, los supervisores deben poseer conocimientos sobre la actividad de los EDE, en general, y sobre las condiciones del mercado local, en particular. Por ejemplo, el análisis del mercado de los EDE (la descripción de la competencia y su estrategia, el tamaño del mercado, el acceso a infraestructura, como servicios de plataformas operativas y trabajo especializado) puede ser inexacto, mientras que otros supuestos (crecimiento del PIB, costo de financiamiento, indicadores socioeconómicos y demográficos, tamaño del segmento de mercado objetivo, tasa de adopción de los clientes, aumento de los ingresos, etc.) pueden ser demasiado optimistas. El objetivo consiste en estimar la razonabilidad de las proyecciones; ningún plan es infalible.

Si se dispone de conocimientos especializados en planificación y análisis financieros, se pueden examinar los cálculos de las proyecciones financieras. Para hacerlo, es necesario que las proyecciones estén en un formato digital (por ejemplo, Excel u otro) que permita analizar las fórmulas. En la siguiente sección se incluye una guía básica para analizar los principales indicadores de desempeño para la concesión de licencias.

A fin de evaluar los planes de desarrollo de los EDE (sobre todo de los proveedores de dinero móvil), los supervisores deben considerar la trayectoria típica de crecimiento de los EDE, en función de los patrones observados con el dinero móvil que utilizan extensas redes de agentes (una trayectoria de esta naturaleza puede no ser aplicable en otros modelos de negocios). A continuación se enuncian tres fases de crecimiento<sup>17</sup>:

- Puesta en marcha: alto crecimiento del gasto de capital y de los gastos operativos, y probables pérdidas.
- Alto crecimiento: aumento de los gastos operativos, aumento de los ingresos, utilidades moderadas, e inversión en captación de clientes a través de la fuerza de ventas y la comercialización.
- Madurez: posibles fuentes de ingresos adicionales a través de la diversidad de productos y las asociaciones; utilidades sólidas.

---

<sup>17</sup> Almazán y Vonthron (2014) señalan que los mayores gastos operativos que deben afrontar los EDE en los primeros años de actividad son la inversión en las plataformas de dinero electrónico y la creación de la red de agentes, lo que incluye gastos de comisiones y actividades comerciales. En el segundo o tercer año pueden generarse pequeños ingresos, mientras que los gastos relacionados con la adquisición de agentes y las comisiones siguen siendo elevados en relación con los ingresos.

#### 4. Seguimiento externo (vigilancia) de EDE

El seguimiento externo continuo—o vigilancia—es fundamental para la supervisión de los EDE basada en los riesgos. El seguimiento continuo ayuda a los supervisores a determinar (y comparar en el tiempo) las variaciones en los perfiles de riesgo de los distintos EDE. También los ayuda a detectar indicios de riesgos con los que se podrían anticipar medidas de supervisión, incluidas las de carácter correctivo (por ejemplo, una inspección de la salvaguardia de los fondos, y de los riesgos estratégicos y de fraude). El seguimiento implica analizar el mercado de los EDE (por ejemplo, desarrollo del mercado) y de cada EDE en particular, por lo que forma parte integral del plan de supervisión, los exámenes de los EDE y el proceso de reglamentación.

*Solo algunos de los supervisores entrevistados de los mercados emergentes y las economías en desarrollo realizan un seguimiento integral del mercado (vigilancia o fiscalización) de manera continua, mientras que dicha práctica es común entre los supervisores de las economías desarrolladas.*

El seguimiento externo puede involucrar el análisis interno de datos estandarizados y datos no estructurados de la autoridad de supervisión (por ejemplo, informes presentados por los EDE) y datos externos (por ejemplo, estadísticas de los Gobiernos y datos de los operadores de redes de telefonía móvil). Se suelen utilizar datos financieros (por ejemplo, indicadores clave) y datos no financieros (por ejemplo, reclamaciones de clientes y volumen de transacciones)<sup>18</sup>. En general, para los análisis se sigue una metodología estandarizada y criterios uniformes definidos por la autoridad de supervisión de acuerdo con sus objetivos (en el cuadro 3 se incluyen algunos ejemplos). En función de los objetivos, la profundidad y la frecuencia de los análisis dependerán de los datos, la tecnología, las aptitudes del supervisor y las prioridades establecidas en la metodología basada en los riesgos.

Si bien la evaluación del desempeño financiero de todos los EDE puede no ser la preocupación principal de los supervisores, el seguimiento eficaz de los indicadores financieros clave y otras mediciones comerciales de forma continua pueden ayudar a establecer las prioridades de supervisión.

<sup>18</sup> Para consultar una descripción de los datos recolectados por los supervisores de emisores de dinero electrónico, véase Dias y Staschen (2017).

**Cuadro 3. Ejemplos de objetivos que se persiguen con el seguimiento externo y los datos relacionados**

Objetivos	Ejemplos de datos empleados
Medir el riesgo sistémico y la importancia relativa de los EDE	Volumen y valor de todas las transacciones de los EDE en relación con las transacciones bancarias o transacciones en el sistema de liquidación bruta en tiempo real u otros sistemas de pago, cantidad de dinero electrónico en circulación y cantidad de clientes, en relación con la totalidad de depósitos y clientes bancarios. Cantidad y tipo de grandes flujos de fondos (por ejemplo, salarios estatales y transferencias sociales), valor total de las transacciones en relación con el PIB o total de pagos bancarios en el sistema de liquidación bruta en tiempo real, interrupción de operaciones en los EDE considerados de importancia sistémica, etc.
Hacer el seguimiento del desarrollo del mercado y la inclusión financiera <sup>a</sup>	<p>Número y ubicación de los agentes; superposición de las sitios de los agentes con cobertura (torres) de operadores de redes de telefonía móvil y otros indicadores demográficos y socioeconómicos oficiales (por ejemplo, escuelas, centros de salud y población total); cantidad de agentes por persona adulta o población total por segmento de población (por ejemplo, rural-urbana); cantidad y valor de las transacciones totales de los EDE por tipo de transacción (por ejemplo, verificar si aumenta la importancia de los medios digitales en comparación con el dinero en efectivo); cantidad de transacciones entre EDE y transacciones entre EDE y bancos (transacciones interoperativas); cantidad de agentes compartidos y exclusivos, etc.</p> <p>Porcentaje de personas adultas en un radio determinado de un agente u otros puntos de acceso; penetración de las cuentas en zonas urbanas y rurales, por población adulta total y en función de otros factores como el género, la edad y el nivel de ingreso; cantidad de clientes de los EDE con cuentas bancarias, seguro o crédito, porcentaje de cuentas activas en EDE, etc.</p>
Evaluar el desempeño individual y relativo de los EDE y establecer parámetros comparativos	Indicadores de desempeño clave (véase el cuadro 4).
Verificar el cumplimiento de los requisitos reglamentarios	Coeficiente mínimo de capital en relación con el total de dinero electrónico emitido, coeficiente mínimo de liquidez, restricciones reglamentarias a los saldos de cuentas o depósitos, total de dinero electrónico emitido frente al saldo en la cuenta flotante, saldo en la cuenta flotante en relación con el total de depósitos de bancos donde se radican las cuentas flotantes, etc.
Luchar contra el lavado de activos y el financiamiento del terrorismo	Patrones del volumen y los valores de las transacciones por tipo, agente y ubicación (incluidas las ubicaciones consideradas más riesgosas, como las ciudades de frontera), estadísticas extraídas de informes sobre transacciones sospechosas, etc.
Protección del cliente y competencia	<p>Número de reclamos por tipo de reclamo y estado, comisiones por tipo de transacción; ubicación y duración de los operadores de redes de telefonía móvil e interrupciones en los EDE; número de transacciones fallidas (incompletas); duración, ubicación y frecuencia de la inactividad del sistema; volumen de los casos de fraude, tipos y ubicación; etc.</p> <p>Comisiones de intercambio por transacciones interoperativas, cuota de mercado de los EDE, ingresos por comisiones en relación con el volumen de transacciones, comisiones sobre tipos específicos de transacciones (transferencias de persona a persona, depósitos, retiros), cantidad y ubicación de los agentes exclusivos, comisiones de agentes, etc.</p>

<sup>a</sup> Para consultar las normas relativas a las estadísticas sobre pagos minoristas para medir el desarrollo del mercado, véase CPMI (2017); para consultar indicadores para el seguimiento de la inclusión financiera, véase CPMI (2016, pp. 59-62).

*Todos los supervisores entrevistados indicaron que es necesario contar, en distinto grado y con distinta frecuencia, con estados financieros (balance general, estado de resultados), indicadores prudenciales (por ejemplo, coeficientes de capital y liquidez) e indicadores de desempeño clave (por ejemplo, rendimiento del activo, rendimiento del patrimonio, gastos de capital, etc.).*

En el cuadro 4 se ofrecen algunos parámetros comerciales y financieros. El tipo y la cantidad de indicadores empleados dependerán de las preferencias y aptitudes analíticas del supervisor y de la capacidad de la tecnología de supervisión y de los datos ingresados. Muchos indicadores pueden extraerse de los estados financieros que periódicamente proporcionan los EDE, mientras que en otros casos es necesario recopilar datos adicionales (por ejemplo, total de dinero electrónico emitido; cantidad de cuentas o clientes; comisiones pagadas a los agentes; comisiones derivadas de asociaciones con terceros, como prestamistas, y comisiones por tipo de producto).

*Todos los supervisores entrevistados se reúnen con los EDE fuera de los exámenes específicos, pero solo unos pocos han incorporado esta oportunidad de recopilar información de inteligencia en su metodología formal de supervisión basada en los riesgos. Por ejemplo, algunos supervisores organizan reuniones anuales de difusión o reuniones de programación con instituciones específicas, mientras que otros se reúnen de manera ad hoc o a solicitud de los EDE.*

Los supervisores también recopilan datos de inteligencia sobre los mercados como parte del seguimiento continuo de estos. Se reúnen con EDE, asociaciones industriales y terceros que poseen conocimientos especializados<sup>19</sup>. Cuando lo hacen con EDE, pueden analizar sus expectativas sobre el cumplimiento, las preocupaciones actuales y las conclusiones generales de la supervisión.

<sup>19</sup> Véase BCBS (2016b) para consultar información sobre inteligencia de mercado.



**Cuadro 4. Ejemplos de indicadores comerciales y financieros para la supervisión de EDE**

<b>Indicadores comerciales</b>
Total de dinero electrónico emitido (dinero electrónico en circulación)
Cantidad de cuentas de dinero electrónico
Cantidad de clientes que reciben servicios de dinero electrónico
Cantidad y valor de las transacciones
<b>Indicadores financieros</b>
EBITDA: beneficios netos antes de intereses, impuestos, depreciaciones y amortizaciones
Margen de EBITDA (margen neto): EBITDA como porcentaje de los ingresos brutos
Coefficiente de gastos operativos: gastos operativos como porcentaje de los ingresos brutos
Coefficiente de gastos de capital: gasto de capital como porcentaje de los ingresos brutos
Rendimiento del capital: ingresos netos como porcentaje del capital
Rendimiento del activo: ingresos netos como porcentaje del activo
Ingresos brutos: ingresos totales derivados de la actividad comercial (por ejemplo, provisión de pagos, y operaciones de retiros y transferencias a clientes contra comisiones)
Flujos de ingresos
<ul style="list-style-type: none"> <li>• Comisiones por transacciones de clientes, por tipo de producto o servicio</li> <li>• Comisiones recaudadas de asociados (por ejemplo, aseguradoras, prestamistas)</li> <li>• Otras fuentes de ingresos (ingresos por intereses e inversiones)</li> </ul>
Ingresos por comisiones como porcentaje de los ingresos brutos
Ingresos por comisiones como porcentaje del número de transacciones
Ingresos por comisiones como porcentaje del número de clientes de dinero electrónico
Gastos operativos, por tipo de gasto (por ejemplo, comisiones de agentes)
Gastos operativos, por número de integrantes del personal
Total de comisiones de agentes y comisiones para gerentes de redes de agentes
Total de comisiones de agentes como porcentaje del número de agentes
Total de comisiones de agentes como porcentaje del número de transacciones
Gastos de capital (por ejemplo, actualización de la plataforma de dinero electrónico)
Capital: dinero reservado en forma de capital (por ejemplo, patrimonio)
Coefficiente de capital (solventia): Con independencia de si la reglamentación exige a los EDE que mantengan un nivel mínimo de capital o patrimonio en relación con los activos o el dinero electrónico en circulación, resulta de utilidad para dar seguimiento a la solventia de los EDE.
Coefficiente de liquidez: activos a corto plazo (dinero en efectivo u otro activo de alta liquidez, como bonos públicos) como porcentaje de los pasivos a corto plazo (por ejemplo, salarios, alquileres y cuentas por pagar)

## 5. Exámenes de los EDE (procedimientos externos e internos)

### 5.1 Presentación

Además de realizar el seguimiento externo de forma continua, los supervisores a menudo llevan a cabo exámenes individuales de los EDE que se centran en una, algunas o en cada una de las áreas de riesgo. El enfoque empleado dependerá del EDE y el país de que se trate. Por ejemplo, un supervisor puede examinar todos los EDE en algún momento con el único objeto de verificar cómo implementan los requisitos de salvaguardia de los fondos, mientras que los exámenes subsiguientes sobre este u otro tema (por ejemplo, protección del cliente) se originarían a partir de las conclusiones del seguimiento externo. En general, cuando la salvaguardia de los fondos es eficaz, el alcance y profundidad de la supervisión pueden ser más limitados, al menos para los EDE que no revisten importancia sistémica. En el caso de los grandes EDE, los supervisores pueden aumentar la profundidad del análisis de la salvaguardia de los fondos y ampliar el alcance de los exámenes incluyendo otras áreas de riesgo, como los controles de riesgos operacionales y del lavado de activos y el financiamiento del terrorismo.

*Pese a utilizar diferentes prácticas de supervisión, todos los supervisores entrevistados coincidieron en que el área más importante de la supervisión de los EDE es la salvaguardia de los fondos de los clientes. Otras prioridades incluían el riesgo operacional, los controles del lavado de activos y el financiamiento del terrorismo, y la protección del cliente. No todos los supervisores se abocan a estos aspectos (algunos ni siquiera controlan la salvaguardia de los fondos), mientras que otros (que no se encuentran en mercados emergentes ni en economías en desarrollo) atienden estas y muchas otras áreas, como el riesgo estratégico.*

Esta sección no ofrece una guía para los exámenes de todas las áreas de riesgo en las que los supervisores se pueden concentrar en el caso de los grandes y pequeños EDE (véase el cuadro 1). Se limita más bien a describir los procedimientos posibles para evaluar tres áreas importantes de la supervisión de los EDE: la salvaguardia de los fondos (sección 5.2), los riesgos operacionales (sección 5.3) y los controles del lavado de activos y el financiamiento del terrorismo (sección 5.4). En cada una de ellas se resumen los requisitos reglamentarios más comunes, se sugiere el alcance de un examen y, por

### **Recuadro 3. Revisión de las políticas y los manuales de procedimiento: Una técnica clave para el examen**

Se espera que las prácticas y operaciones de gestión de riesgos de los EDE se describan por escrito en las políticas y los manuales de procedimiento avalados por el directorio y sean aplicadas en toda la entidad emisora por la administración superior, con la supervisión del directorio. Los supervisores generalmente revisan este tipo de documentos para a) evaluar su exhaustividad, su razonabilidad y su alineación con las reglamentaciones y las normas internacionales, y b) orientar en parte las consultas de seguimiento del supervisor durante los exámenes externos e internos. Los supervisores pueden solicitar y analizar las políticas y los manuales de procedimiento para todas las áreas tratadas en esta sección. Un EDE que no cuenta con políticas ni manuales de procedimiento, o que no los actualiza, debe generar inquietud al supervisor.

último, se incluyen ejemplos de procedimientos externos e internos. Los procedimientos pueden adoptarse de forma total o parcial, en combinación o por separado, como parte de exámenes completos de EDE o de revisiones temáticas<sup>20</sup>.

Muchos exámenes incluyen una revisión de las políticas y los manuales de procedimiento. Para hacerla, se propone un enfoque que consta de tres etapas: i) analizar los manuales y las políticas de forma externa; ii) reunir evidencias sobre su implementación (de forma externa e interna), y iii) constatar la información mediante observaciones, entrevistas y auditorías de sistema (internas).

## **5.2 Salvaguardia de los fondos**

### **5.2.1 Requisitos reglamentarios clave**

La mayoría de las reglamentaciones sobre los EDE incluyen requisitos para la salvaguardia de los fondos que constan de dos elementos:

- **Separación.** Los EDE están obligados a separar un monto mínimo de dinero para respaldar el dinero electrónico emitido o el pasivo en dinero electrónico

<sup>20</sup> Además del seguimiento externo y los exámenes enfocados en los EDE, las revisiones temáticas pueden resultar de utilidad, sobre todo en los primeros años de la supervisión de los emisores. Las revisiones temáticas arrojan información exhaustiva sobre cuestiones específicas y, por lo tanto, resultan de ayuda cuando el supervisor compara buenas y malas prácticas y comunica sus expectativas a los EDE. Las revisiones también pueden ayudar a la autoridad regulatoria a mejorar las reglamentaciones. Estas revisiones se enfocan en un tema o en un número reducido de temas (por ejemplo, la salvaguardia de los fondos), pero incluyen a varios EDE. Pueden comprender procedimientos externos e internos como los que se describen en esta sección. Entre los supervisores entrevistados, solo algunos realizan revisiones temáticas en el sector de los EDE.

(*dinero electrónico en circulación*). Habitualmente, deben respaldar el 100 % del dinero electrónico en circulación depositando el monto equivalente en una cuenta (*cuenta flotante*) distinta de las cuentas del EDE utilizadas para ejecutar las operaciones diarias (por ejemplo, pago de facturas, pago y cobro de comisiones, etc.). Puede haber una o varias cuentas flotantes<sup>21</sup>.

- **Requisito de liquidez.** Las reglamentaciones exigen que el dinero electrónico en circulación se invierta (en caso de que dicha inversión esté autorizada) solo en activos líquidos y de bajo riesgo, como bonos públicos, o simplemente en una cuenta en un banco comercial (que pueda devengar intereses o no).
- **Requisito de diversificación.** Algunas reglamentaciones exigen que los EDE distribuyan el dinero electrónico en circulación en distintos bancos con el fin de protegerlos contra el riesgo de quiebra bancaria<sup>22</sup>.
- **Restricción.** Los mecanismos de restricción protegen el dinero electrónico en circulación contra los acreedores de los EDE (por ejemplo, prestamistas, inversionistas, proveedores, empleados y el gobierno). Esto se puede lograr exigiendo que la cuenta flotante sea de un tipo especial, por ejemplo fiduciaria o de garantía<sup>23</sup>.
  - **Dinero electrónico en circulación libre de gravámenes.** Las reglamentaciones pueden prohibir a los EDE imponer gravámenes sobre el dinero electrónico en circulación (por ejemplo, darlos en prenda como garantía de préstamos) o pueden establecer que los fondos en la cuenta flotante no forman parte del activo de los EDE<sup>24</sup>.

La salvaguardia eficaz de los fondos por parte de los EDE no depende solo de que el dinero electrónico en circulación se encuentre a salvo, sino también de si es posible identificar con claridad los reclamos de los clientes a título individual y de que la información que consta en el reclamo no haya sufrido alteraciones. Por lo tanto, la salvaguardia de los fondos se ve afectada por el modo en que se gestionan los riesgos operacionales (por ejemplo, el riesgo de fraude y de errores, la continuidad de las operaciones, la tecnología de la información, y la seguridad cibernética). Algunas cuestiones operacionales de la salvaguardia de los fondos se abordan en esta sección, mientras que otras se tratan en

---

<sup>21</sup> En esta sección se analiza el enfoque más utilizado por los EDE para salvaguardar el dinero en circulación, que consiste en depositarlo en una cuenta de un banco comercial o colocarlo en inversiones seguras. Otros enfoques, que podrían afectar los asuntos legales, operacionales y de supervisión analizados en este documento, se encuentran descritos en Mehmet y Staschen (2018).

<sup>22</sup> Desde una perspectiva de supervisión bancaria, este requisito limita el riesgo de los grandes depositantes con fondos en bancos individuales. Véase Kerse y Staschen (2018).

<sup>23</sup> Véanse Staschen y Meagher (2018), y Greenacre y Buckley (2014).

<sup>24</sup> Según la legislación aplicable a las cuentas fiduciarias o de garantía en algunos países, las garantías sobre las cuentas flotantes pueden no tener validez.

la sección 5.3. Asimismo, los supervisores deben evaluar si el uso de diversas cuentas flotantes en varios bancos no contribuye a que la salvaguardia sea menos eficaz. Por último, la salvaguardia se enfoca en garantizar liquidez para afrontar los reclamos de los clientes en los siguientes dos escenarios: i) durante el ciclo de vida del EDE (tratado en esta sección), y ii) en caso de quiebra del EDE.

### 5.2.2 *Alcance de los exámenes*

El control del saldo de las cuentas flotantes es la manera más básica de verificar si el EDE cumple con el requisito de salvaguardia de los fondos. Sin embargo, para evaluar la calidad de las políticas, los procedimientos y los sistemas que subyacen a los saldos informados por los EDE (por ejemplo, para validar la exactitud de las cifras y evaluar la gestión de riesgos y los controles internos de los EDE que afectan la salvaguardia de los fondos), los supervisores deberán aplicar procedimientos de examen adicionales. Un examen integral de la salvaguardia de los fondos podría abarcar lo siguiente<sup>25</sup>:

- existencia y suficiencia de fondos en la cuenta flotante;
- términos y situación legal de la cuenta flotante;
- procedimientos para garantizar el saldo exigido (es decir, conciliación);
- administración y gestión de cuentas flotantes;
- liquidez de las cuentas flotantes (es decir, tipos de inversión e inexistencia de gravámenes);
- control preciso del dinero electrónico en circulación y los saldos de clientes, y presentación de informes minuciosos al respecto.

### 5.2.3 *Procedimientos de los exámenes*

#### 5.2.3.1 EXISTENCIA Y SUFICIENCIA DE FONDOS EN LA CUENTA FLOTANTE

Los supervisores pueden comparar informes sobre el dinero electrónico en circulación con los informes sobre el saldo de las cuentas flotantes. Con el objeto de confirmar la veracidad de estos informes, pueden analizar los estados de cuenta bancarios de la cuenta flotante para hacer lo siguiente:

- verificar los datos de identificación de la cuenta flotante (por ejemplo, número, sucursal y titular de la cuenta) con el acuerdo o contrato de cuenta flotante y los informes periódicos enviados;

---

<sup>25</sup> Diversos supervisores de mercados emergentes y economías en desarrollo entrevistados solo controlan la disponibilidad de fondos suficientes en la cuenta flotante.

- controlar el saldo de la cuenta flotante en distintas fechas de corte y compararlo con el total de dinero electrónico en circulación informado en las mismas fechas para corroborar la concordancia<sup>26</sup>;
- si las utilidades por intereses e inversiones se pagan en la cuenta flotante y son utilizadas por el EDE (incluidas las que serán distribuidas entre los clientes), controlar si el saldo total informado excluye estos montos, debido a que puede haber un reclamo separado sobre ellos además del reclamo sobre el dinero electrónico en circulación<sup>27</sup>;
- controlar si los créditos y débitos se concentran en torno a las fechas informadas, lo que podría generar sospechas de una conciliación deficiente o de diferencias intencionadas y su encubrimiento.

En estos procedimientos se presume que el dinero electrónico en circulación informado es exacto. Los supervisores pueden corroborar la exactitud de ese dinero siguiendo los procedimientos descritos en el apartado 5.2.3.6.

#### 5.2.3.2 TÉRMINOS Y SITUACIÓN LEGAL DE LA CUENTA FLOTANTE

Por lo general, las cuentas flotantes se abren en los bancos. Cuando se exige una cuenta fiduciaria, una cuenta de garantía u otra de carácter especial, el supervisor puede revisar los aspectos formales (por ejemplo, si se ajusta a los requisitos legales para dichas cuentas) y sus cláusulas y condiciones (que pueden variar en función del banco donde se encuentre radicada la cuenta flotante). Para ello es necesario analizar el acuerdo de cuenta fiduciaria o de garantía (u otra similar) entre el EDE o el fiduciario y el banco para corroborar si se cumplen los requisitos específicos, como las leyes de fideicomiso u otra legislación pertinente del país. En el caso de los fideicomisos, algunos países exigen que se constituya un fiduciario (que, según el país del que se trate, puede ser el banco donde está radicada la cuenta fiduciaria) para administrar los fondos en nombre de los clientes de dinero electrónico. Otros, en cambio, permiten que la administración de la cuenta flotante sea ejercida por el EDE, con la consecuente variación de los acuerdos.

En el acuerdo fiduciario se puede brindar información acerca de si es posible acceder a la cuenta, cómo hacerlo y cómo retirar los fondos, entre otras cosas para invertirlos en otros activos, etc. Se pueden detallar las facultades y responsabilidades del fiduciario, en comparación con las responsabilidades del EDE, y la función del supervisor, incluidas sus

<sup>26</sup> Las diferencias podrían indicar ineficacias en los controles, diferencias intencionadas e incluso fraude.

<sup>27</sup> Si las utilidades por inversiones e intereses no se distribuyen o no se destinan a ningún otro uso, no existen motivos obvios para no contabilizarlas con miras al cumplimiento de los saldos mínimos exigidos, salvo que ello esté prohibido en la reglamentación.

prerrogativas, cuando estén permitidas por ley, para inspeccionar al fiduciario. En el caso de las cuentas de garantía, pueden existir restricciones similares sobre el uso de los fondos y la manera de acceder a ellos<sup>28</sup>.

### 5.2.3.3 PROCEDIMIENTOS DE CONCILIACIÓN EFICACES

Comprender la manera en que el EDE concilia la cuenta flotante con el dinero electrónico en circulación es fundamental para evaluar la eficacia de la salvaguardia de los fondos. El EDE debe garantizar que siempre exista saldo suficiente en la cuenta flotante y muchas reglamentaciones exigen realizar una conciliación al término de cada día hábil.

*Durante las entrevistas, los supervisores de los mercados emergentes y las economías en desarrollo mostraron tener un conocimiento limitado de cómo los EDE concilian la cuenta flotante con el dinero electrónico en circulación. Existe una gran variación en los procedimientos de conciliación entre los EDE, que van desde procedimientos mayormente manuales (por ejemplo, al término de cada jornada el personal del EDE llama al banco para aumentar o reducir el saldo en la cuenta flotante), hasta procedimientos íntegramente automatizados (por ejemplo, la cuenta flotante se ajusta automáticamente una vez [es decir, una partida] o varias veces [es decir, en tiempo real] a través de sistemas integrados entre el EDE y el banco).*

El primer paso consiste en estudiar las políticas y los procedimientos pertinentes, donde se debe describir el proceso de conciliación y se deben asignar las responsabilidades del personal. La falta de políticas o procedimientos formales puede llevar a que la salvaguardia de fondos sea insuficiente. Asimismo, resulta útil comprender de qué manera se crea el dinero electrónico (es decir, las situaciones que aumentan el dinero electrónico en circulación) y cómo se destruye (por ejemplo, las situaciones que lo reducen). La creación o la destrucción del dinero electrónico puede variar según el EDE de que se trate. Por ejemplo, en el caso de los EDE que trabajan con intermediarios que compran grandes cantidades de dinero electrónico (generalmente denominados superagentes, agentes maestros o distribuidores) para la distribución (venta) entre agentes individuales (que a su vez venden dinero electrónico a clientes minoristas), el dinero electrónico en circulación solo puede verse afectado cuando dichos intermediarios compran dinero electrónico, pero no así cuando los agentes o clientes realizan transacciones (compra y venta de dinero electrónico).

También es importante conocer si la conciliación se realiza una o varias veces al día o si las transferencias se realizan de forma inmediata cuando se crea o destruye el dinero

<sup>28</sup> Algunos supervisores entrevistados en África revisan las cláusulas relativas al pago de intereses y comisiones impuestas por los bancos, en parte debido a que estos han creado obstáculos para los EDE ofreciendo cláusulas deficientes o rechazando el servicio.

electrónico (tiempo real) o de algún otro modo. Por ejemplo, algunos EDE autorizan a ciertos intermediarios, agentes y comerciantes a pagar el dinero electrónico realizando una transferencia directa de fondos a la cuenta flotante. En otros casos, se realiza una única conciliación diaria inmediatamente antes de la hora de cierre de los bancos con el fin de reflejar la creación o destrucción neta del dinero electrónico en el transcurso de la jornada. Por último, las transferencias emitidas y recibidas por la cuenta flotante pueden automatizarse o iniciarse de forma manual. Los supervisores deben determinar si se utilizan distintos tipos de conciliación en el mismo EDE y evaluar los riesgos de esta práctica.

Desde el punto de vista de la supervisión, se espera que la conciliación automatizada eficaz (ya sea en tiempo real o por partida[s]) reduzca los errores y las demoras. Los controles de la seguridad y la integridad de los datos, cuando los hay, suelen reducir el riesgo de fraude y los accesos no autorizados a la cuenta flotante. Incluso en el caso de los procedimientos automatizados, conviene revisar de qué manera se establece el sistema i) preguntando sobre las normas codificadas en dicho sistema para activar las transferencias entre la(s) cuenta(s) bancaria(s) del EDE<sup>29</sup> y la cuenta flotante, y ii) identificando los pasos que requieren una intervención manual para evaluar sus riesgos. Asimismo, los supervisores necesitan estudiar de qué manera se realiza la conciliación cuando un fiduciario participa de la gestión de la cuenta flotante<sup>30</sup>.

Con conocimiento pormenorizado de la totalidad del proceso, los supervisores pueden evaluar el riesgo de deficiencias en la cuenta flotante en función de las fallas de control interno o alteraciones realizadas por empleados del EDE, el banco o el fiduciario. En el caso de la conciliación automatizada, los supervisores pueden analizar el sistema realizando la simulación de variaciones en el dinero electrónico en circulación, el acceso no autorizado a la información sobre dicho dinero y la alteración de dicha información, y compras o ventas de agentes y superagentes o agentes maestros. Otras técnicas posibles incluyen la observación del proceso de conciliación completo (cuando es manual) y la revisión de los registros de auditoría de las conciliaciones (cuando es automatizada). Si en la revisión descrita en el apartado 5.2.3.1 se detectan incongruencias, el supervisor puede analizar los registros de la conciliación en las fechas de las diferencias y solicitar explicaciones<sup>31</sup>.

---

<sup>29</sup> Estas son las cuentas bancarias que emplea el EDE para ejecutar sus actividades, incluidos la recepción de comisiones y depósitos de clientes y el pago de gastos como salarios. Los fondos que se depositarán en la cuenta flotante provendrán de estas cuentas (a menos que los compradores de dinero electrónico puedan pagar dicho dinero mediante depósito directo en la cuenta flotante).

<sup>30</sup> Según el acuerdo, puede resultar necesario realizar los procedimientos del examen en el sitio del fiduciario.

<sup>31</sup> Los supervisores pueden investigar más a fondo las incongruencias verificando si existe algún tipo de informe interno de gestión o auditoría sobre las incongruencias y si estas se informan con regularidad al directorio, el comité de riesgos o el comité de auditoría, si los hubiera, y de qué manera se informan.



Si un EDE utiliza varios bancos para mantener fracciones del dinero electrónico en circulación, los supervisores pueden preguntar de qué manera el EDE divide dicho dinero (por ejemplo, si ello dependerá de los bancos donde el superagente o agente maestro posee cuentas). El EDE debe estar en condiciones de garantizar que la conciliación tenga un grado similar de eficacia para todos los bancos. Los supervisores deben determinar si existen diferencias de conciliación entre bancos y evaluar su eficacia<sup>32</sup>.

#### 5.2.3.4 GESTIÓN Y ADMINISTRACIÓN DE CUENTAS FLOTANTES

La gestión y administración de la cuenta flotante desempeña un papel importante en la conciliación y en la seguridad de los fondos. Los EDE deben contar con políticas y procedimientos operacionales por escrito que rijan el acceso a la cuenta flotante y la operación de esta. En la mayoría de los casos, solo algunos empleados designados tienen autorización para acceder a dicha cuenta y realizar transacciones en ella. Asimismo, el EDE necesita contar con un plan de contingencia que garantice la continuidad de la conciliación según lo previsto en caso de que el operador principal no se encuentre disponible.

Las normas de acceso y reajuste deben corresponderse con la estructura, el tamaño y la complejidad del EDE (por ejemplo, en los grandes EDE, empleados de menor jerarquía pueden tener acceso a la cuenta flotante) y el tipo de mecanismo de conciliación (por ejemplo, totalmente automatizada versus manual). Las normas deben estar documentadas y en ellas deben definirse las transacciones autorizadas para cada perfil de usuario. Los supervisores pueden analizar la lista de empleados y los perfiles de usuario pertinentes para decidir a quién deben entrevistar para obtener más información acerca del cumplimiento de las políticas del EDE y las instancias en que estas no se cumplieron. Deben practicarse controles similares cuando quien opera la cuenta flotante es un fiduciario.

Además de las normas de acceso y los perfiles de usuario, se debe contar con normas formales para administrar los fondos (por ejemplo, transferencias a las cuentas flotantes y desde estas). Esto se relaciona con la conciliación, pero también implica otras situaciones, como las responsabilidades y los procedimientos para controlar periódicamente el interés y otros flujos de ingresos en la cuenta flotante y su retiro o distribución, así como la gestión de los errores, como las transferencias resultantes de fallas en los códigos informáticos. Los supervisores pueden controlar las políticas de los EDE a través de auditorías del sistema.

---

<sup>32</sup> Según la reglamentación, se puede exigir a los EDE que distribuyan el dinero electrónico en circulación entre distintos bancos, conforme a ciertos criterios (por ejemplo, la cantidad máxima del dinero electrónico total emitido por banco). En estos casos, el supervisor puede agregar procedimientos para verificar el cumplimiento de los requisitos y criterios específicos.

### 5.2.3.5 LIQUIDEZ DEL DINERO ELECTRÓNICO EN CIRCULACIÓN

Los supervisores también pueden realizar un control para garantizar que los EDE cumplan los requisitos de liquidez (es decir, inversiones permitidas del dinero electrónico en circulación). Las reglamentaciones de la mayoría de los países son estrictas y prohíben las inversiones (por ejemplo, exigen que los fondos se encuentren en depósitos a la vista) o bien permiten inversiones solo en los activos prescritos o autorizados por el supervisor. Otras permiten (y algunas pueden exigir) invertir un porcentaje del dinero electrónico en circulación en bonos públicos de bajo riesgo. Solo algunas (por ejemplo, las emitidas por el Banco Central de los Estados de África Occidental) permiten inversiones de riesgo como valores<sup>33</sup>.

Los supervisores pueden comenzar preguntando sobre la política o estrategia de inversión (por ejemplo, el perfil de riesgo, el objetivo de rentabilidad y los activos), los cambios reciente (y sus motivos) en la política y el modo en que se toman las decisiones. En general, el directorio debe aprobar la estrategia de inversión y las funciones de la gestión de riesgos, y el comité de riesgos, si lo hubiera, debe hacer el seguimiento de los resultados. Los supervisores pueden también preguntar si la estrategia de inversión varía según la cuenta flotante y solicitar y analizar las constancias de las inversiones realizadas (por ejemplo, estados de cuentas de inversión y estados de la cuenta flotante en los que constan las transferencias a las cuentas de inversión), evaluar su desempeño y el nivel de riesgo, y confirmar la información con la gerencia de inversiones.

Otra área de interés es la prohibición reglamentaria de uso del dinero electrónico en circulación como garantía de préstamos u otro tipo de gravamen. Los supervisores pueden entrevistar a la administración superior y preguntarle acerca de las áreas de preocupación que hayan surgido en las entrevistas separadas que se mantuvieron con el personal del EDE responsable de los empréstitos. Para mayor claridad, los supervisores pueden analizar los empréstitos del EDE (contratos de préstamos)<sup>34</sup>.

### 5.2.3.6 CONTROL PRECISO DEL DINERO ELECTRÓNICO EN CIRCULACIÓN Y LOS SALDOS DE LOS CLIENTES, Y PRESENTACIÓN DE INFORMES MINUCIOSOS AL RESPECTO

El control preciso de los saldos de las cuentas de los clientes es una de las principales obligaciones de los EDE. El EDE debe informar al supervisor sobre el monto exacto del

<sup>33</sup> Véase Kerse y Staschen (2018).

<sup>34</sup> En aquellos países donde la ley de fideicomiso (o de otra índole) reconoce la titularidad de los clientes sobre el saldo de la cuenta flotante, los gravámenes de esta naturaleza suelen ser jurídicamente nulos (por ejemplo, el prestamista del EDE no tendría derecho a reclamar aun cuando la cuenta flotante se ofrece en prenda en el contrato de préstamo entre el EDE y el prestamista).

dinero electrónico en circulación (la suma de los saldos de todas las cuentas de los clientes), lo que resulta fundamental para la supervisión. Para evaluar esto, los supervisores pueden hacer lo siguiente:

- **Analizar si existe un control preciso de los saldos de los clientes<sup>35</sup>:**
  - Revisar los datos de los reclamos para verificar los referidos a saldos insuficientes o incorrectos.
  - Revisar la inactividad de las cuentas del EDE y las prácticas de gestión.
  - Revisar las prácticas del EDE para la liquidación de las transacciones fuera de línea<sup>36</sup>.
  - Verificar las normas que permiten el acceso a la plataforma de dinero electrónico y si existen perfiles autorizados para modificar los saldos de los clientes y en qué condiciones. Investigar las normas mediante pruebas de sistema (por ejemplo, modificación no autorizada de saldos).
  - Si lo que preocupa es la existencia de controles débiles, simular transacciones para verificar si el sistema actualiza correctamente el saldo de la cuenta de un cliente para cada tipo de transacción ofrecido.
  - Preguntar acerca de las normas referidas a los montos que se mantienen temporalmente en cuentas transitorias o de liquidación, y de qué manera afectan a los saldos de los clientes en las instancias de emisión y recepción<sup>37</sup>.
- Evaluar la exactitud de lo informado sobre el dinero electrónico en circulación:
  - Comparar el dinero electrónico en circulación informado con anterioridad en distintas fechas de corte con los informes generados a solicitud del supervisor y en presencia de este (*in situ*) directamente de la plataforma de dinero electrónico del EDE (sistema de cuentas).
  - Preguntar cómo se elaboran los informes periódicos sobre el dinero electrónico en circulación, cuál es el personal responsable de esta labor y si se emplean procedimientos manuales para generar dichos informes. Preguntar al personal a cargo de los informes sobre las debilidades (por ejemplo, si el sistema del EDE no está en condiciones de informar automáticamente el total de dinero electrónico

<sup>35</sup> Los controles deben ser los mismos para cualquier tipo de cliente, incluidos los agentes.

<sup>36</sup> La mayoría de las reglamentaciones de los EDE de mercados emergentes y economías en desarrollo exigen que las transacciones de dinero electrónico se realicen en tiempo real (es decir, con efecto inmediato en el saldo de la cuenta del cliente), aunque existen algunas excepciones. Cuando las transacciones fuera de línea están permitidas, los saldos de las cuentas de los clientes quedarán temporalmente desactualizados antes de que la transacción se liquide finalmente. Este y otros temas relacionados con los riesgos operacionales (por ejemplo, la seguridad de los datos y recuperación después de un desastre) son importantes para facilitar el acceso continuo a información actualizada sobre los saldos en las cuentas de los clientes.

<sup>37</sup> Estas cuentas están destinadas a alojar fondos de manera temporal hasta tanto se resuelvan las transacciones o fondos sin clasificar o cuestionadas (por ejemplo, cuando un cliente envía dinero a un número de teléfono móvil erróneo e informa de este error al EDE antes de que la transacción sea liquidada).

emitido o cualquier otro campo en el informe reglamentario). En caso de surgir alguna inquietud, solicitar al personal que simule la generación de un informe en presencia de los supervisores y preguntar acerca de los pasos que se toman cuando se han encontrado errores en los informes.

- Preguntar si las transacciones pendientes (es decir, los montos registrados temporalmente en cuentas transitorias o de liquidación) se incluyen en el total de dinero electrónico emitido que se informa al supervisor y que se computan a la hora de reponer recursos en la cuenta flotante. Someter a examen las normas mediante pruebas de sistema.

### 5.3 Riesgo operacional

#### 5.3.1 *Requisitos reglamentarios clave*

El riesgo operacional se define como el riesgo de pérdida que resulta de i) procesos, personas o sistemas de la entidad que muestran deficiencias, o ii) acontecimientos externos (Comité de Supervisión Bancaria de Basilea [BCBS], 2011, p. 3). Las reglamentaciones de los EDE pueden contener requisitos generales para que los EDE gestionen sus riesgos operacionales, incluidos los relacionados con los agentes, el fraude, las amenazas cibernéticas, los sistemas informáticos y la continuidad de las operaciones. Estas reglamentaciones en general exigen una estructura mínima de gestión administración de riesgos, como la fiscalización a cargo del directorio y un auditor interno, y las responsabilidades de la administración superior, incluida la formulación de políticas y procedimientos por escrito, controles internos y gestión de riesgos, y las funciones de cumplimiento. En algunos países, los EDE están regidos por una reglamentación específica sobre tercerizaciones que les impone normas como las relativas al almacenamiento de datos (por ejemplo, subcontratación de servicios de computación en la nube) y el acceso del supervisor a las partes subcontratadas (BCBS, 2016a, p. 28 [EC 8]). También puede existir una reglamentación sobre la seguridad de los datos y la continuidad de las operaciones.

#### 5.3.2 *Alcance de los exámenes*

El riesgo operacional es complejo y presenta interdependencias con otras áreas, como la salvaguardia de los fondos, la lucha contra el lavado de activos y el financiamiento del terrorismo, y la protección del cliente. Un examen integral de los riesgos operacionales puede resultar engorroso y es posible que no se justifique para todos los EDE. Los supervisores necesitan determinar en qué medida y con qué frecuencia, según el enfoque basado en los riesgos que apliquen, cada EDE estará cubierto contra los riesgos operacionales y ajustar dicha cobertura en el transcurso del tiempo.

En esta sección no se abordan todos los aspectos de los riesgos operacionales ni se ofrece una estructura para una evaluación integral. Se brinda, más bien, una orientación de alto nivel relacionada con los siguientes aspectos<sup>38</sup>:

- administración del riesgo,
- marco general para la gestión de los riesgos operacionales,
- prevención y gestión del fraude,
- seguridad de los datos (incluida la seguridad cibernética),
- continuidad de las operaciones y recuperación posterior a los desastres.

Si bien la mayoría de los procedimientos pueden ser realizados por un generalista, otros pueden requerir inspecciones especializadas (por ejemplo, para evaluar la solidez de la infraestructura informática, poner a prueba las defensas de la seguridad cibernética, etc.). Los supervisores que no disponen de conocimientos especializados internos pueden contratar auditores externos, siempre que ello esté autorizado por ley (BCBS, 2016a, p. 14 [EC 11]). Asimismo, las herramientas de la tecnología de supervisión pueden ayudar a los supervisores a superar en parte las limitaciones de capacidad, por ejemplo, para analizar los grandes conjuntos de datos sobre transacciones.

### 5.3.3 Procedimientos de examen

#### 5.3.3.1 ADMINISTRACIÓN DE LOS RIESGOS

Todos los EDE deben contar con un marco formal para gestionar los riesgos operacionales, incluidos los riesgos informáticos. Dicho marco debe estar adaptado a las actividades del EDE y deben existir líneas claras de administración y responsabilidades —consagradas en acuerdos formales— entre el EDE y su empresa matriz<sup>39</sup>.

*Muchos de los EDE que se analizaron en esta investigación son propiedad de operadores de redes de telefonía móvil y “utilizan” el marco de gestión de riesgos (e infraestructura clave) de sus empresas matrices, aun cuando la gestión de riesgos del operador se enfoque en los riesgos de la actividad de telecomunicaciones, y no en el sector de dinero electrónico.*

<sup>38</sup> Para obtener más orientación, véase el anexo 4. En esta publicación no se abordan específicamente cuestiones importantes relacionadas con la confiabilidad de los servicios de pago, incluida la finalidad de los pagos y la finalización de las transacciones en caso de pérdida de la comunicación u otro tipo de problemas.

<sup>39</sup> Una buena práctica que pueden adoptar los EDE es contratar personal que se aboque a la gestión de riesgos y que posea experiencia en servicios financieros. Al menos en uno de los países estudiados, los operadores de redes de telefonía móvil pueden tener autorización para actuar como emisores de dinero electrónico (en lugar de que se les exija que creen un ente subsidiario). Esto puede exponer al EDE o al operador de redes de telefonía móvil y viceversa, demorar la adopción de prácticas de gestión de riesgos, e imponer restricciones para los exámenes de supervisión.

Al igual que los bancos, los grandes EDE deben formalizar tres líneas de defensa: i) línea de negocios o controles de gestión, ii) gestión de riesgos y funciones de cumplimiento, y iii) auditores internos y externos independientes. Los pequeños EDE pueden aplicar el mismo concepto a una estructura menos formal, pero el auditor interno debe trabajar siempre con independencia de las unidades de negocios, la gestión de riesgos y las funciones de cumplimiento, y debe rendir cuentas directamente al directorio. La mayoría de las reglamentaciones exigen que los EDE de todos los tamaños contraten auditores externos. En el caso de los grandes EDE, se debe exigir la creación de comités de riesgo a nivel del directorio (alternativamente, la fiscalización de los riesgos podría ser realizada por un comité auditor), mientras que el directorio de los pequeños EDE debe contar con al menos un integrante familiarizado con la gestión de riesgos.

#### 5.3.3.2 MARCO GENERAL DE GESTIÓN DE RIESGOS OPERACIONALES

Los supervisores pueden evaluar la existencia, calidad e implementación de un marco para los riesgos operacionales. En dicho marco se deben identificar, todas las fuentes de riesgos operacionales, como fallas informáticas, fraudes, vulneraciones de la seguridad de los datos, interrupción de los servicios y robos. El directorio debe aprobar el marco y ajustarlo al tamaño y la complejidad del EDE. En general, un marco bien diseñado cumple las siguientes funciones:

- define la estructura de administración de los riesgos;
- describe el ciclo de repetición de las actividades de gestión de riesgos (es decir, procesos de rutina y sistemas empleados para identificar, medir, monitorear, informar y mitigar los riesgos);
- abarca las siguientes tres dimensiones: i) prevención de riesgos, ii) manejo de la materialización de los riesgos, y iii) prevención de la recurrencia mediante la mejora de la gestión de riesgos y los procesos de control;
- establece los procedimientos y sistemas para estimar y monitorear las pérdidas;
- determina la propensión del EDE al riesgo y las contramedidas cuando se toleran altos niveles de riesgo (por ejemplo, reservas de capital y seguros)<sup>40</sup>;
- establece una función de auditoría interna independiente que rinde cuentas directamente al directorio;

---

<sup>40</sup> Esto reviste importancia para los EDE que experimentan una fase de crecimiento rápido, debido a que la calidad de los controles operacionales y la gestión de riesgos puede disminuir durante dicho período.

- proporciona marcos para contratar, monitorear y rescindir acuerdos con terceros, como los de tercerización y asociaciones, y para la debida diligencia inicial y periódica respecto de terceros;
- es objeto de revisiones periódicas.

Para dar inicio al examen se parte de un análisis externo de la documentación pertinente, que incluye políticas y manuales de procedimiento, informes de riesgos, dictámenes de auditorías internas y externas, e informes de incidentes (por ejemplo, fraudes e interrupciones)<sup>41</sup>. La verificación interna, que puede incluir un ejercicio de observación, entrevistas y pruebas de sistemas, se basa en los análisis externos. Lo esencial del trabajo *in situ* es indagar si el marco de gestión de riesgos se implementa con eficacia y dar seguimiento a las conclusiones de la labor de preparación externa. Por ejemplo, el supervisor puede analizar si los controles internos forman parte de las actividades diarias del EDE y si los sistemas informáticos ofrecen una herramienta idónea para identificar, monitorear e informar los riesgos, incluidos los datos sobre las pérdidas estimadas y las pérdidas sufridas (por ejemplo, reintegros a clientes por transacciones no autorizadas, pagos deducibles de seguros por reclamos de cobertura, pérdida de equipos por cortes eléctricos, etc.)<sup>42</sup>.

Los supervisores pueden revisar de qué manera se generan los informes sobre riesgos operacionales que reciben y si los datos de estos informes se corresponden con la información disponible en el sistema informático de gestión de riesgos del EDE (es decir, si son exactos y completos). En caso de encontrar discrepancias, el supervisor puede requerir informes internos sobre la gestión de riesgos operacionales en lugar de la plantilla habitual de informe.

#### 5.3.3.3 PREVENCIÓN Y GESTIÓN DEL FRAUDE

Existen diferentes tipos de fraude que pueden afectar a los EDE<sup>43</sup>. El EDE necesita catalogarlos e incluirlos en el marco de gestión de riesgos operacionales y en el sistema informático de detección de fraude. La gestión informal, incompleta o laxa de los fraudes en los EDE (por ejemplo, sin investigación de los casos de fraude) debe generar inquietud a los supervisores.

---

<sup>41</sup> El supervisor debe intentar evaluar el grado de independencia del auditor interno. Si dicha independencia se ve comprometida, los informes tendrán poco valor. Los informes del auditor externo también pueden brindar información relevante.

<sup>42</sup> En los *Principios para una eficaz agregación de datos sobre riesgos y presentación de informes de riesgos* del BCBS (2013), si bien están destinados a bancos de gran tamaño y complejidad, se brinda una guía que podría adaptarse para instituciones menos complejas, como los EDE.

<sup>43</sup> Véanse las tipologías de los fraudes en Buku y Mazer (2017).

*El riesgo de fraude, como el acceso no autorizado a los fondos de los clientes por parte del personal de los EDE, es una preocupación importante entre las autoridades entrevistadas de los mercados emergentes y las economías en desarrollo. El fraude interno merece especial atención; la mayoría de los casos de fraude que aparecen en los titulares de los periódicos de los mercados emergentes y las economías en desarrollo fueron cometidos por integrantes del personal, en ocasiones en colusión con los agentes.*

Los supervisores pueden hacer lo siguiente<sup>44</sup>:

- Verificar (de manera externa) que existan políticas y procedimientos adecuados para evitar e identificar los casos de fraude, y responder a ellos; que se identifiquen las tipologías de fraude, y que se esclarezcan las responsabilidades.
- Evaluar con cuánta eficacia el EDE comunica internamente su política orientada a identificar y sancionar a miembros del personal y a agentes que comentan fraude.
- Revisar los antecedentes de casos de fraude (de manera externa) en el transcurso de un período extenso para determinar los tipos de fraude, el aumento del índice de fraude, las áreas afectadas y las pérdidas sufridas. En esta revisión se deberá evaluar la observancia de las políticas de los EDE, la eficacia de la gestión de riesgos de fraude y los efectos de las pérdidas en la salud financiera del EDE. Comparar los resultados con los de otros EDE.
- Indagar por qué ocurrieron los fraudes y qué se hizo para evitar su recurrencia. Prestar especial atención a la recurrencia.
- En caso de contar con capacidad y sistemas informáticos analíticos, solicitar y auditar (de manera externa) los conjuntos de datos pormenorizados para corroborar la información sobre fraudes suministrada por el EDE, de tal modo que sea posible identificar los patrones inusuales en el comportamiento de las transacciones (por ejemplo, concentración de grandes retiros en un corto lapso y su ubicación geográfica)<sup>45</sup>.
- Corroborar la información proporcionada por los EDE sobre sus antecedentes de señales de alerta enviadas por el sistema de detección de fraude y sobre los parámetros empleados para emitir dichas alertas.

<sup>44</sup> Dada la alta incidencia de los fraudes en algunos tipos de transacciones con dinero electrónico (por ejemplo, el dinero móvil en África al sur del Sahara), es conveniente que los supervisores efectúen una revisión temática de la prevención y gestión del fraude.

<sup>45</sup> Pese a los posibles beneficios de auditar grandes conjuntos de datos pormenorizados para evaluar de qué manera un EDE gestiona e informa sus riesgos operacionales, incluido el riesgo de fraude, la mayoría de los supervisores entrevistados en los mercados emergentes y las economías en desarrollo no poseían los conocimientos especializados ni el programa analítico necesarios.



- Controlar los derechos de acceso al sistema de cuentas de dinero electrónico e indagar qué integrantes del personal pueden eliminar y alterar datos, transferir fondos, etc. Consultar sobre los controles para limitar el acceso a la plataforma y proteger los detalles de inicio de sesión, y sobre las excepciones a las reglas. Emplear las consultas y las pruebas de sistema para evaluar si el personal tiene capacidad para crear o destruir dinero electrónico de modo manual.
- Analizar los registros de auditoría para, por ejemplo, detectar accesos inusuales o intentos no autorizados por integrantes del personal o agentes (por ejemplo, actividad del personal en horas de la noche) y simular acciones no autorizadas.
- Consultar sobre la frecuencia de las actualizaciones del sistema de detección de fraude y gestión de actualizaciones (adquisición, prueba, instalación y seguimiento de cambios de códigos).
- Evaluar cómo se gestionan las cuentas de liquidación (cuentas temporales o transitorias). Una conciliación anómala puede constituir una oportunidad para estafadores<sup>46</sup>.

#### 5.3.3.4 SEGURIDAD DE LOS DATOS (INCLUIDA LA SEGURIDAD CIBERNÉTICA)

La seguridad cibernética es importante para la gestión de riesgos de los EDE, dado que estos operan valiéndose de datos digitales, redes de agentes ampliamente extendidas y la creciente conectividad con terceros. Los EDE de cualquier tamaño requieren estrategias eficaces para la seguridad de los datos formalizadas en un **programa para tal fin**. Un programa de seguridad de datos bien diseñado reúne las siguientes características<sup>47</sup>:

- Es aprobado por el directorio del EDE y se encuentra bajo la responsabilidad de dicho órgano.
- En él se designa a un ejecutivo (por ejemplo, un oficial de seguridad de la información) como funcionario responsable.
- Se basa en la evaluación de los riesgos realizada por el EDE o expertos externos.
- En él se identifican y clasifican los datos en función de su sensibilidad.
- Abarca todas las instalaciones y sistemas empleados para acceder, recolectar, almacenar, utilizar, transferir, asegurar y desechar datos.

<sup>46</sup> Ejemplo de ello es el renombrado caso de fraude de dinero móvil de Uganda relacionado con la transferencia no autorizada de fondos a dichas cuentas o desde ellas. Véase Morawczynski (2015).

<sup>47</sup> La seguridad de los datos y la confidencialidad de los datos, aunque guardan relación entre sí, son áreas distintas de la tarea de supervisión. En esta sección no se aborda el tema de la confidencialidad de los datos (por ejemplo, si el EDE solicita el consentimiento de los clientes antes de intercambiar datos para fines de comercialización).

- En él se clasifican los riesgos para la seguridad de los datos en internos y externos, y se identifican sus fuentes, probabilidades y efectos.
- Contiene las salvaguardias administrativas, técnicas y físicas para garantizar la seguridad, confidencialidad e integridad de los datos a fin de i) evitar riesgos (**prevención**), ii) identificar los riesgos (**detección**) y responder a la materialización de los riesgos (**tratamiento**). Para consultar algunos ejemplos de salvaguardia, véase el recuadro 4.

#### **Recuadro 4. Ejemplos de medidas de seguridad de los datos que pueden adoptar los EDE**

Como parte de su programa de seguridad de los datos, un EDE puede aplicar las siguientes medidas:

- Implementar un doble sistema de control y distinguir obligaciones.
- Verificar antecedentes e impartir capacitación especializada para el personal esencial.
- Revocar de inmediato los derechos de acceso de los empleados salientes.
- Mantener un inventario de los recursos tecnológicos (por ejemplo, dispositivos físicos, conexiones de redes).
- Realizar actualizaciones periódicas de los sistemas y gestionar los cambios de código (gestión de actualizaciones).
- Emplear herramientas de seguimiento actualizadas para detectar casos de fraude e intrusiones.
- Disponer de un programa de seguridad cibernética que brinde un marco para la identificación de riesgos, protección contra ellos, detección, respuesta y recuperación, pruebas y elaboración de informes. Esta medida de seguridad debe incluir i) la encriptación de los datos en tránsito y en almacenamiento (CGAP, 2018), ii) contrafuegos y controles de virus, y iii) análisis de vulnerabilidad y pruebas de penetración.
- Participar en grupos de intercambio de información y adoptar medidas para el aprendizaje continuo.
- Controlar el acceso a los sistemas y centros clave, efectuar pruebas de resiliencia a los controles manuales, y contar con mecanismos de seguridad física.
- Disponer de medidas de protección contra la destrucción, pérdida o daño de datos en caso de incendio o inundación, y para reaccionar frente a estos fenómenos.
- Contar con un marco de seguridad de los datos en los acuerdos de tercerización y asociación.

- En él se enmarca la evaluación continua y periódica de la eficacia del programa y su consecuente mejora.

Dependiendo del EDE y de los conocimientos especializados disponibles, en un examen se pueden combinar la revisión de documentos, entrevistas, observaciones y pruebas de sistema. Algunas de las posibilidades son las siguientes<sup>48</sup>:

- reunir evidencias de que el programa de seguridad protege al EDE contra los riesgos y seguirá haciéndolo en virtud de la estrategia de negocios y crecimiento de dicho emisor;
- analizar y realizar consultas ulteriores sobre los resultados de las evaluaciones de riesgos;
- analizar los dictámenes de auditoría y la implementación de las recomendaciones contenidas en estos;
- analizar los aspectos relativos a la seguridad de los datos en los acuerdos de subcontratación, incluidos, entre otros, la computación en la nube, el procesamiento de las transacciones y el desarrollo de interfaces para programas de aplicación<sup>49</sup>;
- analizar datos sobre riesgos (por ejemplo, las vulneraciones a la seguridad de los datos denunciadas, la piratería informática, las inyecciones de virus, etc.);
- evaluar la seguridad física de centros sensibles (por ejemplo, almacenamiento y procesamiento de datos);
- poner a prueba controles clave realizando un análisis de vulnerabilidad, pruebas de penetración, análisis de registros de auditoría, etc.

El programa de seguridad de un EDE es apenas tan sólido como su eslabón más débil. Por ejemplo, muchos EDE de África y Asia utilizan el servicio suplementario de datos no estructurados, considerado un canal de baja seguridad para transportar los datos de los clientes. Asimismo, muchos EDE a menudo utilizan números de identificación personal para autenticar a los clientes, pero muchos de ellos revelen estos números a los agentes de los EDE. Si bien numerosos países utilizan el servicio de datos mencionado y agentes para facilitar la inclusión financiera, los supervisores deben evaluar de qué manera

---

<sup>48</sup> Para consultar otros recursos, véase el anexo 4.

<sup>49</sup> Todos los supervisores de los mercados emergentes y las economías en desarrollo entrevistados manifestaron su preocupación por la tercerización de la computación en las nubes por parte de los EDE, sobre todo más allá de las fronteras, debido a que ello podría dificultar el acceso a los datos y los centros de almacenamiento de datos para fines de supervisión. Por ejemplo, India emitió recientemente una directiva que exige a los proveedores de sistemas de pago que almacenen todos los datos relacionados con sus operaciones exclusivamente en el país, con lo que se les prohíbe utilizar servicios en la nube con carácter transfronterizo (véase Baur-Yazbeck, 2018).

los EDE reducen los riesgos relacionados con la seguridad de los datos (por ejemplo, mediante autenticaciones biométricas, *tokens* con contraseñas de un solo uso, detección de anomalías o una salida gradual del servicio suplementario de datos no estructurados.

#### 5.3.3.5 CONTINUIDAD DE LAS OPERACIONES

La gestión de la continuidad de las operaciones es importante para la gestión de los riesgos operacionales y debe estar bien desarrollada en los grandes EDE<sup>50</sup>. Los acuerdos para la continuidad de las operaciones deben permitir al EDE reanudar con rapidez las actividades esenciales y restaurar la infraestructura informática clave en caso de interrupciones menores o severas (por ejemplo, interrupción de las telecomunicaciones, cortes eléctricos y desastres naturales). La gestión de la continuidad de las operaciones permite a las empresas responder a las crisis y atenuar sus efectos.

Los supervisores deben evaluar el plan de continuidad de las operaciones del EDE con el objeto de garantizar lo siguiente:

- que en el plan se prevean escenarios de crisis y se analicen sus posibles efectos<sup>51</sup>;
- que se cuente con estrategias de contingencia y recuperación que permitan identificar las instalaciones, personas, procesos, sistemas informáticos, datos y capacidades alternativas de procesamiento de datos que revisten importancia crítica;
- que el personal reciba la capacitación adecuada (entre otras cosas, mediante simulaciones) para ejecutar el plan;
- que el plan se ponga a prueba y se revise en forma periódica (los supervisores pueden analizar los resultados de las pruebas);
- que los sistemas esenciales del EDE sean sometidos a pruebas de tensión;
- que las políticas, controles manuales y automatizados, y los acuerdos de distribución de riesgos se encuentren en vigor y garanticen la eventual conclusión de las transacciones, incluso cuando la comunicación se vea interrumpida antes de concluirse o en caso de fallas en los sistemas de terceros (por ejemplo, servicios de iniciación de pagos)<sup>52</sup>.

<sup>50</sup> Para obtener más orientación, véase el anexo 4.

<sup>51</sup> Una buena práctica consiste en realizar un análisis integral de los efectos sobre las operaciones y una evaluación de riesgos como base para el diseño y la estrategia de contingencia.

<sup>52</sup> Numerosas leyes y reglamentaciones sobre los sistemas de pago contienen requisitos pertinentes para atender estas situaciones, pero en los mercados emergentes y las economías en desarrollo incluidas en esta investigación se observa un nivel de cumplimiento limitado, lo que coloca a los clientes en una situación vulnerable.

*Los mercados emergentes y las economías en desarrollo del estudio informaron que eran frecuentes las fallas en las telecomunicaciones y la infraestructura eléctrica, lo que provocaba interrupciones operativas en los servicios de los EDE. Esta dependencia de terceros genera riesgos. Al parecer, existe escasa inversión en planes de contingencia y escasa presión desde la supervisión para realizar mejoras. Otras interrupciones informadas obedecen a eventos inesperados o incluso planificados en los sistemas de los EDE. En los países africanos investigados se registraron casos de importantes interrupciones generadas por las actualizaciones de la plataforma de dinero electrónico. Uno de ellos fue la interrupción de aproximadamente 12 horas de M-PESA registrada en Kenya con motivo de una actualización del sistema en 2017 (Capital Business, 2017).*

El supervisor puede coordinar con la entidad reguladora de las telecomunicaciones para acceder a datos o información analítica que podrían brindar un panorama más amplio de las interrupciones en los servicios de telecomunicaciones. Dichas interrupciones podrían compararse con las producidas en los EDE para determinar la forma de mejorar los planes de contingencia. Muchos EDE de los mercados emergentes y las economías en desarrollo dependen de un único operador de redes de telefonía móvil y habitualmente no buscan otros operadores, lo que los expone aún más a interrupciones operativas.

Como parte del examen externo, el supervisor puede analizar los datos sobre la frecuencia, ubicación y duración de las interrupciones, las transacciones fallidas o incompletas, y el tiempo de inactividad del sistema y sus motivos (y soluciones), y dar seguimiento a los compromisos previos asumidos en relación con las mejoras. Los supervisores con conocimientos especializados pueden solicitar y auditar conjuntos de datos pormenorizados sobre las transacciones y los registros en el sistema para determinar los patrones inusuales que podrían implicar fallas en los planes de contingencia y para detectar las interrupciones que no se hayan informado al supervisor.

## **5.4 Lucha contra el lavado de activos y el financiamiento del terrorismo**

### **5.4.1 Requisitos reglamentarios clave**

Los EDE a menudo están alcanzados por las leyes de lucha contra el lavado de activos y el financiamiento del terrorismo, por lo que deben presentar informes sobre las transacciones sospechosas a la unidad de inteligencia financiera e instrumentar sistemas y controles destinados a reducir el riesgo de este tipo de delitos. Las reglamentaciones relativas a los EDE se enfocan en imponer límites de saldos y transacciones para las cuentas de dinero electrónico de clientes y agentes, como los límites a los saldos mensuales, el importe de cada transacción o el volumen total de transacciones mensuales, y, ocasionalmente, restricciones al número de cuentas que cada cliente puede poseer. Si los EDE cumplen estas

reglamentaciones, el riesgo de lavado de activos y financiamiento del terrorismo podría reducirse considerablemente. Asimismo, la reglamentación exige que los EDE lleven a cabo el procedimiento de debida diligencia con respecto a los clientes verificando la identidad de estos y de los agentes (incluida la recopilación y el almacenamiento de los datos de apertura de cuentas), y que realicen el seguimiento de las transacciones con el objeto de identificar las desviaciones de los comportamientos esperados en función del perfil de los clientes y agentes.

*La mayoría de los supervisores de los mercados emergentes y las economías en desarrollo entrevistados para esta investigación no aplican procedimientos especiales de supervisión (externos ni internos) para evaluar la eficacia de los EDE en el manejo de los riesgos de lavado de activos y financiamiento del terrorismo. Unos pocos, sin embargo, han creado equipos especializados que se dedican a evaluar la lucha contra estas prácticas. Las prácticas observadas en el sector sugieren que el seguimiento de las operaciones de lavado de activos y financiamiento del terrorismo y la debida diligencia con respecto al cliente no siempre bastan. En África, por ejemplo, existen casos de clientes que se registran con varias cuentas de dinero electrónico en el mismo EDE y en distintos EDE y que incumplen los límites de transacciones, lo que deja al descubierto las debilidades de los sistemas y controles de la gestión de riesgos.*

#### 5.4.2 Alcance de los exámenes

Los límites de transacciones y saldos surten efecto solo si los procedimientos para la apertura de cuentas se ajustan a las normas y si el seguimiento de las transacciones es eficaz. De lo contrario, los clientes pueden tener varias cuentas, operar en colusión con los agentes y otros clientes, y evadir los límites con fines delictivos. Los controles deben estar incorporados (encriptados) en los sistemas de los EDE, y para que el seguimiento sea eficaz es necesario contar con programas informáticos especializados. Un examen sobre la lucha contra el lavado de activos y el financiamiento del terrorismo debe enfocarse como mínimo en lo siguiente:

1. el cumplimiento de los límites reglamentarios;
2. los procedimientos de apertura de cuentas (para clientes y agentes);
3. el perfil de los productos, clientes y agentes;
4. el seguimiento de las transacciones.

#### 5.4.3 Procedimientos de los exámenes

Al igual que en otras áreas, los supervisores pueden analizar (de manera externa) las políticas y los procedimientos manuales escritos donde se describen los controles internos de los EDE, su política de gestión de riesgos, las responsabilidades del personal y los sistemas

informáticos relacionados con la lucha contra el lavado de activos y el financiamiento del terrorismo<sup>53</sup>. Como mínimo, las políticas y los procedimientos manuales deben estar en consonancia con la reglamentación aplicable; sin embargo, resulta conveniente proporcionar una cantidad mucho mayor de detalles. El examen puede enfocarse en lo siguiente:

- si las normas escritas se cumplen en la práctica y si existen importantes oportunidades para vulnerarlas;
- cuán eficaz es la comunicación en toda la organización en lo concerniente a las obligaciones y los controles relacionados con la lucha contra el lavado de activos y el financiamiento del terrorismo y los cambios que experimentan dichas obligaciones y controles;
- si existen tipologías razonables de lavado de activos incorporadas en el programa de gestión de riesgos;
- de qué manera se realiza la detección, confirmación y denuncia de transacciones sospechosas, y de qué modo actúa el EDE a partir de ello;
- si el sistema o el personal operativo o los agentes han detectado numerosas transacciones sospechosas que no se han denunciado ante la unidad de inteligencia financiera (y por qué razón);
- el análisis externo de los informes de auditoría interna y externa y su seguimiento interno.

Al igual que con los riesgos operacionales, los supervisores pueden realizar análisis automatizados o manuales de los datos pormenorizados sobre las transacciones y los acontecimientos informados, como registros de aperturas de cuenta, para identificar las situaciones sospechosas y las excepciones a las reglamentaciones y las políticas del EDE. Estos datos pueden obtenerse *in situ* o recopilarse antes de realizar los procedimientos internos<sup>54</sup>.

#### 5.4.3.1 CUMPLIMIENTO DE LOS LÍMITES REGLAMENTARIOS

Los supervisores pueden hacer lo siguiente:

- analizar (de forma externa) las políticas y los procedimientos orientados al cumplimiento de los límites, evaluar el grado de implementación (de forma externa e interna) y evaluar las excepciones;

<sup>53</sup> Sin embargo, varios EDE de los mercados emergentes y las economías en desarrollo investigados no cuentan con unidades, personal ni programas informáticos especializados en la lucha contra el lavado de activos y el financiamiento del terrorismo, sino que más bien utilizan el programa análogo de las respectivas empresas matrices. Habida cuenta de las diferencias entre dinero electrónico y servicios de operadores de redes de telefonía móvil, los controles relacionados con la lucha contra el lavado de activos y el financiamiento del terrorismo deben adaptarse por completo a las necesidades de los EDE.

<sup>54</sup> Solo algunos de los supervisores de los mercados emergentes y las economías en desarrollo entrevistados tienen acceso a datos muy pormenorizados de las transacciones de los EDE, pero no realizan análisis sofisticados (por ejemplo, mediante el uso de programas informáticos analíticos modernos) para identificar los riesgos operacionales y los relacionados con el lavado de activos y el financiamiento del terrorismo.

- evaluar la eficacia de los controles automatizados incluidos en los sistemas con el fin de identificar, tratar y denunciar operaciones sospechosas;
- ejecutar pruebas de sistema para simular transacciones prohibidas;
- formular preguntas acerca de la demostración de los controles automatizados y de los criterios de alerta, y solicitar dicha demostración;
- analizar el registro de vulneraciones de los límites o intentos de vulneraciones, e indagar cuáles fueron sus causas y qué medidas se adoptaron para solucionarlos;
- analizar la evolución de los conjuntos de datos pormenorizados en el tiempo para corroborar la información suministrada por el EDE y controlar el grado de constancia en el cumplimiento de los límites reglamentarios;
- constatar si existe algún tipo de control con el que se intente identificar a los clientes que poseen varias cuentas en un mismo EDE y en distintos EDE;
- profundizar las consultas acerca del tipo de cuentas que despiertan preocupación (por ejemplo, cuentas autorregistradas y cuentas que hayan activado alertas reiteradas);
- solicitar información sobre los empleados autorizados para modificar los límites u otras normas del sistema, y consultar si se han realizado modificaciones en el pasado y cómo se proponen y aprueban dichas modificaciones.

#### 5.4.3.2 PROCEDIMIENTOS DE APERTURA DE CUENTAS

A fin de verificar si los procedimientos de apertura de cuentas cumplen con las políticas y reglamentaciones de los EDE, los supervisores pueden hacer lo siguiente:

- consultar con el personal de operaciones y los agentes sobre los procedimientos (incluidos los realizados de forma remota) de apertura de cuentas (por ejemplo, que describan cada paso y cada norma), si existen excepciones, si les resulta difícil aplicarlos (por ejemplo, la verificación de identidad) y si los clientes han podido abrir varias cuentas;
- en caso de contar con datos pormenorizados sobre las transacciones, verificar si existe una concentración de volúmenes de apertura de cuentas en determinados períodos/ ubicaciones o sucursales/agentes, y solicitar y analizar documentación de una muestra de cuentas cuando exista algún tipo de sospecha;
- observar las aperturas de cuentas de clientes reales realizadas por agentes o miembros del personal;
- realizar compras de incógnito<sup>55</sup>;

---

<sup>55</sup> Para consultar información sobre compras de incógnito, véase Mazer y cols. (2015).



- evaluar la gestión de riesgos cuando se utilizan datos biométricos u otros procedimientos electrónicos como el conocimiento del cliente y la debida diligencia aplicada a los clientes;
- revisar los procedimientos para identificar y seguir de cerca a los individuos políticamente expuestos, y el uso de listas de sanciones;
- indagar acerca de la capacitación reiterada destinada a todo el personal de los agentes que realizan transacciones de dinero electrónico, y buscar constancias de dicha capacitación, recopilando documentación y entrevistando a los involucrados.

#### 5.4.3.3 PERFIL DE LOS PRODUCTOS, CLIENTES Y AGENTES

Los supervisores pueden corroborar y evaluar de qué manera los EDE definen el perfil de los clientes y agentes (por ejemplo, clientes minoristas, agentes pequeños, agentes grandes, agentes maestros, etc.), la ubicación (por ejemplo, grandes centros urbanos, zonas de frontera, aldeas rurales, etc.) y otras características (por ejemplo, ingresos y fecha de creación de cuenta) cuya combinación puede conducir a distintos grados de riesgo de lavado de activos y financiamiento del terrorismo y los respectivos patrones de transacciones previstas. En la mayoría de los mercados emergentes y economías en desarrollo estudiados, la reglamentación impone límites a las cuentas y las transacciones para todos los clientes y productos de los EDE, pero estos últimos pueden aplicar límites menores en el caso de clientes (por ejemplo, los que residen en zonas de frontera) o productos (por ejemplo, remesas) que suponen mayores riesgos. Los agentes pueden contar con mayor flexibilidad para los límites debido a que requieren transacciones de mayor volumen para atender a sus clientes finales. Es importante comprender de qué manera los EDE definen el perfil de los clientes y agentes, ya que ello constituye la base para identificar posibles comportamientos de riesgo a través del seguimiento de las transacciones.

#### 5.4.3.4 SEGUIMIENTO DE LAS TRANSACCIONES

Los EDE pueden utilizar programas informáticos especializados para hacer el seguimiento de las transacciones y comparar comportamientos sospechosos frente a los comportamientos esperados. Si bien la sofisticación de estos sistemas se debe adaptar al tamaño y la complejidad de cada EDE, todos los EDE deben contar con un sistema totalmente automatizado. El sistema debe ser capaz de identificar los intentos de transacciones que superen los límites permitidos, las transacciones incompatibles con los perfiles preestablecidos y otras situaciones sospechosas, como un volumen elevado de transacciones entre pocas cuentas, oleadas de transacciones, concentración geográfica, múltiples transacciones realizadas por el mismo cliente, etc.

Los sistemas de identificación de riesgos de fraude y lavado de activos y financiamiento del terrorismo son cada vez más sofisticados e innovadores. Algunos aplican un análisis complejo de aprendizaje automático de numerosos factores y datos en tiempo real para identificar comportamientos sospechosos, que permitirían, por ejemplo, identificar la posible multiplicidad de cuentas que esté usando un mismo individuo con datos de identificación falsos o de familiares y amigos. Estos sistemas pueden bloquear de forma automática ciertas cuentas y activar las alertas entre el personal.

La calidad del seguimiento de las transacciones está supeditada a la calidad y variedad de los datos empleados por el programa informático analítico. Si no se cuenta con datos de calidad, un sistema costoso y sofisticado que utiliza aprendizaje automático presentará las mismas debilidades que cualquier otro sistema. El supervisor puede consultar acerca de las fuentes de los datos utilizados y su calidad para establecer con cuánta eficacia el sistema de seguimiento identifica los riesgos y con cuánta rapidez los informa, el desempeño del personal a la hora de denunciar las situaciones alertadas por el sistema y responder a ellas, y si se ha informado al supervisor sobre las situaciones de riesgo confirmadas.

*Algunos supervisores de los mercados emergentes y las economías en desarrollo prefieren recopilar datos muy pormenorizados sobre las transacciones para hacer el seguimiento en tiempo real del riesgo de lavado de activos y financiamiento del terrorismo, de manera similar a lo que hacen algunas de las instituciones financieras de hoy cuando utilizan sistemas de seguimiento sofisticados. Si bien esto es posible, la relación costo-beneficio no es clara en todos los casos. Los supervisores pueden recopilar datos pormenorizados durante un examen y realizar los análisis que estimen convenientes. Por otra parte, el seguimiento en tiempo real que efectúan los supervisores nunca debe reemplazar la obligación de los EDE de llevar a cabo su propio seguimiento en tiempo real. En FSI (2018) y Dias (2018) se describen algunos ejemplos del uso de datos muy pormenorizados y programas informáticos analíticos sofisticados para el seguimiento de la lucha contra el lavado de activos y el financiamiento del terrorismo que llevan adelante los supervisores.*

## 6. Conclusiones

---

Los EDE desempeñan una función crucial en los avances de la inclusión financiera en muchos mercados emergentes y economías en desarrollo; los supervisores, por su parte, son los responsables de mantener a salvo los mercados de dinero electrónico a través de una supervisión proporcional que establezca un equilibrio de prioridades y se enfoque en los riesgos más significativos. Si bien el enfoque basado en los riesgos es un componente fundamental para la supervisión eficaz de los EDE, la tecnología de la supervisión puede emplearse para aliviar la intensa carga de trabajo que supone dicha tarea y aumentar la exhaustividad de los análisis.

La supervisión de los EDE es más simple que la de los bancos, debido a que los primeros tienen, por reglamentación, un ámbito de actividad mucho más limitado, por lo que suelen plantear menos riesgos que los segundos. Asimismo, las reglamentaciones más comunes sobre los EDE imponen requisitos de salvaguardia destinados a respaldar todos los fondos debidos a los clientes de los EDE con activos seguros y líquidos. Cuando los EDE implementan con eficacia la salvaguardia de los fondos, disminuyen sustancialmente los riesgos de que los clientes pierdan su dinero. En consecuencia, dicha salvaguardia constituye una preocupación central en la supervisión de los EDE.

No existe una receta única para determinar el alcance y la profundidad que debería tener la supervisión de los EDE para ajustarse a la realidad de todos los países. Los supervisores necesitan contar con un enfoque basado en los riesgos que se adapte a sus contextos y centrar las evaluaciones en los EDE más importantes y los riesgos más importantes que estos presentan. En el caso de los grandes EDE, es conveniente que la mayoría de los supervisores abarquen, en mayor medida que cuando se trata de pequeños EDE, una amplia gama de riesgos, incluidos los operacionales, relacionados con el lavado de activos y el financiamiento del terrorismo, y relativos a la protección del cliente. Una metodología adecuada basada en los riesgos depende de que se cuente con datos idóneos, comenzando por un seguimiento constante de los mercados que permita establecer comparaciones entre distintos EDE y preparar a los supervisores para examinar a cada EDE en particular. Las orientaciones que se brindan en el presente documento, sobre todo el detalle de los procedimientos de los exámenes, deben utilizarse con prudencia según el enfoque específico basado en los riesgos que cada supervisor adopte para los EDE. No todos los procedimientos podrán aplicarse a todos los EDE y algunos de estos

pueden necesitar otras medidas además de las aquí descritas. Por otra parte, en el presente documento no se incluyen algunos aspectos importantes, como las facultades o medidas correctivas y la resolución de los EDE.

Por último, si bien no existe un modelo único en lo que se refiere al lugar donde debería ubicarse la supervisión de los EDE dentro de una autoridad de supervisión financiera, los supervisores deben poseer experiencia en evaluación del sector financiero y conocimientos específicos sobre las actividades de los EDE.

## Anexo 1. Instituciones entrevistadas

<b>País/región</b>	<b>Organizaciones</b>
África Occidental	Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO)
Austria	Oesterreichische Nationalbank
	Autoridad para los Mercados Financieros
Brasil	Banco Central do Brasil (BCB)
Colombia	Superintendencia Financiera
Filipinas	Bangko Sentral ng Pilipinas (BSP)
Francia	Autoridad Francesa de Supervisión Prudencial y de Resolución (ACPR)
Ghana	Banco de Ghana
	MTN Mobile Money
	Airtel Money
	Tigo Cash
	Vodafone Ghana Mobile Financial Services
Hong Kong	Autoridad Monetaria de Hong Kong
India	India
Jordania	Jordania
Luxemburgo	Luxemburgo
Malasia	Bank Negara Malaysia
México	Comisión Nacional Bancaria y de Valores (CNBV)
	Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR)
Myanmar	Banco Central de Myanmar
	Wave Money
Nigeria	Banco Central de Nigeria
Pakistán	Banco Estatal del Pakistán
Paraguay	Banco Central del Paraguay
Perú	Superintendencia de Banca, Seguros y AFP (SBS)
Reino Unido	Autoridad de Conducta Financiera
Singapur	Autoridad Monetaria de Singapur
Tanzanía	Banco de Tanzania
	Autoridad Reguladora de las Comunicaciones de Tanzania
	Autoridad Reguladora de Seguros de Tanzania
	Vodacom Tanzania
	Jumo
	Airtel Tanzania
Uganda	Banco de Uganda

## Anexo 2. Referencias bibliográficas

---

### Principales referencias bibliográficas

- Staschen, S. y P. Meagher (2018), *Basic Regulatory Enablers for Digital Financial Services*, *Enfoques* n.º 109, Washington, DC, CGAP, <http://www.cgap.org/sites/default/files/Focus-Note-Basic-Regulatory-Enablers-for-DFS-May-2018.pdf>.
- Dias, D. y S. Staschen (2017), *Data Collection by Supervisors of DFS*, documento de trabajo, Washington, DC: CGAP, <http://www.cgap.org/sites/default/files/Working-Paper-Data-Collection-by-Supervisors-of-DFS-Dec-2017.pdf>.
- (2015), *Supervision of Banks and Nonbanks Operating through Agents. Practice in Nine Countries and Insights for Supervisors*, documento de trabajo. Washington, DC, CGAP, <https://www.cgap.org/sites/default/files/Working-Paper-Supervision-of-Banks-and-Nonbanks-Operating-through-Agents-August-2015.pdf>.

### Bibliografía

- AFI (Alliance for Financial Inclusion) (2014), *Supervision and Oversight of Mobile Financial Services*, nota de orientación n.º 12, febrero, <http://www.afi-global.org/publications/1451/Guideline-Note-12-Mobile-Financial-Services-Supervision-and-Oversight-of-MFS>.
- Almazán, M., y N. Vonthron (2014), *Mobile Money Profitability: A Digital Ecosystem to Drive Healthy Margins*, Londres: Mobile Money for the Unbanked, noviembre, [https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/11/2014\\_Mobile-money-profitability-A-digital-ecosystem-to-drive-healthy-margins.pdf](https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/11/2014_Mobile-money-profitability-A-digital-ecosystem-to-drive-healthy-margins.pdf).
- APRA (Australian Prudential Regulatory Authority) (2015), *Outsourcing Involving Shared Computing Services (including Cloud)*, documento informativo, julio, <https://www.apra.gov.au/sites/default/files/information-paper-outsourcing-involving-shared-computing-services.pdf>.

- Bauguess, S. W. (2018), *The Role of Machine Readability in an AO World*, discurso inaugural pronunciado en la Conferencia sobre Gestión de la Información Financiera, Boston, Massachusetts, 3 de mayo, [https://www.sec.gov/news/speech/speech-bauguess-050318?utm\\_source=Master+List&utm\\_campaign=036e369e76-EMAIL\\_CAMPAIGN\\_2018\\_05\\_04&utm\\_medium=email&utm\\_term=0\\_da5920711b-036e369e76183267633#\\_edn7](https://www.sec.gov/news/speech/speech-bauguess-050318?utm_source=Master+List&utm_campaign=036e369e76-EMAIL_CAMPAIGN_2018_05_04&utm_medium=email&utm_term=0_da5920711b-036e369e76183267633#_edn7).
- BCBS (Comité de Supervisión Bancaria de Basilea) (2016a), *Orientaciones sobre la aplicación de los principios básicos para una supervisión bancaria eficaz a la regulación y supervisión de instituciones relevantes para la inclusión financiera*, Basilea, Banco de Pagos Internacionales, septiembre, <https://www.bis.org/bcbs/publ/d383.htm>.
- (2016b), *Market Intelligence Gathering at Central Banks*, Basilea, Banco de Pagos Internacionales, diciembre, <https://www.bis.org/publ/mktc08.htm>.
- (2013), *Principios para una eficaz agregación de datos sobre riesgos y presentación de informes de riesgos*, Basilea, Banco de Pagos Internacionales, enero, [https://www.bis.org/publ/bcbs239\\_es.pdf](https://www.bis.org/publ/bcbs239_es.pdf).
- (2011), *Principles for Sound Management of Operational Risk*, Basilea, Banco de Pagos Internacionales, junio, <https://www.bis.org/publ/bcbs195.htm>.
- (1998), *Risk Management for Electronic Banking and Electronic Money Activities*, Basilea, Banco de Pagos Internacionales, marzo, pp. 18-20, <https://www.bis.org/publ/bcbssc215.pdf>.
- Broeders, D. y J. Prenio (2018), *Innovative Technology in Financial Supervision (Suptech)—The Experience of Early Users*, notas sobre implementación de políticas de FSI, n.º 9, Ginebra, Financial Stability Board, <https://www.bis.org/fsi/publ/insights9.pdf>.
- Buku, M. y R. Mazer (2017), *Fraud in Mobile Financial Services: Protecting Consumers, Providers and the System*, *Reseña*, Washington, DC, CGAP, <http://www.cgap.org/sites/default/files/Brief-Fraud-in-Mobile-Financial-Services-April-2017.pdf>.
- CPMI (Comité de Pagos e Infraestructuras del Mercado) (2016), *Payment Aspects of Financial Inclusion*, Basilea, Banco de Pagos Internacionales, abril, <https://www.bis.org/cpmi/publ/d144.htm>.
- (2014a), *Non-Banks in Retail Payments*, Basilea, Banco de Pagos Internacionales, septiembre, <https://www.bis.org/cpmi/publ/d118.pdf>.
- (2014b), *Recovery of Financial Market Infrastructures*, Basilea, Banco de Pagos Internacionales, octubre, <https://www.bis.org/cpmi/publ/d121.pdf>.

- (2012), *Principios aplicables a las infraestructuras del mercado financiero*, Basilea, Banco de Pagos Internacionales, abril, [https://www.bis.org/cpmi/publ/d101\\_es.pdf](https://www.bis.org/cpmi/publ/d101_es.pdf).
- (2001), *Principios Básicos para los sistemas de pago de importancia sistémica*, Basilea, Banco de Pagos Internacionales, enero, <https://www.bis.org/cpmi/publ/d43es.pdf>.
- (2000), *Clearing and Settlement Arrangements for Retail Payments in Selected Countries*, Basilea, Banco de Pagos Internacionales, septiembre, <https://www.bis.org/cpmi/publ/d40.pdf>.
- Dias, D. (2018), *SupTech: Leveraging Technology for Better Supervision*, Toronto, Toronto Centre, julio, <http://res.torontocentre.org/guidedocs/SupTech%20-%20Leveraging%20Technology%20for%20Better%20Supervision.pdf>.
- ENISA (Agencia de Seguridad de las Redes y de la Información de la Unión Europea) (2009), *Cloud Computing Risk Assessment*, noviembre, <https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment>.
- FSB (Consejo de Estabilidad Financiera) (2018), *Stocktake of Remittance Service Providers' Access to Banking Services*, Ginebra, FSB, marzo, <http://www.fsb.org/wp-content/uploads/P160318-3.pdf>.
- (2014), *Key Attributes of Effective Resolution Regimes for Financial Institutions*, Ginebra, FSB, octubre, [http://www.fsb.org/wp-content/uploads/r\\_111104cc.pdf](http://www.fsb.org/wp-content/uploads/r_111104cc.pdf).
- G7 (Grupo de los Siete) (2016), *G7 Fundamental Elements of Cybersecurity for the Financial Sector*, [https://www.ecb.europa.eu/paym/pol/shared/pdf/G7\\_Fundamental\\_Elements\\_Oct\\_2016.pdf](https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf).
- Greenacre, J. y R. P. Buckley (2014), “Using Trusts to Protect Mobile Money Customers”, *Journal of Legal Studies*, pp. 59-78.
- Grupo Banco Mundial (2018), *Financial Sector's Cybersecurity: Regulations and Supervision*, Washington, DC, Grupo Banco Mundial, <http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf>.
- Izaguirre, J. C., T. Lyman, C. Mcguire y D. Grace (2016), *Seguro de depósitos e inclusión financiera digital, Reseña*, Washington, DC, CGAP, <https://www.cgap.org/sites/default/files/researches/documents/Brief-Deposit-Insurance-and-Digital-Financial-Inclusion-Spanish.pdf>.
- Kemp, K. y R. P. Buckley (2017), *Resolution Powers over E-Money Providers*, documento de investigación jurídica de la universidad de Nueva Gales del Sur n.º 49, diciembre, <http://classic.austlii.edu.au/au/journals/UNSWLRS/2017/49.html>.



- Piechocki, M. y T. Dabringhausen (2015). “Reforming Regulatory Reporting: From Templates to Cube”, Irving Fischer Committee on Central Bank Statistics, “Combining Micro and Macro Financial Statistical Data for Financial Stability Analysis: Experiences, Opportunities and Challenges”, Varsovia: BearingPoint, 14 y 15 de diciembre, <http://www.bis.org/ifc/publ/ifcb41o.pdf>.
- Wright, P. (2018), *Risk-Based Supervision*, Toronto, Toronto Centre, marzo, <https://res.torontocentre.org/guidedocs/Risk-Based%20Supervision.pdf>.

## Anexo 3. Material de referencia para supervisores

### Guías, manuales y demás material para supervisores

- AMHK (Autoridad Monetaria de Hong Kong) (2016), *Guideline on Supervision of Stored Value Facility Licensees*, Hong Kong, AMHK, <http://www.hkma.gov.hk/eng/key-functions/international-financial-centre/regulatory-regime-for-svf-and-rps/regulation-of-svf.shtml>.
- Asociación de Bancos de Singapur (2016), *Cloud Computing Implementation Guideline 1.1 for the Financial Industry in Singapore*, Singapur, Asociación de Bancos de Singapur, agosto, <https://abs.org.sg/docs/library/abs-cloud-computing-implementation-guide.pdf>.
- Banco Central de Irlanda (2016), *Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks*, Dublín, Banco Central de Irlanda, <https://www.centralbank.ie/docs/default-source/news-and-media/speeches/cross-industry-guidance-information-technology-cybersecurity-risks.pdf>.
- BCE (Banco Central Europeo) (2018), *Tiber-EU Framework. How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming*, Frankfurt, BCE, mayo, [https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber\\_eu\\_framework.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf).
- CPMI (Comité de Infraestructura de Pagos y Mercados) (2017), *Methodology of the Statistics on Payments and Financial Market Infrastructures in the CPMI Countries*, Red Book Statistics, Ginebra, Banco de Pagos Internacionales. <https://www.bis.org/cpmi/publ/d168.htm>
- Dias, D. (2013), *Aplicación de la protección del consumidor en las economías de mercados emergentes y en desarrollo. Guía técnica para supervisores bancarios*, Washington, DC: CGAP, <https://openknowledge.worldbank.org/handle/10986/21825>.
- FDIC (Corporación Federal de Garantía de Depósitos de Estados Unidos) (2016), *Information Technology Risk Examination (InTREx). Information Technology Profile*, plantilla para el examen de riesgos informáticos, julio, <https://www.fdic.gov/news/news/financial/2016/fil16043a.pdf>.

- (2015), “Internal Routine and Controls”, *Security Safety Manual RMS Manual of Examination Policies*, marzo, <https://www.fdic.gov/regulations/safety/manual/section4-2.pdf>.
- FFIEC (Consejo Federal de Examen de Instituciones Financieras), “Appendix A. Examination Procedures”, *IT Examination Handbook, Retail Payments Systems*, <https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-a-examination-procedures.aspx>.
- , “Appendix E: Mobile Financial Services on e-mobile Services”, *IT Examination Handbook, Retail Payments Systems*, <https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-e-mobile-financial-services.aspx>.
- , “Business Continuity Planning”, *IT Examination Handbook, Retail Payments Systems*, <https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management/operational-risk/business-continuity-planning.aspx>.
- . “Principles of the Business Continuity Testing Program”, *IT Examination Handbook, Business Continuity Planning*, <https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/risk-monitoring-and-testing/principles-of-the-business-continuity-testing-program.aspx>.
- Sistema de la Reserva General de Estados Unidos, Junta de Gobernadores, “Interagency Guidelines Establishing Information Security Standards”, <https://www.federalreserve.gov/supervisionreg/interagencyguidelines.htm>.
- , “Interagency Guidelines Establishing Information Security Standards”, <https://www.federalreserve.gov/supervisionreg/interagencyguidelines.htm>.

### Otras guías

- ABE (Autoridad Bancaria Europea) (2017), “Guidance for the Use of Cloud Service Providers”, Frankfurt, ABE, diciembre, <https://eba.europa.eu/-/eba-issues-guidance-for-the-use-of-cloud-service-providers-by-financial-institutions>.
- CGAP (2018), *Cybersecurity for Mobile Financial Services: FAQs for Regulators, Supervisory Authorities and Digital Financial Services Providers*, <https://www.cgap.org/events/cybersecurity-mobile-financial-services>.
- CPMI (Comité de Pagos e Infraestructuras del Mercado) e IOSCO (Organización Internacional de Comisiones de Valores) (2016), *CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures*, Basilea, Banco de Pagos Internacionales, <https://www.bis.org/cpmi/publ/d146.pdf>.

- (2014), *Principles for Financial Market Infrastructures: Assessment Methodology for Oversight Expectations Applicable to Critical Service Providers*, Basilea, Banco de Pagos Internacionales, diciembre, <https://www.bis.org/cpmi/publ/d123.pdf>.
- FCA (Financial Conduct Authority) (2006), *Mystery Shopping Guide*, Londres, FCA, noviembre, <https://www.fca.org.uk/publication/archive/fsa-mystery-shopping-guide.pdf>.
- IFC (Corporación Financiera Internacional) y Mastercard Foundation (2016), *Manual de servicios financieros digitales y gestión de riesgo*, Washington, DC: IFC, pp. 28-39, 48-53, 68-86, 93, 95-108, [https://www.findevgateway.org/sites/default/files/publication\\_files/es\\_ifc\\_risk\\_handbook\\_spanish\\_final.pdf](https://www.findevgateway.org/sites/default/files/publication_files/es_ifc_risk_handbook_spanish_final.pdf)
- Kerse, M. y S. Staschen (2018), *Safeguarding Rules for Customer Funds Held by EMIs*, nota técnica. Washington, DC: CGAP.
- Mazer, R., X. Gine y C. Martinez (2015), *Mystery Shopping for Financial Services*, Washington, DC, CGAP, <https://www.cgap.org/research/publication/mystery-shopping-financial-services>.
- SEC (Securities and Exchange Commission) (2017), “Observations from Cybersecurity Examinations”, *National Exam Program Risk Alert*, volumen VI, número 5, 7 de agosto, <https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf>.
- USAID (Agencia de los Estados Unidos para el Desarrollo Internacional) y Kenya School of Monetary Studies (2010), *Mobile Financial Services Risk Matrix*, Washington, DC, USAID y Escuela de Estudios Monetarios de Kenya, pp. 30-39. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilefinancialservicesriskmatrix100723.pdf>.

## Ejemplos de revisiones temáticas

### *Autoridad de Conducta Financiera del Reino Unido*

- Seguro de teléfonos móviles: <https://www.fca.org.uk/publication/thematic-reviews/mobile-phone-findings.pdf>.
- Tratamiento de consumidores que se vieron afectados por operaciones no autorizadas: <https://www.fca.org.uk/publication/thematic-reviews/tr15-10.pdf>.



