



Definición y promoción de la excelencia en la prestación de servicios de dinero móvil



Tabla de Contenidos

Introducción	2
Principio 1: Salvaguarda de Fondos	4
Principio 2: Prevención del Fraude/ ALA/ CFT	5
Principio 3: Gestión de Personal	6
Principio 4: Calidad de Operaciones	7
Principio 5: Seguridad de Sistemas	8
Principio 6: Transparencia	9
Principio 7: Servicio al Cliente	10
Principio 8: Privacidad de Datos	11
Anexo: Definición de Dinero Móvil	12

Introducción



La GSMA Mobile Money Certification

La GSMA Mobile Money Certification es una iniciativa mundial para ofrecer servicios financieros seguros, transparentes y resilientes y millones de usuarios del dinero móvil en todo el mundo.

Durante la última década, el dinero móvil pasó de ser un producto de nicho disponible solo en unos pocos mercados a convertirse en un fenómeno presente en los mercados emergentes, que ofrece servicios financieros confiables a poblaciones anteriormente no bancarizadas. El dinero móvil ha evolucionado hasta convertirse en la plataforma de pagos líder para la economía digital en muchos mercados emergentes. Con 866 millones de cuentas registradas hasta diciembre de 2018, ahora la industria está procesando más de \$1.3 mil millones por día.

La confianza ha sido un ingrediente clave para el éxito del dinero móvil. La Certificación ayudará a que la industria llegue al próximo nivel al mejorar la calidad de los servicios y la satisfacción del cliente, facilitando la implementación de asociaciones de confianza, desarrollando confianza con los reguladores y promoviendo la implementación de normas reglamentarias adecuadas y proporcionales.

Antecedentes

La GSMA Mobile Money Certification es el resultado de años de colaboración entre la GSMA y la industria del dinero móvil para aumentar la confianza y la transparencia en la prestación de servicios de dinero móvil. A partir del lanzamiento del Código de Conducta de la GSMA a fines de 2014, la GSMA trabajó junto con proveedores de África, América Latina y Asia para entender los desafíos de sus negocios y las mejores prácticas de estos mercados.

Para desarrollar los criterios de la Certificación, la GSMA llevó a cabo un proceso de consulta de tres años con la participación de proveedores de dinero móvil y consultores expertos independientes. Los criterios fueron desarrollados y probados a través de las autoevaluaciones de 39 proveedores de dinero móvil. En 2017, la GSMA contrató a Alliances Management, una compañía de gestión de certificaciones, para gestionar el esquema.

Los beneficios de la Certificación

Las organizaciones certificadas están a la vanguardia de la industria del dinero móvil. Han demostrado seriedad para proteger los derechos de los consumidores, ofreciendo servicios confiables y seguros y combatiendo el lavado de activos y el financiamiento del terrorismo. Y sus prácticas comerciales se ubican entre las mejores de la industria.

Básicamente, la Certificación consiste en aumentar la confianza y brindar herramientas a los consumidores para que tomen decisiones más informadas sobre sus servicios financieros. Esto alienta la adopción del dinero móvil y promueve la inclusión financiera. Ofrece garantías a los socios financieros potenciales de que existen controles robustos, facilitando la interoperabilidad y promoviendo la integración al ecosistema financiero.

También aumentará el potencial de colaborar, innovar e integrarse con socios comerciales.

Al ofrecer una definición de la mejor práctica de la industria, el objetivo de esta Certificación es desarrollar confianza con los reguladores y promover la implementación de normas reglamentarias adecuadas y proporcionales. El interés compartido por el sector privado, los gobiernos, los reguladores y los consumidores es aumentar la confianza en el dinero móvil. La sociedad en general tiene probabilidades de obtener beneficios gracias a la digitalización de los servicios financieros.

Los Principios de la Certificación

La Certificación consta de ocho principios que, a su vez, están divididos en subprincipios. Estos principios se explican en detalle en el cuerpo del presente documento. Los ocho principios son:

1. Salvaguarda de Fondos:	Salvaguardar los fondos de los clientes contra el riesgo de pérdida
2. Fraude/ ALA/ CFT:	Combatir el lavado de activos, el financiamiento del terrorismo y el fraude
3. Gestión de Personal:	Gestionar adecuadamente el personal, agentes y terceros
4. Calidad de Operaciones:	Operar el servicio de manera correcta y confiablemente
5. Seguridad de Sistema:	Proteger la seguridad de los sistemas que soportan el servicio
6. Transparencia:	Comunicar las tarifas, los términos y condiciones y toda la información relevante de manera transparente a los clientes
7. Servicio al Cliente:	Atender de manera efectiva las solicitudes y reclamos de servicio al cliente
8. Privacidad de Datos:	Proteger los datos personales de los clientes

El proceso de Certificación



Para más información sobre la Certificación de Dinero Móvil de la GSMA, incluyendo los detalles del proceso de certificación, visitar gsmamobilemoneycertification.com o enviar un correo electrónico a mm@gsmamobilemoneycert.com.

Principio 1: Salvaguarda de Fondos



Safeguard customer funds against the risk of loss

1.1 Protección contra pérdidas debido a la quiebra de un banco, proveedor u otra parte

Los proveedores deberán tomar medidas para asegurarse de que los fondos se encuentren protegidos ante la insolvencia del proveedor, del banco custodiante u otra entidad

- 1.1.1 Los proveedores deberán asegurarse de mantener fondos equivalentes al valor total de los pasivos de dinero móvil pendientes, en una o más cuentas de custodia, a favor de los usuarios de dinero móvil
- 1.1.2 Los proveedores deberán asegurarse de que los fondos de los usuarios se encuentren legalmente protegidos para prevenir su embargo por parte de acreedores del proveedor, en caso de insolvencia
- 1.1.3 Los proveedores deberán tomar medidas para mitigar el riesgo de pérdidas de fondos debido a la insolvencia del banco, del emisor de bonos u otra entidad en la que se hayan invertido los fondos

1.2 Protección contra el riesgo de liquidación

Los proveedores deberán tomar medidas para asegurarse de que los fondos no corran riesgos debido al proceso de liquidación con bancos y otros asociados financieros

- 1.2.1 De ser factible, los proveedores solo deberán autorizar transacciones de los clientes cuando el débito y el crédito de las cuentas de dinero móvil sean procesados en tiempo real
- 1.2.2 Los proveedores deberán conciliar regularmente las transacciones y liquidar los saldos con sus asociados del ecosistema financiero*

* Para los propósitos del Código, los "asociados del ecosistema financiero" son entidades que están conectadas a los servicios de dinero móvil a fin de proporcionar un servicio financiero. Los ejemplos incluyen, pero no se limitan a, bancos (bancos de custodia) y otros bancos titulares de cuentas, entidades que envían o reciben pagos en bloque, agregadores, comerciantes que utilizan dispositivos de Punto de Venta, proveedores de cajeros automáticos y otros proveedores de servicios de pago (nacionales e internacionales).

Principio 2: Fraude/ ALA/ CFT Prevención



Combatir el lavado de activos, la financiación del terrorismo y el fraude

2.1 Políticas y procedimientos efectivos de ALA/CFT

Los proveedores deberán desarrollar políticas y procedimientos para combatir el lavado de activos y la financiación del terrorismo (ALA/CFT)

2.2 Compromiso de los cargos directivos con ALA/CFT

Los cargos directivos deberán demostrar su compromiso con el cumplimiento de ALA/CFT a través de una supervisión apropiada

2.3 Nombramiento de un gerente para ALA/CFT (director de reporte de lavado de activos)

Los proveedores deberán nombrar un director de reporte de lavado de activos (MLRO por sus siglas en inglés) para promover y supervisar el cumplimiento de las obligaciones relacionadas con ALA/CFT

2.4 Software para monitorear las transacciones

Los proveedores deberán crear un sistema para monitorear las transacciones con fines de prevenir y combatir el lavado de dinero, el financiamiento del terrorismo (ALA/CFT) y el fraude.

2.5 Requisitos de conocimiento del cliente basados en riesgos y límites de transacciones / saldos

Los proveedores deberán obtener conocimiento y verificación del cliente, y aplicar límites o bloqueos de transacciones o saldos basados en riesgos

2.5.1 Los proveedores deberán identificar adecuadamente a sus clientes

2.5.2 Los proveedores deberán establecer límites adecuados para las transacciones y saldos basados en el riesgo, dependiendo de la confiabilidad de los procesos de identificación y verificación del cliente.

2.5.3 Los proveedores deberán tener la capacidad para bloquear las transacciones de cuentas bajo ciertas circunstancias

2.5.4 Los proveedores deberán verificar que los titulares de sus cuentas no se encuentren en listas locales ni internacionales de vigilancia del lavado de dinero, del financiamiento del terrorismo y de sanciones

2.6 Procedimientos de capacitación del personal y agentes acerca de ALA/CFT

Los proveedores deberán capacitar al personal y los agentes acerca de los procedimientos de ALA/CFT, supervisar su cumplimiento y tomar medidas contra infracciones

2.6.1 Los proveedores deberán asegurarse de que el personal y los agentes estén adecuadamente capacitados en los procedimientos de ALA/CFT

2.6.2 Los proveedores deberán supervisar el cumplimiento por parte del personal y los agentes de los procedimientos de ALA/CFT

2.7 Administración del fraude

Los proveedores deberán desarrollar políticas y medidas basadas en riesgos para la detección y prevención del fraude

Principio 3: Gestión de Personal



Administrar adecuadamente el personal, agentes y terceros

3.1 Políticas y procedimientos de debida diligencia

Los proveedores deberán llevar a cabo una adecuada debida diligencia del personal, agentes y entidades potenciales que proporcionen servicios subcontratados

3.2 Capacitación del personal y los agentes

Los proveedores deberán desarrollar e implementar programas de capacitación para el personal y los agentes

3.2.1 Los proveedores deberán desarrollar e implementar programas de capacitación para el personal

3.2.2 Los proveedores deberán desarrollar e implementar programas de capacitación para los agentes

3.3 Acuerdos contractuales

Los proveedores deberán establecer acuerdos por escrito que regulen sus relaciones con los agentes y las entidades que proporcionan servicios subcontratados

3.3.1 Los proveedores deberán establecer acuerdos por escrito que regulen sus relaciones con los agentes y las entidades que proporcionan servicios subcontratados

3.3.2 Los proveedores deberán asumir la responsabilidad por las acciones realizadas en su nombre por sus agentes (y cualquier subagente) bajo el contrato entre proveedor y agente

3.4 Administración de personal, agentes y entidades que proporcionan servicios subcontratados

Los proveedores deberán desarrollar políticas y procedimientos para una continua administración y supervisión del personal, agentes y entidades que proporcionen servicios subcontratados



Principio 4: Calidad de Operaciones

Operar el servicio de manera correcta y confiable

4.1 Supervisión por parte de la junta directiva y la gerencia superior del servicio de Dinero Móvil

Los proveedores deberán asegurarse de que la Junta Directiva y la gerencia superior establezcan una efectiva supervisión gerencial

4.2 Administración y presentación de informes a nivel de servicios

Los proveedores deberán administrar las operaciones técnicas y comerciales según los niveles de servicios

4.2.1 Los proveedores y asociados deberán operar los servicios técnicos de manera correcta y administrar los niveles de servicios

4.2.2 Los proveedores y asociados deberán administrar las operaciones comerciales y niveles de servicios

4.3 Administración de capacidades

Los proveedores deberán tomar medidas para asegurar una capacidad suficiente del servicio mediante pronósticos, monitoreos y pruebas

4.4 Manejo de incidentes y problemas

Los proveedores deberán establecer un proceso para manejar incidentes, a fin de restablecer el servicio dentro de los niveles de servicios acordados e investigar la causa de los problemas

4.5 Manejo de cambios y configuración

Los proveedores deberán desarrollar procesos para asegurar la solidez y seguridad de los sistemas y aplicaciones después de realizar cambios en el sistema y la configuración

4.6 Administración del riesgo empresarial

Los proveedores deberán establecer una estructura para la administración de riesgos a fin de identificar, evaluar y controlar los riesgos

4.7 Continuidad del negocio

Los proveedores deberán desarrollar planes de contingencia para una efectiva continuidad del negocio

Principio 5: Seguridad de Sistemas



Proteger la seguridad de los sistemas que soportan el servicio

5.1 Gobernanza de la seguridad

Los proveedores deberán implementar mecanismos de gobernanza para asegurarse de que se definan e implementen políticas de seguridad de manera continua

- 5.1.1 Los proveedores deberán desarrollar, implementar y revisar constantemente políticas formales de seguridad para los servicios de dinero móvil
- 5.1.2 Los proveedores deberán entrenar al personal en cuanto a las responsabilidades de seguridad
- 5.1.3 Los proveedores deberán asegurarse de que hay políticas establecidas para un manejo seguro de la información y los activos
- 5.1.4 Los proveedores deberán asegurar la protección de sus activos a los que pueden acceder los proveedores y terceras partes

5.2 Diseño y desarrollo de sistemas, aplicaciones y redes seguros

Los proveedores deberán asegurarse de que los sistemas, aplicaciones y red que soportan dinero móvil se han diseñado y desarrollado con seguridad

- 5.2.1 Los proveedores deberán asegurarse de que los datos están protegidos por criptografía y controles de seguridad de la red
- 5.2.2 Los proveedores deberán asegurar que los sistemas y las aplicaciones se han diseñado y desarrollado con seguridad y se han probado cuidadosamente

5.3 Operaciones de seguridad

Los proveedores deberán implementar procesos para el manejo seguro de todos los sistemas y operaciones

- 5.3.1 Los proveedores deberán identificar, evaluar y supervisar los riesgos de seguridad
- 5.3.2 Los proveedores deberán identificar y autenticar adecuadamente a los usuarios del sistema
- 5.3.3 Los proveedores deberán restringir el acceso a los datos de los clientes de acuerdo con “la necesidad de conocerlos”
- 5.3.4 Los proveedores deberán restringir el acceso físico a los sistemas
- 5.3.5 Los proveedores deberán asegurar la correcta y segura operación del procesamiento de la información
- 5.3.6 Los proveedores deberán establecer procesos para asegurar que todas las transacciones y actividades del usuario están registradas con apropiados registros de auditoría
- 5.3.7 Los proveedores deberán probar regularmente los sistemas y procesos de seguridad
- 5.3.8 Los proveedores deberán garantizar la continuidad de la seguridad de la información
- 5.3.9 Los proveedores deberán establecer un proceso para identificar, abordar y supervisar los incidentes de seguridad y las quejas relativas a la seguridad

Principio 6: Transparencia



Comunicar las tarifas, los términos y condiciones y toda la información relevante de manera transparente a los clientes

6.1 Efectiva divulgación y transparencia

Los proveedores deberán asegurarse de que se les suministre a los usuarios información clara, oportuna y bien visible, con respecto a los costos, y a los términos y condiciones

6.2 Instrucción a los clientes sobre seguridad

Los proveedores deberán instruir a los clientes sobre la manera de utilizar los servicios de dinero móvil de manera segura

Principio 7: Servicio al Cliente



Atender de manera efectiva las solicitudes y reclamos de servicio al cliente

7.1 Políticas y procedimientos de servicio al cliente

Los proveedores deberán desarrollar y publicar políticas y procedimientos de servicio al cliente

- 7.1.1 Los proveedores deberán desarrollar políticas y procedimientos de servicio al cliente
- 7.1.2 Los proveedores deberán informar a los clientes acerca de políticas y procedimientos de servicio al cliente
- 7.1.3 Los proveedores deberán desarrollar políticas específicas para atender solicitudes de reversión de transacciones

7.2 Disponibilidad de servicio de atención al cliente

Los proveedores deberán suministrar un mecanismo apropiado para que los clientes presenten consultas y problemas

7.3 Mecanismos de recursos externos

Los proveedores deberán especificar los mecanismos de resolución de aquellas disputas que no se solucionen internamente



Principio 8: Privacidad de Datos

Proteger los datos personales de los clientes

8.1 Gobernanza de privacidad de datos

Los proveedores deberán tener buenas prácticas y cumplir con la regulación adecuada que gobierna la privacidad de la información de los clientes

8.2 Transparencia de privacidad de datos

Los proveedores deberán asegurarse de que se les suministre a los usuarios información clara, oportuna y bien visible, con relación a sus prácticas sobre privacidad de la información

8.3 Control de los datos personales de los clientes

Los proveedores deberán asegurarse de que los clientes estén informados acerca de sus derechos y que cuenten con las debidas oportunidades para su ejercicio en relación con el control de su información personal

8.4 Minimización de la recopilación y retención de Datos Personales

Los proveedores deberán limitar la información personal que se recopila de los clientes y que es guardada, utilizada o compartida

Anexo: Definición de Dinero Móvil

El dinero móvil es un servicio transformacional que utiliza tecnologías de la información y comunicación para extender el suministro de servicios financieros a los clientes a los que no se puede llegar a través de los servicios financieros tradicionales basados en sucursales.

En 2018, revisamos nuestra definición de dinero móvil. Ahora consideramos un servicio como dinero móvil si cumple con las siguientes características:

1. El servicio debe incluir la transferencia de dinero y la realización de pagos utilizando un teléfono móvil.
2. El servicio debe estar disponible para los no bancarizados, por ejemplo, aquellas personas que no tienen acceso a una cuenta en una institución financiera.
3. El servicio debe ofrecer una red de puntos físicos para transacción que incluyan agentes, que no sean sucursales bancarias o cajeros automáticos, y que lo hagan ampliamente accesible para todos.
4. Los servicios de banca móvil o servicios de pago (como Apple Pay and Google Wallet) que ofrecen el teléfono móvil como otro canal para acceder a un producto bancario tradicional no se consideran dinero móvil.

Para más información sobre la Certificación del Dinero Móvil de la GSMA, incluyendo los detalles del proceso de certificación, visitar [gsmamobilemoneycertification.com](https://www.gsma.com/mobilemoney/certification)



