Código de Conducta para Proveedores de Dinero Móvil

VERSIÓN 2 - OCTUBRE 2015

Introducción

Este Código de Conducta identifica principios destinados a promover la adopción de prácticas consistentes para la mitigación de riesgos por parte de los proveedores de dinero móvil[1], en áreas fundamentales de su negocio.

Para que el sector del dinero móvil continúe impulsando el crecimiento del ecosistema financiero digital, los proveedores de dinero móvil ("proveedores") han adoptado un Código de Conducta con el propósito de asegurar la solidez de sus servicios, la seguridad del canal y un trato justo del cliente. El Código de Conducta apoyará el continuo crecimiento de la industria:

- Mejorando la calidad de los servicios y la satisfacción del cliente;
- Facilitando la implementación de asociaciones de confianza; y
- Desarrollando la confianza con las autoridades reguladoras y promoviendo la implementación de estándares reguladores apropiados y proporcionados.

Los proveedores que se suscriban al Código formalizan su compromiso con los ocho principios que respaldan tres áreas clave de importancia:

i. solidez de los servicios;

ii. seguridad de la red y el canal móviles; y

iii. un trato justo de los clientes.

Al respaldar el Código, los proveedores se comprometen a[2]:

1. Salvaguardar los fondos de los clientes contra el riesgo de pérdida;
2. Mantener mecanismos efectivos para combatir el lavado de dinero y el financiamiento del terrorismo;
3. Equipar y supervisar al personal, agentes y entidades que proporcionan servicios subcontratados, para asegurar que ofrezcan servicios seguros y confiables;
4. Asegurar la provisión de servicios confiables con suficiente capacidad por parte de la red y del sistema;
5. Tomar fuertes medidas para garantizar que la red y el canal móviles son seguros;
6. Comunicar información clara, suficiente y oportuna para empoderar a los clientes para que tomen decisiones informadas;
7. Desarrollar mecanismos para asegurarse de que se atienden las quejas de manera efectiva y se resuelven los problemas oportunamente; y
8. Seguir buenas prácticas en cuanto a la privacidad de datos, al recoger, procesar y/o transmitir datos personales de los clientes.

UNA NOTA ACERCA DE LAS ENMIENDAS A LA VERSIÓN 2

Se han realizado las siguientes enmiendas a fin de simplificar el Código y asegurar una cobertura completa de todos los temas relevantes.

- Los Subprincipios dentro de los Principios 1, 3, 4 y 5 han sido modificados.
- El Principio 8 se ha reelaborado para aclarar que se refiere a la privacidad de los datos, no a la seguridad de éstos. Los subprincipios continúan sin cambios.
- Los Principios 2, 6 y 7 permanecen sin cambios.

1. Véase el Anexo para una definición de dinero móvil para los fines de este documento.
2. En varios países, las leyes y las regulaciones locales contemplan algunos o la totalidad de los temas identificados en los Principios. Este Código de Conducta identifica buenas prácticas que deben adoptar los proveedores, independientemente de si se lo requiere la regulación local. El Código no altera la responsabilidad de los proveedores de cumplir con los requisitos legales locales. De igual manera, el Código no pretende limitar o de otro modo afectar a los derechos contractuales de los proveedores. .

Principios

Principio 1: Los proveedores de dinero móvil ("proveedores") salvaguardan los fondos de los clientes contra el riesgo de pérdida.

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

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 ("usuarios").

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

1.2.1 De ser factible, los proveedores sólo 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.[3]

3. 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). Estas entidades normalmente se conectarían a los servicios de dinero móvil a través de Interfaces de Aplicación del Programa (API, por sus siglas en inglés).

Principio 2: Los proveedores cuentan con mecanismos efectivos y proporcionales en función del riesgo, para prevenir, detectar y reportar el uso indebido de los servicios con el propósito de lavado de activos o financiamiento del terrorismo (LA/FT).

2.1 Políticas y procedimientos efectivos

2.1.1 Los proveedores deberán desarrollar políticas y procedimientos efectivos para dar cumplimiento a las normas contra el lavado de activos y el financiamiento del terrorismo (ALA/CFT).

2.2 Compromiso de los cargos directivos

2.2.1 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

2.3.1 Los proveedores deberán nombrar a un empleado cualificado para promover y supervisar el cumplimiento de las obligaciones relacionadas con ALA/CFT.

2.4 Software para monitorear las transacciones

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

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

2.5.1 Los proveedores deberán identificar adecuadamente a sus clientes y utilizando un enfoque basado en el riesgo, si las leyes y regulaciones locales lo permiten.

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 que 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

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.

2.6.3 Los proveedores deberán establecer políticas y procedimientos claros para abordar las infracciones de ALA/CFT por parte del personal y los agentes.

Principio 3: Los proveedores seleccionan, capacitan y supervisan al personal, a los agentes y a las entidades que proporcionan servicios subcontratados para asegurar que ofrecen servicios seguros y confiables, y que cumplen con todos los requisitos operacionales y legales relevantes.

3.1 Políticas y procedimientos de debida diligencia

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

3.2 Capacitación

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

3.3 Acuerdos contractuales

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 y supervisión

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

Principio 4: Los proveedores cuentan con políticas y procedimientos bien desarrollados, así como con una capacidad suficiente en sus redes y sistemas para asegurar la provisión confiable de servicios.

4.1 Supervisión por parte de la junta directiva y la gerencia superior

4.1.1 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

4.2.1 Los proveedores deberán desarrollar e implementar sistemas de control y de presentación de informes a nivel de servicios.

4.3 Administración de Capacidades

4.3.1 Los proveedores deberán tomar medidas para asegurar una capacidad suficiente de la red y sistemas, mediante pronósticos, monitoreo y pruebas.

4.4 Manejo de incidentes y problemas

4.4.1 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

4.5.1 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

4.6.1 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

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

Principio 5: Los proveedores toman medidas sólidas para garantizar la seguridad de la red y del canal móvil.

5.1 Gobernanza de la seguridad

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 seleccionar, capacitar y supervisar al personal interno.

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

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 y manejo del fraude de manera contínua

5.3.1 Los proveedores deberán identificar y evaluar los riesgos de seguridad antes de ofrecer servicios de dinero móvil y deberán seguir controlando tales riesgos de manera continua.

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.

5.3.10 Los proveedores deberán establecer políticas basadas en el riesgo y medidas para detectar y prevenir el fraude.

Principio 6: Los proveedores comunican información clara, suficiente, oportuna y de manera tal que los clientes puedan comprender y tomar decisiones informadas.

6.1 Efectiva divulgación y transparencia

6.1.1 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 Seguridad y confiabilidad

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

Principio 7: Los proveedores cuentan con mecanismos para asegurarse de que las quejas se atienden de manera efectiva y los problemas se resuelven oportunamente.

7.1 Políticas y procedimientos para establecer una resolución eficiente de las quejas de los clientes

7.1.1 Los proveedores deberán desarrollar políticas y procedimientos para responder las quejas de los clientes.

7.1.2 Los proveedores deberán informar a los clientes acerca de la existencia de políticas y procedimientos para la atención de sus quejas.

7.1.3 Los proveedores deberán desarrollar normas específicas para atender solicitudes de reversión de transacciones.

7.2 Disponibilidad de servicio de atención al cliente

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

7.3 Mecanismos de recursos externos

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

Principio 8: Los proveedores siguen buenas prácticas de privacidad de datos al recoger, procesar y/o transmitir los datos personales de los clientes.

8.1 Dirección

8.1.1 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 y Notificaciones

8.2.1 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 Elección y Control del Usuario

8.3.1 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.

8.3.2 Los proveedores deberán obtener el consentimiento del cliente ante cualquier evento que afecte significativamente la privacidad de su información personal.

8.4 Minimización de la Recopilación y Retención de Datos

8.4.1 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

Para los propósitos del Código de Conducta, el dinero móvil es un servicio transformacional que utiliza tecnológicas de la información y comunicación (TIC) y canales de distribución no bancarios, para extender el suministro de servicios financieros a los clientes a los que no se puede llegar de manera rentable a través de los servicios financieros tradicionales basados en sucursales. Ejemplos típicos de servicios de dinero móvil son las billeteras electrónicas, que se utilizan para hacer transferencias de persona a persona (P2P, por sus siglas en inglés) y una gama de pagos, o para recibir pagos de salarios o subsidios del gobierno (G2P, por sus siglas en inglés).

Las características clave de un servicio de dinero móvil son:

- Los clientes introducen y extraen dinero del servicio, utilizando una red de agentes, que operan fuera de las sucursales bancarias; y
- Los clientes inician transacciones utilizando una interfaz que está disponible en los teléfonos móviles básicos.

Aunque actualmente no existe una definición regulatoria estándar de dinero móvil y dinero electrónico (e-money) a nivel global, los países que han desarrollado sus propias definiciones, suelen incluir varios elementos comunes. El dinero móvil es un valor monetario que:

- está disponible para que un usuario realice transacciones a través de un dispositivo móvil;
- está aceptado como un medio de pago por otras partes, distintas del usuario;
- es emitido tras la recepción de fondos;
- es registrado de manera electrónica; y
- es redimible por efectivo

En jurisdicciones en donde el dinero electrónico ha sido definido en las regulaciones o la legislación, el dinero móvil es una forma de dinero electrónico.

Para obtener mayor información,
ponerse en contacto con:
mmu@gsma.com
GSMA London Office
T +44 (0) 20 7356 0600