



USAID
FROM THE AMERICAN PEOPLE

BANCA SIN SUCURSALES/DINERO MOVIL: SUPERVISIÓN

USAID/EL SALVADOR IMPROVING ACCESS TO FINANCIAL SERVICES
PROJECT

JULY 2012

This publication was produced for review by the United States Agency for International Development. It was prepared by Ricardo Estrada and Weidemann Associates and submitted by Global Business Solutions, Inc.

BANCA SIN SUCURSALES/DINERO MOVIL: SUPERVISIÓN

USAID/EL SALVADOR IMPROVING ACCESS TO
FINANCIAL SERVICES PROJECT

Submitted by:

Global Business Solutions, Inc.

Authored by:

Ricardo Estrada, Weidemann Associates, Inc.

Submitted to:

USAID/El Salvador

AID-519-C-12-00001

USAID/El Salvador Improving Access to Financial Services Project

DISCLAIMER

The views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

CONTENIDOS

I. RESUMEN EJECUTIVO.....	1
II. ANTECEDENTES.....	1
III. OBJETIVOS DE LA CONSULTORÍA	1
IV. ACTIVIDADES REALIZADAS	2
V. RESULTADOS	2
VI. RECOMENDACIONES	2
ANEXOS.....	4

II. Taller de Administración de Riesgos de SFM (día 1, 31/5/2012)

III. Taller de Modelos Internacionales de Supervisión y Regulación de SFM (día 2, 1/6/2012)

IV. Administración de Riesgos en la Prestación de Servicios Financieros Móviles

V. Modelos Internacionales de Supervisión y Regulación de Servicios Financieros Móviles

VI. Recomendaciones de Supervisión y Regulación de Servicios Financieros Móviles

I. RESUMEN EJECUTIVO

Con el objetivo de apoyar el desarrollo de un marco normativo para regular la prestación de servicios financieros móviles así como el marco de prácticas de supervisión correspondiente, en elaboración por parte de funcionarios del Banco Central de Reserva y de la Superintendencia del Sistema Financiero de El Salvador, se participó en la consultoría de mérito con el objetivo de proporcionar orientación técnica. Para el efecto se realizaron una serie de presentaciones magistrales, se condujeron talleres de trabajo y se participó directamente en la mesa de trabajo encargada de la elaboración de los proyectos de normativa. Dentro de las principales recomendaciones a las que se arribó como resultado y conclusión de la consultoría cabe destacar la importancia de una sólida regulación para fundamentar el modelo de supervisión, así como que se fomente un esquema que permita la existencia de modelos de prestación de servicios financieros móviles bancarios y no bancarios.

II. ANTECEDENTES

El Banco Central de Reserva de El Salvador se ha trazado el objetivo de desarrollar un marco normativo para regular la prestación de servicios financieros móviles, los cuales incluyen la banca móvil y el dinero electrónico, durante el año 2012. Esto con la intención de crear un ambiente regulatorio que incluya los aspectos prudenciales pertinentes más importantes, destacando entre ellos la efectiva supervisión de las actividades de las entidades participantes del ecosistema de servicios financieros móviles implementado. Como parte de estos esfuerzos, representantes del Banco Central de Reserva –BCR- y de la Superintendencia del Sistema Financiero –SSF-, de El Salvador, realizaron en marzo de 2012 un viaje de intercambio de conocimientos sobre la materia hacia Colombia y Paraguay. Después de su retorno, estos funcionarios se encuentran participando activamente en una serie de talleres y actividades técnicas de formación, las cuales han tenido lugar desde abril hasta junio del año en curso.

III. OBJETIVOS DE LA CONSULTORÍA

El objetivo principal de la consultoría sobre Supervisión fue proporcionar orientación técnica para los funcionarios del BCR y de la SSF que están participando en el desarrollo del marco regulatorio necesario así como en los planes de supervisión, todo enmarcado en la actividad de prestación de servicios financieros móviles.

Los objetivos específicos de la consultoría fueron los siguientes:

- Presentar y discutir los diferentes modelos de negocio sobre servicios financieros móviles así como su regulación y supervisión, en el contexto de esfuerzos para la inclusión financiera.
- Presentar los principales riesgos asumidos en la prestación de servicios financieros móviles, dando particular énfasis en los riesgos operativo y tecnológico, así como las modalidades de gestión de los mismos.
- Desarrollar mediante talleres de trabajo, conjuntamente con los participantes, propuestas de modelos de administración de riesgos, marcos de supervisión, y contenidos mínimos de la normativa por desarrollarse para El Salvador en la materia de mérito.
- Presentar modelos internacionales de supervisión y regulación destacados.

- Colaborar, conjuntamente con los funcionarios participantes y con el consultor principal, en la elaboración de proyectos de normativa para regular los servicios financieros móviles desde una perspectiva de modelos abiertos, es decir, modelos liderados por entidades bancarias y por entidades no bancarias.

IV. ACTIVIDADES REALIZADAS

Como parte del trabajo en El Salvador realizado presencialmente entre el 30 de mayo y el 4 de junio, se realizaron una serie de presentaciones magistrales, se condujeron talleres de trabajo y se participó directamente en la mesa de trabajo encargada de la elaboración de los proyectos de normativa. Para leer los detalles de las presentaciones vea el anexo indicado:

- Presentación magistral del tema “Administración de Riesgos en la Prestación de Servicios Financieros Móviles”. (Anexo 1)
- Presentación magistral del tema “Modelos Internacionales de Supervisión y Regulación de Servicios Financieros Móviles”. (Anexo 2)
- Conducción del taller sobre políticas o disposiciones para gestionar el riesgo tecnológico proveniente de la prestación de Servicios Financieros Móviles, considerando la temática discutida. (Anexo 3)
- Conducción del taller sobre desarrollo del bosquejo de la Norma para regular a los Corresponsales Bancarios, la Norma para regular los Servicios Financieros Móviles y de Prácticas y procedimientos para la supervisión de los proveedores de Servicios Financieros Móviles. (Anexo 4)
- Presentación magistral del tema “Recomendaciones de Supervisión y Regulación de Servicios Financieros Móviles” enfocado en el caso de El Salvador. (Anexo 5)
- Participación directa, conjuntamente con el Consultor Principal y los funcionarios designados del BCR y de la SSF, en las mesas de trabajo de desarrollo de proyectos de normativa.

V. RESULTADOS

Dentro de los resultados cabe mencionar el desarrollo y conclusión exitosa de cada una de las presentaciones magistrales, la preparación de dos documentos que reúne todas las propuestas elaboradas por los participantes de los dos talleres efectuados, así como la preparación de los proyectos de normativa relacionados con la prestación de los servicios financieros móviles. En particular los proyectos relacionados con los Agentes Financieros (corresponsales bancarios) y de Pagos Móviles.

VI. RECOMENDACIONES

Derivado de la interacción del consultor con los participantes en las distintas actividades realizadas fue posible determinar las siguientes recomendaciones atendiendo los aspectos más relevantes del tema en cuestión:

- Es importante comprender que el punto de partida para la supervisión de los Servicios Financieros Móviles, debe ser desarrollar un marco regulatorio sólido.
- Es necesario un marco regulatorio que además de ser prudencial y de abordar temas de administración de riesgos, también fomente la inclusión financiera, y para lograr esto, es

importante que el marco regulatorio permita la entrada de varios participantes del mercado y permita la existencia de modelos bancarios y no bancarios.

- Es importante que la superintendencia, como órgano supervisor del sistema financiero, se coordine estrechamente con el banco central, por ser el regulador del sistema de pagos. Ambas instituciones tienen un interés directo respecto del sano desarrollo de los servicios financieros móviles.
- Es recomendable también que se forme un grupo de especialistas en esta materia, que es muy específica y novedosa. Asimismo, que se realice supervisión extra situ, es decir de gabinete o remota, y también supervisión in situ o supervisión de campo. Esto con el afán de que los especialistas visiten a las entidades que están proporcionando el servicio para verificar que se cumplan las normativas y que las prácticas de gestión de riesgo sean las más adecuadas.

ANEXOS

- I. Taller de Administración de Riesgos de SFM (día 1, 31/5/2012)**
- II. Taller de Modelos Internacionales de Supervisión y Regulación de SFM (día 2, 1/6/2012)**
- III. Administración de Riesgos en la Prestación de Servicios Financieros Móviles**
- IV. Modelos Internacionales de Supervisión y Regulación de Servicios Financieros Móviles**
- V. Recomendaciones de Supervisión y Regulación de Servicios Financieros Móviles**

ANNEX I: ADMINISTRACIÓN DE RIESGOS EN LA PRESTACIÓN DE SERVICIOS FINANCIEROS MÓVILES

CONTENIDO

1. Conceptos fundamentales
2. Modelos de negocio de SFM
3. Proceso de Administración de Riesgos
4. Administración del Riesgo Tecnológico SFM

Conceptos fundamentales

- **Banca sin sucursales (*branchless banking*):** el suministro de servicios financieros fuera de las sucursales bancarias tradicionales, utilizando agentes u otros intermediarios como el principal contacto con los clientes, aprovechando tecnologías como terminales POS y teléfonos móviles para transmitir los detalles de las transacciones.
- **Servicios Financieros Móviles:** la utilización de un teléfono móvil para tener acceso a servicios financieros y ejecutar transacciones financieras. Incluye tanto a la banca móvil como a los pagos móviles.
- **Banca móvil (*m-banking*):** la utilización de un teléfono móvil para tener acceso a servicios bancarios y ejecutar transacciones financieras. Comúnmente se aplica a clientes con cuentas bancarias. Es un subcomponente del concepto de banca electrónica.
- **Dinero móvil (*m-money*):** un tipo de servicio electrónico transaccional que se ejecuta con redes móviles. El emisor del dinero móvil puede ser un operador de telefonía o un tercero, como un banco. Frecuentemente utilizado como un sinónimo de SFM.
- **Dinero electrónico (*e-money*):** un tipo de valor monetario registrado electrónicamente y que es (i) emitido contra la recepción de fondos por un monto equivalente, (ii) almacenado en un dispositivo electrónico (e.g. un chip, tarjeta prepagada, teléfono móvil o computadora), (iii) aceptado como un medio de pago por terceros distintos del emisor, y (iv) convertible a efectivo.
- **Cuenta de dinero electrónico:** una cuenta del titular mantenida con el emisor del dinero electrónico. Los fondos que respaldan estas cuentas pueden ser agrupados con otros fondos del mismo emisor de dinero electrónico y colocarse en una cuenta bancaria, o bien en un fideicomiso.
- **Emisor de dinero electrónico:** la entidad que inicialmente emite el dinero electrónico contra la recepción de fondos.
- **Aislamiento de fondos (*funds isolation*):** medidas destinadas a aislar los fondos de los clientes (recibidos para la emisión de dinero electrónico) de otros fondos que puedan ser requeridos por

el emisor o los acreedores del emisor. Conjuntamente con las medidas de protección son el medio primordial de protección de fondos en un modelo nonbank-based.

- **Protección de fondos (*funds safeguarding*):** medidas destinadas a asegurar que los fondos estén disponibles para atender el requerimiento de efectivo a cambio de valor electrónico. Típicamente estas medidas incluyen (i) restricciones en el uso de los fondos, (ii) requerimiento de que dichos fondos se coloquen en cuentas bancarias o inversiones en activos líquidos, y (iii) diversificación del *float* en distintas instituciones financieras.
- **Debida diligencia al cliente:** políticas y procedimientos de una institución financiera para obtener información del cliente y evaluar que dicha información sea útil para detectar, monitorear y reportar actividades sospechosas. Incluye las medidas KYC que pretenden identificar al cliente y sus motivaciones para realizar actividades financieras.
- **Debida diligencia al agente:** las medidas emprendidas por un proveedor de SFM para evaluar agentes potenciales y su capacidad para llevar a cabo funciones propias de agente en un esquema de SFM. Debido a que los agentes por lo general están exentos de límites transaccionales, regulatorios o no regulatorios, se requiere una mayor debida diligencia a los agentes en comparación con la de los clientes.
- **Inteconectividad:** la capacidad de habilitar la conexión técnica entre dos o más esquemas de modelos de negocio de SFM, tales como el de un banco o un proveedor de servicios de pagos conectándose a una red internacional de pagos. Requiere procesos de certificación.
- **Interoperabilidad:** una situación en la cual los instrumentos de pago pertenecientes a un esquema de modelo de negocio de SFM pueden ser utilizados por otros sistemas e instalados en otros esquemas. Requiere convenios comerciales.

1. Modelos de negocio de SFM

- **Modelo bank-based:** Modelo de negocio de SFM (sea o no sea bank-led) en el cual (i) el cliente tiene una relación contractual con el banco y (ii) el banco tiene autorización del regulador para ofrecer el servicio.
- **Modelo bank-led:** Modelo de negocio de SFM (sea o no sea bank-based) en el cual el banco es quien principalmente dirige el producto o servicio, liderando labores de mercadeo, manejo de la marca y gestión de la relación con el cliente.
- **Modelo nonbank-based:** Modelo de negocio de SFM (sea o no sea nonbank-led) en el cual (i) el cliente tiene una relación contractual con una institución no bancaria y (ii) dicha institución tiene autorización del regulador para ofrecer el servicio.
- **Modelo nonbank-led:** Modelo de negocio de SFM (sea o no sea nonbank-based) en el cual la institución no bancaria es quien principalmente dirige el producto o servicio, liderando labores de mercadeo, manejo de la marca y gestión de la relación con el cliente.

2. Proceso de Administración de Riesgos

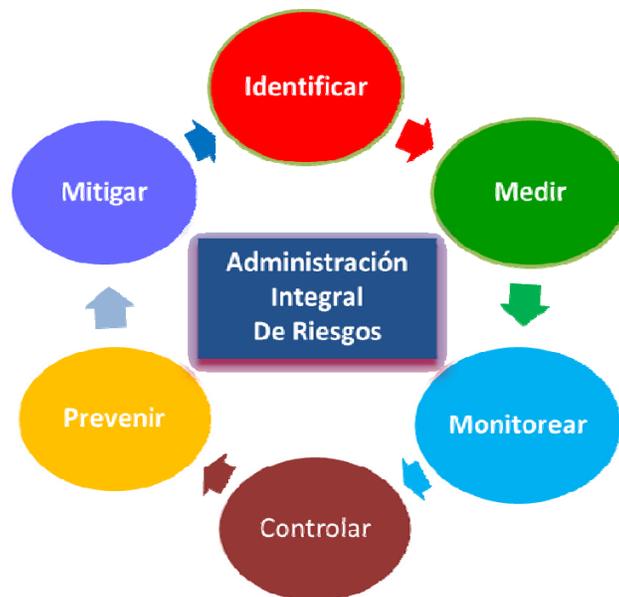
En la prestación de SFM la confiabilidad y la credibilidad son fundamentales.

La administración de riesgos es indispensable tanto en entidades bancarias como en no bancarias. Algunos de los principales riesgos asumidos:



PRINCIPIOS BÁSICOS PARA UNA SUPERVISIÓN BANCARIA EFICAZ COMITÉ DE BASILEA (Octubre 2006)

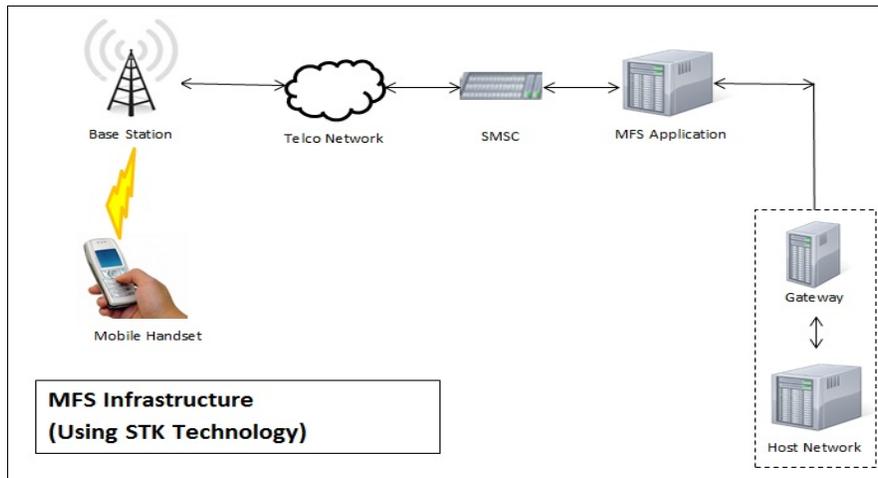
- Principio 7 – Proceso para la gestión del riesgo: los supervisores deben tener constancia de que los bancos y grupos bancarios cuentan con un proceso integral de gestión de riesgos (que incluya la vigilancia por el Consejo y la alta dirección) para identificar, evaluar, vigilar y controlar o mitigar todos los riesgos sustanciales y para evaluar su suficiencia de capital global con respecto a su perfil de riesgo. Estos procesos han de ser proporcionales a las dimensiones y complejidad de la institución.
- Principio 15 – Riesgo operacional: los supervisores deben tener constancia de que los bancos cuentan con políticas y procesos de gestión de riesgos para identificar, evaluar, vigilar y controlar/mitigar el riesgo operacional. Estas políticas y procesos han de ser proporcionales a las dimensiones y complejidad del banco en cuestión.



3. Administración del Riesgo Tecnológico de SFM

- **Riesgo operacional:** El riesgo de sufrir pérdidas debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal.
- **Riesgo Tecnológico:** Es la posibilidad de que la interrupción, alteración, o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, provoque pérdidas financieras a la institución.

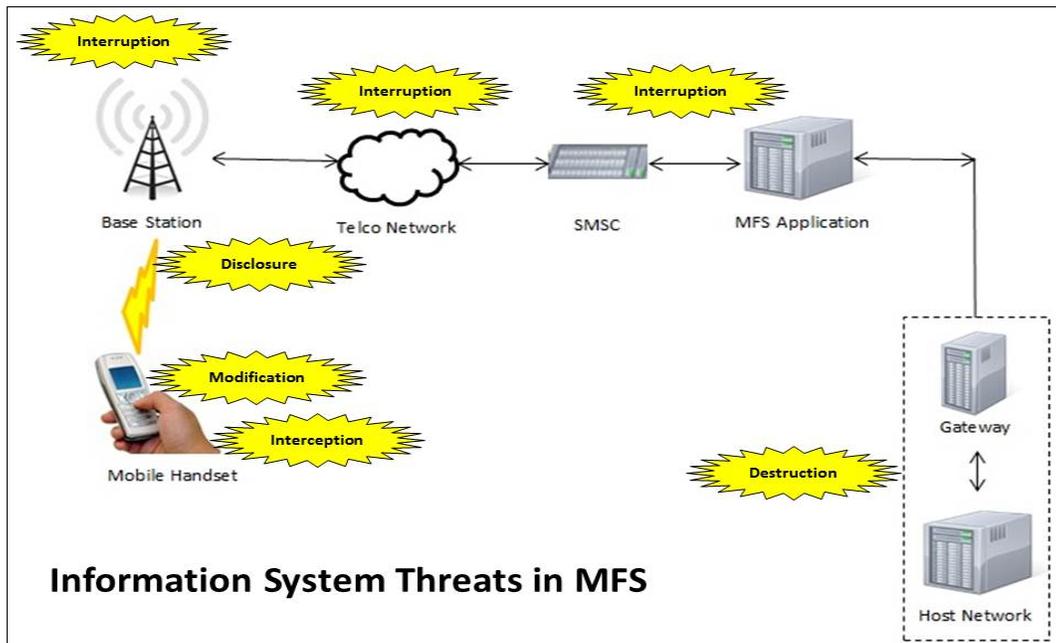
Flujo de información en un esquema de SFM



Los eventos de riesgo tecnológico en SFM pueden ser organizados en las siguientes 6 amenazas:

1. **Modificación:** la información en el sistema es accesada y cambiada sin autorización. Ocurre durante el almacenamiento, transmisión o cambio de hardware, o cuando se altera el software.
2. **Destrucción:** el hardware, el software, la información o el canal es dañado, destruido o perdido.
3. **Revelación:** la información es revelada sin el consentimiento del propietario.
4. **Intercepción:** acceso no autorizado a recursos de la información lo que permite que se copien programas u otra información confidencial.
5. **Interrupción:** el servicio o los recursos quedan no disponibles para su uso, accidental o intencionalmente. Se borran programas o algunas de sus funcionalidades.
6. **Fabricación:** transacciones falsas son insertadas en un registro o adicionadas a la base de datos por un usuario no autorizado.

Flujo de información en un esquema de SFM y sus posibles amenazas



La Administración del Riesgo Tecnológico en SFM se basa en 5 principios clave:

- 1. Confidencialidad:** la protección de los datos del usuario del acceso no autorizado o del robo.
 - La información financiera requiere estándares de cifrado, almacenamiento y transmisión; la no financiera firewalls, sistemas de detección y prevención de intrusos y controles de acceso.
 - Los PINs deben guardarse de forma cifrada y no estar disponibles al staff del proveedor del servicio.
 - Estándares de criptografía deben aplicarse a la transmisión de datos por redes públicas como internet o redes de móviles.
- 2. Integridad:** que la información esté completa, exacta y confiable.
 - Para validar la integridad de la información se debe verificar el proceso que identifica campos vacíos, ejecuta chequeos de secuencia, longitud y exactitud de las variables.
- 3. Disponibilidad:** la accesibilidad a los datos cuando los usuarios necesitan utilizar los SFM.
 - Muchos escenarios pueden afectar este principio tales como calamidades naturales, cortes de energía, o acciones maliciosas como ataques.
- 4. Autenticación:** establecer la identidad de los usuarios y del proveedor del servicio.
 - Incluye incorporar control de accesos, control de permisos y autenticación de passwords.
 - Bitácoras o registros de auditoría para evaluar la validez y la consistencia de los datos en la red y para verificar que los comandos se han ejecutado por usuarios legítimos.

- Procedimientos administrativos para controlar el acceso a la información de los clientes; y comprender las vulnerabilidades de los sistemas, iniciando desde el flujo de la información.
5. **No repudio:** es la manera en la que el proveedor del servicio se protege de una posible conducta abusiva del consumidor, para asegurar conclusión y seguridad.
- Evita que un individuo niegue haber ejecutado una acción particular, al hacerlo aceptar los términos y condiciones del servicio de forma previa.
 - La utilización de firmas digitales previene que los individuos rechacen sus acciones.



1. Evaluación del Riesgo Tecnológico de SFM

- Criterios útiles para esta fase:
 - Factibilidad de la amenaza
 - Incidentes registrados
 - Medidas para contrarrestar el riesgo
 - Preparación de los proveedores del servicio
 - Susceptibilidad de los usuarios

2. Análisis por impacto esperado y probabilidad de ocurrencia

- El riesgo tecnológico de SFM puede ser analizado por el nivel de impacto de sus consecuencias y por la probabilidad de su ocurrencia.
- El resultado es una tabla de criterios para priorizar la atención respectiva.

	Catastrófico	Alto	Moderado	Bajo	Insignificante
Casi certero	EXTREMO	EXTREMO	EXTREMO	ALTO	MODERADO
Muy probable	EXTREMO	EXTREMO	ALTO	ALTO	MODERADO
Posible	EXTREMO	EXTREMO	ALTO	MODERADO	BAJO
Poco probable	EXTREMO	ALTO	MODERADO	BAJO	BAJO
Raro	ALTO	ALTO	MODERADO	BAJO	BAJO

3. Monitoreo de acuerdo a prioridades establecidas

- Una vez los riesgos se han identificado es necesario llevar a cabo el monitoreo de su comportamiento.
- Se debe definir un checklist de problemas encontrados antes de gestionar los eventos de riesgo.
- Se le debe dar seguimiento a la estabilidad y a la efectividad de las acciones tomadas.
- Implementar auditorías de sistemas de manera periódica para asegurar que las vulnerabilidades son atendidas y que no se están pasando por alto actividades maliciosas.

Sitio en riesgo (Elemento de la red)	Amenaza	Principio violado	Riesgo probable	Controles de seguridad recomendados
Aplicación de la red móvil	Revelación Interceptación	Confidencialidad	Información crítica enviada vía SMS es leída	<ul style="list-style-type: none"> • Los números de cuentas de los clientes son cifrados cuando se transportan • PINs son cifrados cuando se despliegan y cuando son transmitidos
Teléfono móvil del usuario	Modificación	Integridad Autenticación	Infección causada por malware	<ul style="list-style-type: none"> • Políticas sobre información pueden ser descargadas en los teléfonos móviles • Utilización de anti-virus específico para teléfonos móviles (smart phones)
Centro de servicio de mjes cortos, aplicación de SFM, Red del banco	Interrupción	Disponibilidad No repudio	Ataque <i>Denial-of-Service</i>	<ul style="list-style-type: none"> • Implementar un sistema que restrinja el tiempo de respuesta de los paquetes de datos • Requerir una red con un ambiente de elevada seguridad por medio de la adopción de estándares como ISO9001
Teléfono móvil del usuario	Fabricación	Autenticación No repudio	Ataques de Phishing	<ul style="list-style-type: none"> • Campaña de conciencia/educación del cliente con relación a mensajes maliciosos • Alentar a los consumidores para reportar el # de atacantes maliciosos para que se envíen mjes de advertencia y se bloquee el # permanentemente.

- Los reguladores deben tener **una noción sólida de la arquitectura de los sistemas de los SFM** que están siendo ofrecidos en su plaza, en particular con relación a cómo se traslada la información de un elemento de red hacia otro.
- Con una lista de **eventos de riesgo y sus prioridades**, los reguladores pueden identificar los tipos de controles de seguridad necesarios para mitigar los riesgos.
- Estos controles serán la base para crear e implementar **políticas y procedimientos sobre riesgo tecnológico en el ambiente de SFM**.

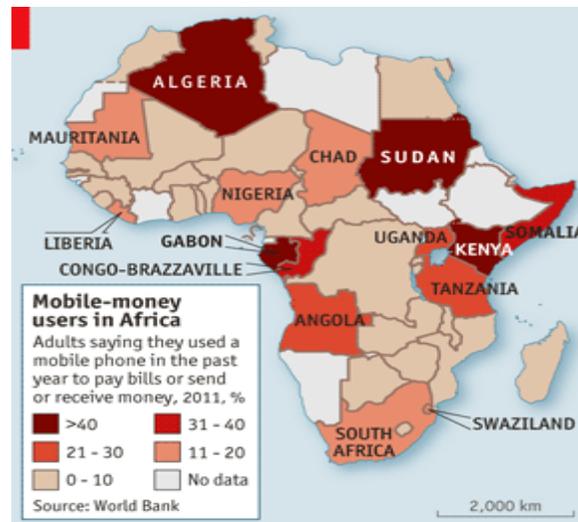
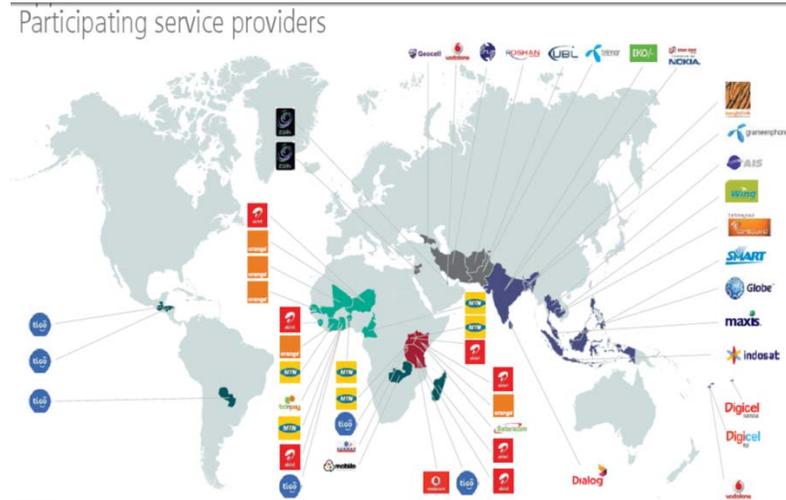
ANNEX II: MODELOS INTERNACIONALES DE SUPERVISIÓN Y REGULACIÓN DE SERVICIOS FINANCIEROS MÓVILES

CONTENIDO

1. Contexto mundial
2. Caso de Kenia
3. Caso de Filipinas
4. Caso de Guatemala

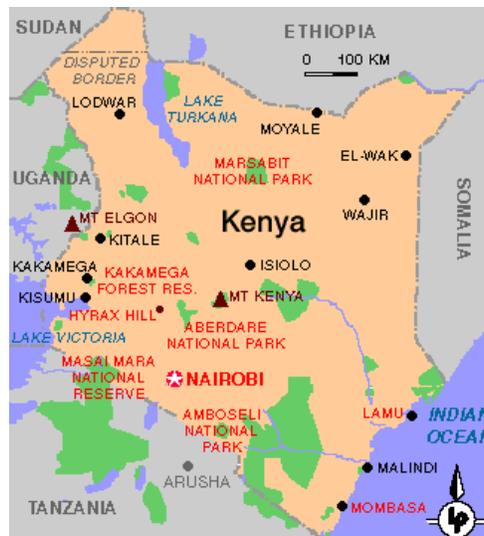
1. Contexto Mundial

- En 3 años pasaron de 17 a 123 modelos en el mundo (abril 2012, GSMA).
- *Global Mobile Money Adoption Survey 2011.*
- 52 proveedores provenientes de 35 países.
- **Resultados a junio 2011:**
 - 60 millones de usuarios registrados.
 - 6 millones activos (últimos 90 días / no MPESA ni SMART / no transacciones administrativas).
 - Los usuarios registrados y activos se duplicaron durante el 1er semestre de 2011.
 - 11 modelos tienen más de 1 millón de usuarios registrados (85% del total de usuarios registrados del estudio).
 - 2 modelos tienen más de 1 millón de usuarios activos (excluyendo MPESA y SMART).
- **Resultados:**
 - El crecimiento anual de los 8 modelos más exitosos fue de +38%.
 - Los modelos más exitosos del mundo: M-PESA (Kenia), SMART Money y GCASH (Filipinas).
 - El 80% de las transacciones globales se procesaron en el Este de África.
 - En junio 2011 se procesaron 142 millones de transacciones.
 - Safaricom procesó el 34% de las transacciones de junio 2011.
 - 264,000 agentes de dinero móvil a junio 2011.
- **Resultados de estadísticas de transacciones funcionales:**
 - 68% compra de aire
 - 27% P2P
 - 5% pagos de facturas
 - 1% pagos colectivos (e.g. G2P, planillas).



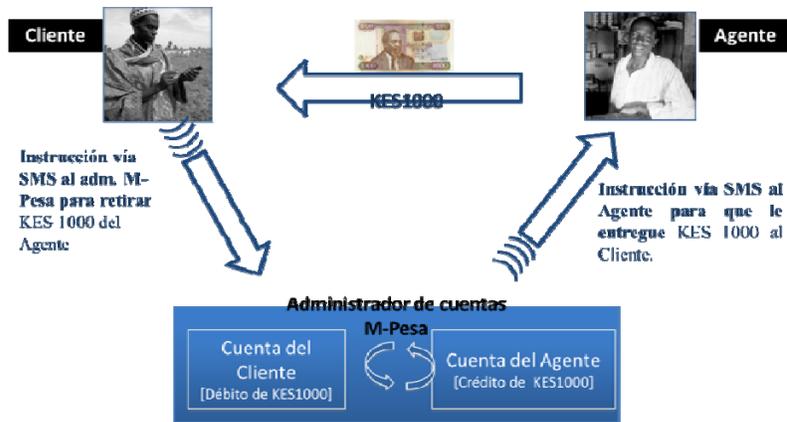
Tres cuartos (15 de 20) de los países que utilizan dinero móvil activamente en todo el mundo (es decir, al menos el 10% de los adultos de cada país) **están en África.**

2. Caso de Kenia



- Población: 40.5 millones.
- Pib per cápita: US\$1,600.00.
- Población rural: 78%.
- División administrativa: 7 provincias y 1 área.
- Penetración de telefonía celular de 50% VS bancaria de 21%.
- **Situación general de los SFM en Kenia a febrero 2011:**
 - 4 telcos
 - 15.4 millones de clientes
 - 39,449 agentes
 - Ksh2.45 millardos al día (US\$28.9 millones)
 - Ksh 76 millardos al mes (US\$894.1 millones)
 - El 68% de los adultos utilizan dinero móvil (la proporción más alta del mundo).
- **Datos del modelo M-PESA a marzo 2012:**
 - 15 millones de usuarios (19,671 en 2007)
 - 37,000 agentes (355 en 2008)
 - El valor mínimo de transacciones bajó de Ksh 50.00 (US\$0.59) a Ksh 10.00 (US\$0.12)
 - El valor máximo por transacción se elevó de Ksh 35,000 (US\$411.76) a Ksh 70,000 (US\$823.53)
 - Red de 25 bancos conectados
 - 700 ATMs

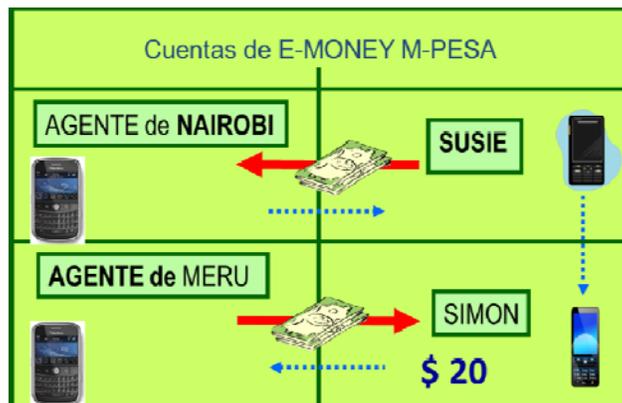
- Recibe remesas desde 70 países por alianza con WU
- La transferencia de dinero se hace vía mensajes SMS.
- No requiere una cuenta bancaria.
- No hay costo para afiliarse.
- No hay cargos mensuales.
- No es necesario mantener saldos mínimos en las cuentas M-Pesa.
- Los agentes tienen tanto efectivo como “float” (E-money).
- El 70% de los usuarios de M-Pesa ya estaban bancarizados.
- 50% envían/ reciben dinero
- 20% guardan el dinero
- 60% de los que envían son urbanos; más del 50% de los que reciben son rurales
- El 90% de los usuarios cree que el dinero está a salvo con M-Pesa
- **Registro de usuarios**
 - Se visita a un agente autorizado.
 - Se obtiene una tarjeta SIM de nueva generación (3G desde 2007).
 - Registrar la cuenta de M-Pesa.
 - Enviar a M-Pesa un mensaje SMS.
 - M-Pesa envía un SMS de confirmación con el nuevo menú M-Pesa.
- **Adquisición de emoney**
 - El cliente visita a un agente autorizado.
 - El agente utiliza su propio teléfono móvil para enviar E-money a la cuenta M-Pesa del cliente.
 - El cliente entrega el dinero en efectivo al agente.
 - Al concluirse el envío ambos reciben SMS de confirmación.
- **Transferencia de fondos**
 - En el menú M-Pesa elegir “send money” y luego ingresar:
 - El número telefónico del que recibirá los fondos
 - El monto que se va a enviar
 - El PIN secreto
 - Al concluir ambos reciben SMS de confirmación.
- **Retiro de efectivo utilizando M-Pesa**

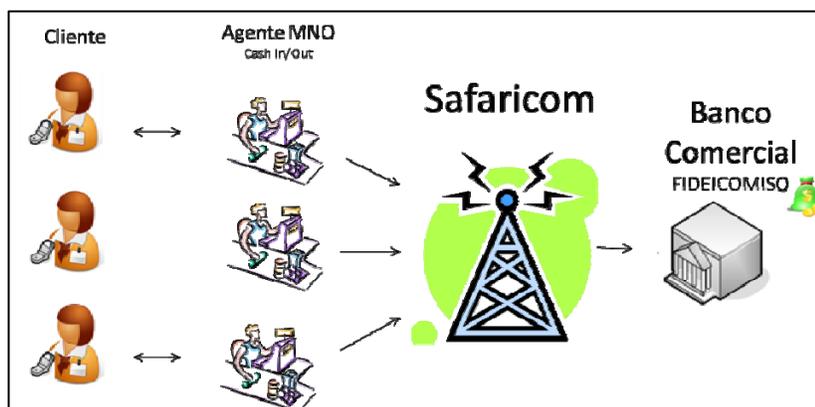


- Los agentes compran emoney para tener “float” almacenado mediante depósitos de efectivo en la cuenta bancaria de M-PESA.
- Los clientes compran el emoney con dinero en efectivo.



1. Susie convierte \$20 de M-Pesa en el Agente de Nairobi quien los envía con su móvil.
2. Susie los envía a Simon por medio de su móvil.
3. Simon los cambia con el Agente de la ciudad de Meru.





Las billeteras M-Pesa las tiene Safaricom y no son clasificadas como depósitos. El E-Money está respaldado 1:1 por fondos en un pool depositado por Safaricom en un fideicomiso en un banco comercial.

- **M-KESHO**
 - M-Kesho es una cuenta bancaria de ahorro.
 - Esta cuenta es abierta por medio de M-Pesa.
 - El producto nace por la alianza entre Safaricom, quien administra M-Pesa y el banco Equity Bank.
 - Los requerimientos para abrir la cuenta son los mismos que tienen las demás cuentas bancarias.
 - M-Kesho permite que los usuarios realicen transacciones bancarias básicas como depósitos, retiros, aplicación para préstamos, todo desde su teléfono móvil.

- Para que una telco ofrezca SFM debe constituir una subsidiaria.
- Esta entidad debe recibir la autorización previa de la autoridad de telecomunicaciones.
- Posteriormente el BCK emite una carta de aprobación como emisor de dinero electrónico.
- El BCK autoriza a las entidades que desean emitir emoney, y a sus agentes, puesto que su ley orgánica le confiere la atribución de ser el regulador del sistema de pagos.
- No ha emitido normativa específica todavía por lo que asegura que aplica “regulation de facto”.
- Previo a conceder la autorización, el BCK requiere la constitución de un fideicomiso para respaldar el dinero electrónico emitido.
- El BCK autoriza a determinados bancos para que actúen como fiduciaries.

- **PROCEDIMIENTOS DE SUPERVISIÓN**
 - El BCK realiza supervisión análisis de gabinete, es decir supervisión extra situ.
 - Se analizan los reportes que se reciben de parte de los proveedores de SFM, tales como los que envía Safaricom (propiedad de Vodafone de Inglaterra) quien opera el modelo M-PESA.
 - El énfasis de supervisión se hace:

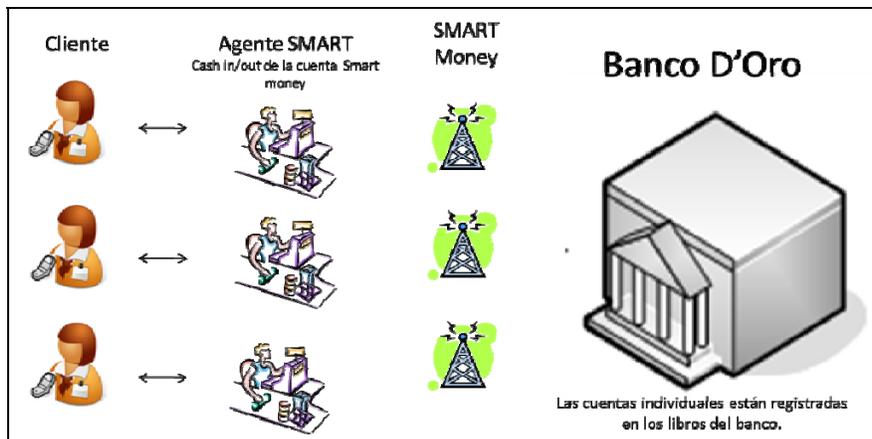
- Incidentes de fraudes
- Resolución de disputas
- Comportamiento de los flujos de fondos
- Liquidaciones y cuadros diarios de float VS fondos en el fideicomiso.

3. Caso de Filipinas



- Población: 93.2 millones.
- PIB per cápita: US\$3,300.00.
- División administrativa: 80 provincias y 120 ciudades principales.
- De un total de 1803 pueblos, 658 no tienen bancos (36.5%).
- 75.5 millones de usuarios de teléfonos móviles.
- Principales telcos: Smart con 45.3 millones de usuarios y Globe, con 23.4 millones.
- Record de 1 millardo de mensajes SMS al día en el 2007.
- 10 millones de filipinos envían remesas del exterior.
- Penetración de telefonía celular de 80% VS penetración bancaria de 35%.
- La industria de telefonía móvil atiende a sectores de todo nivel de ingresos, en particular al de bajos ingresos.

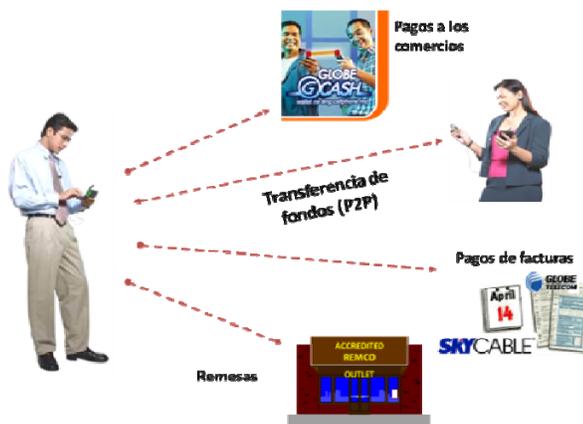
- **SMART MONEY**
 - Banco de Oro es el responsable del servicio.
 - El banco es el dueño de la tarjeta de acceso.
 - El papel de Smart es de proporcionar la infraestructura tecnológica.
 - Requiere que el cliente tenga una cuenta de registro con el banco pero no se da el tratamiento de depósito.



En el modelo de Smart Money centrado en el banco es el Banco D'oro quien emite el E-money utilizando la plataforma de billetera electrónica de SMART.

- **G-CASH**

- Modelo nonbank-based
- La telefónica es la responsable del servicio, quien emite el emoney.
- No se requiere tener una cuenta bancaria.
- En este modelo el registro se hace por medio del teléfono móvil y el cliente únicamente suministra información en formas (KYC) al hacer cash-in o cash-out.



- El BSP ha desarrollado un marco regulatorio basado en la experiencia y en las lecciones aprendidas.
- Pretende impulsar el desarrollo de mecanismos de transferencia de fondos y de pagos al menudeo.

- **Leyes relacionadas:**

- **Ley del Comercio Electrónico:** Establece el marco regulatorio básico para regular el comercio electrónico.

- **Ley Bancaria General de 2000:** Le confiere al BSP la autoridad para regular los servicios bancarios electrónicos.
- **Normativa específica relacionada:**
 - Circular No. 471 –**Operaciones de operadores de moneda extranjera y agentes de remesas.**
 - Circular No. 511 –**Administración del riesgo tecnológico.**
 - Circular No. 542 –**Protección al consumidor de E-banking.**
 - Circular No. 606 –**Otros servicios bancarios para subsidiarias, afiliados y otras entidades.**
 - Circular No. 608 –**Identificación válida para transacciones financieras.**
 - Secciones X162 y X169 del Manual de Normativa para Bancos– **Outsourcing de Sistemas y Procesos de Tecnología.**
 - Circular No. 269 (2000): **Lineamientos respecto de actividades de banca electrónica.**
 - El BSP confiere una aprobación previa.
 - El proceso de aprobación incluye la verificación de:
 - Adecuado proceso de gestión de riesgos.
 - Manual de política de seguridad corporativa.
 - Realización de pruebas satisfactorias de utilización del sistema.
 - Planes de continuidad del negocio.
 - Cumplimiento de la normativa prudencial del BSP.
 - Descripción de los servicios bancarios a ser ofrecidos y de la configuración del sistema (software y hardware).
 - Los contratos con los proveedores de software, hardware o servicios de telecomunicaciones.
 - Circular No. 269:
 - La aprobación final de la Junta Monetaria está condicionada a:
 - Supervisión continua de la gestión de riesgos.
 - Adecuados controles de seguridad.
 - Educación del consumidor.
 - Divulgación clara y adecuada de términos y condiciones así como el reconocimiento por escrito del cliente.
 - Evaluaciones periódicas y continuas de la seguridad.
 - Apego estricto a la normativa del BSP sobre transferencias de fondos.
 - Cumplimiento de prácticas Contra Lavado de Dinero.
 - Notificaciones anticipadas de mejoras en el sistema.

- Circular No. 649 (2009): **Lineamientos para regular la emisión de dinero electrónico y las operaciones de los emisores de dinero electrónico**
 - Se entiende por dinero electrónico al valor monetario representado por una reclamación ante su emisor que
 - Puede ser almacenado electrónicamente en un instrumento o dispositivo.
 - Es emitido contra la recepción de fondos.
 - Es aceptado como medio de pago por personas o entidades distintas del emisor.
 - Puede ser convertido en efectivo o equivalentes de efectivo.
 - Posibles emisores de dinero electrónico:
 - Bancos
 - Instituciones financieras no bancarias
 - Instituciones no bancarias registradas con el BSP como agentes de transferencia de fondos.
 - Las instituciones deben recibir aprobación similar a la de actividades de banca electrónica.
 - Límite mensual de emisión de E-money: P100,000.00 (US 2,222.22). Diario: P40,000.00 (US\$888.88).
 - Las instituciones deben tener un sistema que mantenga registro completo y exacto de la emisión de emoney y los movimientos.
 - El emoney solo puede ser redimido a su valor nominal. No puede ganar intereses ni comprarse con descuento.
 - El emoney no es considerado depósito.
 - Los emisores deben informar por escrito a los usuarios que no tienen cobertura del seguro de depósito, así como las condiciones y cuotas pertinentes.
 - Los emisores deben asegurarse que sus distribuidores o agentes cumplan con todos los requerimientos de la normativa Contra Lavado de Dinero.
 - De manera previa los emisores deben adecuar la implementación de control interno, sistemas informáticos, medidas y políticas de seguridad, función de auditoría de la seguridad, entre otros aspectos.
 - Para proteger a los usuarios del emoney y asegurarse de que la redención del emoney será adecuada en todo momento, la institución no bancaria debe tener suficientes activos líquidos (sin gravamen) en un monto igual al del emoney emitido pendiente de redención:
 - Depósitos bancarios
 - Títulos valores del Estado
 - Otros activos líquidos que el BSP pueda aprobar.
 - Otras disposiciones para instituciones no bancarias:
 - Capital pagado mínimo (P100 millones/ US\$2.2 millones)
 - Únicamente pueden dedicarse al negocio del emoney u otras actividades estrechamente relacionadas. Instituciones ya existentes deben constituir una entidad separada para dedicarse al emoney.
 - No pueden conceder créditos.

- **Procedimientos de Supervisión**

- Marco de Supervisión:
 - Guías sobre Riesgo Tecnológico, Outsourcing/Insourcing, Protección al Consumidor, Continuidad del Negocio.
 - Normativa sobre banca electrónica, dinero electrónico y registro de remesadoras.
 - Manuales de regulación para bancos y para entidades no bancarias.
 - Toda la normativa relacionada con tecnología es revisada y renovada cada 5 años.
 - El BSP tiene inspectores de supervisión general, supervisión financiera y supervisión de TI (certificados CISA = Certified Information Systems Auditor).
 - El BSP lleva a cabo supervisión in situ de los sistemas y bases de datos de los proveedores de SFM.
 - La unidad encargada de supervisar a los proveedores de SFM se llama: Core Information Technology Specialists Group –CITSG-.
 - Al CITSG le corresponde hacer el examen y supervisión de instituciones bancarias y no bancarias en las áreas de Gobierno de TI, banca electrónica, dinero electrónico y otras áreas relacionadas con sistemas de pagos y liquidación.
- Las funciones principales del CITSG son:
 - Desarrollar el programa de examen de TI basado en riesgos.
 - Llevar a cabo la supervisión de TI de campo.
 - Desarrollar políticas de TI
 - Analizar expedientes de aplicaciones para ofrecer servicios de banca electrónica.
 - Medir y gestionar riesgos relacionados con TI.
- Para validar el trabajo realizado en el campo, el BSP lleva a cabo también supervisión extra situ, mediante el análisis de la información reportada por las instituciones con licencia otorgada.
- La supervisión busca verificar el cumplimiento de la normativa.
- Un aspecto importante que se supervisa regularmente es el requisito de activos líquidos para respaldar la emisión de emoney.

4. Caso de Guatemala

- **Contexto a diciembre de 2011**

- Población: 14.7 millones.
- Celulares activos: 20.7 millones.

- Pib per cápita: US\$2,600.00; Pobreza: 50%.
 - 18 bancos, 3118 agencias bancarias, 21/100,000 habitantes.
 - 3000 agentes bancarios, 4000 establecimientos.
 - Captaciones/PIB: 41.4%.
 - Créditos/PIB: 25.1%.
- **Reglamento para la Prestación de Servicios Financieros Móviles: Resolución JM-120-2011**
 - **Objeto:** regular aspectos mínimos que deben cumplir los bancos y las empresas de tarjetas de crédito en la prestación de servicios financieros móviles.
 - **Servicios financieros móviles:** realización de operaciones y transacciones de una cuenta de depósitos o de una línea de crédito por medio de un dispositivo móvil que utilice servicios de telefonía.
 - Los Consejos de Administración aprobarán el modelo de negocio de acuerdo a sus estrategias
 - Las instituciones deberán realizarán pruebas previas con resultados satisfactorios antes del lanzamiento de su modelo.
 - El modelo comprenderá:
 - Estrategia a la que obedece la prestación de SFM.
 - Esquema operativo que incluya el rol de los participantes.
 - Procedimientos de afiliación y de uso de los servicios por parte de los usuarios.
 - Límites máximos (cantidad de operaciones y monto).
 - Descripción de la plataforma tecnológica (confidencialidad, integridad, disponibilidad de la información y seguridad informática).
 - **Registro de operaciones:** deberán quedar registradas en tiempo real, de manera que se mantenga actualizado el saldo disponible.
 - **Asistencia al usuario:** las instituciones deberán contar con infraestructura adecuada para la atención de los usuarios.
 - **LD/FT:** las instituciones serán las directamente responsables del cumplimiento de las obligaciones que les impone la normativa sobre LD/FT.
 - **Participación de terceros:** las instituciones deberán celebrar un contrato con terceros participantes que incluya obligaciones referentes a: acceso, disponibilidad y confidencialidad de la información, cumplimiento de las políticas, procedimientos y sistemas aprobados, no realizar cobros no autorizados, no ceder derechos ni obligaciones.
 - **Responsabilidad por los SFM:** las instituciones serán las responsables por las operaciones y transacciones realizadas.
 - **Autorización del rol de los agentes bancarios complementario de servicios financieros móviles: Acuerdo No 25-2011**
 - Autorización para:
 - Recibir información y documentación para abrir cuentas de depósitos monetarios y de ahorro

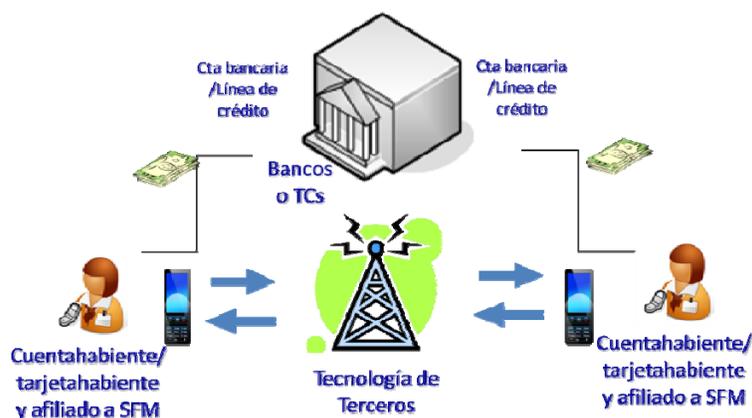
- Gestionar la afiliación de clientes a los SFM según con el proceso definido
- **Reglamento para la Realización de Operaciones y Prestación de Servicios por medio de Agentes Bancarios: Resolución JM-65-2010**
 - **Objeto:** regular las operaciones y prestación de servicios que los bancos realicen por medio de agentes bancarios.
 - **Agentes bancarios:** personas individuales o jurídicas que ejerzan actividades comerciales, con las que un banco suscribe un contrato para que, por cuenta de éste, puedan realizar determinadas operaciones y servicios.
 - El Consejo de Administración debe aprobar el esquema denominado modelo operativo.
 - El estudio por escrito para selección de agentes bancarios debe abordar:
 - Negocio o actividad del agente.
 - Características del canal de distribución.
 - Entorno geográfico.
 - Operaciones a ser realizadas.
 - Riesgos reputacional, operacional y de LD/FT.
 - Requisitos para los agentes bancarios:
 - Acreditar ser persona solvente e idónea.
 - Inscritos en el Registro Mercantil y Registro Tributario.
 - Acreditar 1 año de operación, como mínimo, del negocio.
 - Mayoría de edad.
 - No haber sido condenado por delitos por falta de probidad, LD/FT, malversación de fondos.
 - No afectar la reputación del banco.
 - Residente legal de Guatemala.
 - Responsabilidad de los bancos consignada en todo comprobante de operaciones efectuadas.
 - Los bancos son responsables del cumplimiento de la normativa LD/FT.
 - El agente bancario no puede conocer los saldos de las cuentas de depósito.
 - Los bancos deben poner a la vista del público su identificación y anuncio de operaciones y servicios realizados por medio del agente.
 - Los bancos están obligados a capacitar al personal de los agentes bancarios.
 - Principales obligaciones a incluirse en el contrato:
 - Confidencialidad
 - Cumplimiento del manual operativo
 - Que no realizarán cobros no autorizados.
 - Identificación como agente bancario.
 - No condicionar las operaciones o servicios.
 - Operaciones y servicios permitidos:
 - Recibir depósitos y atender retiros de cuentas de ahorro y monetarias.

- Cobros por cuenta ajena.
 - Recepción y envío de transferencias de fondos.
 - Pagos de préstamos del banco.
 - **Recibir información y documentación para abrir cuentas.**
 - **Gestionar la afiliación de cuentahabientes a Servicios Financieros Móviles.**
-
- Principales aspectos a incluir en el modelo operativo:
 - Estrategia del banco para utilizar agentes bancarios.
 - Disposiciones para administrar riesgos.
 - Perfil de agentes bancarios.
 - Criterios para determinar límites máximos.
 - Modelo de contrato.
 - Manual operativo.
 - Descripción de hardware y software, controles informáticos y seguridad informática.

Apertura de cuenta / Afiliación a SFM



Transferencias / Pagos de bienes y servicios



Otra normativa complementaria del caso de Guatemala:

- **Reglamento para la Administración Integral de Riesgos (Vigencia: 1-6-2011)**
Resolución JM-56-2011
- **Formulario para Inicio de Relaciones Simplificado (Circulado: 2-6-2011)**
Oficio IVE No. 721-2011
- **Reglamento para la Administración del Riesgo Tecnológico (Vigencia: 1-9-2011)**
Resolución JM-102-2011

ANNEX III: TALLER DE ADMINISTRACIÓN DE RIESGOS DE SFM (DÍA I, 31/5/2012)

Instrucciones:

En 6 grupos de 5 personas, coordinados con un tecnólogo cada uno, discutir y definir políticas o disposiciones para gestionar el riesgo tecnológico proveniente de la prestación de Servicios Financieros Móviles. Considerar las amenazas expuestas en la presentación (Modificación, Destrucción, Revelación, Interceptación, Interrupción, Fabricación) y los principios clave (Confidencialidad, Integridad, Disponibilidad, Autenticación y No Repudio). Si se estima necesario se puede incluir una matriz de criterios de calificaciones cualitativas para la evaluación del riesgo tecnológico por SFM. Al concluir se debe hacer la presentación de los resultados al resto del grupo de participantes.

Resultados:

GRUPO I MOTUR S.A

Política en caso de robo y siniestro

1. En caso que el móvil sea robado, la empresa está en la obligación de desvincular la cuenta y asignar un nuevo pin.
2. El pin se debe de ser cambiar al momento que el móvil es robado, el pin se desactiva y se proporciona otro pin en el nuevo aparato.
3. Money express cuenta con un servidor de contingencia, en caso que el principal sea destruido por algún accidente, el servidor de respaldo entra en acción. Por lo tanto los usuarios se sienten seguros y confiados del servicio.
4. Una de las políticas que se debe de reflejar en el contrato de la empresa con el usuario, es que si hay perdida accidental recurrentes de aparatos móviles por parte de los clientes, la empresa se reserva el derecho de ir aumentando la prima del seguro del móvil si este es extraviado más de dos veces.
5. La empresa realizará un monitoreo constante de todos los movimientos de pago de sus clientes para detectar irregularidades de pagos.
6. Existirá un monto máximo en cada una de las transacciones por un período determinado. (\$ 500 dólares mensuales)
7. La cantidad de operaciones no tendrá límites siempre y cuando no sobrepase el monto máximo mensual.
8. El riesgo de liquidez estará cubierta por una garantía que la empresa tiene en una fianza bancaria.
9. La empresa ofrecerá sus transacciones a través del sistema USSD, con el cual se puede encriptar tanto a la hora del envío y a la hora de recepción.

**GRUPO 2
DINEROLISTO**

<i>Amenaza</i>	<i>Elementos en Riesgo</i>	<i>Riesgo Probable</i>	<i>Programa de Gestión</i>	<i>Principio Violado</i>
Modificación	Red	Alternación del mensaje	Mecanismo encriptado y verificación del contenido (algoritmo de suma de verificación)	Integridad
Dstrucción	Sistemas de Almacenamiento Teléfono	Desastres naturales o provocados	Mecanismos de contingencia y replicación (datos y aplicaciones). En zonas separadas y diferentes redes. Mecanismos para reportar pérdida (SIM) y reasignación de un nuevo dispositivo (incluye PIN). La red almacena la información.	Confidencialidad Autenticación Disponibilidad
Revelación	Red	Descubrimiento de PIN	Mensajes encriptados. Cambio de PIN de forma periódica y según mecanismos alternativos (llamada, internet o desde el mismo celulares).	Autenticación
Intercepción	Teléfono	Negación de autoría de transacciones.	Incluir en la aplicación de transferencias, la confirmación de la misma La aplicación incluiría la solicitud del PIN del usuario	Repudio
Fabricación Intercepción	Teléfono Red Aplicación del	Transacciones fraudulentas	El monto máximo mensual es de \$1,000, pero el cliente puede solicitar aumentar este	Integridad Confidencialidad

	Operador		nivel, para lo cual el operador creará mecanismos de seguridad. Operador incluye un seguro para respaldar las transacciones.	
Interrupción	Red	Denegación de Servicio, No acceso a red	Mecanismo de invalidación en casos extremos de saturación	Integridad Disponibilidad

GRUPO 3

Políticas y Procedimientos de FLASHMOVIL

1. Modificación

- Política 1: Implementar mecanismos de doble autenticación, no solo usuario y clave.
- Procedimiento 1: Que cada usuario utilice un token
- Política 2: Utilización de software antivirus
- Procedimiento 2: Enviar alertas de nuevos virus a usuarios través de mensajes de texto.

2. Destrucción

- Política: Implementar planes de continuidad y mecanismos de contingencia.
- Procedimiento: Contar con centro de datos alternos y red de comunicación secundaria

3. Revelación

- Política 1: Contar con mecanismos de cifrado de información de identificación del usuario
- Procedimiento 1: Utilización de técnicas de cifrado 3DES

4. Interceptación

- Política 1: Contar con mecanismos de cifrado de información de identificación y envío del usuario
- Procedimiento 1: utilización de técnicas de cifrado 3DES
- Procedimiento 2: utilizar firewalls
- Política: implementar sistemas de alerta de operaciones sospechosas
- Procedimiento: parametrizar operaciones que se tipificarían como sospechosas

5. Interrupción

- Política: Implementar planes de continuidad y mecanismos de contingencia.
- Procedimiento: contar con centro de datos alternos y red de comunicación secundaria

6. Fabricación

- Política 1: Implementar programas de información al usuario sobre diferentes tipos de suplantación de identidad y robo de información
- Política 2: Implementar mecanismos de confirmación de transacciones
- Política 3: Límites a número y monto de transacciones.

- Policita 4: Limitar las operaciones a solamente un número móvil, asociadas al documento de identidad
- Procedimiento 1: llevar control de bitácoras de registro de usuarios
- Procedimiento 2: En la semana se pueden hacer operaciones por un máximo de \$700.
- Procedimiento 3: realización de auditorías semestrales

GRUPO 4
BANCA FACIL
POLÍTICA PARA EL OTORGAMIENTO DE SFM

MODIFICACIÓN:

- El banco utilizará tecnología mediante la cual se cifrará de extremo a extremo las transacciones mediante cifrado fuerte.
- Se suscribirán contratos de confidencialidad con la operadora telefónica que preste el servicio móvil, con relación a las transacciones que realizará el cliente
- Efectuar pruebas de vulnerabilidad por lo menos 1 vez al año.
- Se efectuará notificación de los nuevos saldos de nuestros clientes, después de cada transacción.

DESTRUCCIÓN:

- Se crearan planes de contingencia y continuidad del servicio
- Los planes deben ser probados y certificados por lo menos 1 vez al año.

REVELACIÓN

- Se suscribirán contratos de confidencialidad con la operadora telefónica que preste el servicio móvil, para la resguarda de la información de nuestros clientes
- Establecer procedimientos para la debida diligencia e identificación de nuestros clientes
- Se implementará un sistema informático de control de transacciones inusuales

INTERCEPCIÓN

- El banco utilizará tecnología mediante la cual se cifrará de extremo a extremo las transacciones mediante cifrado fuerte

INTERRUPCIÓN

- Se crearan planes de contingencia y continuidad del servicio

FABRICACION

- Se establece un maximo de 3 transacciones diarias que no superen el acumulado diario de us\$500 y que el acumulado mensual no supere us\$1000
- Se utilizaran mecanismos de autenticación de 2 o mas factores tales como: pim, tokens, certificados de seguridad, entre otros.
- Realizar 3 campañas en el año de concientización y educación de los **SFM**

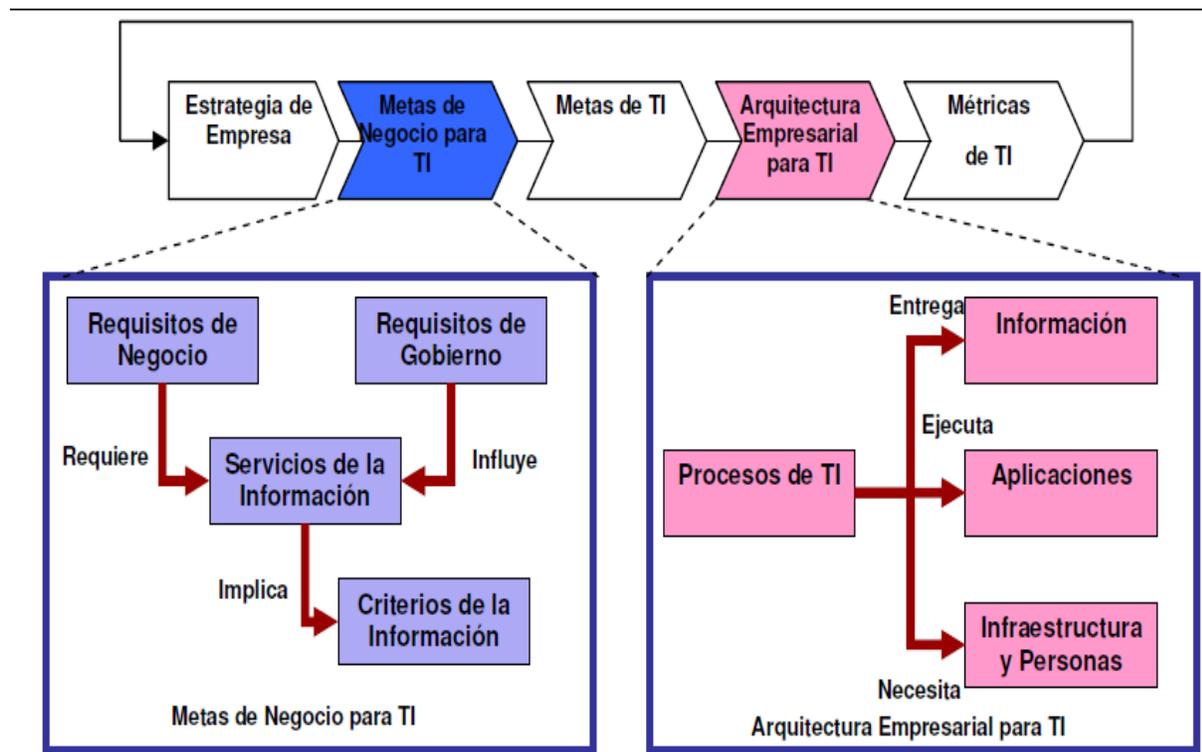
GRUPO 5

Servicios Salvadoreños Móviles (SSALVA MOVIL)

TIPO DE OBJETIVO	VULNERABILIDAD	AMENAZA	RIESGO	POLITICA-PRINCIPIOS
Usuario	La transmisión inalámbrica entre el teléfono y el punto de venta del Banco.	La intersección del tráfico. (Interceptación y revelación)	Robo de identidad, divulgación de información y ataques por repetición.	Creación de un modulo confiable, protocolo seguro y cifrado. (Confidencialidad e Integridad)
Usuario	Instalación inadvertida de software malicioso del teléfono del usuario.	La aplicación descargada que intercepta los datos de la autenticación. (Interceptación y revelación)	Robo de parámetros de autenticación, divulgación de información, repudio de transacciones.	Autenticación del usuario (pin) y aplicación de firma digital por entidad externa confiable. (Confidencialidad y Autenticación)
Usuario	Ausencia de autenticación de 2 factores.	Enmascaramient o del usuario. (Modificación)	Transacciones fraudulentas, responsabilidad del proveedor	Autenticación de dos factores: lo que conozco (contraseña o pin) y lo que tengo (token) (Confidencialidad y Autenticación)
Usuario	Cambio o sustitución del teléfono móvil	Complejidad en la configuración y el establecimiento de parámetros. (Fabricación)	Escasa adopción de la tecnología "seguridad por ofuscación de código"	Interfaz del usuario simplificada, establecimiento de parámetros por una entidad confiable. (Integridad)
Proveedor de servicios.	Debilidad de cifrado del sistema global de sistema móvil (GSM). Datos de SMS en texto legible en la red móvil.	Modificación de mensajes, repetición de transacciones, evasión de controles de fraude. (Modificación) y Fabricación)	Robo de servicios o de contenido, pérdida de ingresos, transferencia ilegal de fondos.	Protocolo criptográficos fuertes, autenticadores de mensajes SMS, encriptación. (Confidencialidad, No repudio y Autenticación)
Proveedor de servicios.	Dispositivos de pos instalados en el local del comerciante.	Ataques enmascarados, manipulación de los puntos de venta.	Robo de servicios, repetición y modificación de mensajes.	Investigador del proveedor del POS. Autenticadores de mensajes, control de autorizaciones y contabilidad. (Confidencialidad, No repudio y Autenticación)

Proveedor de servicios.	Sistema de punto de venta POS, acepta transmisiones inalámbricas.	Entidad malintencionada que satura el sistema POS con solicitudes sin sentido. (Interrupción)	Denegación del servicios (DoS).	Filtrado de solicitudes en el lector del dispositivo móvil. (Disponibilidad)
Banco	Sistema sin mecanismos de bloqueo para la identificación de transacciones repetidas o ilimitadas de un mismo móvil	Exceso de transacciones que saturan la red. (Interrupción)	Suspensión del Servicio.	Establecer monitoreo en sistema por el proveedor y definir límites en el numero de transacciones. (Confiabilidad y Disponibilidad)
Banco	Posibilidad de utilizar el canal para transacciones ilícitas.	Personas vinculadas al lavado de activos y extorsiones utilizando el medio.	Riesgo reputacional	Asignación de límites en términos de monto y número de transacciones. Monto-hasta 2 salarios mínimos mensuales por móvil. No. de transacciones diarias: hasta 5.

GRUPO 6
BANCAFÉ “MONEY-MOVIL”



Cada vez más, la alta dirección se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa. La dirección espera un alto entendimiento de la manera en que la tecnología de información (TI) es operada y de la posibilidad de que sea aprovechada con éxito para tener una ventaja competitiva. En particular, la alta dirección necesita saber si con la información administrada en la empresa es posible que:

- Garantice el logro de sus objetivos
- Tenga suficiente flexibilidad para aprender y adaptarse
- Cuente con un manejo juicioso de los riesgos que enfrenta
- Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas

Las empresas exitosas entienden los riesgos y aprovechan los beneficios de TI, y encuentran maneras para:

- Alinear la estrategia de TI con la estrategia del negocio
- Asegurar que los inversionistas y accionistas logran un debido cuidado estandarizado para la mitigación de los riesgos de TI
- Lograr que toda la estrategia de TI, así como las metas fluyan de forma gradual a toda la empresa
- Proporcionar estructuras organizacionales que faciliten la implementación de estrategias y metas
- Crear relaciones constructivas y comunicaciones efectivas entre el negocio y TI, y con socios externos
- Medir el desempeño de TI

MONEY MOVIL DE BANCAFÉ

AMENAZAS

PRINCIPIOS

PROCEDIMIENTOS GENERALES

Modificación	Confidencialidad Integridad Autenticación	Políticas debidamente autorizadas Software de acceso Bitácoras de auditoría
Destrucción	Integridad Disponibilidad	Política de BCP (BIA DRP) Centro alternativo Comunicaciones alternas (Proveedores de servicio)
Revelación	Confidencialidad Integridad Autenticación	Criptografía en información Clasificación de información crítica, privada y pública IDS
Intercepción	Confidencialidad Integridad Autenticación No repudio	Implementación de hardware y software con mínimos de seguridad Política de transacciones máximas
Interrupción	Integridad Disponibilidad Autenticación	Servicios alternos de energía (Plantas eléctricas, UPS's, mantenimiento preventivo)
Fabricación	Confidencialidad Integridad Disponibilidad Autenticación No repudio	Sistemas de alertas IDS Políticas y procedimientos de uso de dispositivos Políticas KYC

ANNEX IV: TALLER DE MODELOS INTERNACIONALES DE SUPERVISIÓN Y REGULACIÓN DE SFM (DÍA 2, 1-6-2012)

Instrucciones:

Tomando en consideración lo expuesto con relación a los 3 modelos de SFM internacionales (Kenia, Filipinas y Guatemala) discutir y definir, en grupos integrados con al menos dos participantes que trabajen en la Superintendencia del Sistema Financiero, el bosquejo de lo siguiente:

- Norma para regular a los Corresponsales Bancarios
- Norma (como mínimo 1) para regular los Servicios Financieros Móviles
- Prácticas y procedimientos para la supervisión de los proveedores de SFM

Resultados:

GRUPO I

Bosquejo de Temas a Regular en Norma de Corresponsales Bancarios

1. Cumplimiento de obligaciones formales mercantiles y tributarias del corresponsal.
2. Formalización mediante contrato de servicios que regule la relación entre las partes.
3. establecimiento de limites a operaciones
4. mecanismos para garantizar la disponibilidad de los fondos.
5. Reporteria y mecanismos de control

Bosquejo del Contenido de Norma de Servicios Financieros Móviles

1. Definición de operaciones y montos máximos a realizar
2. Aplicación de políticas **kyc** para efectos de mitigar riesgos lda/ft. Requerimientos mínimos de infraestructura y seguridad tecnológica.
3. Mecanismos de continuidad de las operaciones.
4. Procedimientos para la atención de quejas y reclamos
5. Medios para la salvaguarda del secreto bancario

Bosquejo de procedimientos de Supervisión a Servicios Financieros Móviles

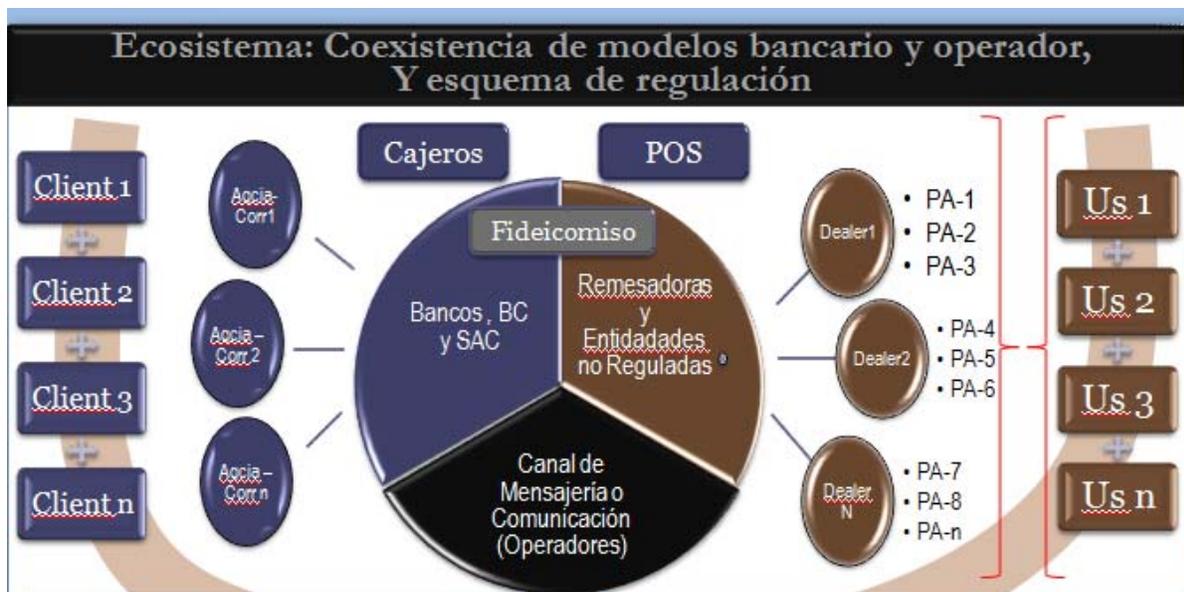
1. Verificación de clausulas contractuales
2. Auditoria de sistemas
3. Cumplimiento de existencia y aplicación de políticas y procedimientos
4. Verificación de parámetros en la prestación de los servicios (numero de transacciones y montos).
5. Evaluación de políticas para la selección de operadores o corresponsales.

GRUPO 2

Bosquejo de norma corresponsal bancario

1. **Condiciones mínimas para la representación de Banco:** Seguridad informática, requisitos de honorabilidad (riesgo reputacional), límites de transaccionalidad (por día: 2 SM, número de operaciones diarias: 2operaciones, límite mensual: 3 SM, confidencialidad de la información de los clientes.
2. **Servicios prestados**
 - a) Recepción de documentación para apertura de cuentas con requisitos simplificados.
 - b) Asociación de servicios financieros por medio de Banca Móvil.
 - c) Retiros de cuentas.
 - d) Depósitos a cuentas propias y de terceros.
 - e) Pago de créditos.
 - f) Pago de tarjetas de crédito.
 - g) Pago de servicios básicos.
 - h) Trámite de solicitudes de créditos.
3. **Manual de identificación y gestión de riesgos.**
4. **Delimitación de responsabilidades.**
5. **Disposiciones generales**

Bosquejo de SFM



Regulación de Pagos y Transferencias Móviles:

- a) Requerimientos de Seguridad Informática.
- b) Regulación de montos y número de transacciones.
- c) Constitución de fideicomisos.

- d) Servicios permitidos.
- e) Delimitación de responsabilidades.

Regulación Banca Móvil:

- a) Sujetos de aplicación.
- b) Definiciones.
- c) Servicios autorizados.
- d) Contratos con terceros.
- e) Asociación del Producto Financiero.
- f) Delimitación de responsabilidades.
- g) Seguridad informática.
- h) Comisiones e información al cliente.

Procedimientos de Supervisión:

1. Alcance de supervisión.
2. Verificación insitu de las transacciones a través de SFM realizadas con periodicidad trimestral.
3. Vigilancia del calce de los respaldos de las operaciones realizadas (Fideicomiso y el flotante en los corresponsales bancarios) .
4. Revisión de cumplimiento de norma relacionada con LAFT.
5. Revisión de Planes de Contingencia ante la ocurrencia de eventos naturales o provocados que eleven el Riesgo Operativo.
6. Disposiciones Generales.

GRUPO 3

Temas a regular en una norma de corresponsales bancarios.

- Requisitos mínimos
- Solvencia financiera
- Solvencia legal (no antecedentes relacionados al lavado de dinero y antecedentes penales)
- Relación Contractual entre la entidad bancaria o el operador para la prestación del servicio.
- Límites de transacciones y monto de las operaciones.
- Tipos de establecimientos. (Reputación de la entidad)

Norma de servicios financieros móviles.

- Entidades que pueden prestar el servicio.
- Límites de transacciones y monto de operaciones
- Operaciones a realizar
- Requerimientos tecnológicos para la implementación del producto
- Contratación con terceros.
- Autorizaciones previas del ente regulador del teleoperador para la prestación del servicio.
- Autorización para prestar servicios móviles. (Bancos o teleoperadores)
- Constitución de fideicomiso en entidad bancaria.

Procedimientos de supervisión de servicios financieros móviles.

- Información a requerir al Banco o al administrador. (actualización de agentes corresponsales, verificación del cumplimiento de medidas contra lavado de dinero, información financiera.)
- Monitoreo de saldo float con disponibilidad en cuenta de fideicomiso, diario.
- Cumplimiento de límites de transacciones y monto de operaciones

Bosquejo de normativa par corresponsales bancarios

- I. Definición de conceptos:
 - i. Corresponsales bancarios
 - ii. Operaciones o transacciones
 - iii. Servicios financieros, etc.
- II. Establecer requisitos de elegibilidad de corresponsales bancarios.
- III. Establecer claramente operaciones que puedan realizar corresponsales bancarios.
- IV. Establecer medidas de seguridad (físicas y tecnológicas).
- V. Normas obligatoriedad de los bancos para llevar control de sus corresponsales.
- VI. Establecer políticas y procedimientos autorizadas por las JD del banco para la elegibilidad de los corresponsales.
- VII. Remisión de información a la SSF: registro de agentes, volumen de transacciones y otros a solicitud.
- VIII. Establecer políticas y procedimientos de operatividad de los corresponsales: límite de monto y número transacciones, informes de operaciones sospechosas, registro en línea y diario de las operaciones, etc.
- IX. Establecer mecanismo de protección al consumidor y educación financiera.
- X. Normar publicidad de los corresponsales: protección por IGD, afiliación a banco, identificación del corresponsal.
- XI. Establecer lineamientos de gestión de riesgo.
- XII. Establecer políticas sobre planes de continuidad del negocio.

Bosquejo de normativa para servicios Financieros Móviles

- I. Definición de conceptos:
 - i. Servicios móviles
 - ii. Tipo de operaciones
- II. Solicitar autorizaciones a BCR para la operatividad
- III. Establecer límites de montos de operaciones así como del número.
- IV. Lineamientos sobre medidas de seguridad informática y lavado de dinero.
- V. Establecer cláusulas mínimas en contratos de relación operador-banco.
- VI. Establecer lineamientos sobre gestión de riesgo.
- VII. Remisión de información a SSF.
- VIII. Establecer políticas de continuidad del negocio.

Procedimientos de supervisión para imprimir supervisión de los SFM

- I. Verificación del plan estratégico del banco, si contempla los SFM.
- II. Verificación de autorización y vigencia de las políticas para SFM.
- III. Verificar los procesos de gestión de riesgo.
- IV. Verificación de existencia de contratos y requerimientos de normativa entre bancos y agentes.
- V. Verificación de una debida identificación de clientes o usuarios.
- VI. Realización de liquidación y cuadros diarios de las operaciones electrónicas contra fideicomiso o fianzas bancarias, según sea el caso.
- VII. Verificar y controlar operaciones fraudulentas.
- VIII. Verificaciones de medidas de seguridad informática y físicas.
- IX. Verificación in situ de la existencia de planes de contingencia y continuidad del negocio.
- X. Efectuar visitas in situ a los corresponsales bancarios.

GRUPO 4

A. Regulación de corresponsales bancarios

personas naturales o jurídicas que funcionan en establecimientos propios o de terceros, distintos de los del sistema financiero, que conforme a un acuerdo contractual y bajo responsabilidad de la entidad financiera, pueden prestar las operaciones y servicios contemplados en la presente propuesta.

1. Sobre requisitos de información a las entidades financieras para iniciar operaciones a través de corresponsales u otros canales alternativos:

2. Copia del acuerdo del Órgano Director
3. Remisión de un modelo operativo para la realización de operaciones y prestación de servicios:
 - Estudio de factibilidad: el nicho de mercado, el tipo de productos y servicios, el área geográfica y el plan de mercadeo
 - Informe sobre la identificación y gestión de los riesgos financieros, operativos y reputacionales, incluyendo los relativos a la prevención de los delitos de lavado de dinero u otros activos y del financiamiento del terrorismo, y sus mitigadores
4. Política para determinar el límite máximo de monto y de número de transacciones permitidas a los corresponsales o que podrán ser realizadas por los clientes a través de canales alternativos. (dentro del rango permitido por la SSF)
5. Política para la selección de personas naturales o jurídicas que podrán desempeñarse
6. Las entidades deberán publicar en su sitio web u otros medios, el primer día de cada mes, el detalle de los corresponsales que operan con ellas; así mismo, deberán remitir dicho detalle a la Superintendencia en el mes de enero de cada año y siempre que haya cambios.
7. Mecanismo de dotación de efectivo a los corresponsales en los puntos de atención al público ~ otras medidas para asegurar que éstos cuenten con la liquidez necesaria
8. Los corresponsales deberán ser proveídos de una identificación uniforme, para evitar impostores e identificarlo con la entidad financiera.
9. Modelo del contrato a ser suscrito con corresponsales, el cual deberá considerar lo siguiente:

Obligaciones del corresponsal sobre:

- Recibir visitas domiciliadas y brindar toda la información relacionada con las operaciones bancarias que sea requerida por la Superintendencia del Sistema Financiero y del personal de la entidad financiera.
 - Informar con antelación (30 días) de cualquier reforma a su objeto social o su organización intema que pueda afectar la prestación de servicios a la entidad financiera
 - Guardar confidencialidad respecto de la información relativa a las operaciones pasivas, activas y de servicios que celebre con los clientes bancarios, así como la información relativa a éstos últimos.
 - Mantener elementos publicitarios que, de forma visible al público, muestren de forma clara la condición de proveedor de servicios de la empresa financiera con la que suscriban contratos.
- b. Las siguientes prohibiciones para los corresponsales:
- Realizar operaciones diferentes y fuera de los límites definidos por la entidad financiera.
 - Condicionar a la adquisición de un producto o servicio propio.
 - Publicitarse o promocionarse de cualquier forma a través de la papelería
 - Realizar la operación objeto de la corresponsalía en términos distintos a los pactados con la Institución correspondiente.
 - Subcontratar los servicios relacionados a la corresponsalía .
 - Cobrar comisiones, por cuenta propia,

USAID/El Salvador Improving Access to Financial Services Program

- Llevar a cabo las operaciones con los clientes bancarios a nombre propio.
 - Asumir frente al cliente la responsabilidad por todos los servicios ofrecidos a través de corresponsales.
10. Manual o Guía para corresponsales :
- a) El procedimiento que emplearán en la identificación de clientes,
 - b) Los conceptos básicos de las operaciones bancarias que tienen autorizado realizar, descripción de las operaciones y servicios que tienen autorizado realizar,
 - c) Pasos para la atención de las operaciones y prestación de los servicios
 - d) Especificaciones técnicas del equipo necesario para operar;
 - e) Una guía rápida para la solución de problemas y teléfonos de contacto en caso de emergencias o fallas operativas;
11. La descripción del hardware y software a utilizar, el diagrama técnico del envío y recepción de información entre los corresponsales y los servidores de la entidad financiera, los controles informáticos que se implementarán para garantizar la confidencialidad, integridad, transferencia y disponibilidad de la información, la seguridad informática que se implementará y cualesquiera otra documentación para la comprensión del funcionamiento informático y de seguridad de los sistemas;
12. Planes de contingencia para mantener la continuidad de las operaciones y servicios a través de corresponsales u otros canales alternativos;
13. Programa de Capacitación a Corresponsales, cuando el canal alternativo utilizado implique que sea personal a cargo del corresponsal el que tenga contacto directo con el cliente.
Sobre las operaciones y servicios que deberían permitirse:
- 1. Apertura y Retiro de cuentas de ahorro,
 - 2. Desembolsos de créditos,
 - 3. Retiro de remesas recibidas,
 - 4. Depositar en cuentas de ahorro propias o ajenas,
 - 5. Transferencias entre cuentas,
 - 6. Pagar créditos (tarieta o no),
 - 7. Servicios de pagaduría y colecturía.
 - 8. Trámite de solicitudes de crédito.

B. Bosquejo de norma de SFM

Objetivos de la norma:

- i) Interoperabilidad (servicios entre bancos);
- ii) Posibilidad Funcionamiento independientemente del operador de telefonía móvil con que el cliente guarde una relación comercial; y
- iii) Seguridad de la información al más alto nivel

Contenido de la Norma:

- Se normaran de forma separada Banca Móvil y Pagos Móviles
- Coexistencia de SFM prestados por IFIs y por empresas vinculadas a las operadoras telefónicas con respaldo de Fideicomisos administrados por Bancos.

- Establecer requisitos mínimos de carácter general sobre la gestión de los riesgos operativos y de lavado de dinero y financiamiento al terrorismo asociados al desarrollo de los SFM; así como requerimientos de información para monitoreo de operaciones.
- Primera fase tecnología con cifrado de información de punto a punto y luego migración a cifrado de información fuerte.
- Acreditación y cargo de fondos en tiempo real de las operaciones en servicios financieros móviles.
- Montos Máximos de las Operaciones y número de transacciones:
- Las instituciones deberán remitir mensualmente información de sus operaciones diarias para ejercer su rol de vigilancia.

- Procedimientos y prácticas de supervisión que se deberían implementar para SFM

- Las entidades deberán mantener las bitácoras de monitoreo de las transacciones realizadas mediante los SFM
- Verificar la existencia y cumplimiento de políticas establecidas para la operatividad de los SFM
- Revisión de contratos suscritos entre los entes participantes
- Revisión de planes de contingencias y continuidad de operaciones de los SFM

Sobre los límites a las transacciones:

Se sugiere no imponer límites a las entidades financieras sobre las transacciones que se realicen a través de corresponsales u otros canales alternativos, ni en cuanto a su número ni en los valores de éstas; si no más bien requerir a dichas entidades que los establezca en sus manuales y políticas y que demuestren técnicamente el por qué de las consideraciones adoptadas. (dentro de un max establecido por el regulador).

ANNEX V: RECOMENDACIONES DE SUPERVISIÓN Y REGULACIÓN DE SERVICIOS FINANCIEROS MÓVILES

CONTENIDO

1. Beneficios de los SFM
2. Supervisión y vigilancia
3. Recomendaciones para la Regulación de SFM
4. Requerimientos de información
5. Recomendaciones para la Supervisión de SFM
6. Simplificación de medidas LD/FT

1. Beneficios de los SFM

- Acceso a servicios financieros.
- Propician el ahorro en los usuarios.
- Facilitan la realización de transferencias, pagos cotidianos y retiros/cash-out.
- Facilitan el envío de remesas.
- Ofrecen mayor seguridad para los recursos almacenados/ahorrados.
- Propician planes presupuestarios.
- Reducen costos en el manejo de los recursos.
- Permiten realizar transacciones financieras de manera remota.
- Generan historiales transaccionales que pueden permitir acceso a productos financieros más complejos.
- Reducen el costo de traslado de usuarios hacia una agencia/agente de efectivo.
- Ofrecen una efectiva rastreabilidad por medio del registro electrónico de toda transacción u operación efectuada.
- Resguardan la seguridad del titular de los fondos (PIN).

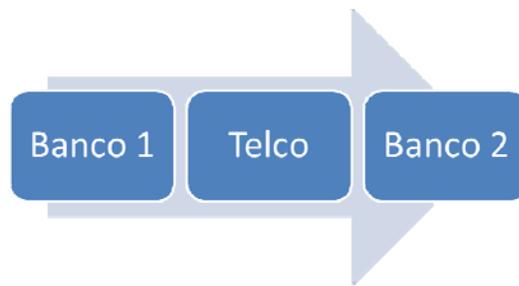
- El potencial de alcance se incrementa notablemente:
 - Mayor cobertura geográfica
 - Mayor cobertura socioeconómica
- La innovación tecnológica e institucional que representan propicia la inclusión financiera (Principio 3, G20).
- En modelos bancarios:
 - Se cuenta con el respaldo de una institución supervisada con regulación prudencial.
 - Se propicia una mayor y más efectiva intermediación financiera con sus consecuentes beneficios en la economía.
 - Se reduce la necesidad de agencias bancarias por lo que se incurre en menores gastos de inversión en infraestructura y en mano de obra.
- En modelos no bancarios (Telcos):
 - Amplia base de clientes actual.
 - Efectividad en las capacidades de mercadeo.
 - Infraestructura física de distribución acorde.
 - Experiencia en administración de transacciones de bajo monto y alto volumen.

2. Supervisión y vigilancia

- La supervisión y vigilancia de los SFM está surgiendo como una nueva y muy distinta área en la comunidad internacional de reguladores.
- Los SFM ponen a prueba los procesos de supervisión y vigilancia tradicionales mediante la introducción de nuevos productos, nuevos canales de distribución y nuevas alianzas corporativas.
- En el contexto de SFM se puede entender la **Supervisión** como las actividades realizadas por las autoridades competentes para asegurar que los proveedores de servicios cumplan con los requerimientos regulatorios aplicables y gestionen adecuadamente los riesgos.
- La **Vigilancia** se refiere a las actividades realizadas por las autoridades competentes para monitorear y analizar los indicadores claves de los SFM como parte de un sistema de pagos, para lograr una valoración objetiva de los requerimientos regulatorios actuales y para hacer propuestas para su ajuste.

3. Recomendaciones para la Regulación de SFM

- Un sistema de supervisión efectivo para SFM no puede desarrollarse si no existen ciertas **condiciones en el marco regulatorio**:
 - Definición clara de los SFM.
 - La creación de un ambiente que habilite la entrada de nuevos participantes del mercado.
 - La identificación de criterios específicos para la prestación de servicios por parte de entidades bancarias y no bancarias.
- En materia de **protección al consumidor** a regulación debe requerir
 - Transparencia plena mediante divulgación de los términos y condiciones incluyendo todos costos o cargos relacionados con la utilización de los SFM.
 - La atención permanente al usuario.
 - Procedimientos de resolución disputas.
 - Educación financiera para los clientes.
 - Capacitación para los agentes
- La normativa debe diseñarse no solo para requerir la adecuada y segura prestación de los SFM sino también para incorporar procesos robustos y acordes de **administración de riesgos**.
- Al desarrollar regulación es importante buscar un **balance en cuanto a los costos** de la misma de tal manera que los SFM no sean más costosos que los canales tradicionales.
- La regulación debe ser **tecnológicamente neutral**, es decir no debe favorecer ni prescribir ningún esquema tecnológico en particular.
- El supervisor/regulador debe tener la facultad de **aprobar los modelos de SFM**, o en su defecto de requerir cualquier tipo de ajuste con tal de estar satisfecho con el rigor de los mismos.
- La regulación debe establecer **límites máximos** de operaciones y de montos para las transacciones para mitigar riesgos de LD/FT y de riesgo operacional.
- El regulador debe fomentar/incentivar la **interoperabilidad** así como la interconectividad entre todos los participantes del ecosistema:



- Todo ecosistema de SFM requiere de una amplia **red de agentes de efectivo**, por lo tanto es imprescindible que la regulación incluya:
 - Definición de agentes.
 - Sus funciones permitidas.
 - Contenido de los contratos.
 - Proceso de aprobación.
 - Procedimientos de evaluación, capacitación y supervisión.
 - Reportes regulatorios.
- La regulación debe considerar **medidas de salvaguardia de los fondos**, las cuales tienen como objetivo garantizar que los fondos estén disponibles para satisfacer la demanda del cliente en sus operaciones de cash out.
- Estas medidas se convierten en particularmente relevantes para modelos nonbank-based.
- Estas medidas incluyen el requisito de que las entidades no bancarias mantengan **activos líquidos aprobados** cuya suma sea igual al monto de dinero electrónico emitido y pendiente de reembolso.
- Generalmente estos activos líquidos comprenden:
 - Cuentas bancarias en entidades sujetas a normativa prudencial
 - Activos financieros de bajo riesgo como títulos valores del Estado, o bien títulos emitidos por entidades aprobadas
- Otras medidas de salvaguardia de los fondos incluyen:
 - Requerir que los proveedores de SFM tengan como **única línea de negocio** la emisión de dinero electrónico
 - Requerir que para la prestación de SFM se constituya una **entidad jurídica independiente**
 - **Restringir el uso de los fondos**, particularmente lo relativo a la concesión de financiamientos.
- Estas medidas también buscan facilitar la supervisión y aislar el negocio de dinero electrónico de otros riesgos institucionales asumidos mediante otras actividades.
- La regulación también debe considerar **medidas de aislamiento de los fondos**, las cuales requieren que los fondos que impliquen dinero electrónico emitido deban aislarse del riesgo institucional de reclamaciones por parte de acreedores diversos de la entidad.
- La **utilización de un fideicomiso** puede ser una medida recomendable para asegurar el aislamiento de los fondos de las reclamaciones de los acreedores de la entidad.
- Esta gestión separada facilita la labor de supervisión y el cumplimiento de medidas de salvaguardia.

4. Requerimientos de información

- El regulador debe requerir información y datos estadísticos de parte de todos los participantes que suministren SFM, independientemente del modelo adoptado.
- La información debe revelar la situación del **acceso y del uso** de los SFM.
- Dada la naturaleza dinámica e intangible de los SFM la recepción de la información relevante y exacta de forma oportuna se vuelve sumamente importante.
- La información será útil para medir los SFM y el impacto de los mismos, así como para poder tomar decisiones prudentiales con bases ciertas.

- Objetivos de los requerimientos de información:
 - Evaluar incremento de riesgos para proveedores individuales así como para el sistema como un todo.
 - Asegurar que la entidad tiene las condiciones financieras para adecuadamente apoyar las actividades de SFM.
 - Promocionar operaciones de mercado estables y transparentes para fomentar la adecuada divulgación pública.
 - Verificar la adecuación de los procesos de administración de riesgos
 - Verificar que los derechos e intereses de los consumidores financieros están siendo protegidos y que hay transparencia
 - Valorar el alcance de los SFM y el impacto de los mismos en la inclusión financiera.

- Los requerimientos de información para SFM inician con la aplicación y autorización.

- Los aplicantes deben entregar información financiera y no financiera sobre las operaciones que pretendan realizar:
 - Plan de negocios y servicios a ofrecer.
 - Modelo operativo y terceros participantes y contratos.
 - Información financiera y del negocio.
 - Estudio de factibilidad y ejecución de pruebas con resultados satisfactorios.

- Una vez las entidades están licenciadas los requerimientos de información deben de incluir aspectos cualitativos (ocasionales) y cuantitativos (periódicos)
- Los reportes periódicos deben de procurar estandarización y convergencia entre los distintos modelos.
- Los requerimientos a las entidades aprobadas deben permitir verificar el cumplimiento de la normativa y la eficiencia de los modelos.



- Información sobre protección del consumidor:
 - Proceso de diseminación de información al consumidor sobre: cuotas, tasas y costos por medio de todos los canales disponibles.
 - Proceso de atención de quejas de clientes.
 - Cantidad y monto de operaciones no notificadas reportadas por clientes.
 - Cantidad de clientes que reportaron reclamos.
 - Proporción de reclamos resueltos a favor del consumidor.
 - Estado de las resoluciones y fecha del reclamo por parte de los clientes.
- Información sobre alcance e inclusión financiera:
 - Cantidad y distribución geográfica de agentes y/o puntos de cash in/cash out.
 - Cantidad de clientes, registrados y activos.
 - Cantidad de cuentas activas e inactivas.
 - Cantidad de nuevas cuentas en período de tiempo reportado.
 - Cantidad de operaciones por tipo de canal (P2P, P2B, B2P, G2P y P2G).
 - Saldos por cuenta.

5. Recomendaciones para la Supervisión de SFM



- El supervisor debe verificar que las entidades que ofrezcan SFM cuentan con:
 - Un proceso de identificación de agentes.
 - Un proceso de identificación de clientes.
 - Procedimientos de LD/FT propios de SFM.

- Que las transacciones se realizan en tiempo real.
- Que los clientes reciben notificaciones de cada transacción realizada
- Plataforma de seguridad, confidencialidad e integridad (hardware y software).
- Es importante que el supervisor verifique que se están aplicando convenientemente las medidas de salvaguardia y de aislamiento de los fondos
- Como parte de esto, se debe supervisar que los fondos están almacenados en cuentas colocadas en entidades reguladas y que están restringidos en su naturaleza.
- El proveedor del servicio es responsable de la protección y aislamiento de los fondos.
- Los procedimientos de supervisión de SFM deben enfocarse en:
 - Asegurar el cumplimiento de los requerimientos regulatorios.
 - Asegurarse que todas las partes cumplen sus obligaciones respecto. de la relación legal que surge por la prestación de los SFM.
 - Determinar horizontes de tiempo para resultados tales como liquidación y compensación, notificaciones a clientes, entre otros.
 - Verificar el cumplimiento de límites.
- Metodología de trabajo para la supervisión:
 - Planificación por áreas de interés.
 - Elaborar matriz de análisis del riesgo inherente acompañada de las cédulas de trabajo complementarias.
 - Elaborar matriz de análisis de la gestión y control aplicada por la entidad acompañada de las cédulas de trabajo complementarias.
 - Informe final con recomendaciones para entidad supervisada.
- El registro de los teléfonos móviles por persona es fundamental para facilitar la simplificación de apertura de cuentas (DUI por SIM).
- Identificar a los participantes del ecosistema: emisores de emoney, proveedores de servicios de pagos.
- Desarrollar normativa y adicionalmente también guías.
- Es importante que al desarrollar normativa para entidades bancarias y no bancarias se procure fomentar igualdad de condiciones de tal manera que se permita la sana competencia sin arbitrajes regulatorios.

6. Simplificación de medidas

- Es importante buscar el equilibrio entre facilitar el acceso para fomentar la Inclusión Financiera y mantener el adecuado control y prevención de LD/FT
- Un enfoque basado en riesgos permite evaluar los riesgos y utilizar medidas que los mitiguen, pero que al mismo tiempo apoyen la Inclusión Financiera
- El alto volumen de las transacciones y los bajos montos bajos justifican la simplificación.
- El establecimiento de límites máximos a saldos acumulados, en montos por operaciones, en la frecuencia de transacciones contribuyen a reducir los riesgos de LD/FT y consecuentemente esto permite que se simplifiquen las medidas de KYC.
- La fijación de límites también contribuye a mitigar muchos de los principales riesgos operacionales relacionados con el suministro de SFM.

Otros aspectos relacionados:

- Licenciamiento directamente por parte del encargado del sistema de pagos.
- Simplicidad en documento de identificación para el registro y activación del servicio.
- Habilitación de los agentes para el registro o apertura de cuentas.
- Facilidad en la transmisión de la información entre los agentes y el encargado del servicio.

- En Guatemala desde junio de 2011 se usa el formulario IRS-01, que exige a las instituciones llevar un control sobre límites para evitar que las “personas obligadas” puedan ser utilizadas para lavar dinero o financiar el terrorismo:
 - Operaciones por Q5,000 (US\$625) en el transcurso de un mes.
 - Operaciones por Q20,000 (US\$2500) en el transcurso de un año.
 - 5 operaciones al mes.