SERVICIOS FINANCIEROS DIGITALES Y GESTIÓN DE RIESGO

MANUAL

mastercard foundation

IFC International Finance Corporation WORLD BANK GROUP

AGRADECIMIENTOS

Mastercard Foundation y el Programa de IFC, The Partnership for Financial Inclusion, desean reconocer el generoso apoyo de las instituciones participantes en nuestro estudio: Tigo Tanzania, Kopo Kopo Kenya, FINCA DRC, Fidelity Bank Ghana, y Zoona, así como Genesis Analytics su apoyo en las evaluaciones de riesgo y aportes a este manual. Los autores también desean agradecer a Anna Koblanck por su extensa edición y a los clientes de IFC, proveedores de Servicios Financieros Digitales, y las partes interesadas de la industria que participaron en las entrevistas, incluyendo Software Group, GSMA, y CGAP. Finalmente, Mastercard Foundation e IFC quisieran agradecer especialmente a los autores, Lesley Denyes y Susie Lonie, y a los revisores por sus aportes; David Crush, Ruth Dueck-Mbeba, Justice Durland, Cameron Evans, John Gutin, Richard Ketley, Andrew Lake, Joseck Mudiri, Patricia Mwangi y Gabriela Rojas.

Número ISBN: 978-0-620-71506-5

MANUAL

SERVICIOS FINANCIEROS DIGITALES Y GESTIÓN DE RIESGO

01_
RESUMEN
de técnicas de gestión de riesgo

02_
Riesgo
DEFINICIONES

03_
MARCO
de Gestión de riesgo aplicado

04_
INSIGHTS Y HERRAMIENTAS

Prólogo

Este manual fue diseñado para cualquier tipo de institución financiera que ofrezca o planee ofrecer servicios financieros digitales, tales como dinero electrónico y banca de corresponsales. Se puede tratar de instituciones microfinancieras, bancos, operadores de redes móviles, o proveedores de servicios de pago. El marco conceptual para el riesgo y la gestión de riesgo se basa en estándares mundiales de gestión de riesgo empresariales y mejores prácticas (ISO 31000), pero la aplicación de principios, ilustraciones y descripciones abordan el riesgo desde todas las perspectivas y todos los tipos de proveedores. Los ejemplos y estudios de caso son únicamente ilustrativos y se anonimizan en ocasiones con el fin de reservar la identidad de la institución para permitir una descripción más completa de las circunstancias alrededor de los eventos que ocurrieron. Los ejemplos son característicos del tipo de institución y el entorno de mercado específico, y se deben adecuar antes de aplicarse en diferentes contextos.

El manual no presupone conocimientos previos de gestión de riesgo; sin embargo, si supone una idea moderada de los Servicios Financieros Digitales y Canales de Distribución Alternativos, incluyendo productos, la función de los corresponsales, el papel de la tecnología y los reguladores. En aras de la consistencia, el manual se referirá a Servicios Financieros Digitales, una definición más amplia que se aplica a muchos canales y productos. Se puede encontrar un glosario en la página 109 para descripciones adicionales de los términos utilizados en el manual.

El manual se organiza en cuatro partes:

- La Parte I presenta el marco conceptual para la gestión de riesgo y los elementos clave del proceso. También presenta un contexto general para la gestión de riesgo en Servicios Financieros Digitales.
- La Parte II describe los tipos principales de riesgos que enfrentan los proveedores de Servicios Financieros Digitales, incluyendo ejemplos de varios mercados.
- La Parte III presenta el proceso paso a paso para implementar un marco de gestión de riesgo. Se puede utilizar para guiar el diseño y despliegue de una estrategia de Servicios Financieros Digitales, así como para monitorear y manejar los riesgos durante la implementación de la estrategia.
- La Parte IV destaca las lecciones aprendidas por los clientes de IFC en África, y considera cómo pueden transformarse los servicios financieros digitales en los próximos años, y los riesgos y oportunidades que presentan los Servicios Financieros Digitales a los proveedores de servicios financieros.

Adicionalmente, el capítulo de herramientas ofrece una base de datos de riesgo completa y un glosario que se puede utilizar como guía de referencia cuando una institución desarrolla una estrategia de gestión de riesgo.

CONTENIDO

PARTE III: MARCO DE GESTIÓN DE RIESGO APLICADO 68

ACRÓNIMOS

AfDB	Banco de Desarrollo Africano (African Development Bank)
ALA/CFT	Lucha contra el Lavado de Activos/Lucha contra el Financiamiento del Terrorismo
API	Interfaz de Programación de Aplicaciones
ATM	Cajero Automático
CDA	Canales de Distribución Alternativos
ERM	Gestión de Riesgo Empresariales
GSMA	Groupe Speciale Mobile Association
IFC	Corporación Financiera Internacional
IMF	Instituciones Microfinancieras
ISO	Organización Internacional de Normalización
KPI	Indicador Clave de Desempeño
KRI	Indicador Clave de Riesgo
KYC	Know your Client, Conozca a su Cliente
MNO	Operador de Red Móvil
MOU	Memorando de Entendimiento

ONG	Organización No Gubernamental
P2P	Persona a Persona
PAR	Portfolio en Riego
PIB	Producto Interno Bruto
PIN	Número de Identificación Personal
POS	Punto de Venta
PSP	Proveedor de Servicios de Pago
OTC	Servicios Financieros en Mostrador
SFD	Servicios Financieros Digitales
SIM	Módulo de Identificación del Suscriptor
SLA	Acuerdo de Nivel de Servicio
SMS	Servicio de Mensajes Cortos
TI	Tecnología de Información
TPS	Transacciones Por Segundo
USD	Dólares Americanos
USSD	Servicio Suplementario de Datos no Estructurados

Resumen Ejecutivo

La última década ha visto una ola de servicios financieros innovadores que tienen por objetivo atender a las poblaciones desbancarizadas en mercados emergentes. Individuos de bajos ingresos, microempresarios y poblaciones rurales que anteriormente habían sido excluidos del mercado debido a los altos costos de la expansión física, están teniendo acceso a servicios financieros a través de teléfonos móviles y redes de corresponsales que actúan como representantes de proveedores de servicios financieros. Esto ha resultado en un aumento asombrosamente rápido en la inclusión financiera en algunos países. En otros mercados la adopción ha sido más lenta y los resultados son menos catalizadores, pero todos los mercados están creciendo y se espera que sigan haciéndolo a medida que se desarrollan servicios y productos. Se espera que la expansión de los servicios financieros digitales haga una contribución importante hacia la meta de alcanzar el acceso financiero universal para el 2020.

Sin embargo, con las amplias oportunidades ofrecidas por nuevas tecnologías y las operaciones de negocios innovadoras, también vienen nuevos riesgos. Los riesgos relacionados con la implementación de los servicios financieros digitales se extienden mucho más allá de los riesgos operacionales y técnicos. Para que la industria de la inclusión financiera pueda capitalizar plenamente los beneficios de los servicios financieros digitales, es importante que los riesgos asociados sean entendidos y abordados en forma adecuada. En este campo de rápida evolución, se ha vuelto evidente que lo que le importa a un proveedor le importa a todos, ya que los grandes casos de fraude, a modo de ejemplo, no solo afectan la confianza del consumidor en un proveedor sino en el mercado y en la promesa de la inclusión financiera digital como un todo.

The Partnership for Financial Inclusion es una iniciativa conjunta de IFC y Mastercard Foundation para expandir las microfinanzas y avanzar los servicios financieros digitales en África subsahariana. A través de interacciones con los clientes del programa, así como la industria en general en la región y más allá, identificamos la necesidad de un manual sobre cómo manejar mejor la gestión de riesgo para los servicios financieros digitales. Existen un buen número de publicaciones de la industria que se enfocan en los riesgos específicos, tales como el fraude o el riesgo regulatorio, y algunos documentos enfocados en los retos específicos de ciertas instituciones, tales como el Kit de Herramientas de Gestión de Riesgo de GSMA para los Operadores de Redes Móviles, a modo de ejemplo.

Sin embargo, no existe un manual integral para los riesgos asociados con las implementaciones de Servicios Financieros Digitales en general, que pueda ayudar en términos sencillos a una institución a aprender desde el comienzo qué es el riesgo, cómo el riesgo afecta el despliegue de Servicios Financieros Digitales, y cómo manejarlo. En 2015, nos embarcamos en una serie de proyectos de investigación para responder a estas preguntas y para desarrollar este manual.

En el desarrollo de este manual, entrevistamos a más de treinta profesionales en este tema, proveedores de software y partes interesadas de la industria, y realizamos cuatro evaluaciones a fondo de riesgo organizacional. La mayoría de estos expertos en el área tienen sede en África Subsahariana, pero sus experiencias también pueden ser útiles para otras regiones. Durante la investigación, aprendimos que hay muy pocas instituciones, incluyendo bancos, IMFs y MNOs, con algún tipo de marco de riesgo para Servicios Financieros Digitales. Solamente una institución había desarrollado un marco de gestión de riesgo integral que se utilizaba de manera habitual y reportaba, a nivel de grupo, en forma mensual.

Probablemente no sea coincidencia que también era una de las pocas instituciones que no había tenido ningún fraude públicamente reportado, pequeño o grande. Nos sorprendió que los bancos, en nuestra muestra, tenían los niveles más bajos de marcos de riesgo desarrollados, dado que los bancos son tradicionalmente conocidos como instituciones con aversión al riesgo con departamentos de riesgo y cumplimiento fuertes. Nuestra conclusión es que los proveedores de servicios financieros tienen una necesidad grande de fortalecer las prácticas de gestión de riesgo en Servicios Financieros Digitales para que puedan lograr sus objetivos de negocios.

A través de esta iniciativa de investigación, también se hizo evidente que pese a que los riesgos se pueden describir en varias categorías diferentes, estos a menudo están fuertemente relacionados. Los riesgos tecnológicos, estratégicosy de gestión de corresponsales pueden llevar todos al riesgo reputacional, y el fraude puede incurrir en pérdidas financieras aún mayores por daños reputacionales que por el fraude mismo. También hubo estrategias clave que fueron identificadas como las más efectivas en la gestión de riesgo: por ejemplo, el uso de call centers para hacer seguimiento, monitoreo, y predicción de eventualidades; utilizar procesos robustos de conciliación y liquidación para reducir las pérdidas potenciales; y tomar en serio las alianzas y asegurarse que los aliados se responsabilicen de sus acciones.

Este manual sigue las normas ISO 31000 para la Gestión de Riesgos Empresariales con el fin de establecer principios para la gestión de riesgo de Servicios Financieros Digitales. Las normas ISO utilizan un marco de 7Rs y 4Ts para desarrollar marcos de riesgo, que son:

- Reconocimiento o identificación de riesgos
- Clasificación o evaluación de riesgos
- Responder a riesgos significativos
  - » Tolerar
  - » Tratar
  - » Transferir
  - » Terminar
- Controles de recursos
- Planeación de reacción
- Reporte y monitoreo de desempeño de riesgos
- Revisión del marco de gestión de riesgo

Al hacer una evaluación de riesgo, es importante analizar las causas de los riesgos e identificar las tendencias. La prevención es mucho más eficaz que el control de daños después del hecho. Un ejemplo que surgió de forma repetida en nuestra investigación fue que, la falta de procesos de negocio o su cumplimiento laxo es la causa de la mayor parte del fraude interno a gran escala. El fraude interno a gran escala tiene la capacidad de acabar con un servicio, así como de causar tal grado de daño reputacional como para hacer desaparecer la totalidad del mercado. A menudo se culpa a la tecnología del fraude, pero en muchos casos la oportunidad para el fraude surge por una falta de buenas prácticas operacionales.

A futuro, hay tendencias claves que dictarán cómo miramos el riesgo y los Servicios Financieros Digitales. El ritmo de las mejoras tecnológicas y la penetración de los teléfonos inteligentes determinará cómo se desarrollarán y ofrecerán los servicios al mercado, y las regulaciones seguirán cambiando según las dinámicas del mercado. En un número creciente de jurisdicciones los reguladores están comenzando a exigir la interoperabilidad entre los servicios de pagos, incluyendo dinero electrónico, así como impedir que los proveedores firmen acuerdos de exclusividad con los corresponsales. Aunque la visión a más largo plazo es una reducción en el uso de efectivo a medida que las personas adoptan los Servicios Financieros Digitales para más transacciones, en el momento, el efectivo sigue dominando. Es esencial, por tanto, que los proveedores sigan enfocándose en la gestión de la liquidez y que permitan a los clientes hacer retiros de forma habitual, y gestionen los riesgos asociados.

Nuestra esperanza es que este manual sirva como orientación y soporte útil a las organizaciones que emplean servicios financieros digitales para expandir la inclusión financiera. La buena gestión de los riesgos implícitos es necesaria para consolidar plenamente las oportunidades de las nuevas tecnologías y modelos de negocio con el fin de beneficiar a los proveedores, aliados, clientes y economías emergentes por igual.

Introducción

IFC apoya a las instituciones que buscan desarrollar servicios financieros digitales con el objetivo de aumentar la inclusión financiera, y está comprometida con múltiples iniciativas a lo ancho de una gama de mercados a través de su portafolio de inversiones y proyectos de asesoría. En África Subsahariana, muchos proyectos de asesoría son implementados en alianza con Mastercard Foundation en una iniciativa conjunta que también incluye una agenda integral de investigación. Muchos de los aprendizajes tempranos de estos proyectos fueron capturados en el Manual de Canales de Distribución Alternativos y Tecnología[1] que ofrece una guía integral de los componentes de una estrategia de Servicios Financieros Digitales y, en particular, cómo entender los elementos básicos tecnológicos para un despliegue exitoso. Junto con el apoyo en la expansión de la inclusión financiera a través de Servicios Financieros Digitales, es importante asegurar la sostenibilidad y confiabilidad por medio de la implementación de prácticas de gestión de riesgo efectivas y responsables.

La investigación para este manual incluyó tres componentes: entrevistas con aproximadamente 30 expertos; cuatro estudios de caso exahustivos con Tigo Tanzania (MNO), FINCA DRC (IMF), Kopo Kopo Kenya (Proveedor de Servicios de Pago) y Fidelity Bank en Ghana; y un taller de clientes de dos días llevado a cabo en Ciudad del Cabo en noviembre de 2015. Los objetivos de la investigación fueron:

- Definir claramente y describir todos los tipos de riesgo a los que pueden enfrentarse los proveedores de servicios financieros que utilizan Servicios Financieros Digitales.
- Ofrecer lineamientos fáciles de usar para realizar diagnósticos de riesgo, evaluaciones, desarrollar marcos de riesgo, e implementar herramientas de gestión de riesgo.
- Analizar cómo los diferentes tipos de instituciones financieras evalúan actualmente el riesgo e implementan herramientas de gestión de riesgo.
- Identificar las lecciones aprendidas generales de los proveedores de servicios financieros acerca de la gestión de riesgo en Servicios Financieros Digitales, que sean relevantes para otros mercados y organizaciones, en temas tales como la integración con marcos de riesgo existentes en las instituciones; indicadores de riesgos claves; los tipos más comunes de riesgos afrontados; cómo mitigar mejor el riesgo; y las mejores prácticas para la gestión de riesgo en Servicios Financieros Digitales.

Encontramos que, aunque la mayoría de los proveedores han extendido sus marcos de riesgo existentes para incluir los canales alternativos, solo hay una incipiente comprensión del riesgo adicional que conllevan los Servicios Financieros Digitales. Esto es particularmente pertinente debido a que los despliegues de Servicios Financieros Digitales a menudo significan que las organizaciones se dedican a actividades de negocio por fuera de su negocio principal, tales como, los operadores de redes móviles ofreciendo servicios financieros a través de billeteras electrónicas, o bancos e IMFs aliándose con MNOs para ofrecer productos bancarios tradicionales a través de canales nuevos. Hay una necesidad creciente de orientación acerca de la gestión de riesgo en Servicios Financieros Digitales que sea relevante y esté al alcance de todo tipo de proveedores.

Hay varios documentos de referencia excelentes que presentan detalles técnicos acerca de la creación de un marco de gestión de riesgo (ver página 111) y esta publicación no busca replicar éstos. Nuestro foco es describir los principios básicos subyacentes de la gestión de riesgo para expertos que no son especialistas en riesgo pero que están involucrados en el establecimiento y la protección de un negocio de Servicios Financieros Digitales. Al igual que con cualquier servicio nuevo, hay mucho que aprender y muchos retos y riesgos no anticipados que se deben abordar. Este manual sirve como orientación para expertos en la identificación, evaluación, y mitigación de los riesgos específicos a los Servicios Financieros Digitales.

[1] Manual de Canales de Distribución Alternativos y Tecnología, IFC, 2015

01

PARTE 1

Resumen de Técnicas de Gestión de Riesgo

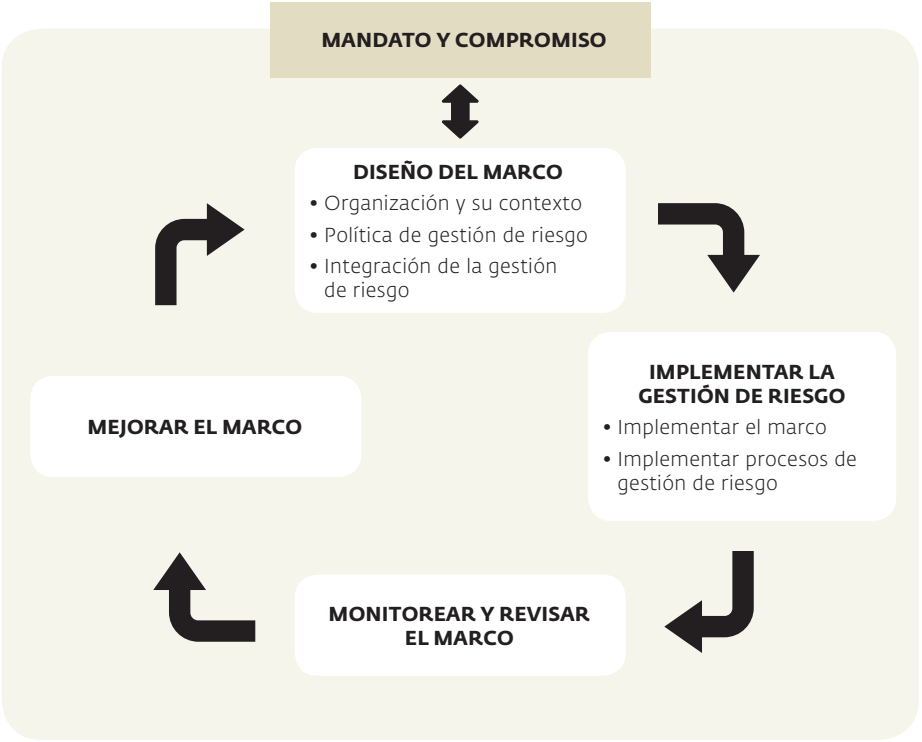
El riesgo se puede describir[2] como el efecto de la incertidumbre sobre los objetivos. Hay muchas definiciones, aproximaciones, y marcos utilizados a lo largo de varios negocios e industrias, siendo uno de los estándares globales el ISO 31000. Las consecuencias del cambio en circunstancias o eventos puede ser positivo o negativo. Esta sección del manual plantea los principios conceptuales de un marco de gestión de riesgo, el proceso de gestión de riesgo, y los componentes clave del desarrollo de un marco de gestión de riesgo para Servicios Financieros Digitales.

La gestión de riesgo comienza con el mandato y el compromiso de los entes de la dirección y gobernanza de la institución, y es seguida por el diseño de un marco, la implementación de gestión de riesgo, el monitoreo y revisión del marco, y finalmente, hacer las mejoras continuas del marco. Establecer un marco de riesgo efectivo es un aspecto esencial de una buena gobernanza corporativa para todas las compañías y debe ser una prioridad clave para las Juntas Directivas y la alta dirección. La implementación de un marco de gestión de riesgo requiere un departamento de riesgo apropiado para el tamaño y complejidad de la organización. Casi todas las instituciones financieras deben tener una jefatura de gestión de riesgo, con funcionarios o departamentos responsables de las diferentes áreas de riesgo. Para los Servicios Financieros Digitales, el área que generalmente está menos desarrollada es la de riesgo operacional, y ésta es la que requiere la mayor atención. Los equipos que participan en la gestión de operaciones de Servicios Financieros Digitales tienen mayor conciencia de lo que se requiere y qué puede salir mal, y se deben incluir tan pronto como sea posible en el proceso de planeación de una estrategia de riesgo en Servicios Financieros Digitales. Esto ofrece un contrapeso muy útil a los equipos de desarrollo de negocios que a menudo no llegan a anticipar los riesgos en las estrategias que están promoviendo y ven a las evaluaciones de riesgo como un impedimento al progreso.

[2] Guía ISO 73 del ISO 31000

"La Gestión de Riesgo comienza con el mandato y el compromiso de la administración."

Figura 1: *Marco para la gestión de riesgo (basado en ISO 31000)*



Fuente: AIRMIC, Alarm, IRM: 2010

Marcos de Gestión de Riesgo

Todos los negocios están sujetos a una gama de riesgos, algunos de los cuales se anticipan, pero muchos de los cuales no son esperados o no se manejan de manera efectiva. La adopción de un marco de gestión de riesgo formal, puede ayudar a los negocios a una planificación más efectiva, entendiendo por qué las cosas no han salido como se planearon e idealmente en la toma de acción antes de incurrir en pérdidas. El objetivo de tener un marco de gestión de riesgo efectivo es ser proactivos en lugar de reactivos en la gestión de los riesgos inherentes en un modelo de negocios.

Según ISO 31000, hay siete Rs y cuatro Ts de marcos de gestión de riesgo:

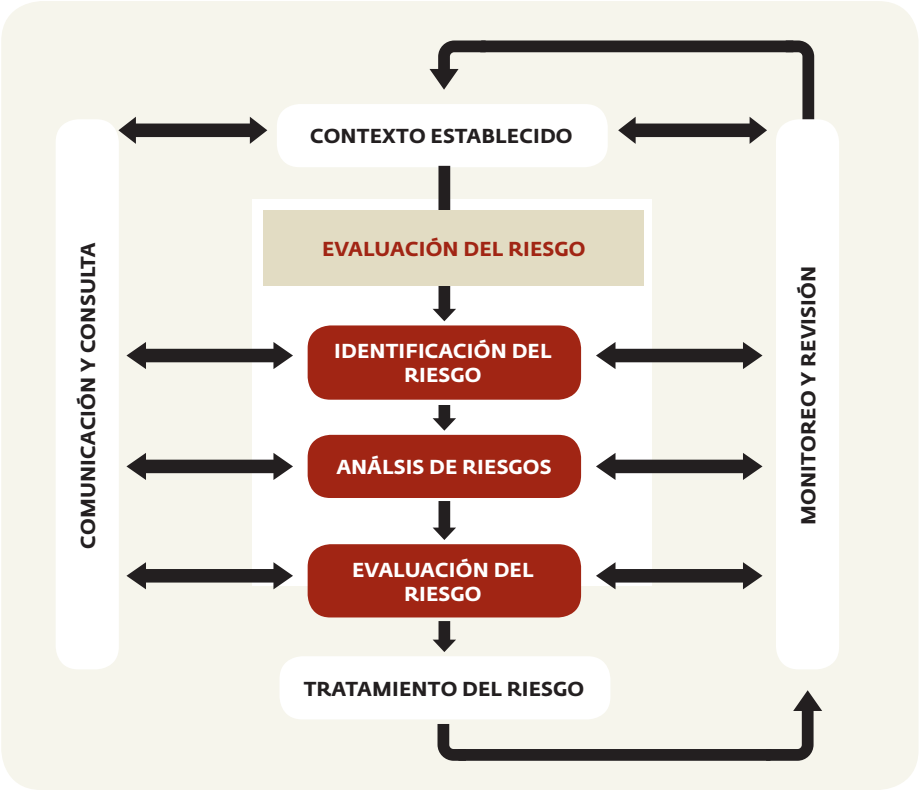
- Reconocimiento de los riesgos: Las lluvias de ideas e identificación de todos los tipos y subtipos de eventos de riesgo que pueden ocurrir e impactar la implementación de los Servicios Financieros Digitales;
- Clasificación o evaluación de riesgos: Uso de criterios cualitativos basados en la probabilidad e impacto potencial para clasificar los riesgos de importancia más alta a la más baja;
- Responder a riesgos significativos: desarrollo de estrategias de riesgo basadas en probabilidad e impacto potencial:
  - » Tolerar: Para los riesgos de baja probabilidad de ocurrencia y bajo impacto potencial, los riesgos se pueden aceptar o tolerar debido a que el costo de mitigar o eliminar el riesgo puede ser mayor que su impacto potencial.
  - » Tratar: Para los riesgos con probabilidad de ocurrencia e impacto potencial moderado, el tratamiento puede ser aplicado para mitigar la pérdida potencial si ocurren los eventos.
  - » Transferir: Para los riesgos con alta probabilidad de ocurrencia y alto impacto potencial, el riesgo se puede transferir a un tercero por medio de la tercerización o la compra de seguros.
  - » Terminar: Para los riesgos con muy alta probabilidad de ocurrencia e impacto potencial, el riesgo se puede terminar, descontinuando la oferta de Servicios Financieros Digitales o recurriendo a alternativas como conseguir aliados o proveedores nuevos.
- Controles de recursos: Desarrollo de presupuestos para aplicar respuestas a riesgos.
- Planeación de reacción: Desarrollo de respuestas tácticas al riesgo.
- Reporte y monitoreo de desempeño de riesgos: Informes periódicos sobre el desempeño en riesgo para determinar si, el riesgo ha ocurrido y si se han presentado pérdidas; ha ocurrido y se ha mitigado; o si no ha ocurrido aún.
- Revisión del marco de gestión de riesgo: Revisar y reiterar la gestión de riesgo en forma periódica o cuando ocurren eventos significativos.

Los marcos de gestión de riesgo son un conjunto integral de políticas que apuntan a reducir el impacto de los riesgos asociados con Servicios Financieros Digitales. El marco es la culminación de todos los procesos de planeación y evaluación, y el registro de riesgo es el cuerpo y documento de trabajo principal. La metodología para el desarrollo de un marco de gestión de riesgo se puede encontrar en la Parte III de este manual.

Proceso de gestión de riesgo

El desarrollo de un Marco de Gestión de Riesgo conlleva a hacer un proceso de valoración de riesgo en el que se identifica, evalúa, y desarrolla la estrategia de tratamiento del riesgo para los riesgos asociados a los Servicios Financieros Digitales.

Figura 2: Proceso de Gestión de Riesgo



Fuente: AIRMIC, Alarm, IRM: 2010

01_RESUMEN

Un marco de gestión de riesgo comienza con el establecimiento de un contexto de riesgos; debe buscar identificar y clasificar los riesgos involucrados (e idealmente medir los riesgos); evaluar, ponderar, y analizar los riesgos; evaluar y planear cómo minimizar estos riesgos; desarrollar tratamientos para el riesgo; y monitorear y revisar los resultados del tratamiento del riesgo.

El producto final de una evaluación de riesgo es un marco de gestión de riesgo, incluyendo un registro de riesgo. También conocida como una matriz de riesgos, el registro de riesgo se usa en forma intercambiable para describir la base de datos central de los riesgos identificados, junto con la descripción de los mismos, sus causas, efectos, y políticas, sea que se toleren, traten, transfieran o terminen. Los registros de riesgo son el centro de un marco de gestión de riesgo, ya que capturan todos los eventos posibles y permiten a los usuarios monitorear, reportar, y reevaluar los riesgos en forma continua. Los registros de riesgo también permiten a los proveedores plantear todos los sub-niveles de riesgo y crear estrategias de riesgo de manera que, si se presenta un evento de un nivel, hay una estrategia para evitar que este vaya al siguiente nivel, del mismo modo que el malware que infiltra un sistema, pero se detiene antes de lograr acceso a datos sensibles.

Los registros de riesgo incluyen:

CATEGORÍA DEL RIESGO
Riesgo Estratégico, Regulatorio, Operacional, Tecnológico, Financiero, Político, Fraude, Gestión de Corresponsales, Reputacional o de Socios

NOMBRE DEL RIESGO
Nombre claramente definido del riesgo identificado

DESCRIPCIÓN
Descripción elaborada del riesgo

DUEÑO
Persona responsable de monitorear el riesgo e implementar una estrategia de tratamiento

CAUSA
El evento que llevaría a que se actualizara el riesgo, si ocurriera este

EFECTO
El impacto al que llevaría el evento si llegase a ocurrir

ESTRATEGIA DE RIESGO
Tolerar, Tratar, Transferir o Terminar

ESTRATEGIA DE TRATAMIENTO DE RIESGO
La estrategia sobre cómo mitigar o controlar el riesgo

RESPUESTA TÁCTICA DE TRATAMIENTO
Las implicaciones en cuanto a política o procedimiento de la estrategia de tratamiento de riesgo

INDICADOR CLAVE DE RIESGO
Un indicador utilizado como alerta temprana de que los efectos adversos del riesgo particular pueden ocurrir

ESTADO ACTUAL
Si el evento de riesgo no ha ocurrido aún; ha ocurrido y se ha tratado con éxito; o ha ocurrido y causó pérdidas.

Se han incluido ejemplos en la siguiente sección para ilustrar este proceso. El registro de riesgo es un documento vivo que se reevalúa y actualiza con base en un período predefinido o cuando ocurre un evento mayor o inesperado. Se utiliza como el cuerpo del conocimiento de los riesgos para la institución y su implementación de Servicios Financieros Digitales. Se incluye una plantilla para un registro de riesgo en la sección de Herramientas, de este documento.

02_

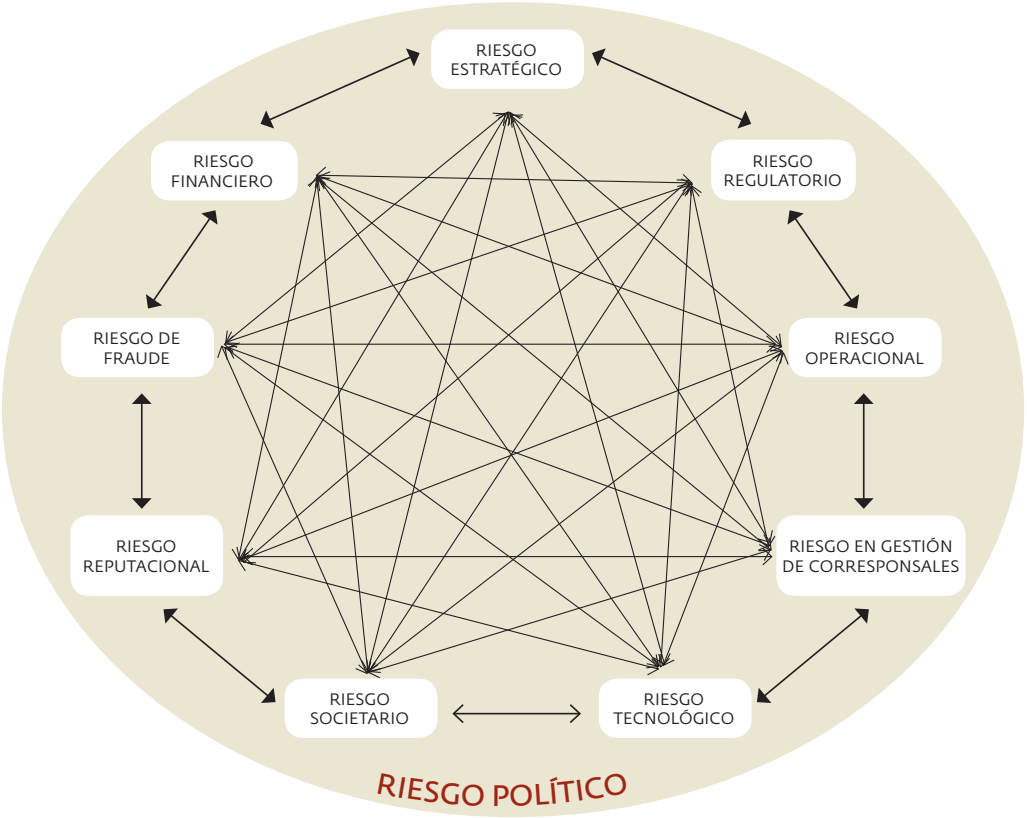
Parte II

Definiciones de Riesgo

El potencial de los Servicios Financieros Digitales viene acompañado de riesgos inherentes en la medida que las operaciones e interacciones con clientes son tercerizadas a corresponsales, quienes abren cuentas y realizan transacciones en representación del proveedor. En la historia reciente, unos pocos casos notables de fraude han afectado la reputación y viabilidad financiera de algunas operaciones. Si bien el riesgo de fraude en los Servicios Financieros Digitales es el riesgo más importante y mejor entendido, hay muchos otros que no siempre se incorporan en el marco de gestión de riesgo de un proveedor, aunque pueden ser igualmente dañinos. Estos incluyen: riesgos estratégicos, regulatorios, operacionales, tecnológicos, financieros, políticos, de fraude, gestión de corresponsales, reputacional o de socios.

Cada una de estas categorías de riesgo se describen y explican en esta sección, incluyendo un número sustancial de sub-categorías. Con cada riesgo, también se identifican y exploran estrategias apropiadas de mitigación. Los estudios de caso y ejemplos prácticos dan una comprensión más profunda de los conceptos. Cada categoría de riesgo también ilustra cómo se podría usar un registro de riesgo como parte de la estrategia de gestión de riesgo de una organización para documentar elementos claves tales como la identificación de riesgos, dueño del riesgo, evaluación, tratamiento, e indicadores. Está incluida una lista de control útil que le hace preguntas críticas al lector y le reta a reflexionar sobre sus propios riesgos organizacionales.

Figura 3: Categorías e Interacciones de Riesgo



Los riesgos no caen estrictamente en una categoría. Si surge una situación de riesgo en un área puede crear a menudo una situación de riesgo en otra área, y todos los riesgos se deben considerar en conjunto. Por ejemplo, las malas decisiones estratégicas respecto del servicio y la selección de tecnología pueden llevar a riesgo tecnológico, el cual a su vez lleva a muchos otros tipos de riesgo, tales como riesgo operacional y de gestión de corresponsales si no hay sistemas de back office apropiados; o al riesgo de fraude si no se suministran las características de prevención de fraude esperadas;o al riesgo reputacional si la experiencia del cliente es mala. Por tanto, una necesidad estratégica de reducir el riesgo de fraude también puede llevar a la necesidad de medidas de prevención de riesgos en operaciones, tecnología, gestión de corresponsales y así sucesivamente.

¿Cuál es su apetito y tolerancia al riesgo?

1. Riesgo Estratégico

El riesgo estratégico se define en sentido amplio como las pérdidas reales que resultan de seguir un plan de negocios equivocado o las pérdidas potenciales resultantes de oportunidades perdidas. Algunos ejemplos de esto pueden ser productos ineficientes; no ser capaces de responder al cambio del entorno de negocios, o distribución inadecuada de recursos.

A medida que crece la dependencia de la tecnología, los proveedores se ven altamente expuestos al riesgo resultante de la innovación y las tecnologías disruptivas del mercado. Establecer la estrategia de la empresa es generalmente responsabilidad de la Junta, la cual debe aportar su experiencia de otras empresas e industrias a la identificación de los riesgos a la estrategia de Servicios Financieros Digitales de la compañía. Los riesgos estratégicos incluyen aquellos relacionados con el branding, las tendencias económicas, la reputación, los modelos de negocios y las posiciones competitivas. También está relacionado con la tecnología, que requiere un sistema confiable, utilizable, escalable y seguro para minimizar el riesgo estratégico.

Los proveedores deben tener un entendimiento profundo de la naturaleza y alcance de los riesgos relacionados con su estrategia de negocios y la tolerancia a su impacto potencial. Para abordar el riesgo estratégico, los proveedores deben centrarse en recoger datos y entender las perspectivas de fuentes externas, incluyendo clientes, bloggers, quienes establecen tendencias en la información, los competidores y analistas del mercado. Para muchas ofertas de Servicios Financieros Digitales, la competencia puede ser muy diferente de la de la organización central, y estos nuevos competidores deben ser identificados y entendidos. Se pueden utilizar modelos financieros para construir análisis de escenarios y pruebas de estrés para comprender mejor los principales factores de la rentabilidad, tales como volumen, valor, ingresos y costos.

La Parte III describe como desarrollar un registro de riesgo. A continuación, se muestra un ejemplo de riesgo estratégico en un registro de riesgo y se incluye la categoría, descripción, dueño, causa, efecto, probabilidad, impacto, estrategia e Indicador Clave de Riesgo.

Registro de Riesgo

Riesgo Estratégico - caso de negocios poco realista

Ejemplo de Proveedor de Servicios Financieros Digitales:	MNO que ofrece una billetera de dinero electrónico
Categoría de riesgo:	Riesgo Estratégico
Categoría Secundaria:	Reputacional
Nombre:	La billetera electrónica del MNO no logra alcanzar la sostenibilidad en el plazo designado
Descripción	El Servicio Financiero Digital no cumple metas de ingresos y gastos, y resulta en ingresos y retorno de la inversión negativos.
Dueño:	Jefe de Dinero Electrónico
Causa:	Mal diseño del producto o del canal, demanda del mercado y/o competencia mal entendidos
Efecto:	Pérdida de inversión
Probabilidad:	2 de 5 Probabilidad relativamente baja basada en estudios de mercado y modelos financieros
Impacto:	3 de 5 Impacto medio basado en que probablemente se darán oportunidades a las operaciones para abordar los problemas antes que las operaciones se detengan
Estrategia de Riesgo:	Tratar
Estrategia de Tratamiento:	• Utilizar la investigación de mercados y benchmarks de la industria para establecer supuestos • Iterar el modelo financiero a medida que avanza la implementación • Asegurar que las metas se difundan y están alineadas con los KPIs • Monitorear el desempeño y actualizar la estrategia según sea necesario
Respuesta Táctica de Tratamiento:	• Determinar las causas del bajo desempeño (diseño del producto, respuesta del mercado) y crear planes para resolverlo • Ajustar el caso de negocios y los objetivos para reflejar la nueva fase del ciclo de vida del producto
Indicador Clave de Riesgo:	• Ingresos netos • Clientes activos • Transacciones por cliente • Corresponsales activos • Clientes por corresponsal • Tipo de interés de encaje
Estado actual:	No ha ocurrido

Cuadro 1

Estudios de Caso de Riesgo Estratégico

A) Lanzamiento de un servicio mal definido: Cuando se lanzó el primer servicio dinero electrónico en África subsahariana, rápidamente logró una enorme popularidad y fue visto por el MNO como un freno a la rotación [NT: churn-buster] significativo que protegería su negocio principal de telecomunicaciones por medio de mayor adquisición y retención de clientes. Como resultado, muchos MNOs africanos estaban preocupados por el riesgo estratégico para su negocio principal si no ofrecían un servicio similar. Esto hizo que muchos MNOs lanzaran servicios de dinero electrónico sin entender adecuadamente el mercado, la propuesta al cliente, la funcionalidad técnica requerida o los recursos necesarios para suministrar un servicio exitoso. El resultado irónico de esto fue que fueron sometidos a las consecuencias de un riesgo estratégico diferente al entrar en un nuevo mercado para el cual estaban mal preparados y al que suministraban servicios de mala calidad.

Los síntomas de la implementación apresurada y la mala ejecución de las decisiones estratégicas se pueden ver en los muchos servicios fracasados lanzados de manera temprana. El mercado estalló con más de 200 servicios lanzados o en desarrollo en los primeros cinco años y con, quizás, un cinco por ciento logrando algo cercano al éxito. La situación está mejorando, pero todavía hay muchos servicios que sufren como resultado directo de estas malas decisiones, manifestadas en falta de personal y presupuesto insuficiente para desarrollar el negocio, y que luchan con una tecnología inadecuada.

B) Pérdida del negocio principal de telecomunicaciones: Generalmente sucede que, para registrarse en un servicio de dinero electrónico de un MNO, el cliente tiene que suscribirse al negocio de telecomunicaciones de ese MNO y utilizar su tarjeta SIM. Esto ofrece beneficios comerciales obvios para el MNO en la adquisición y retención de clientes, pero también restringe el tamaño máximo potencial del Servicios Financieros Digitales al tamaño de la base de clientes del MNO, y si el negocio central de telecomunicaciones disminuye, también lo hace el negocio de dinero electrónico. En los comienzos del dinero electrónico, muchos MNOs consideraron que el beneficio clave de los Servicios Financieros Digitales era su potencial para ofrecer un elemento diferenciador que mejoraba el atractivo de su principal negocio de telecomunicaciones. Hoy en día, la mayoría de los operadores móviles en África subsahariana ofrecen dinero electrónico como parte de su cartera, por lo que eso ya no supone una diferenciación, a menos que tenga algún beneficio convincente que no ofrezca la competencia.

Tanzania tiene varios MNOs exitosos, y la competencia en el espacio de las telecomunicaciones es feroz. Muchos clientes tienen múltiples tarjetas SIM y utilizan el que tenga la mejor oferta en ese momento.

Todos ellos ofrecen servicios de dinero electrónico similares y es común que los clientes se registren para múltiples cuentas de dinero electrónico[3]. Por lo tanto, existe un problema real cuando un MNO ofrece un negocio de telecomunicaciones sostenido y atractivo a los clientes, el negocio de Servicios Financieros Digitales también crece, mientras que los Servicios Financieros Digitales de la competencia sufren por defecto. Para mitigar este riesgo, se están introduciendo Servicios Financieros Digitales de valor agregado en muchos mercados, incluyendo cuentas de ahorro, acceso a créditos y reparto de utilidades de los fondos depositados en cuentas.

C) Aumento en lasTransaccionesde Depósito Directo: El proceso típico para remitir fondos por medio de una billetera es que el cliente deposite dinero en efectivo en un corresponsal y luego remita los fondos realizando una transacción persona a persona. Aunque el depósito es generalmente gratis, casi todos los servicios cobran una comisión por cada transferencia P2P. Los clientes pueden saltarse la transacción P2P y evitar este cobro en el momento en que hacen el depósito, dándole al corresponsal el número de teléfono de la billetera del destinatario en lugar del suyo propio. Los fondos se depositan directamente en la cuenta del destinatario sin nunca tocar la de la persona que realiza el depósito. Esto va en contra de los términos de operación porque no hay registro de la identidad del remitente, que puede infringir las regulaciones de KYC. Saltarse la transacción P2P también puede tener un serio impacto negativo en el modelo de ingresos del negocio. Al corresponsal se le tiene que pagar una comisión por suministrar el servicio de depósitos, y esto se financia típicamente, al menos en parte, con los ingresos P2P. Además, el remitente ni siquiera tiene que ser un suscriptor móvil.

Los depósitos directos son, por lo tanto, una fuente de riesgo regulatorio y financiero potencial, pero el mayor impacto posiblemente sea que socavan el rol estratégico de los Servicios Financieros Digitales de apoyar y proteger el negocio de telecomunicaciones. La mayoría de los operadores de redes móviles están sufriendo niveles crecientes de depósitos directos. Algunos corresponsales son activamente cómplices en ofrecer depósitos directos, mientras que otros no saben que esto está sucediendo. Se están haciendo esfuerzos para identificar a los corresponsales infractores haciendo seguimiento de si un retiro se produce poco después del depósito y en otro lugar. Parece poco lógico depositar y retirar en rápida sucesión, y si el retiro se llevó a cabo lejos del depósito, la transacción fue probablemente un depósito directo. Otro enfoque es rastrear la ubicación del corresponsal y el destinatario del depósito usando el identificador celular; diferentes ubicaciones de nuevo sugieren un depósito directo. Los corresponsales propensos a altos niveles de depósitos directos son advertidos y retirados del servicio si es necesario. Este proceso de detección es costoso en tiempo y mano de obra, pero es actualmente el mejor medio disponible para proteger al negocio del riesgo de los depósitos directos.

RIESGO ESTRATÉGICO - PREGUNTAS CLAVE

- ¿Qué tan bien definida está mi estrategia?
- ¿Qué tan amplios son los riesgos que estamos considerando? ¿Hemos considerado todos los factores internos y externos?
- ¿Cuáles escenarios de riesgo hemos considerado para probar nuestros planes?
- ¿Cuál es nuestro apetito y tolerancia al riesgo?
- ¿Hemos mapeado nuestros riesgos en función de indicadores clave de desempeño y medidas de valor?

[3] En 2014, los usuarios de Servicios Financieros Digitales de Tanzania tenían en promedio 2 cuentas de dinero electrónico http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/03/Tanzania-Enabling-Mobile-Money-Policies.pdf

¿He identificado áreas potenciales para el riesgo de incumplimiento?

2. Riesgo Regulatorio

El riesgo regulatorio se refiere a los riesgos asociados con el cumplimiento (o incumplimiento) de las directrices y normas reglamentarias, como las ALA/CFT, Conozca a su Cliente (KYC, por sus siglas en inglés), protección de datos, límites de cuentas y transacciones, cuentas fiduciarias, y normas respecto al uso de corresponsales. El riesgo regulatorio también incluye normas más amplias relacionadas con el funcionamiento de una institución en particular, como por ejemplo, la concesión de licencias, capital y liquidez. El incumplimiento puede ser en áreas que no están directamente relacionadas con Servicios Financieros Digitales, pero pueden tener un impacto significativo en las operaciones del negocio, incluyendo multas, sanciones e incluso la pérdida de la licencia. El banco central de cada país establece los requisitos para la banca móvil, el dinero electrónico y la banca de corresponsales dentro de su jurisdicción[4]. Generalmente incluyen las políticas que rigen los Servicios Financieros Digitales, a menudo una ley nacional de pagos, una ley de inclusión financiera o una ley de protección al cliente. Los bancos centrales de cada país deciden si permitirán a los bancos, operadores móviles, proveedores de servicios de pagos, o una combinación de estos, prestar servicios a través de Servicios Financieros Digitales. Junto con las instituciones a las que se les permitirá ofrecer servicios, los bancos centrales también dictan requerimientos sobre los siguientes temas:

Debida Diligencia del Cliente: Una de las áreas clave cubiertas por las regulaciones de Servicios Financieros Digitales es la debida diligencia del cliente, incluyendo KYC, lucha contra el lavado de activos y la financiación del terrorismo. Estas regulaciones también pueden ser grandes obstáculos para el desarrollo y el escalamiento de servicios financieros digitales en mercados emergentes, por ejemplo, obstaculizando la capacidad de los clientes para registrarse en un servicio debido a documentos de identificación personal de mala calidad, pruebas insuficientes de residencia o falta de herramientas de verificación biométrica.

Varios bancos alrededor del mundo han permitido un KYC en capas como forma de introducir la proporcionalidad en la gestión de riesgo en los servicios móviles. El riesgo de que se canalicen grandes montos de dinero a través de cuentas móviles para el lavado de dinero o el financiamiento del terrorismo es probable que sea limitado, ya que la mayoría de las cuentas se limitan como cuentas de valor, se pueden rastrear los números de teléfono móvil con cantidades y fechas, requieren PIN de seguridad, y son continuamente monitoreadas. El KYC en capas usa un enfoque basado en riesgo y extiende el acceso proporcional a la cuenta basado en el nivel de requisitos KYC. Se aplican límites proporcionales al monto por transacción, al volumen de movimiento de la cuenta al día, mes o año y al saldo máximo que se puede mantener en cualquier momento.

Gestión de Corresponsales: En la mayoría de los mercados, el uso de corresponsales para actuar en nombre de las instituciones financieras está estrictamente regido por los reguladores. Pueden existir requisitos de negocios para la inscripción de corresponsales, incluyendo si están registrados o tienen licencia, requisitos mínimos de capital, o incluso restricciones al tipo de negocio.

Los reguladores también dictan las funciones que pueden realizar los corresponsales, por ejemplo, si pueden abrir cuentas o no, recoger datos (KYC), realizar transacciones de depósitos y retiros, o realizar transacciones OTC. El regulador puede incluir estipulaciones con respecto a la exclusividad de los corresponsales, por ejemplo, exigiendo que los corresponsales no puedan ser exclusivos a una sola institución financiera.

Los reglamentos de gestión de corresponsales varían de un país a otro. En algunos países, las regulaciones de banca de corresponsales y de dinero electrónico están claramente establecidas e incluyen requisitos completos para la contratación, aprobación, capacitación y la gestión continuada de los corresponsales. En países como Tanzania, el regulador

[4] En algunos mercados, estas normas están todavía en desarrollo y aún no se han implementado.

tiene que aprobar individualmente cada corresponsal que un banco o MFI contrata. En otros mercados, como en Madagascar, actualmente no existen regulaciones y el Banco Central no ha dado ninguna indicación formal de lo que se permite o prohíbe sobre los tipos de corresponsales a contratar, sus requisitos de negocios o las funciones que se les permite realizar. En mercados como estos, el riesgo regulatorio se convierte en uno de los principales riesgos para una implementación de Servicios Financieros Digitales, ya que las instituciones operan bajo circunstancias completamente desconocidas.

Además de los riesgos regulatorios asociados con los corresponsales, existen otro tipo de riesgos que se detallan en la sección Riesgo de Gestión de Corresponsales de este documento.

Seguro de Depósito: El seguro de depósito es un seguro proporcionado a los depositantes para proteger sus depósitos en casos de insolvencia de las instituciones financieras. Por lo general, es un aspecto obligatorio de las leyes que rigen las instituciones financieras, ya que la protección de los depósitos de los clientes es clave para evitar el pánico financiero y mantener un sector financiero estable. El seguro de depósito no suele ser requerido por los bancos centrales para los operadores de redes móviles o proveedores de pagos, ya que no se les permite intermediar los fondos y los saldos de cartera están respaldados al cien por cien en cuentas fiduciarias, normalmente en instituciones financieras de terceros.

Privacidad: Al igual que con todos los servicios financieros, la protección de los datos de los clientes es primordial y se puede mitigar mediante el control de acceso al sistema de TI y la encriptación para proteger el abuso de datos por parte del personal del proveedor. Las regulaciones de protección de datos pueden ser tratadas a través de leyes nacionales de privacidad, regulaciones de telecomunicaciones y/o regulaciones de servicios financieros. La protección de datos es una preocupación cada vez mayor para las instituciones, ya que los grandes hackeos públicos de datos han sido bien documentados en los medios de comunicación, causando pérdidas financieras y reputacionales. La falta de integridad en torno a los datos de los clientes puede llevar a demandas, así como ofrecer oportunidades para el robo de identidad y el fraude.

Interoperabilidad: La interoperabilidad se define como la capacidad de un usuario de una cuenta o billetera de un proveedor para recibir o enviar transferencias a la cuenta de un usuario o billetera de otro proveedor. La interoperabilidad también puede describirse a nivel de corresponsal, cuando un cliente de un proveedor puede realizar transacciones con el corresponsal de otro proveedor. La mayoría de los reguladores no han exigido la interoperabilidad entre los proveedores nacionales, pero algunos han dejado que el mercado autorregule la interoperabilidad. A medida que los mercados maduran, podremos llegar a ver una interoperabilidad más obligatoria en la medida que los reguladores busquen intensificar la competencia en un intento por aumentar las opciones de los clientes y reducir los precios. En África subsahariana, las transferencias interoperables de cuenta a cuenta están actualmente disponibles[5] en Tanzania, Ruanda y Madagascar.

Cuentas Fiduciarias: Todos los proveedores no bancarios de Servicios Financieros Digitales, incluidos los MNOs y los proveedores de servicios de pago, son aprobados por los reguladores, ya sea mediante licencias o 'cartas de no objeción', por un banco central, una comisión de valores o un regulador de comunicaciones con provisiones respecto de tenencia de fondos en una o varias cuentas fiduciarias. Los fondos de dinero electrónico y los fondos depositados en el banco deben coincidir, y a los proveedores no se les permite intermediar los fondos de la manera que lo haría una institución financiera regulada. El objetivo es asegurar que los fondos de los clientes estén protegidos y fácilmente disponibles a solicitud. Estos fondos están protegidos y los proveedores no pueden usarlos para pagar gastos de operación o para pagar a los acreedores. Dependiendo de la regulación, los intereses devengados en la cuenta fiduciaria puede que tenganque ser pagados al cliente o se pueden utilizar como ingresos para el proveedor.

Requisitos Mínimos de Capital: Para los bancos los requisitos mínimos de capital son una parte normal de reglamentaria en la concesión de licencias. En algunos mercados, los reguladores también los requieren para MNOs y Proveedores de Servicios de Pago. Además de los requisitos para que los MNOs y los Proveedores de Servicios de Pago tengan fondos en cuentas fiduciarias, los reguladores también pueden imponer requisitos mínimos de capital para asegurar a los acreedores contra el riesgo de insolvencia y asegurar que la institución tenga suficiente capital para atender los costos operativos iniciales.

[5] Informe GSMA: Estado de la Industria 2015

Registro de Riesgo

Riesgo regulatorio - vinculación inadecuada del cliente

Ejemplo de Proveedor de Servicios Financieros Digitales:	MNO que ofrece una billetera de dinero electrónico
Categoría de riesgo:	Riesgo Regulatorio
Categoría Secundaria:	Riesgo de gestión de orresponsales
Nombre:	El corresponsal no registra adecuadamente al cliente con el procedimiento de KYC completo
Descripción	Los corresponsales pueden cumplir parcialmente con los requisitos de KYC, ya que las comisiones están diseñadas para incentivar la apertura de cuentas y realizar transacciones, no para la diligencia regulatoria.
Dueño:	Jefe de Cumplimiento
Causa:	Mal diseño del producto o del canal, entrenamiento deficiente del corresponsal
Efecto:	Aumento de gastos para seguimiento y recolección de datos de KYC o cierre de cuentas si éstos no pueden ser adecuadamente registrados
Probabilidad:	3 de 5 Probabilidad media basada en una buena formación, pero problema común
Impacto:	1 de 5 Impacto muy bajo basado en la respuesta probable de los reguladores en cuanto a dar advertencias antes que las violaciones sean castigadas
Estrategia de Riesgo:	Tratar
Estrategia de Tratamiento:	• Educación de corresponsales • Alinear los incentivos de los corresponsales únicamente hacia cuentas plenamente registradas • Rediseñar los procesos de negocios para que sean más eficientes en la gestión de cualquier documentación • Cuando los reglamentos lo permitan, abrir cuentas a niveles inferiores de KYC hasta que se pueda recopilar toda la información • Comprador secreto • Sanciones por incumplimiento
Respuesta Táctica de Tratamiento:	• Formación adicional del corresponsal • Aplicar sanciones a corresponsales y/o funcionarios de gestión de corresponsales
Indicador Clave de Riesgo:	• Porcentaje de clientes con registros incompletos • Porcentaje de clientes con registros rechazados
Estado actual:	Ocurrido y mitigado

Cuadro 2

Estudios de Caso de Riesgo Regulatorio

Los riesgos regulatorios más comunes son causados por los dos casos extremos de "falta de regulación" y "exceso de regulación", y ambos pueden conducir a una inversión desperdiciada y pérdida de ingresos.

En los mercados donde hay poca o ninguna supervisión clara de los Servicios Financieros Digitales, hay incertidumbre acerca de lo que el regulador requiere o qué regulaciones pueden ser impuestas en una fecha posterior. Por ejemplo, un importante MNO decidió lanzar su exitoso servicio de dinero electrónico africano en un gran mercado de Asia meridional que apuntaba a un lanzamiento en 2008. La opinión legal era que, en ausencia de una regulación específica, podría construirse un marco adecuado para adherirse a una regulación de pagos más general. Se invirtió una cantidad sustancial de dinero en la adaptación de la tecnología existente a las necesidades específicas del mercado, y se reclutó y formó un gran equipo para administrar las operaciones locales. Apenas dos meses antes del lanzamiento planeado en el primer estado, el regulador expidió algunas nuevas directrices a la regulación existente que efectivamente prohibieron el lanzamiento. Pese a intensas negociaciones, el lanzamiento se retrasó y finalmente se canceló, y el equipo se disolvió. Tres años más tarde, la regulación había sido modificada nuevamente y el servicio finalmente fue lanzado. El costo del retraso para la MNO, tanto directo como en forma de ingresos perdidos, no ha sido revelado.

En un mercado africano, el banco central decidió imponer ciertas limitaciones reglamentarias a cualquier despliegue de dinero electrónico con la intención de asegurar que habría una interoperabilidad total entre los servicios desde el comienzo, y que los riesgos y recompensas potenciales asociados con cada servicio serían compartidos entre varios bancos locales. Desafortunadamente, el regulador no estaba familiarizado con el estado de la tecnología en este mercado naciente y había asumido que tenía una gama de funcionalidades y capacidades que no iba a estar ampliamente disponible durante varios años. Además, el caso de negocios para estos servicios se basó en un entorno de circuito cerrado ("close loop") con sólo una fuente de ingresos. Como resultado, lo que se esperaba que fuera uno de los principales mercados de Servicios Financieros Digitales ha tenido dificultades para lograr impulso y tuvo una mala adopción durante varios años hasta que se modificó la reglamentación para tener en cuenta las realidades del mercado.

RIESGO REGULATORIO - PREGUNTAS CLAVE

- ¿Entiendo completamente todos los requisitos e implicaciones regulatorias aplicables a mi institución, a mis corresponsales y a mis clientes?
- ¿Estoy cumpliendo completamente con estas regulaciones?
- ¿He identificado áreas potenciales para el riesgo de incumplimiento?
- ¿Tengo la seguridad de que los procesos son adecuados para asegurar el cumplimiento continuo?
- ¿He establecido una relación positiva y productiva con mi regulador?

¿Existe un manual de operaciones que detalle todos los procesos de negocios?

3. Riesgo Operacional

El riesgo operacional es inherente a cualquier negocio y se refiere a los riesgos asociados con productos, prácticas comerciales, daños a los activos físicos, así como la ejecución, entrega y gestión del proceso del servicio. En la práctica se refiere a la amplia y diversa gama de actividades necesarias para administrar el negocio. Los riesgos operacionales, en su mayoría, son internos a la organización y por lo tanto pueden ser manejados cuidadosamente. En términos de Servicios Financieros Digitales, la nueva área crítica de operación es el negocio diario de apoyar al canal. Esto puede incluir funciones que tocan todas las partes del negocio, tales como:

- Operaciones de ventas: incluyendo contratación de corresponsales, capacitación y administración continua de corresponsales
- Operaciones de servicio al cliente: prestación de asistencia a usuarios externos del servicio (clientes, corresponsales y otros) y escalamiento de problemas que no puedan resolver
- Operaciones de back office: tales como la creación y edición de cuentas de corresponsales y otras empresariales, solución de problemas y pruebas de cualquier cambio en el servicio (normalmente actualizaciones operativas menores)
- Operaciones financieras: incluyendo la creación de dinero electrónico y asegurar que la cuenta bancaria y de dinero electrónico (control) coincidan, y presentar informes de negocios
- Operaciones técnicas: proveer el ambiente de hosting y soporte para la tecnología.

Procesos de negocio: La clave para operaciones eficientes que minimizan el riesgo es tener procesos de negocio de alta calidad, eficientes y efectivos. Los procesos de negocio siempre deben agregar valor a los clientes y mitigar los riesgos. Aunque muchas instituciones culpan a la tecnología o gobernanza como la causa del fraude, muchos casos de fraude interno importante de Servicios Financieros Digitales se pueden ubicar en procesos de negocios inadecuados (o inexistentes) que permitieron a los estafadores abusar del servicio. Ver página 48 para obtener una descripción completa de los posibles riesgos de fraude.

Cada proceso operacional que se lleva a cabo de manera habitual debe documentarse, describiendo lo que se debe hacer, cómo hacerlo y quién es el responsable de hacerlo. Los procesos de negocios también deben atender las excepciones, especificando qué hacer si algo sale mal en cualquier momento del proceso y no se puede seguir la ruta estándar. Las auditorías internas se utilizan para asegurar que los procesos de negocios sean respetados por el personal.

Los procesos de negocio deben revisarse y actualizarse periódicamente para asegurar que siguen siendo pertinentes. Esto es particularmente importante en la primera parte del ciclo de vida del servicio. A las pocas semanas de lanzar un servicio, la brecha entre la expectativa y la realidad para muchos procedimientos se vuelve obvia. Se recomienda que los borradores de los procesos de negocios creados antes del lanzamiento sean revisados y finalizados tres o cuatro meses después del lanzamiento, cuando el equipo de operaciones tenga experiencia en operaciones reales. Después de eso, idealmente se deben revisar anualmente. Si se introduce una nueva funcionalidad, por ejemplo, la participación de un nuevo socio, tales como las transferencias de banco a billetera, se requerirán nuevos procesos de negocio para gestionar las nuevas actividades.

La tecnología adecuada puede utilizarse para prevenir la aparición de muchos eventos de riesgo, pero en última instancia, en particular porque la tecnología para muchos Servicios Financieros Digitales aún no está madura, la mejor protección contra el riesgo operacional son los procesos de negocios bien construidos que son adecuadamente seguidos y actualizados, y que se revisan periódicamente durante las auditorías internas para asegurar el cumplimiento.

Control interno: Los procedimientos de control interno se utilizan para proteger contra el fraude, las interrupciones, el riesgo reputacional y el riesgo de crédito, asegurando la adherencia a los procesos de negocio. El departamento de control interno realiza auditorías operativas en la organización y sus corresponsales para asegurar que se usen procedimientos correctos en términos de transacciones, apertura de cuentas, KYC y estándares de branding. El departamento de control interno evalúa la efectividad de dichos procedimientos y normas, y hace sugerencias y revisiones de políticas y procedimientos basados en un proceso continuo de retroalimentación y aprendizaje.

Auditoría interna: Las auditorías internas proporcionan garantía y verificación de procesos y controles. El departamento de auditoría interna es responsable de asegurar que la información financiera sea precisa y refleje el estado real de los asuntos financieros de la institución; que los riesgos empresariales sean evaluados y mitigados; y que los controles sean efectivos. La auditoría interna puede realizar auditorías financieras mensuales de la institución, funciones y procesos de alto riesgo, así como auditorías operacionales de sucursales y corresponsales, asegurar una adecuada gestión de liquidez, registro de transacciones y detectar fraude de corresponsales y otros delitos.

Separación de Funciones: La separación de funciones es una metodología de procedimientos que asegura que existan pesos y contrapesos adecuados para proteger contra conflictos de intereses y fallas de control. Un ejemplo de separación de funciones es el principio contable (a veces conocido como, ejecutor, verificador y aprobador) por el cual la persona que lleva a cabo una transacción o proceso está separada de la que registra o revisa la actividad y la que valida la actividad, para minimizar los errores y las oportunidades de fraude y mala gestión de los fondos. Los sistemas informáticos pueden configurarse para que haya acceso basado en roles según los requisitos de cada función de trabajo. Un ejemplo de acceso basado en roles es hacer cumplir la separación de funciones de manera que un operador solo pueda acceder a las funciones requeridas para desempeñar su trabajo. Por ejemplo, atención al cliente no necesita acceso al área financiera donde se crea el dinero electrónico; finanzas no necesita tener acceso al área de ventas donde se crean las cuentas de corresponsales; los miembros junior del equipo pueden tener acceso a las tareas ejecutor, pero no a las tareas del verificador; y así sucesivamente.

Informes Externos: Los grandes financiadores, donantes y accionistas, como las instituciones matrices, pueden requerir informes adicionales para monitorear el desempeño, minimizar el riesgo de sus inversiones y asegurar la detección temprana de problemas, ya sean operacionales o financieros. Generalmente, los informes se realizan trimestralmente para la presentación de informes financieros, y semestrales para la presentación de informes cualitativos sobre el progreso, los retos y las lecciones aprendidas.

Auditoría Externa (Financiera): La mayoría de las instituciones, especialmente las instituciones reguladas o transadas en bolsa, deben hacer auditorías externas al menos una vez al año. Una auditoría externa se centra principalmente en la información financiera de la institución y para garantizar la contabilización exacta de las transacciones, así como una adecuada depreciación y valoración de los activos de la institución. También puede incluir revisiones adicionales a los controles, particularmente para actividades y procesos de alto riesgo.

Daños a Activos Físicos: El daño a los activos físicos puede resultar del desgaste normal, desastres naturales, actos de terrorismo o vandalismo. Los riesgos pueden ampliarse usando Servicios Financieros Digitales, ya que los activos físicos están en fideicomiso a partes externas, tales como corresponsales, y pueden estar en lugares geográficos donde la institución no hace visitas regulares en persona. Es importante que el daño potencial a los activos físicos se incluya como parte de los planes de continuidad de negocio y planes de recuperación de desastres. Las posibles estrategias de mitigación pueden incluir seguros patrimoniales, sistemas de respaldo y almacenamiento externo de datos.

Ejecución, Entrega y Gestión de Procesos: El riesgo operacional derivado del error del operador en la ejecución, la entrega y la gestión de procesos incluye riesgos tales como, errores en el procesamiento de datos, errores contables, falta de informes obligatorios y pérdida negligente de activos del cliente. Está estrechamente vinculado al riesgo tecnológico y es más frecuente en Servicios Financieros Digitales debido a la tercerización de la transacción a los corresponsales. En algunas regiones, los reguladores están implementando nuevas directrices para reducir este riesgo y proteger los fondos de los clientes. La mitigación del riesgo de error del operador puede incluir la separación de funciones entre la persona que realiza la transacción u otra actividad, la persona que la registra o revisa y la persona que la aprueba; el acceso basado en roles a los sistemas; formación de corresponsales y personal; supervisión; transacciones en cuentas transitorias; el monitoreo de transacciones sospechosas para alertar de errores frecuentes en la secuencia de la transacción o corresponsales o personal específico que cometen errores frecuentemente. Análisis de datos, paneles de control y algoritmos pueden ser herramientas poderosas para mitigar los errores de los operadores si son seguidos por resolución, capacitación o mejoras de políticas que reducen el riesgo de errores continuados.

Variaciones en Conciliación y Cuentas: El riesgo de que el valor real de las cuentas en fideicomiso sea diferente del monto reflejado en el sistema de dinero electrónico, así como el riesgo de que las transacciones fuera de la red (por ejemplo, retiros de cajeros automáticos y pagos de facturas) no se concilien con cuentas internas. Siempre puede haber alguna diferencia, pero los altos niveles de variación, o aquellos que son irreconciliables, pueden conducir a pérdidas financieras.

EJEMPLO 3

Registro de Riesgo

Riesgo Operacional - manuales insuficientes

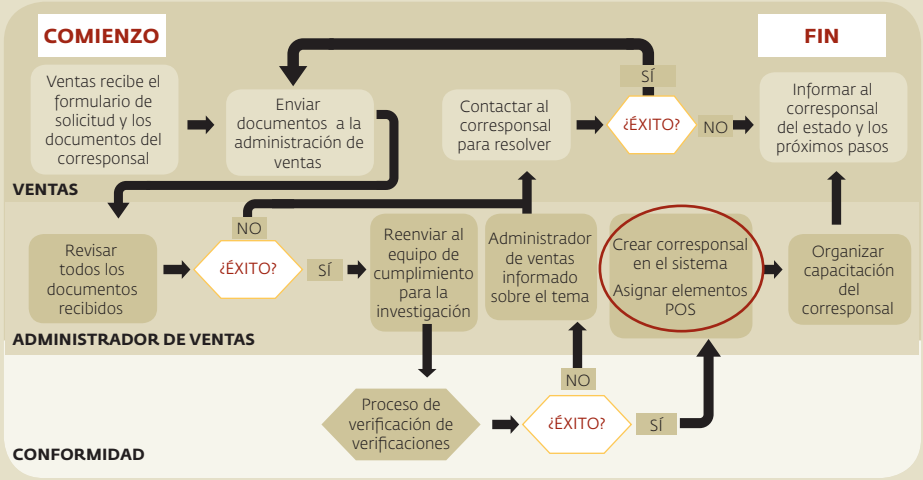
Ejemplo de Proveedor de Servicios Financieros Digitales:	Ya sea un servicio de banca de corresponsales o un MNO que ofrece una billetera de dinero electrónico
Categoría del riesgo:	Riesgo Operacional
Categoría Secundaria:	Riesgo Regulatorio
Nombre:	Falta de manuales operativos y procesos de negocio
Descripción	Ineficiencia del back office porque los manuales de operación están incompletos, careciendo de los procesos de excepción cuando las cosas no van según el plan.
Dueño:	Jefe de Servicios Financieros Digitales
Causa:	Mala planificación e implementación de procedimientos operacionales para apoyar Servicios Financieros Digitales
Efecto:	Podría conducir a una mala administración de sistemas, cuentas de clientes o fondos que resulten en violaciones del cumplimiento o pérdida de fondos
Probabilidad:	2 de 5 Moderadamente bajo, basado en el conocimiento del riesgo y el desarrollo de herramientas, sin embargo, sigue siendo un riesgo que no todos los escenarios están cubiertos
Impacto:	3 de 5 Impacto moderado, basado en pérdidas de reputación y financieras, pero no suficiente para cesar operaciones
Estrategia de Riesgo:	Tratar
Estrategia de Tratamiento:	• Revisar el manual de operación en relación con la lista de procedimientos que se están llevando a cabo. Agregue cualquier procedimiento que falte, actualice los procedimientos existentes según sea necesario y agregue los casos de uso de excepciones a todos. Asegúrese de que los departamentos pertinentes firmen cada proceso • Crear listas de verificación de procesos y asegurar que todos los procesos han sido documentados y son revisados y actualizados periódicamente, si es necesario • Hacer que el mantenimiento de procesos de negocio sea un producto clave del equipo de operaciones.
Respuesta Táctica de Tratamiento:	• Identificar los procedimientos de excepción que faltan. Convocar a un equipo para determinar cuáles deben ser y cuáles son las funciones responsables de ellos • Documentar estas excepciones de proceso • Capacitar al personal en la implementación
Indicador Clave de Riesgo:	• Productividad del equipo de back office medido por » Números de transacciones transitorias resueltas » O el número de días que permanece la transacciónen cuentas transitorias » O tiempo para resolver disputas • Excepciones de transacciones con estado en curso • El centro de llamadas emite una resolución
Estado actual:	No ha ocurrido

Cuadro 3
Estudios de Caso de Riesgo Operacional

Tras el éxito del dinero electrónico en África oriental, como se mencionó anteriormente, muchos operadores móviles decidieron que necesitaban tener su propio servicio de dinero electrónico lo antes posible. Por lo general, poco se pensó en los requisitos técnicos u operativos cuando estaban buscando un sistema de dinero electrónico, y se basaron en el proveedor de tecnología para entender lo que se requería. Como se trataba de un nuevo tipo de servicio, no se disponía de soluciones técnicas, pero muchos proveedores, principalmente proveedores de software con sistemas exitosos de transferencia de dinero o transferencia de tiempo aire, estaban dispuestos a llenar el vacío. La mayoría de ellos había adquirido una buena comprensión de la experiencia del usuario, tanto de clientes como de corresponsales, pero no tenían acceso o comprensión del sistema de back office y las tareas que los operadores de dinero electrónico tenían que realizar. Como resultado, muchos sistemas tempranos parecían buenos desde una perspectiva de usuario, pero no proporcionaban la funcionalidad o los informes necesarios para operar los servicios de manera eficiente. La industria de Servicios Financieros Digitales está llena de historias de proveedores de servicios decepcionados con la tecnología que inicialmente compraron y su incapacidad para realizar las operaciones necesarias (a pesar de que a menudo existía una incapacidad para articular lo que se esperaba de la tecnología cuando se compró).

La tecnología debe reforzar, no reemplazar, procesos empresariales sólidos que especifiquen cómo se debe operar un servicio. Desafortunadamente, sigue siendo común que los proveedores de Servicios Financieros Digitales no tengan procesos de negocio formales o procedimientos incompletos que no se han actualizado desde que se escribieron y que rara vez se utilizan. Cuando se les pregunta por sus procesos operativos, simplemente producen manuales de capacitación para operar la tecnología. Por ejemplo, con el siguiente diagrama podría representarse un proceso de negocio simple para la inducción de nuevos corresponsales[6]:

Figura 4: Los procesos de negocio cubren la tarea de extremo a extremo, no sólo las instrucciones para operar el sistema Servicios Financieros Digitales



[6] Este ejemplo es para propósitos ilustrativos y no es una descripción completa de todo el proceso de negocio descrito.

El diagrama describe todas las tareas necesarias para integrar al corresponsal, de las cuales la introducción de sus datos en el sistema Servicios Financieros Digitales (resaltado en rojo) es sólo una parte. En ausencia de procesos documentados, es fácil para los operadores olvidar algunos pasos en el proceso, particularmente las excepciones donde las cosas van mal, por ejemplo, si el corresponsal falla en algunos chequeos de visto bueno o si no se recibe la documentación completa. Esto puede dar lugar a que aplicaciones de corresponsales potencialmente buenas sufran retrasos, o que minoristas inapropiados sean aceptados como corresponsales.

En ausencia de procesos de negocios integrales, algunas tareas esenciales de operación pueden ser pasadas por alto. Los procesos que faltan a menudo son excepciones cuando las cosas no van de acuerdo al plan. Un buen ejemplo es el reciclado de tarjetas SIM. Debido a que hay un número limitado de números de teléfono que pueden ser utilizados por cualquier MNO, si un número no se utiliza durante un período prolongado, por lo general seis meses, la tarjeta SIM con ese número se desconecta, y el número es reciclado y se utiliza en una nueva tarjeta SIM. Si no hay un proceso para separar la cuenta de Servicios Financieros Digitales de ese número de teléfono, entonces la nueva tarjeta SIM ya tiene una cuenta Servicios Financieros Digitales viva asociada con su número de teléfono. Dado que el nuevo propietario de ese número no configuró la cuenta de Servicios Financieros Digitales, no se conoce el código PIN y no se puede utilizar esa cuenta; ni pueden documentar una nueva cuenta de Servicios Financieros Digitales con ese número. Los MNO reciclan muchos miles de números cada mes, pero debido a que se trata de un problema que sólo se hace evidente mucho después del lanzamiento de los Servicios Financieros Digitales, a menudo se pasan por alto los procesos para separar cuentas de Servicios Financieros Digitales de números reciclados.

Además, el equipo de operaciones debe ser capaz de responder rápidamente a nuevos problemas imprevistos. Por ejemplo, hubo un problema importante cuando los pagos de facturas se introdujeron por primera vez en un mercado, ya que durante el pago de la factura se pedía a los clientes que introdujeran su número de cuenta de servicio público como referencia.

Los números de cuenta que aparecían en las facturas de servicios públicos tenían un espacio en el medio, pero en el sistema de la compañía eléctrica no había dicho espacio. A los clientes que incluían el espacio cuando pagaban sus facturas se les deducía el dinero de su billetera, pero la referencia no podía ser reconocida por el sistema de servicios públicos y sus cuentas quedaban marcadas como vencidas, y muchas se cortaban. El equipo de operaciones de Servicios Financieros Digitales tuvo que encontrar rápidamente una forma para identificar cuentas de clientes con este problema, revertir el pago para devolver el dinero a las billeteras de los clientes y, seguidamente, ponerse en contacto con el cliente y explicarle cómo realizar el pago correctamente.

RIESGO OPERACIONAL - PREGUNTAS CLAVE

- ¿Tiene una Junta Directiva independiente y un departamento de auditoría interna?
- ¿Existe un manual de operaciones que detalle todos los procesos de negocio, que sea revisado y actualizado de manera habitual?
- ¿Se identifican procesos de negocios críticos y se evalúan los controles pertinentes?
- ¿Existe una adecuada separación de funciones?
- ¿Existe un proceso diario de conciliación entre el banco y las cuentas de dinero electrónico para minimizar los errores y detectar el fraude?
- ¿Existen auditorías periódicas, rigurosas y adecuadas, tanto internas, como auditorías externas independientes?

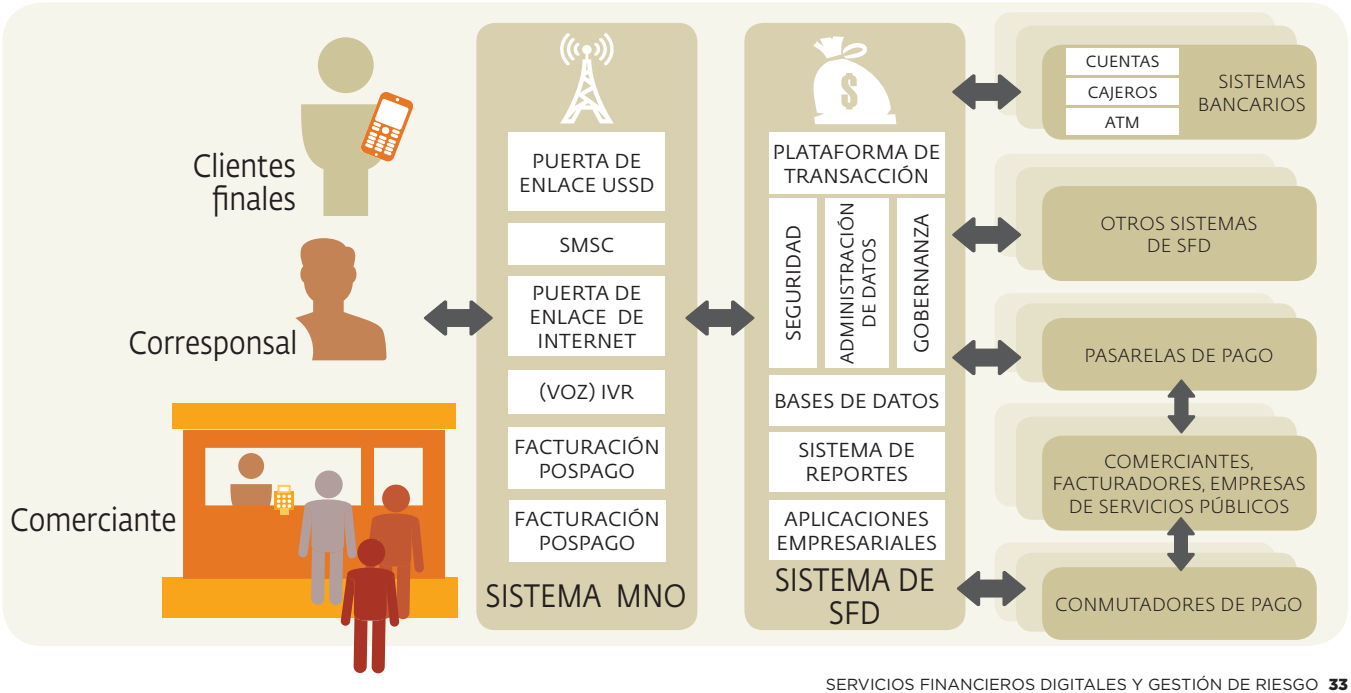
¿Puedo medir el nivel de servicio desde una perspectiva de usuario final?

4. Riesgo Tecnológico

El riesgo tecnológico tiene varias implicaciones para los proveedores. Con la incapacidad de realizar transacciones, tanto los corresponsales como los clientes pueden perder la confianza en el producto si no pueden acceder a sus fondos. Esto puede crear riesgos reputacionales y pérdidas financieras a medida que los clientes y corresponsales se vuelven inactivos y la presión competitiva les proporciona opciones alternativas. Los fallos tecnológicos también dejan oportunidades para que los estafadores aprovechen las insuficiencias del sistema para realizar transacciones no autorizadas que resulten en robo de fondos. Vea la sección de Riesgo de Fraude abajo para descripciones completas de los tipos de fraude que podrían ocurrir.

Riesgo Tecnológico se refiere al fracaso tecnológico que conduce a la incapacidad para realizar transacciones. Está estrechamente vinculado al riesgo operacional. Las transacciones dentro de un Servicio Financiero Digital viajan a través de varios sistemas y dispositivos de comunicaciones para iniciar la transacción, transferir fondos y enviar confirmaciones a los clientes. El proceso puede estar expuesto a averías potenciales de una serie de fuentes, por ejemplo, hackeo, fallas de energía, fallas del sistema, etc., y cualquier ruptura en esta cadena conduce a la incapacidad para completar una transacción. Si el fallo tecnológico es persistente y severo, el regulador puede intervenir e imponer sanciones o revocar la licencia, o los clientes pueden abandonar el servicio.

Figura 5: A medida que los sistemas Servicios Financieros Digitales se vuelven más conectados, el número de puntos potenciales de fallas aumenta



Al determinar los niveles de servicio proporcionados por la tecnología, la mayoría de los departamentos técnicos se centran en la calidad y disponibilidad de la tecnología de la que son responsables. Para Servicios Financieros Digitales complejos de múltiples componentes, esto puede conducir a una mentalidad de silo en la que cada equipo intenta pasar la culpa de un fallo del sistema a otro socio. Por lo tanto, es importante contar con procesos claros y acordados de diagnóstico, resolución y escalamiento de fallas. Otro riesgo potencial en la división de responsabilidades es que cada equipo técnico mide la calidad de servicio de su parte del sistema solamente y puede ser difícil obtener una imagen completa de la experiencia del usuario final. En el momento de firmar acuerdos de alianzas para proporcionar Servicios Financieros Digitales, es esencial determinar de antemano los KPIs de la tecnología como Transacciones Por Segundo o el tiempo en vivo del sistema, y asegurar que estos se puedan medir en su totalidad.

Fallo de Software: El potencial de problemas de software es inherente a cualquier sistema técnico. Existen muchas causas potenciales de fallos de software, como errores, cambios en sistemas aparentemente no relacionados, tanto internos como en sistemas de socios, y malos procedimientos de actualización y mantenimiento. Si los sistemas no reciben el mantenimiento adecuado y no están disponibles para que los clientes, comerciantes y corresponsales puedan acceder a sus fondos y realizar transacciones cuando sea necesario, puede resultar en una pérdida de negocio para el proveedor de Servicios Financieros Digitales y en daños reputacionales significativos. No es realista imaginar que algún sistema pueda tener disponibilidad del cien por cien, pero los cortes de servicio pueden minimizarse empleando buenas prácticas rigurosas.

La identificación de posibles fallos de software comienza con la identificación de todos los sistemas involucrados en cada tipo de transacción. Existen varios sistemas y tipos de software que pueden estar involucrados en una implementación de Servicios Financieros Digitales, incluyendo sistemas de core bancario , sistemas de pagos, conmutadores, sistemas de gestión de corresponsales, aplicaciones POS/ATM, aplicaciones móviles, sistemas biométricos y software de administración de relaciones con clientes. Una vez identificado, se puede llevar a cabo un análisis de riesgo para comprender las vulnerabilidades potenciales de los propios sistemas de las instituciones y sus interacciones con otros sistemas. En la medida de lo posible, los proveedores también deben entender los puntos de presión en los sistemas de sus socios para asegurar que los socios puedan suministrar completamente los niveles de servicio requeridos. En cada capa, los proveedores deben tener un plan consistente de capacitación, pruebas y mantenimiento del software, con medidas proactivas para prevenir y detectar posibles problemas que pudieran afectar al servicio. Además, los proveedores deben asegurarse que tienen un acuerdo de nivel de servicio con sus proveedores de servicios y proveedores de tecnología, que detalle no sólo los tiempos de respuesta y resolución de problemas, sino que confirme las funciones y responsabilidades de cada parte.

Normalmente, para los sistemas críticos de negocios, el proveedor de Servicios Financieros Digitales debe especificar la disponibilidad del sistema y otros KPI para garantizar la calidad del servicio y luego trabajar para aplicar estos estándares con todas las partes involucradas en el canal. El desempeño del sistema es influenciado fuertemente por la escala de las operaciones, y un KPI de uso común es el número de transacciones por segundo que se pueden manejar. A medida que el negocio crece, es importante que haya reuniones regulares entre los equipos técnicos y comerciales para asegurar que haya suficiente planeación de capacidad para hacer frente al crecimiento y para apoyar cualquier campaña de marketing que podría causar un aumento en la demanda.

Fallos de Hardware: Los fallos de hardware suponen la incapacidad de realizar transacciones debido a fallos de dispositivos físicos incluyendo cajeros automáticos, dispositivos POS y teléfonos móviles, así como servidores de back-office y componentes de redes. Además, algunos canales pueden depender de dispositivos periféricos como lectores biométricos, impresoras o lectores de tarjetas. Claramente, el mayor riesgo reside en los servidores que alojan las aplicaciones de Servicios Financieros Digitales. Los proveedores deben asegurarse que tienen establecido un plan de continuidad de negocio sólido. Esto debe incluir servidores de respaldo que se puedan utilizar fácilmente en caso de fallo, idealmente a través de un servicio 'espejo' que garantice que los servidores en vivo se replican en tiempo real para que, en caso de fallo, el respaldo esté disponible inmediatamente. Los cortes de energía pueden ser un problema en muchos mercados emergentes, por lo que se necesitan suministros de reserva de energía. Éstos pueden ser generadores en establecimientos grandes como las oficinas del proveedor, o tan simple como cargadores solares para los dispositivos POS. Además, hay una necesidad de sistemas de recuperación de desastres que se puedan poner en línea con poca anticipación en caso de un fallo catastrófico de los

servidores principales, como incendios, inundaciones o un ataque terrorista.

Muchos países tienen una regulación que dicta la distancia mínima entre el sitio principal y el del sistema de recuperación de desastres, y la duración máxima de la transición antes que el servicio esté de nuevo disponible.

El inevitable desgaste requiere un mantenimiento y actualización periódicos del hardware. Muchas compañías ahora operan sistemas en la nube y asumen que esto asegura un sistema distribuido constantemente mantenido y actualizado en el cual la capacidad aumenta y la recuperación de desastres está garantizada. Estas suposiciones deben ser aclaradas en el contrato de hosting y reconfirmadas regularmente. Sin embargo, el uso de la nube presenta otros riesgos potenciales. Los servicios basados en la nube dependen de enlaces de alta calidad a Internet, y el proveedor debe utilizar un mínimo de dos servicios independientes de Internet en el país con capacidad y disponibilidad suficientes en diferentes rutas de Internet. Otro riesgo de los servicios en la nube es la seguridad; los servidores basados en la nube hacen que el proveedor de Servicios Financieros Digitales dependa del proveedor de la nube para asegurarse que existan las medidas de seguridad adecuadas, y para asegurarse que este es realmente el caso, el proveedor Servicios Financieros Digitales podría tener que realizar una auditoría de los sitios y protocolos de hosting.

El hardware del corresponsal puede ser suministrado directamente por el proveedor de Servicios Financieros Digitales, o puede ser adquirido de forma independiente por el corresponsal. Normalmente, los dispositivos no están cubiertos por acuerdos de nivel de servicio, sino por garantías del fabricante. Al seleccionar los dispositivos del corresponsal, deben existir acuerdos legales relacionados con el mantenimiento, la reparación y el reemplazo del dispositivo, incluidos los pasivos, los tiempos y los costos, así como los índices normales de fallos previstos para los dispositivos. Es importante tener en cuenta que el fallo de hardware puede ser causado por una falla del propio dispositivo, o una falla de su conexión al software de back-end. Es importante que el proveedor pueda diagnosticar rápidamente la causa fundamental del fallo del hardware con el fin de conocer el tipo de solución que se aplicará para mantener el servicio.

Error de conectividad de red: El fallo del hardware también incluye problemas de conectividad, que siguen siendo un desafío importante en los mercados en desarrollo, particularmente en las zonas rurales. La cobertura intermitente, la disponibilidad insuficiente y el tiempo de inactividad de la red inhiben las transacciones y pueden resultar en pérdida de negocios. La conectividad comienza con las redes internas del proveedor y se extiende a la infraestructura de comunicaciones que se conecta a terceros involucrados en la oferta de canales, y al cliente.

Si las redes están inactivas, el usuario no podrá iniciar una transacción. Si se trata de un problema persistente, dará lugar a un riesgo reputacional, ya que afecta la experiencia del cliente cuando esperan largos periodos de tiempo para que las redes vuelvan a conectarse. Dado que los canales de voz y SMS son relativamente más estables y tienen una mayor disponibilidad que las redes de datos, muchos proveedores optan por utilizar esos canales en lugar de datos. En un ejemplo, una IMF adquirió dispositivos POS con SIM dual para que sus corresponsales pudieran cambiar de tarjeta SIM cuando un operador estaba inactivo.

Retrasos de Transacciones: Los retrasos en las transacciones pueden ser causados por la capacidad insuficiente de la tecnología para hacer frente a la demanda, causando colas en el sistema. Hay múltiples sistemas interconectados involucrados en Servicios Financieros Digitales y un daño en cualquier punto de la cadena podría hacer que una transacción se retrase, a menudo dejando al cliente y al corresponsal sin saber si la transacción se ha completado o no. Esto puede incluir demoras en la recepción de un SMS de confirmación al dispositivo del cliente. Las filas de transacciones también pueden tener consecuencias más significativas, como el fallo del sistema para procesar las transacciones o dejarlas colgadas indefinidamente.

Repetición de Transacciones: Los operadores móviles utilizan patrones de reintento de transacción, que reenvían automáticamente las solicitudes de transacción si no se recibe una confirmación inmediata. Estas repeticiones conllevan el riesgo que el usuario inicie solicitudes de transacción duplicadas porque no se da cuenta que la transacción tuvo éxito la primera vez hasta después de realizar varios intentos. También existe el riesgo que la red cree varios mensajes basados en un solo mensaje del usuario.

Pérdida de Datos: La protección de datos se debe incluir en los planes de continuidad de negocio de los proveedores para asegurar que los datos de los clientes no se pierdan o se vean comprometidos por robo, pérdida, negligencia o prácticas inseguras. Los datos del cliente se deben almacenar externamente con copias de seguridad.

Ataques Cibernéticos: Los ataques cibernéticos son amenazas a la integridad del cliente y datos transaccionales de un proveedor, así como ataques potenciales de espionaje corporativo para obtener acceso a procesos internos y estrategias tecnológicas por medio de la piratería informática o el malware. Los servicios financieros fueron el segundo sector más atacado en 2015[7], después de servicios de salud. La introducción de Servicios Financieros Digitales proporciona a los hackers potenciales puntos de acceso adicionales en los que pueden atacar sistemas y datos, y pueden crear nuevos riesgos.

Hay una variedad de factores que están impulsando la exposición a las amenazas de seguridad cibernética. La interacción entre los avances tecnológicos, los cambios en los modelos de negocios y los cambios en la forma en que las empresas y sus clientes utilizan la tecnología, crean vulnerabilidades en los sistemas de tecnología de la información. Por ejemplo, las actividades basadas en la web pueden crear oportunidades para que los atacantes interrumpan o tengan acceso a información corporativa y de clientes. Del mismo modo, los empleados y los clientes están utilizando dispositivos móviles para acceder a la información de las instituciones financieras, lo que crea una variedad de nuevas vías de ataque. El ecosistema de los actores de amenaza incluye a los ciberdelincuentes, cuyo objetivo puede ser robar dinero o información para obtener ganancias comerciales; naciones que pueden adquirir información para avanzar en objetivos nacionales; y hacktivistas cuyos objetivos pueden ser perturbar y avergonzar a una entidad. Los atacantes, y las herramientas disponibles para ellos, son cada vez más sofisticadas. Las partes internas, igualmente, pueden representar amenazas significativas.

Los ataques cibernéticos se llevan a cabo a menudo en cuatro etapas: infiltración, cuando el atacante logra el primer acceso; propagación, donde el atacante expande el acceso a través de puertas traseras o con minería de contraseñas; agregación, donde el atacante recopila registros y datos; y exfiltración cuando se exportan los datos. La mayoría de las defensas se centran en la etapa de infiltración, pero como los atacantes suelen ser los más expertos en esta área, la defensa exitosa debe incluirse en todas las etapas. Para manejar el riesgo de ataques cibernéticos, los proveedores pueden trabajar con auditores para desarrollar modelos de amenazas donde se trazan los puntos de incumplimiento y se desarrollan estrategias de mitigación. Además, los proveedores pueden protegerse ellos mismos mediante el uso de servicios en la nube que probablemente sean más seguros que los de propiedad, o comprar un seguro de ataque cibernético para protegerse de pérdidas financieras y de pérdida de datos, o de gastos legales.

Las instituciones deben desarrollar sus capacidades cibernéticas teniendo en cuenta los siguientes puntos:

- Es esencial contar con un sólido marco de gobernanza con un fuerte liderazgo. La participación de la Junta Directiva y la participación también a nivel directivo en temas de ciberseguridad, es crítico para el éxito de los programas de seguridad cibernética.
- Las evaluaciones de riesgos sirven como herramientas fundamentales para que las instituciones comprendan los riesgos de seguridad cibernética que enfrentan en toda la gama de actividades y activos de la empresa, independientemente del tamaño de la empresa o del modelo de negocios.
- Los controles técnicos, un componente central en el programa de ciberseguridad de una empresa, dependen mucho de situaciones individuales.
- Las instituciones deben desarrollar, implementar y probar planes de respuesta a incidentes. Los elementos clave de dichos planes incluyen la contención y mitigación, erradicación y recuperación, investigación, notificación y comunicación con el cliente.
- Las instituciones normalmente utilizan proveedores para servicios que proporcionan al proveedor acceso a información sensible de la empresa o del cliente, o acceso a sistemas corporativos. Deben gestionar las exposiciones al riesgo cibernético que surgen de estas relaciones mediante el ejercicio de la debida diligencia a lo largo del ciclo de vida de las relaciones con los proveedores.
- El personal bien formado representa una defensa importante contra los ciberataques. Incluso el personal bien intencionado puede convertirse en un vector inadvertido para los ciberataques exitosos, por ejemplo a través de la descarga involuntaria de malware. Una formación eficaz ayuda a reducir la probabilidad que dichos ataques tengan éxito.
- Las instituciones deben aprovechar las oportunidades de compartir inteligencia para protegerse de las amenazas cibernéticas. Hay oportunidades significativas de participar en la autodefensa colaborativa a través de este intercambio con otras instituciones financieras y reguladores.

[7] Auditing Cyber Security in an Unsecured World, The Institute of Internal Auditors, 2015

EJEMPLO 4

Registro de Riesgo

Riesgo tecnológico: falla de conectividad de red

Ejemplo de Proveedor de Servicios Financieros Digitales:	Ya sea un corresponsal de servicios bancarios que utiliza la tecnología móvil como su principal medio de transacción o un MNO que ofrece una billetera de dinero electrónico
Categoría del riesgo:	Riesgo Tecnológico
Categoría Secundaria:	Riesgo Reputacional
Nombre:	Error de conectividad de red
Descripción	El cliente no puede realizar transacciones a través de una aplicación móvil o donde un corresponsal debido a: • No está disponible el servicio de teléfonos móviles • El sistema del proveedor está experimentando tiempo de inactividad temporal del sistema
Dueño:	Jefe de TI
Causa:	Mal desempeño de la tecnología del proveedor, capacidad insuficiente en el sistema de Servicios Financieros Digitales, servicio MNO inadecuado
Efecto:	Las transacciones no se pueden realizar, lo que resulta en la pérdida de ingresos y la mala experiencia del cliente
Probabilidad:	2 de 5 Moderadamente baja, basada en la selección diligente de proveedores y acuerdos de nivel de servicio
Impacto:	3 de 5 Moderado en el corto plazo ya que es probable que el cliente intente de nuevo hasta que tenga éxito. Sin embargo, los problemas persistentes conducirán a pérdidas reputacionales y financieras
Estrategia de Riesgo:	Tratar
Estrategia de Tratamiento:	• Probar la capacidad del operador móvil para entregar mensajes en el nivel de servicio requerido, de forma periódica • Probar periódicamente el tiempo que toma el proceso de transacción de punto a punto y la tasa de éxito • Instale monitores de desempeño para mostrar el tráfico del sistema y haga una alerta si se acerca al pico de TPS • Todas las transacciones están definidas con límites claros de terminación, permitiendo así procedimientos claros de reversiones en caso de transacciones incompletas • Acuerdos de nivel de servicio con proveedores de sistemas que tienen estrategias detalladas para su cumplimiento • Actualizaciones del sistema • Utilizar el POS habilitado con USSD como apoyo a datos móviles (3G) para reducir la dependencia en la conectividad de datos
Respuesta Táctica de Tratamiento:	• Aplicar sanciones de acuerdos de nivel de servicio con proveedores • Desarrollar modos de transacciones sin conexión
Indicador Clave de Riesgo:	• Tasa de éxito de transacciones (de las solicitudes de transacción que llegan al sistema) • Capacidad suficiente para hacer frente a la tasa máxima de transacciones • Llamadas a servicio al cliente sobre transacciones fallidas
Estado actual:	Ocurrido y controlado

Cuadro 4

Estudios de casos de Riesgo Tecnológico

A) Cuando se lanzó M-PESA en Kenia, se encargó un sistema a la medida a un desarrollador de software. Existían pocas evidencias concretas sobre las cuales basar la proyección de volumen que a su vez proporcionaría la base para los requisitos de capacidad del sistema. Se pensó que una proyección optimista pero realista era que para el final del primer año habría alrededor de un tercio de millón de clientes activos, cada uno haciendo transacciones alrededor de tres veces al mes. El sistema fue construido con la capacidad para atender este requisito, más un margen de error razonable. Agregar capacidad para permitir el procesamiento de un mayor número de transacciones, bases de datos más grandes para mantener más registros de clientes y transacciones, y toda la arquitectura de soporte necesaria en caso de una mayor demanda" sería muy costosa e injustificada, por lo que el sistema fue construido para satisfacer la demanda esperada. Por supuesto, el éxito de M-PESA fue más allá de cualquier expectativa y a los tres meses de su lanzamiento estaba claro que la proyección era demasiado baja. La tecnología estaba batallando para seguir el paso del enorme número de transacciones imprevistas que se presentaban. Se creó un grupo de trabajo para encontrar maneras de aumentar la capacidad rápidamente, pero aun así, los clientes comenzaron a experimentar retrasos en las transacciones y caídas ocasionales del sistema que requerían una intervención manual para procesar las transacciones por parte de un equipo grande de representantes de servicio al cliente.

Durante varios meses el equipo de tecnología estuvo constantemente haciendo esfuerzos para no avanzar, encontrando maneras de agregar capacidad que quedaba llena al momento que se desplegaba. Paralelamente, estaban construyendo soluciones a largo plazo para las limitaciones arquitectónicas intrínsecas. Aunque los problemas de capacidad eventualmente se resolvieron, fue significativo el costo incremental de hacer mejoras constantes a una tecnología de lanzamiento demasiado pequeña.

B) Fidelity es un banco de primer piso en Ghana con cerca de un millón de clientes, 80 sucursales, 110 cajeros automáticos y 1000 corresponsales bancarios. Para hacer frente a la exclusión financiera del 70 por ciento de los ghaneses, el banco estableció una Unidad de Inclusión Financiera para innovar con la banca de corresponsales en 2013. El producto estrella es la Smart Account [Cuenta Inteligente], un producto en tarjeta de nivel básico que utiliza corresponsales para servicios básicos normalmente proporcionados en sucursales bancarias.

Para soportar el negocio de la Smart Account, se adquirió un nuevo sistema autónomo. La banca de corresponsales era un sector de negocios nuevo en ese momento con muchos proveedores de tecnología creando nuevos sistemas, y pocos servicios tenían un historial probado. Fidelity decidió probar, seleccionando una plataforma tecnológica adicional a su sistema de core bancario. El despliegue de nuevas tecnologías siempre es fuente de riesgo.

Como el negocio de corresponsales era nuevo para Ghana y Fidelity Bank, le llevó tiempo evaluar las necesidades totales del mercado y, como resultado, no pudo incorporar desde el comienzo la flexibilidad que el sistema necesitaba para permitir cambios a medida que avanzaba el proyecto.

"Uno tiene que investigar a fondo y anticipar sus necesidades, y hacer y rehacer. De lo contrario, el proveedor puede darle una solución para hoy y no para mañana".

~Dr. William Derban

La Smart Account se lanzó en julio de 2013 con expectativas muy altas. Al final de los primeros seis meses, Fidelity había abierto más de 55.000 cuentas. El número de corresponsales creció rápidamente, así como el volumen de transacciones. Sin embargo, a medida que el número de transacciones creció, Fidelity comenzó a experimentar una serie de desafíos. Algunos se relacionaban con el hecho que se trataba de un nuevo servicio en el país, y el personal y los corresponsales no tenían otros ejemplos de corresponsales bancarios para compararse o aprender. En segundo lugar, el sistema técnico parecía inflexible e incapaz de hacer frente a las crecientes exigencias de un mercado en rápida evolución. El tiempo de inactividad no planificado ha mejorado significativamente, pero sigue siendo un gran problema. Junto con los índices inaceptables de transacciones caídas (los dispositivos POS de los corresponsales empezaron a mostrar tasas de error de alrededor del 20 por ciento y se encontraron problemas al conectar los sistemas de core bancario y los de corresponsales de Smart Account), se obliga al equipo a concentrarse constantemente en apagar incendios en lugar de desarrollar el negocio, especialmente a medida que el número de Smart Accounts aumentaba (hasta aproximadamente 300.000).

Aunque la Smart Account y el canal de banca de corresponsales han crecido exponencialmente desde su creación, las metas altas establecidas por Fidelity Bank aún no se han alcanzado. Con mayores avances en los sistemas de gestión de corresponsales en los últimos años, Fidelity está invirtiendo en mejorar su plataforma tecnológica y mover su banca de corresponsales y el negocio de Smart Account a la misma plataforma del banco principal.

La tecnología puede ser una fuente importante de riesgo, especialmente cuando uno es un pionero, como en el caso de Fidelity Bank. Hoy, con más de dos años de experiencia y aún el único banco comercial con corresponsales bancarios en Ghana, Fidelity se muestra optimista} que su riesgo tecnológico se ha reducido considerablemente a medida que mejora su plataforma tecnológica actual.

RIESGO TECNOLÓGICO - PREGUNTAS CLAVE

- ¿Tengo acuerdos de nivel de servicio con el proveedor de mi sistema para asegurar el tiempo de disponibilidad del software?
- ¿Tengo acuerdos establecidos con mis socios de nivel de servicio, así como procedimientos de diagnóstico y reparación de fallos?
- ¿Puedo medir el nivel de servicio desde una perspectiva de usuario final?
- ¿Mi software se está comunicando adecuadamente con los dispositivos para minimizar los fallos de las transacciones?
- ¿Los proveedores y vendedores son eficaces y adecuados en sus protocolos de seguridad y enfoques de gestión de riesgo?
- ¿Se restringe el acceso a los activos de TI corporativos y se otorga solo con base en un marco de acceso basado en roles establecidos?
- ¿Tengo algún mecanismo establecido para prevenir la pérdida o fuga de información confidencial (información confidencial, propiedad intelectual, información personal identificable) de la organización?

¿Mis cuentas fiduciarias están adecuadamente diversificadas?

5. Riesgo Financiero

El riesgo financiero es uno de los riesgos de mayor impacto relacionados con Servicios Financieros Digitales. Si bien todos los riesgos comentados en este documento pueden tener pérdidas financieras directas o indirectas, existen riesgos específicos relacionados con la administración financiera de un proveedor de Servicios Financieros Digitales como se describe a continuación.

Riesgo de liquidez: El riesgo de liquidez es el riesgo de que la institución no pueda cumplir con sus obligaciones de fondos de efectivo y se vuelva insolvente. Los patrones transaccionales, tales como cantidades promedio de depósito, flujos entrantes, salientes, y plazos, deben monitorearse de cerca después del lanzamiento de un Servicios Financiero Digitale, ya que el comportamiento del cliente puede verse afectado por tener acceso conveniente a los fondos y esto puede cambiar el perfil activo/pasivo de la institución financiera.

Riesgo crediticio: El riesgo crediticio es el riesgo de que los clientes no paguen sus préstamos y no tengan suficientes garantías o la institución no pueda cobrar. En este caso, la institución sigue siendo responsable ante sus titulares de depósitos y debe encontrar formas alternativas para repagarles en caso que los préstamos se vuelvan incobrables.

Riesgo de tipo de interés: El riesgo de que las tasas de interés sobre los fondos prestados aumenten, mientras que, al mismo tiempo, no se pueda aumentar la tasa de interés cobrada a los clientes debido a tasas inmodificables sobre préstamos a largo plazo. En este caso, la institución estaría pagando más intereses a los acreedores que lo que están ganando por prestar, creando pérdidas financieras significativas.

Riesgo cambiario: Las pérdidas sobre divisas pueden ser incurridas cuando se negocian divisas, o al tener un desajuste en las monedas en las que se denominan préstamos y depósitos. Los valores en libros de las obligaciones de deuda pueden crecer sustancialmente por fluctuaciones adversas en la moneda, resultando en pérdidas. El riesgo cambiario también puede ser un problema si los ingresos de la organización se generan en un país diferente a donde se incurren sus costos.

Riesgo de concentración: El riesgo de concentración se refiere a la sobreexposición a una contraparte (crédito) o sector particular. Si hay una concentración de fondos en un banco particular, la institución corre el riesgo de una pérdida excesiva de fondos de clientes en caso que el banco se vuelva insolvente. La colocación de fondos en múltiples bancos ayudará a mitigar este riesgo, aunque genera una carga administrativa adicional. Del mismo modo, la excesiva dependencia en un segmento de clientes en particular puede arriesgar grandes cantidades de ingresos si las preferencias de los clientes cambian de forma que se retiren grandes cantidades de depósitos.

EJEMPLO 5

Registro de Riesgo

Riesgo Financiero - Exposición Cambiaria

Ejemplo de Proveedor de Servicios Financieros Digitales:	Cualquier proveedor de Servicios Financieros Digitales que incurra en una alta proporción de sus costos en una moneda diferente a la que recibe ingresos. Por ejemplo, un Proveedor de Servicios de Pago que opera en varios mercados desde una oficina central.
Categoría del riesgo:	Riesgo Financiero
Categoría Secundaria:	Riesgo Estratégico
Nombre:	Riesgo Cambiario
Descripción	El riesgo de incurrir en pérdidas financieras debido a fluctuaciones en los tipos de cambio
Dueño:	Jefe de Finanzas
Causa:	Causas externas tales como el desempeño económico y la política monetaria de los gobiernos locales
Efecto:	Lleva a pérdidas reales o en libros si los pasivos están en moneda extranjera y esta se aprecia
Probabilidad:	2 de 5 Probabilidad moderadamente baja debido a tipos de cambio estables en los últimos diez años
Impacto:	4 de 5 Impacto moderadamente alto si la fluctuación es suficientemente severa
Estrategia de Riesgo:	Transferir
Estrategia de Tratamiento:	• Conseguir préstamos locales o préstamos extranjeros en moneda local en la mayor medida posible • Negociar contratos con proveedores y suministradores en la moneda de préstamos • Transferir el riesgo restante que no se pueda evitar
Respuesta Táctica de Tratamiento:	• Compra de swaps de divisas para riesgos expuestos
Indicador Clave de Riesgo:	• Tasa de cambio de divisas
Estado actual:	No ha ocurrido

Cuadro 5

Estudios de Caso de Riesgo Financiero

Zoona es un proveedor independiente de servicios financieros que ofrece servicios financieros en mostrador (OTC)a través de redes de corresponsales en Zambia y, más recientemente, en Malawi. Sus 1.400 corresponsales activos primordialmente suministran servicios de remesas locales a 1.3 millones de clientes individuales, con más del 90 por ciento de las transacciones procedentes de su negocio establecido anteriormente en Zambia.

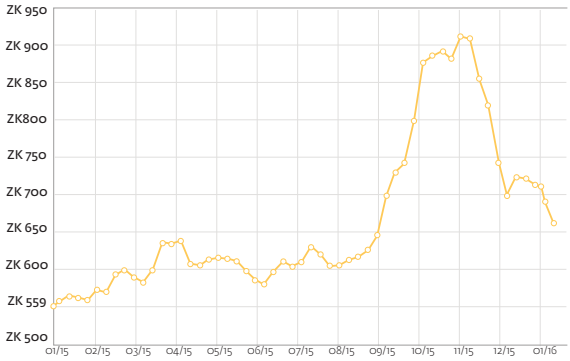
Zoona cuenta con una oficina de soporte centralizada, que maneja soporte técnico, atención al cliente y ciertas otras funciones corporativas para todas las entidades operativas. Por lo tanto, sólo se necesita un equipo relativamente pequeño en los países de operación para proveer soporte en ventas, configuración y cualquier otra función operativa que debe hacerse localmente. Esta centralización tiene la intención de proporcionar economías de escala a medida que el negocio se expande hacia nuevos mercados. Se utiliza tecnología basada en la nube, reduciendo costos fijos técnicos y permitiendo una rápida expansión cuando sea necesario. De este modo, el nivel de personal es bajo, con alrededor del 60 por ciento de la fuerza de trabajo basada en la oficina de soporte y el resto en los mercados locales. Sin embargo, el mayor costo para el negocio son los costos relacionados con el personal.

Esta separación geográfica entre operaciones y mercados, significa que Zoona tiene un desajuste en monedas porque recibe ingresos en moneda local, pero tiene una gran proporción de sus gastos en Rand sudafricano y dólar de los EE.UU. Cuando los tipos de cambio estaban relativamente estables, esto no era un problema. Sin embargo, la mayoría de sus ingresos proviene actualmente de Zambia, y el Kwacha bajó en valor frente al Rand en casi un 60 por ciento a finales de 2015.[8]

[8] (Gráfico Forex de http://fx-rate.net/ZAR/ZMK/)

Afortunadamente, el tipo de cambio parece estar volviendo a los niveles anteriores. Las fluctuaciones en monedas están obviamente fuera del control de Zoona, pero el riesgo es tan alto que se necesita establecer pasos para mitigar este riesgo. Aparte de las técnicas normales de cobertura de tesorería, la administración está adoptando el enfoque de diversificación en varios mercados diferentes, para ayudar a mitigar el impacto de los cambios en una moneda.

Tipo de cambio histórico Rand a Kwacha ZAR/ZMK



RIESGO FINANCIERO - PREGUNTAS CLAVE

- ¿Tengo suficiente financiación y caja para cumplir con las obligaciones, y amortiguar los flujos de efectivo inesperados?
- ¿Tengo políticas de riesgo crediticio implementadas, incluyendo evaluaciones de riesgo crediticio y KPIs para monitoreo de cartera?
- ¿Estoy controlando la edad de mi cartera en riesgo y provisionando reservas por incobrables según mis requisitos reglamentarios?
- ¿Mi(s) cuenta(s) de fideicomiso está(n) adecuadamente diversificada(s) y está (n) cubierta(s) por un seguro de depósitos?
- ¿Está cubierta mi moneda extranjera?
- ¿Los procesos internos de back-office, las reconciliaciones y los controles están diseñados adecuadamente, verificados y monitoreados habitualmente?

¿Hay amenazas políticas previsibles?

6. Riesgo Político

El riesgo político es la posibilidad que decisiones políticas, acontecimientos o condiciones afecten significativamente la rentabilidad de un negocio o el valor esperado de una determinada acción económica. Las instituciones se enfrentan a riesgos políticos como resultado, entre otras cosas, de desórdenes civiles, terrorismo, guerra, corrupción, crecimiento económico lento o en retroceso o condiciones económicas negativas tras cambios en política fiscal o monetaria establecidos por el gobierno. Los eventos causados por el riesgo político tienen impacto en el riesgo operacional, en particular la interrupción del negocio, y deben ser incluidos en los planes de continuidad del negocio.

Los riesgos políticos están fuera del control de las organizaciones y los clientes afectados por ellos, pero pueden tener un impacto grave en el negocio. Aunque no pueden evitarse, en algunos casos se pueden predecir, como en las elecciones conocidas, y las contingencias establecidas en caso que se materialicen los riesgos, como ocurrió con dos socios de IFC analizados en el Cuadro 6 abajo.

EJEMPLO 6

Registro de Riesgo

Riesgo Político - interrupciones repentinas del sistema

Ejemplo de Proveedor de Servicios Financieros Digitales:	Cualquier proveedor de Servicios Financieros Digitales que como todos depende de corresponsales y tecnología de comunicaciones.
Categoría del riesgo:	Riesgo Político
Categoría Secundaria:	Riesgo reputacional
Nombre:	Incapacidad para acceder a la cuenta o realizar transacciones
Descripción	La violencia post-electoral, la agitación civil, guerra o actividad terrorista perturban las operaciones comerciales normales, cerrando el negocio directamente o cerrando una función esencial del socio, como la red móvil, o los minoristas que actúan como corresponsales
Dueño:	Jefe de Riesgo
Causa:	Inestabilidad política, elecciones, guerra, ataque terrorista y/o contingencia externa
Efecto:	Los clientes no pueden acceder a las cuentas debido a la pérdida de conectividad o la incapacidad de los corresponsales de operar como de costumbre
Probabilidad:	1 de 5 Muy bajo, dada la historia o paz civil en el mercado local
Impacto:	3 de 5 Impacto moderado basado en el potencial de interrupción del negocio
Estrategia de Riesgo:	Tolerar
Estrategia de Tratamiento:	• Desarrollar un plan de interrupción del servicio para corresponsales, personal y/ o sucursales
Respuesta Táctica de Tratamiento:	• Aplicar un plan de interrupción del servicio para los corresponsales y personal
Indicador Clave de Riesgo:	• PAR • Disponibilidad del servicio (tiempo de disponibilidad) • Actividad del corresponsal • Actividad del cliente
Estado actual:	No ha ocurrido

Cuadro 6

Estudios de Caso de Riesgo Político

A) FINCA DRC es una institución de microfinanzas fundada en 2003 que lanzó un servicio de banca de corresponsales en 2011 para expandir su huella más allá de sus 18 sucursales. Sus 548 corresponsales forman la mayor red de banca de corresponsales en la República Democrática del Congo, donde solo el 4 por ciento de una población de 75 millones tiene una cuenta con una institución financiera formal. FINCA tiene ahora un cuarto de millón de cuentas de clientes que pueden usarse para ahorros y préstamos. Más de la mitad de los negocios de FINCA se realizan a través de corresponsales que utilizan terminales POS biométricas. Los detalles de la transacción se comunican desde el dispositivo POS del corresponsal mediante una red de datos móviles a un conmutador que enlaza con los servidores de FINCA a través de una conexión segura a Internet.

En respuesta a las manifestaciones contra las prórrogas propuestas para el mandato presidencial en enero de 2015, el gobierno de la República Democrática del Congo inhabilitó todos los servicios de internet, voz y datos móviles. Los MNOs y proveedores de servicios de internet se quejaron de haber perdido millones de dólares en negocios durante el cierre. Los dispositivos POS de los corresponsales de FINCA se volvieron inoperables y los clientes no pudieron acceder a sus cuentas. Como resultado, los clientes no podían pagar las obligaciones pendientes de créditos a FINCA. La calificación de la cartera en riesgo de FINCA aumentó y no volvió a su nivel anterior en los meses posteriores a la interrupción. Puesto que el PAR es un indicador clave de desempeño para evaluar la calidad de la cartera, los pocos días de interrupción a principios de 2015 llevaron a un desempeño negativo a largo plazo y a pérdidas financieras significativas.

La red de telefonía móvil (voz) se restableció a los dos o tres días, y después de diez días se restableció internet para las empresas, incluidas las instituciones financieras, pero el impacto se seguía sintiendo mucho tiempo después. Se espera que continúe la inestabilidad Política en la RDC, y es comprensible que FINCA esté muy preocupada por esto, haciendo planes para minimizar el impacto al negocio. Los factores políticos siguen fuera de su control, y las consecuencias de un período prolongado sin conectividad de red podrían ser profundas.

B) LAPO Microfinance Bank, es un banco de microfinanzas nigeriano que opera en 26 estados, actualmente suministrando servicios de microfinanzas a 1.3 millones de clientes. Se encuentra en el proceso de crear un servicio de banca de corresponsales para complementar sus sucursales regionales.

LAPO tiene activos significativos en el noreste de Nigeria donde han habido varios ataques terroristas graves en los últimos años.

Esto ha causado que las sucursales se cierren con poco preavisoy en un caso, el personal y los clientes quedaron atrapados dentro de una sucursal durante varias horas debido a un incidente cercano. En términos financieros, la incertidumbre causada por los desórdenes civiles también tiene un impacto en la calidad de los activos crediticios, lo que afecta su capacidad de crecimiento de la cartera.

LAPO lanzó su red de corresponsales en 2016, y la interrupción causada por los grupos terroristas es probable que continúe. LAPO ha instaurado una serie de medidas para mitigar los riesgos, incluyendo el suministro de capacitación y un manual para el personal que da orientación sobre qué hacer en caso de estar cerca de una situación de terrorismo. El modelo de corresponsales es particularmente vulnerable a las alteraciones políticas dado que LAPO depende de sus relaciones con sus corresponsales para manejar la interrupción del negocio. Las técnicas de mitigación se deben integrar en los sistemas de capacitación y gestión de los corresponsales.

RIESGO POLÍTICO - PREGUNTAS CLAVE

- ¿Existen amenazas políticas previsibles o acontecimientos inminentes que puedan crear una amenaza política? De ser así, ¿estoy preparado?
- ¿Tengo contingencias establecidas para manejar las implicaciones de un corte debido a eventos políticos?
- ¿Cuál es mi plan de comunicación para los clientes, socios e inversionistas, en caso de riesgo político que afecte a mi negocio?

¿Hemos desarrollado controles detectores de fraude?

7. Riesgo de Fraude

El fraude es un riesgo importante para los Servicios Financieros Digitales y es causa de mucha preocupación para los proveedores de Servicios Financieros Digitales. El riesgo de fraude es multifacético y se relaciona con varios otros riesgos. El riesgo operacional y tecnológico puede causar riesgo de fraude, y el fraude puede conducir a un riesgo financiero. El fraude también es un factor importante de riesgo reputacional. Grandes casos de fraude en dinero electrónico se han reportado en los últimos años que han causado daños financieros de millones de dólares. Estos han sido debido al fraude de clientes, corresponsales y empleados al crear cuentas fantasma y realizar transacciones fraudulentas. Han sido robados fondos a proveedores, corresponsales y clientes. El fraude puede tener un gran impacto en la reputación de una institución y en la industria en su conjunto. Si los fondos son robados de cuentas de clientes por culpa del proveedor, los proveedores deben asegurarse que los fondos se devuelven a los clientes de inmediato. El proceso de prevención del fraude incluye el desarrollo de evaluaciones para entender dónde se puede detectar y prevenir el fraude, determinar el apetito de riesgo y establecer controles efectivos.

En general, el fraude puede definirse como fraude mayor, que implica sumas muy grandes y generalmente se realiza contra la institución financiera, a menudo por parte del personal; y el fraude menor, que involucra a corresponsales o clientes como víctimas o autores y sumas menores de dinero.

Hay muchas razones por las que las personas cometen fraude, pero un modelo común para juntar a una serie de éstas es El Triángulo del Fraude[9]. La premisa es que el fraude es probable que resulte de una combinación de tres factores generales: Presión (o motivación para cometer fraude); Oportunidad (típicamente debido a sistemas o procesos deficientes); y Racionalización (típicamente que no serán atrapados).

Una de las maneras más eficaces para prevenir el fraude es reducir la oportunidad, al tener una excelente tecnología, y procedimientos de prevención y detección. Esto refuerza la necesidad de la gestión de riesgo de fraude.

Los tipos más comunes de fraude relacionado con Servicios Financieros Digitales se definen en la publicación de Micro Save 'Fraud in Mobile Financial Services' [Fraude en los Servicios Financieros Móviles] (2012)[10] y se resumen abajo según el tipo de fuente del fraude.

---

[9] http://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf

[10] MicroSave Fraud in Mobile Financial Services, Mudiri, 2012

Figura 6: El Triángulo del Fraude: marco para detectar situaciones de fraude de alto riesgo

Fraude de Clientes

CLIENTES DEFRAUDANDO CORRESPONSALES

- Moneda falsa: el riesgo de que los clientes le depositen moneda falsa a un corresponsal que no se dé cuenta de ello a cambio de valor electrónico y luego retiren moneda legítima de otro corresponsal.
- Acceso no autorizado a las herramientas transaccionales de los corresponsales: los clientes entran a los dispositivos POS para realizar transacciones fraudulentas.
- Fraude en el canal web del corresponsal: Los clientes entran al canal web del corresponsal sin autorización y realizan transacciones fraudulentas.
- Fraude de comprobantes: se hacen comprobantes falsos para representar los comprobantes genuinos de las ONG o del gobierno y se les entregan a los corresponsales a cambio de efectivo o valor electrónico.

CLIENTES DEFRAUDANDO CLIENTES

- Acceso PIN no autorizado: los clientes consiguen los números PIN de otros clientes y realizan transacciones no autorizadas.
- Robo de identidad: los clientes usan identificaciones de otros clientes para acceder a las cuentas.
- Phishing, suplantación (spoofing) de SMS, SMS falsos: los clientes fraudulentos envían SMS falsos a los corresponsales, ya sea desde sus propias terminales o generados desde computadoras. El SMS parece genuino para el destinatario.

Fraude de Corresponsales

CORRESPONSALES DEFRAUDANDO CLIENTES

- Acceso no autorizado al PIN de los clientes: los corresponsales obtienen acceso al PIN del cliente y realizan transacciones fraudulentas.
- Imposición de cargos no autorizados a los clientes: los corresponsales cobran a los clientes cargos por transacciones muy superiores al precio cotizado y conservan fraudulentamente los cargos en lugar de remitir al proveedor.
- Retiros divididos: los clientes solicitan un retiro al corresponsal, y el corresponsal divide el retiro en dos o más transacciones con el fin de recoger más comisiones por retiros a los clientes.

CORRESPONSALES DEFRAUDANDO A PROVEEDORES

- Depósitos divididos: los clientes solicitan un depósito al corresponsal, y el corresponsal divide el depósito en dos o más transacciones con el fin de recoger más comisiones por depósitos del proveedor.
- Depósitos directos: los corresponsales depositan directamente fondos de un cliente en la cuenta de otro cliente en lugar de depositar, y luego envían una solicitud de transferencia de fondos para evitar la tarifa.
- Vinculación de clientes con detalles falsos: los corresponsales vinculan clientes que no proporcionan información precisa de KYC.
- Vinculación de clientes inexistentes: los corresponsales vinculan cuentas fantasmas para recibir la comisión de registro.
- Vinculación de personas como empresas: los corresponsales vinculan clientes como una cuenta de negocio con el fin de recibir una comisión mayor.
- Representación de estado de proveedor: un corresponsal no autorizado actúa como un corresponsal autorizado para realizar transacciones fraudulentas.
- Lavado de dinero en plataforma: los corresponsales realizan, a sabiendas, transacciones declientes con fines de lavado de dinero para recibir la comisión.

EMPLEADOS DE CORRESPONSALES DEFRAUDANDO A CORRESPONSALES

- Robo de fondos: empleado del corresponsal roba fondos de caja al corresponsal.
- Subregistro de saldos de caja: el empleado del corresponsal falsea el saldo en caja del corresponsal.

FRAUDE POR PARTE DE CORRESPONSALES MAESTROS

- Retiros no autorizados de cuentas de corresponsales: los corresponsales maestro acceden de forma abusiva a cuentas de corresponsales y retiran fondos.
- Deducciones ilegales de la comisión percibida por los corresponsales: los corresponsales maestros cobran cargos adicionales repartiendo las comisiones con el corresponsal.

Fraude del Socio Comercial

EMPLEADOS QUE DEFRAUDAN NEGOCIOS

- Los empleados vinculan los números móviles equivocados a las cuentas bancarias: los empleados vinculan su propio móvil o el número de móvil de un verificador a una cuenta bancaria para tener acceso ilegal a la cuenta.
- Reversión ilegal de los pagos de los clientes a la empresa: los empleados revierten los pagos realizados por los clientes y conservan el efectivo.
- Transferencias ilegales de cuentas comerciales: los empleados realizan transacciones fraudulentas, transfiriendo fondos de cuentas comerciales a cuentas fraudulentas.

Fraude de la Administración del Sistema

- Abuso de contraseñas: los empleados utilizan el acceso a contraseñas para realizar transacciones fraudulentas.
- Creación de usuarios falsos/inexistentes: los empleados crean cuentas falsas para realizar transacciones fraudulentas.
- Usuarios individuales con múltiples derechos: a los empleados se les otorga acceso a múltiples niveles dentro de los sistemas y éstos son abusados para realizar transacciones fraudulentas.
- Contraseñas débiles/ PIN de transacción: las contraseñas de los empleados son pirateadas debido a la débil configuración de contraseñas.

Fraude Proveedor

FRAUDE DE CALL CENTER Y SOPORTE OPERATIVO

- Acceso no autorizado a los registros de pago de los clientes: los empleados abusan del acceso a los registros de los clientes.
- Transferencia ilegal de fondos de cuentas de clientes: los empleados realizan transacciones fraudulentas.
- Cambios no autorizados de SIM: el personal del Call Center cambia los números PIN del cliente.
- Acceso no autorizado al sistema con los derechos de acceso de compañeros de trabajo: el personal del call center ingresa a los derechos de acceso de los compañeros de trabajo para realizar transacciones fraudulentas.

Fraude del Personal de Ventas y Canal

- Soborno: el equipo de ventas soborna a corresponsales y/o clientes, o solicita pagos no autorizados.
- Acceso no autorizado a datos transaccionales de corresponsales: el personal de ventas utiliza datos de corresponsales para realizar transacciones fraudulentas.

EJEMPLO 7

Registro de Riesgo

Riesgo de Fraude - depósitos divididos

Ejemplo de Proveedor de Servicios Financieros Digitales:	MNO que ofrece una billetera de dinero electrónico y utiliza corresponsales para depósitos por una comisión fija (o escalonada)
Categoría del riesgo:	Riesgo de Fraude
Categoría Secundaria:	Riesgo Gestión de corresponsales
Nombre:	Depósitos divididos
Descripción	Los corresponsales obligan a los clientes a dividir los depósitos en una serie de pequeñas transacciones, con el fin de generar mayores comisiones a costa del proveedor.
Dueño:	Jefe de Servicios Financieros Digitales
Causa:	Las estructuras de comisiones incentivan el mal comportamiento de los corresponsales.
Efecto:	El proveedor se ve obligado a pagar comisiones más altas al corresponsal de lo originalmente previsto, lo que puede afectar gravemente los ingresos netos.
Probabilidad:	1 de 5 Moderadamente bajo basado en políticas y controles estrictos
Impacto:	1 de 5 Muy bajo basado en que la pérdida potencial más grande es la tarifa de transacción
Estrategia de Riesgo:	Tolerar
Estrategia de Tratamiento:	• Utilizar las herramientas de análisis de datos para alertar sobre transacciones sospechosas, como transacciones múltiples a, o desde, la misma cuenta al mismo corresponsal dentro de un período de 24 horas. • Desarrollar un proceso exhaustivo de debida diligencia en la vinculación de corresponsales para minimizar la vinculación de corresponsales con mala reputación o aquellos más propensos a cometer fraude • Lleve a cabo actividades de comprador secreto para identificar corresponsales que tratan de dividir las transacciones, y practicar buena gestión de corresponsales mediante el uso de medidas correctivas • Educación de corresponsales mediante la inclusión de advertencias sobre el reparto de transacciones, en materiales de capacitación a corresponsales • Call center para que los clientes denuncien actividades sospechosas
Respuesta Táctica de Tratamiento:	• Re-entrenamiento de corresponsales • Aplicación de sanciones por mala administración de corresponsales y cierre de corresponsales
Indicador Clave de Riesgo:	• Informes de transacciones sospechosas
Estado actual:	Ocurrido y controlado

Cuadro 7

Estudios de Caso de Riesgo de Fraude

Uno de los fraudes a gran escala más denunciados experimentado por un proveedor de Servicios Financieros Digitales se debió a malas prácticas operativas. El servicio fue uno de los primeros despliegues de Servicios Financieros Digitales en África y se volvió exitoso muy pronto. Debido a este éxito en un mercado altamente competitivo, el foco de los proveedores de servicios se centró en aumentar el número de clientes y transacciones y como consecuencia, se prestó poca atención a las muchas señales de advertencia de que no todo estaba bien. A los pocos meses del lanzamiento, los empleados encargados de la conciliación diaria, mientras se aseguraban que el dinero electrónico emitido coincidiera con el dinero de la cuenta bancaria, reportaron grandes discrepancias.

Estas advertencias fueron ignoradas por la dirección. Durante casi dos años varios empleados crearon dinero electrónico [e-money] falsificado que no estaba cubierto por dinero real, y se volvieron cada vez más creativos en la búsqueda de formas de cobrarlo, por ejemplo, a través de corresponsales cómplices o creando cuentas falsas de clientes. Esto fue posible debido a la falta de controles operativos que permitieron a los autores abusar del sistema con impunidad. Los operadores podían crear sus propios logins [inicios de sesión], con algunas personas que tenían múltiples identificaciones de usuario para confundir cualquier rastro de auditoría. No hubo separación de funciones impuesta para evitar que los operadores procesaran transacciones falsas y no hubo supervisión de comportamiento sospechoso para identificar fraudes potenciales. Los nuevos empleados no estaban formalmente capacitados para operar el complejo sistema de back office y por lo tanto no podían reconocer el comportamiento inapropiado de sus colegas, ni corregir ningún problema. Posiblemente la peor omisión fue que no existían procedimientos para investigar los asuntos que se informaron, por lo que las diversas actividades fraudulentas duraron varios años antes de ser descubiertas.

Hay muchos casos reportados de fraude de corresponsales a pequeña escala. Uno de los más comunes es dividir grandes transacciones en muchas transacciones más pequeñas. Por ejemplo, retiros divididos tienen lugar cuando un cliente desea sacar una cantidad específica y, en lugar de realizar una sola transacción, el corresponsal realiza múltiples retiros menores y gana una cantidad fija en cada uno.

Esto es posible porque la mayoría de los servicios pagan al corresponsal una cantidad fija por retiro en lugar de un porcentaje, lo que hace posible ganar la misma comisión varias veces en lugar de una sola vez.

Otra forma que usan los corresponsales para estafar al proveedor es registrar a clientes que acuden a recargar tiempo aire en el servicio de dinero electrónico sin su conocimiento o consentimiento con el fin de ganar una comisión. Una sofisticación agregada a esta trampa ocurre ocasionalmente cuando un corresponsal registra a un cliente genuino y luego se ofrece a demostrar cómo funciona el servicio haciendo un depósito, seguido inmediatamente de un retiro utilizando el teléfono del cliente. El corresponsal gana comisión en el depósito y en el retiro pese a no haber ocurrido un intercambio real de dinero.

RIESGO DE FRAUDE - PREGUNTAS CLAVE

- ¿Ha determinado su nivel de pérdidas financieras aceptables debido al fraude?
- ¿Ha identificado las áreas clave para posibles riesgos de fraude de su institución?
- ¿Ha desarrollado controles preventivos y de detección de fraude?
- ¿Está monitoreando y revisando activamente su estrategia de administración de riesgos de fraude?

¿Proporciona formación suficiente para corresponsales y distribuidores?

8. Riesgo de Gestión de Corresponsales

La introducción de corresponsales para actuar en nombre de los proveedores de servicios financieros presenta muchos beneficios en términos de costo, alcance geográfico y escala, pero también introduce nuevos riesgos. La gestión y supervisión de los corresponsales es imprescindible para un servicio que funcione bien y proteja a los clientes. El uso de corresponsales puede provocar riesgos operacionales, tecnológicos, legales, de reputación y de fraude, que están cubiertos en otras secciones. Además, existen riesgos directamente asociados con la gestión de los corresponsales:

Densidad de Corresponsales: Los clientes utilizan corresponsales para acceder a su servicio financiero móvil, especialmente para depósitos y retiros, y requieren cercanía a un corresponsal para realizar transacciones. Sin embargo, suministrar el número adecuado de corresponsales para satisfacer la demanda de los clientes siempre es un reto para cualquier Servicio Financiero Digital. Muy pocos corresponsales pueden referirse a la falta de corresponsales cercanos o a la falta de capacidad del corresponsal cercano para satisfacer la demanda de los clientes, lo que resulta en largas colas o problemas de liquidez (ver más abajo).

Por otra parte, demasiados corresponsales también puede ser un riesgo porque los clientes se diluyen entre ellos de modo que ningún corresponsal tiene la masa crítica de clientes necesaria para ganar suficiente comisión y compensar el costo de la conciliación del dinero electrónico y el efectivoen caja. En estas circunstancias, los corresponsales a menudo no mantienen la conciliación y por lo tanto no pueden atender a los clientes. El uso poco frecuente de los Servicios Financieros Digitales puede hacer que los corresponsales olviden cómo ofrecer el servicio o que olviden su PIN y no puedan servir a los clientes, incluso si tienen liquidez.

Liquidez Insuficiente: Los corresponsales requieren suficiente dinero en efectivo y valor electrónico para administrar las solicitudes diarias de transacciones de depósitos y retiros de los clientes. Para satisfacer estas necesidades, los corresponsales suelen utilizar conciliación de efectivo en caja en sus negocios existentes; viajan con frecuencia a una sucursal u otro corresponsal para cambiar efectivo y dinero electrónico [e-float]; o, para los corresponsales ocupados se establece una relación con un administrador de liquidez, como un súper-corresponsal, con quien pueden acceder a rotación rápida y frecuente de efectivo y dinero electrónico. En algunos casos, el proveedor de servicios financieros o un tercero puede ofrecer facilidades de liquidez en forma de una inyección inicial de capital o un sobregiro de corto plazo, para compensar los déficits de liquidez. Se requieren suficientes procesos y facilidades de gestión de liquidez para asegurar que los corresponsales estén satisfechos y no incomodos, y para que los clientes confíen en que hay fondos inmediatamente disponibles a solicitud.

Robo de Efectivo en Caja: Las operaciones comerciales de un corresponsal pueden quedar en riesgo por depósitos excesivos. El dinero puede ser robado, y este es especialmente el riesgo si el corresponsal llega a desarrollar una reputación de tener grandes cantidades de dinero en efectivo. Los gestores de liquidez deben ofrecer servicios de recolección y entrega para mitigar este riesgo.

Errores de Cajero(a): Los corresponsales y sus cajeros(as) pueden cometer errores de digitación al introducir transacciones o errores de conteo en la gestión de efectivo, que darán como resultado un fondo de caja sin conciliar y podrá sufrir pérdidas, ya sea para el corresponsal o para el cliente.

Los errores de cajeros(as) también incluyen el riesgo de perder o dañar los soportes en papel que pueden poner al corresponsal y el proveedor en riesgo de incumplimiento de la normativa

Entrenamiento Deficiente: La formación de los corresponsales suele estandarizarse y partir de las políticas y procedimientos del proveedor, para cumplir con las directrices reglamentarias. Las políticas de capacitación incluyen el contenido de la capacitación, la frecuencia requerida y el momento de la capacitación del corresponsal, y las cualificaciones requeridas del capacitador. La capacitación del corresponsal debe ser exhaustiva e incluir cursos de actualización para mitigar los riesgos de errores y proporcionar una experiencia de cliente consistente en todos los corresponsales. Es esencial que las personas que atienden clientes corresponsales en las oficinas estén capacitadas, no sólo el propietario del servicio de corresponsalía, y esto puede ser un desafío. Es común que los corresponsales mal entrenados afirmen que el servicio no funciona, en lugar de admitir que no saben cómo usarlo. Los clientes que tienen una mala experiencia inicial con un corresponsal, a menudo se desaniman de usar el servicio de nuevo, e incluso se pueden desanimar por completo de usar Servicios Financieros Digitales.

Mala Gestión del Servicio al Cliente: Los corresponsales son la primera línea de servicio al cliente para los proveedores de Servicios Financieros Digitales. En la capacitación sobre políticas y procedimientos se deben incluir mecanismos para que los corresponsales manejen las quejas y consultas de los clientes, tales como la resolución de problemas básicos, la provisión de números de call centers y el registro de quejas para retransmisión al administrador del corresponsal. El mal manejo del servicio al cliente por parte del corresponsal puede afectar a los proveedores a través de la pérdida de clientes, cuentas inactivas y riesgo reputacional.

Mala Selección de Corresponsales: Las políticas de selección de corresponsales suelen incluir criterios mínimos de idoneidad (basados en los requisitos reglamentarios y en la evaluación de la capacidad requerida por el proveedor). La mala selección de corresponsales puede conducir a corresponsales inactivos, riesgo reputacional, riesgo regulatorio y pérdidas financieras para el proveedor. Los corresponsales deben estar bien entrenados en los requisitos para mantener su estado de corresponsal, monitoreados frecuentemente y deben cerrarse si no cumplen con los criterios mínimos.

Branding y Marketing Inadecuados: Los materiales de branding y marketing deben ser estandarizados e incluidos en las políticas y procedimientos de gestión de corresponsales. El proveedor de servicios financieros debe proporcionar materiales de branding y marketing, puede incluir señalización, folletos u otros subsidios. Una experiencia de usuario consistente es importante para reducir el riesgo de inactividad del cliente y riesgo reputacional. Debe haber suficiente suministro de materiales de marketing para apoyar a los clientes en su uso temprano del servicio.

Aunque en muchos mercados el regulador adopta un enfoque de no intervención para los corresponsales, algunos países pueden requerir que el uso de corresponsales de un proveedor sea aprobado por los reguladores y en algunos, cada corresponsal debe tener una licencia individual. La supervisión de los corresponsales puede ser realizada por los reguladores; sin embargo, incluso si ese es el caso, los proveedores también deben vigilar ellos mismos. La supervisión de corresponsales por parte de los proveedores, incluyendo análisis de datos y visitas personales, reduce las oportunidades de riesgo en las operaciones de Servicios Financieros Digitales, tales como riesgo de fraude, riesgo reputacional, riesgo regulatorio y riesgo estratégico, además de mejorar la probabilidad de éxito, aumentando las tasas de actividad de los corresponsales y de los clientes.

EJEMPLO 8

Registro de Riesgo

Riesgo de Gestión de Corresponsales - restricciones de liquidez

Ejemplo de Proveedor de Servicios Financieros Digitales:	Cualquier proveedor de Servicios Financieros Digitales que depende de los corresponsales que tengan un inventario de valor (o dinero electrónico) en sus cuentas para atender a los depósitos de los clientes. Por ejemplo, un MNO que ofrece una billetera de dinero electrónico.
Categoría del riesgo:	Riesgo Gestión de corresponsales
Categoría Secundaria:	Riesgo Reputacional
Nombre:	Falta de liquidez del corresponsal
Descripción	El cliente no puede realizar transacción de depósito porque el corresponsal no tiene suficiente dinero electrónico
Dueño:	Jefe de Servicios Financieros Digitales
Causa:	El corresponsal tiene restricciones de capital o elige no invertir en operaciones de Servicios Financieros Digitales o no tiene un mecanismo conveniente para acceder rápidamente al dinero electrónico
Efecto:	El cliente no puede hacer retiros porque no hay dinero electrónico disponible, lo que resulta en una mala experiencia del cliente
Probabilidad:	3 de 5 Probabilidad moderada basada en la dificultad de controlar los niveles de liquidez del corresponsal
Impacto:	2 de 5 Impacto moderadamente bajo basado en la capacidad de los clientes para volver más tarde o visitar otro corresponsal. Si el servicio está al comienzo del ciclo de vida, o el problema es persistente, el impacto será mayor.
Estrategia de Riesgo:	Tratar
Estrategia de Tratamiento:	• Uso de corresponsales y súper-corresponsales para la liquidez • Registros del call center • Proceso para alertar a los corresponsales cuando su fondo de dinero electrónico es bajo • Controlar el despliegue de los corresponsales para asegurar que haya suficiente cobertura geográfica y que cada corresponsal tenga suficientes clientes para soportar su negocio • Proceso para identificar cuando los corresponsales están constantemente incumpliendo sus requisitos de liquidez y procedimientos de mitigación • Pre-financiar los requerimientos de capital de los corresponsales a través de préstamos o alianzas con instituciones financieras • Compradores secretos y buena gestión de corresponsales
Respuesta Táctica de Tratamiento:	• Aumentar los requerimientos de capital y la debida diligencia del corresponsal para la vinculación de nuevos corresponsales • Reevaluar la estructura de comisiones para asegurar la existencia de suficientes incentivos.
Indicador Clave de Riesgo:	Saldos de dinero electrónico del corresponsal
Estado actual:	Ocurrido y mitigado

Cuadro 8

Estudios de Caso de Riesgo de Corresponsales

Según la GSMA,[11] en promedio, el 51,4 por ciento de los corresponsales de Servicios Financieros Digitales están activos, o alrededor de la mitad de los corresponsales vinculados para ofrecer Servicios Financieros Digitales a los clientes lo están haciendo. En algunos mercados, el nivel de inactividad es mucho mayor. Esto significa que los clientes pueden entrar donde un corresponsal de Servicios Financieros Digitales totalmente dotado de material promocional para realizar una transacción, sólo para enterarse que el corresponsal no está operando. Peor aún, en un intento por guardar apariencias, estos corresponsales a menudo dicen a los clientes que no pueden ser atendidos porque el Servicio Financiero Digital no está funcionando hoy, cosa que socava el servicio haciéndolo parecer poco confiable e inseguro. Una mala experiencia de corresponsal puede dañar la reputación de los Servicios Financieros Digitales y desencantar a los clientes potenciales de usarlo, especialmente si ocurre en un primer acercamiento de los clientes al servicio. Las causas comunes de inactividad del corresponsal son, que los corresponsales no saben cómo utilizar el servicio, o que han olvidado sus códigos de PIN, o se han quedado sin dinero electrónico.

Los corresponsales debentener una reserva de dinero electrónico disponible para enviar a los clientes que desean depositar dinero; y necesitan efectivo para dar a los clientes que desean hacer retiros. Incluso entre los corresponsales activos, los temas de liquidez son comunes, especialmente en las zonas rurales, lejos del banco más cercano, donde se puede depositar dinero en efectivo para recargar el suministro de dinero electrónico. Si los clientes no pueden acceder fácilmente al dinero en sus cuentas, o si creen que el destinatario del dinero tendrá problemas para hacer el retiro, se abstienen de usar el servicio. Esto crea una espiral descendente, ya que los corresponsales no se molestan en mantener dinero electrónico disponible con regularidad si no están viendo la demanda por parte del cliente, por lo que más clientes tienen una mala experiencia con corresponsales y dejan (o nunca empiezan) de utilizar el Servicio Financiero Digitale. Debido a esto, los proveedores de Servicios Financieros Digitales exitosos tienen una gama de estrategias para asegurar que sus corresponsales tengan acceso a varias maneras de gestión de el fondo de dinero electrónico y efectivo, tales como habilitar a agregadores y súper-operadores para ayudar a los corresponsales, y proporcionar pagos a los comerciantes por Servicios Financieros Digitales para recargar continuamente el saldo de dinero electrónico de los corresponsales.

[11] GSMA state of the industry report: mobile money 2015. Los corresponsales inactivos se definen como los que no han atendido a un cliente en el mes anterior.

RIESGO DE GESTIÓN DE CORRESPONSALES - PREGUNTAS CLAVE

- ¿Tiene acuerdos concretos con corresponsales que cubran todos sus riesgos y cumplan con la regulación local?
- ¿Tiene un programa integral de capacitación para corresponsales y distribuidores?
- ¿Tiene una gama de planes de contingencia para facilitar la gestión de la liquidez?
- ¿Dispone de procesos de retroalimentación para identificar y resolver problemas de desempeño del corresponsal?

¿Se evalúan los socios por su riesgo reputacional?

9. Riesgo Reputacional

El riesgo reputacional se refiere al riesgo de pérdidas por daños a la imagen de un proveedor, socio o parte interesada, llevando a una reducción en la confianza de los clientes y corresponsales. Pueden ocurrir pérdidas en la reducción de ingresos y el valor para los accionistas, así como en el aumento de los costos operativos o responsabilidad legal. El riesgo reputacional no es un riesgo directo, sino que es el resultado de otros problemas relacionados con el riesgo, como muchos de los discutidos a lo largo de este manual. Sin embargo, por su naturaleza, las consecuencias pueden ser graves y perdurables. Los riesgos que es más probable que puedan resultar en daños reputacionales son, un fallo tecnológico que cause imposibilidad para realizar transacciones, falta de transparencia en las políticas y los precios, fraude, mala experiencia del cliente, falta de liquidez de los corresponsales y precios altos.

La mejor manera de proteger al negocio contra el riesgo reputacional es teniendo una función de gestión de riesgo sólida que permita prevenir aquellos riesgos que puedan afectar el servicio o la reputación de la compañía. La prevención de riesgos incluye minimizar las oportunidades de fraude o los riesgos causados por la mala experiencia del cliente, tales como transacciones fallidas, falta de conectividad y liquidez, o mala experiencia del corresponsal. La prevención del riesgo reputacional se puede lograr centrándose en la experiencia del cliente y en la generación de confianza. La creación de una buena experiencia del cliente se puede lograr asegurando que pueden acceder a sus fondos cuando y donde lo necesitan, así como crear vías para el recurso de los clientes, tales como animar y apoyar a los corresponsales para que suministren un servicio al cliente de primer nivel, operando call centers bien administrados a resolver las quejas y consultas de los clientes, y devolver los fondos de los clientes en cualquier caso de fraude. El riesgo reputacional también es un efecto del riesgo societario si los socios no cumplen con las expectativas de los clientes. El proveedor debe estar preparado para abordar los problemas y mantener relaciones con los clientes, incluso si el evento fue culpa del socio.

Para aquellos riesgos que no se pueden evitar, se utiliza una estrategia de mitigación. Un componente clave de una estrategia de mitigación es una estrategia de relaciones públicas que tiene contingencias para manejar la prensa negativa, ya sea reactiva o proactivamente, dependiendo de lo que la situación requiera. La mayoría de las organizaciones ya tienen una estrategia de relaciones públicas para la limitación de daños, y el negocio de Servicios Financieros Digitales debe ser incluido orientando al personal clave sobre el servicio para que puedan reaccionar rápidamente a las amenazas reputacionales. Como los Servicios Financieros Digitales pueden ser bastante complejos, es aconsejable también tener una persona designada del equipo de SFD que interactúe con el gerente de relaciones públicas para asegurarse de estar entregando los mensajes correctos.

Si bien las ruedas de prensa son el primer paso para mitigar el riesgo reputacional, también es aconsejable comunicarse directamente con corresponsales, comerciantes y cualquier otro aliado de Servicios Financieros Digitales para tranquilizarlos respecto a la situación. Además, los servicios al cliente deben ser orientados y se les deben proporcionar declaraciones validadas que se puedan comunicar a los clientes interesados. También es importante comunicarse internamente para evaluar al personal y tranquilizarlo.

EJEMPLO 9

Registro de Riesgo

Riesgo Reputacional: fallas en las transacciones

Ejemplo de Proveedor de Servicios Financieros Digitales:	Por ejemplo, una IMF que ofrece banca de corresponsales
Categoría del riesgo:	Riesgo Reputacional
Categoría Secundaria:	Riesgo Tecnológico
Nombre:	Mala experiencia del cliente causada por el riesgo tecnológico
Descripción	Los corresponsales no pueden realizar una transacción cuando la solicita el cliente porque el servicio no está disponible durante varias horas
Dueño:	Jefe de Servicios Financieros Digitales
Causa:	El Servicios Financieros Digitales están sufriendo una interrupción técnica no planificada
Efecto:	El servicio adquiere la reputación de ser poco fiable. Los corresponsales se sienten avergonzados. Los clientes no están seguros de que puedan acceder a su dinero. Con el tiempo dejan de usar el servicio
Probabilidad:	2 de 5 Moderadamente bajo debido a la fuerte mitigación del riesgo tecnológico
Impacto:	2 de 5 Moderadamente bajo basado en la improbabilidad de perder a todos los clientes
Estrategia de Riesgo:	Tratamiento
Estrategia de Tratamiento:	• Prevención de un evento de riesgo que conduciría a riesgo reputacional • Fuerte SLA con el proveedor de tecnología, basado en tecnología robusta • Proceso de resolución de incidentes y matriz de escalados existente • Servicio de atención al cliente con recursos suficientes • Canales de sugerencias de clientes a través de corresponsales, call centers, redes sociales, correo electrónico, sucursales u otro canal
Respuesta Táctica de Tratamiento:	• Plan de comunicaciones para alertar al negocio de la interrupción y luego para que los corresponsales y otros socios sean advertidos del problema y su tiempo de resolución esperado • Procedimiento establecido para atender consultas de la prensa sobre el incidente • Atención al cliente es asesorada sobre cómo manejar las llamadas de clientes y corresponsales
Indicador Clave de Riesgo:	KPIs a corto y largo plazo (¿el incidente afectó el desempeño esperado del negocio?)
Estado actual:	No ha ocurrido

Cuadro 9

Estudios de Caso Riesgo Reputacional

A) Un proveedor exitoso de SFD descubrió que había sufrido un fraude de un monto significativo por parte de empleados corruptos. La policía fue llamada y los sospechosos acusados. Debido a esto, parecía improbable que pudiera silenciarlo y evitar un escándalo. Después de un debate, se decidió hacerlo público en la prensa, explicando lo sucedido; que el asunto había sido detenido y que ninguno de sus clientes había sufrido como resultado. La reacción del público fue, como era de esperar, que los clientes favorecieron a los competidores debido a consideraciones de seguridad y esto resultó en una consiguiente caída en las ventas. No se sabe cuál habría sido la caída en las ventas si se hubiera guardado silencio y el fraude hubiera sido revelado por los medios de comunicación en los titulares de las noticias. En resumen, el proveedor de Servicios Financieros Digitales ahora cree que debería haber guardado silencio y esperar lo mejor.

B) Un importante MNO africano fue uno de los primeros proveedores de Servicios Financieros Digitales exitosos. Un par de años después del lanzamiento experimentó un fraude interno que fue reportado en la prensa nacional. Siguió un escándalo. El MNO admite el daño que este escándalo causó a su negocio:

"Definitivamente el daño fue mucho más allá del dinero electrónico en nuestro país ... Fue más allá del MNO y tocó todo el mercado del dinero electrónico. El daño reputacional fue múltiple".

Durante un tiempo, el daño reputacional se extendió más allá de Servicios Financieros Digitales a su principal negocio de telecomunicaciones. Además, afectó a todo el sector de SFD en este mercado; su competidor principal confirmó que este incidente también afectó sus ventas porque la pérdida de confianza del consumidor redujo el mercado entero.

RIESGO REPUTACIONAL - PREGUNTAS CLAVE

- ¿Entiendo el valor financiero de la reputación, o el costo potencial de perderla?
- ¿Considero el riesgo reputacional con el riesgo estratégico?
- ¿Tengo normas claras vinculadas a la conservación de la reputación y la integridad?
- ¿Se evalúan los socios por su riesgo reputacional?
- ¿Tengo un plan integral de comunicaciones y relaciones públicas para tratar proactivamente los rumores o preocupaciones con mi servicio?
- ¿Tengo una línea integral de atención para clientes y corresponsales?
- ¿Existen garantías para proteger los fondos de clientes y corresponsales?

¿Comparte los resultados esperados y los KPI con sus socios?

10. Riesgo Societario

Las alianzas de Servicios Financieros Digitales suelen ser necesarias y valiosas al proporcionar servicios ampliados a los clientes y mejorar la eficiencia operativa. En algunos casos, las sociedades son requeridas por las regulaciones. En todos los casos, se requiere cierto grado de cooperación y asociación, ya que los bancos dependen de las redes MNO para la conectividad y los MNOs confían en los bancos para que mantengan sus fondos en fideicomiso. Las alianzas eficaces son relaciones igualmente gratificantes que tienen propuestas de valor únicas para cada parte y proporcionan una experiencia mejorada para el cliente.

El programa de The Partnership for Financial Inclusion publicó un estudio en 2014[12] describiendo las lecciones aprendidas de las alianzas en SFD. Se encontró que existen cuatro factores claves para el éxito en las alianzas de Servicios Financieros Digitales:

- Las deficiencias en las alianzas cuando uno o más de los socios no juegan un papel clave para su éxito, o uno o más de los socios desempeñan un papel para el que están mal equipados o para el que no están motivados;
- Las asociaciones de Servicios Financieros Digitales deben permitir a los socios generar valor para sus respectivas empresas;
- Los roles de aliado en una implementación de Servicios Financieros Digitales deben estar alineados con la ventaja y motivación competitiva y comparativa;
- La falta de condiciones de igualdad competitiva en entornos regulatorios, conduce a acuerdos societarios deficientes.

El riesgo societario empresarial puede incluir la ruptura de relaciones con socios operativos y estratégicos, incluyendo distribuidores, corresponsales maestros, proveedores, proveedores de tecnología, socios de implementación y donantes. También puede ser una fuente de riesgo reputacional.

Sociedades de Bancos y MNOs: A medida que el mundo de Servicios Financieros Digitales se expande para incluir nuevos productos, tales como préstamos basados en algoritmos e integraciones de banca a billetera, las asociaciones de bancos y MNOs son cada vez más comunes. En muchos mercados, a lo largo de África subsahariana, las integraciones de banca a billetera son ahora comunes, permitiendo a los clientes mover fondos entre las cuentas bancarias y las billeteras electrónicas, y hacer depósitos y retiros usando corresponsales bancarios o de MNOs. La fluidez de los fondos crea una mejor experiencia de usuario para el cliente, pero los modelos híbridos que involucran a los bancos y las MNO también tienen un riesgo más alto de ruptura de sociedad. Las dos instituciones tratan de trabajar juntas para construir un solo producto orientado al cliente, y la cuestión de quién es dueño del cliente, a menudo se convierte en una discusión complicada. Si la sociedad se rompiera, tanto el producto como la retención del cliente podrían estar en riesgo.

[12] Partnerships in Mobile Financial Services: Factors for Success, IFC, 2014

Las instituciones necesitan desarrollar una estrategia de mitigación para retener al cliente en caso que esto suceda. Las estrategias de mitigación pueden incluir la gestión proactiva de las relaciones con los clientes a través de campañas de servicio al cliente, marketing y branding, así como estructurando acuerdos de propiedad de los clientes, dentro de los acuerdos societarios, e incluyendo cláusulas en torno a cuestiones de exclusividad y no competencia. En algunos mercados, los bancos son el aliado más pequeño y menos dominante en los Servicios Financieros Digitales y pueden tener dificultades para negociar condiciones equitativas de competencia con los MNO. Se puede llegar a decidir que les resulta mejor jugar un papel de segundo plano teniendo cuentas y préstamos, mientras que el MNO administra las relaciones de cara al cliente.

Distribuidores Corresponsales: Cuando se utilizan estructuras complejas de redes de corresponsales en un modelo de negocio de Servicios Financieros Digitales, el desempeño de los corresponsales puede depender en gran medida de la capacidad del corresponsal maestro para administrarlos. Esto normalmente abarca la formación, suministro de liquidez, materiales de marketing e incentivos. La relación entre el proveedor y el corresponsal maestro desempeña un papel clave, y la ruptura de esta relación puede resultar en una interrupción de la experiencia del cliente. Los acuerdos societarios con distribuidores corresponsales deben abarcar todos los niveles de servicios y establecer claramente las expectativas y la remuneración para reducir el riesgo societario inherente a la relación. También deben contener reglas claras sobre cómo se terminará una sociedad para minimizar el impacto en el cliente o el negocio.

Proveedores: Los proveedores juegan un papel importante en un despliegue de Servicios Financieros Digitales. El riesgo de un fallo tecnológico tiene un gran impacto en la experiencia del cliente y la sociedad que el proveedor de servicios mantiene con sus proveedores, puede afectar el riesgo de fallas en las transacciones y retrasos en el servicio.

Integraciones Técnicas: La mayoría de los servicios dependen de interfaces técnicos con terceros. El primer requisito para la integración técnica es la conectividad. Los Servicios Financieros Digitales tienen el requisito inherente de utilizar redes de datos o voz para ofrecer servicios, utilizando tecnología. Esto incluye el uso de acceso a redes móviles, incluyendo SMS, USSD y servicios 3G.

Más allá de los requisitos básicos de conectividad, a medida que los Servicios Financieros Digitales maduran, se están integrando cada vez más con otras tecnologías, a menudo a través de las Interfaces de Programación de Aplicaciones (APIs). Estos incluyen la integración con los sistemas de core bancario para permitir la transferencia de fondos entre las cuentas de Servicios Financieros Digitales y las cuentas convencionales de los bancos y las IMF; integración con facturadores como las empresas de servicios públicos, ya sea directamente o a través de conmutadores de pago; integración con diversos dispositivos POS; y la integración con las organizaciones de transferencia de dinero para facilitar las remesas internacionales. La interoperabilidad entre Servicios Financieros Digitales también está empezando a ocurrir, ya sea bilateralmente o a través de conmutadores.

Dondequiera que haya una integración técnica, hay una dependencia en el servicio del socio, y la integración misma es un punto de errores potenciales. Por lo tanto, es esencial que la calidad del servicio de la organización asociada sea bien entendido antes de que se confirme la asociación. A menudo se culpa al proveedor de Servicios Financieros Digitales por la mala calidad de un socio. Por ejemplo, si el conmutador de pago está sobre extendido, es posible que el cliente tenga que intentar realizar una transacción varias veces antes que se pague una factura, y esto típicamente será visto como una falla del Servicio Financiero Digital. Debajo de toda alianza técnica, debe haber una comprensión clara de los niveles de servicio alcanzables por el socio y un desempeño (promedio) esperado y acordado. Los socios deben ser sujetos a sanciones por el bajo desempeño continuado, frente a estos niveles de servicio. Un punto importante que a menudo se pasa por alto es la necesidad de definir exactamente lo que se entiende por nivel de servicio y cómo se medirá este.

Es crucial que haya un acuerdo sobre cómo se manejarán los incidentes. Cuando ocurre un incidente técnico que involucra dos o más tecnologías, el mayor problema puede ser determinar dónde se encuentra el fallo, con todo el mundo alegando que la responsabilidad es de la tecnología de la otra parte. Esto puede suceder en una situación de alta tensión si el fallo es grave, por lo que es importante tener procedimientos pre-acordados donde todas las partes trabajan juntas, en la medida de lo razonable, para identificar y resolver el problema. También deben existir procesos de escalamiento para incidentes que no se pueden resolver mediante procedimientos estándar.

EJEMPLO 10

Registro de Riesgo

Riesgo Societario - indisponibilidad de servicio

Ejemplo de Proveedor de Servicios Financieros Digitales:	Un banco que ofrece banca de corresponsales con POS y acceso móvil a clientes, suministrado por medio de la conectividad del MNO socio
Categoría del riesgo:	Riesgo Societario
Categoría Secundaria:	Riesgo Reputacional
Nombre:	Dificultades en la relación entre los propietarios del servicio - que conducen a la interrupción del mismo
Descripción	La dificultad significativa de la relación dentro del consorcio de proveedores resulta en la indisponibilidad del servicio para los clientes.
Dueño:	Jefe de Servicios Financieros Digitales
Causa:	Incapacidad del socio para satisfacer los crecientes requisitos de capacidad del proveedor de SFD a medida que el negocio ha crecido más rápido de lo esperado
Efecto:	La indisponibilidad del servicio para clientes y corresponsales, y los clientes no pueden acceder a las cuentas.
Probabilidad:	2 de 5 Moderadamente baja basada en acuerdos societarios y acuerdos comerciales bien estructurados
Impacto:	5 de 5 Impacto muy alto basado en la dependencia total en el socio para el suministro del servicio
Estrategia de Riesgo:	Transferir
Estrategia de Tratamiento:	• Niveles de servicios detallados en el contrato de sociedad • Revisiones técnicas mensuales con socios, incluyendo los volúmenes esperados, para asegurar que la planificación de la capacidad se anticipa a la curva de demanda • Asegurar que el socio esté suficientemente incentivado para mantener el servicio funcionando y crecer con él.
Respuesta Táctica de Tratamiento:	• Acción legal contra el socio por falla en la prestación del servicio • Siempre que sea posible, calificar a un proveedor secundario para que trabaje en paralelo o en espera
Indicador Clave de Riesgo:	• Tiempo de disponibilidad del sistema • Desempeño vs KPIs
Estado actual:	No ha ocurrido

Cuadro 10

Estudios de Caso de Riesgo Societario

A) El negocio de Kopo Kopo fue fundado originalmente en Kenia en 2012 con el fin de explotar el potencial de M-PESA y ser utilizado para pagos en tiendas de bienes y servicios. Safaricom, empresa proveedora de M-PESA, había lanzado "Lipa na M-PESA" (Pago con M-PESA) a los consumidores un año o dos antes, por lo que existía la capacidad, pero pocos comerciantes la aceptaban y el uso era muy bajo. Kopo Kopo formó una sociedad con Safaricom con el objetivo de proporcionar un servicio a comerciantes para aumentar el número de minoristas aceptando Lipa na M-PESA y así impulsar el uso en los consumidores. El servicio es gratuito para los clientes, pero los comerciantes pagan un pequeño porcentaje del valor de la transacción como un cargo que se reparte entre Kopo Kopo y Safaricom.

Kopo Kopo vinculó a los comerciantes proporcionándoles datos de transacción, inteligencia de negocios y acceso rápido a fondos a través de aplicaciones web y Android, así como capacidades de pago masivo y SMS masivo. Además, asumió la tarea de intermediación en las disputas. A finales de 2015, Kopo Kopo había vinculado a 4.000 comerciantes activos centrados en canales específicos de ventas minoristas, tales como catering, peluqueros, distribuidores agrícolas y estaciones de servicio. Debido a este crecimiento, Safaricom vio la oportunidad de administrar este negocio internamente y ahora está compitiendo directamente con Kopo Kopo para vincular nuevos comerciantes. Safaricom tiene las ventajas de escala, reputación y de ofrecer un servicio más barato, ya que cobra sólo su parte de la tarifa de transacción. Ha mostrado ser muy exitoso. Anticipando el riesgo de un cambio en la relación de socio a competidor, Kopo Kopo trató de diversificarse en dos direcciones:

- *Para mantenerse competitivo en el mercado keniano, ha desarrollado un servicio popular de anticipos de dinero con comerciantes, ofreciendo fondos basados en una calificación crediticia constantemente actualizada basada en el desempeño histórico de los comerciantes a través de Lipa na M-PESA. (Esta iniciativa no está exenta de riesgos financieros, pero no habían surgido problemas al momento de la redacción del presente manual.) A finales de 2015 ganaba más por sus avances en efectivo en Kenia, que por su negocio principal.*
- *Al apalancar su inversión existente en el software de adquirencia de comerciantes para Lipa na M-PESA, lo ha convertido en un desarrollo libre para su uso por otras instituciones fuera de Kenia. El software se venderá con base en una tarifa por licencias y Kopo Kopo ha firmado acuerdos comerciales con varios proveedores. El producto estaba pendiente de ser lanzado en 2016 en Ghana, Uganda y Zimbabue, y proporcionará un flujo de ingresos adicional siempre que el servicio de soporte no supere las expectativas.*

La preparación de Kopo Kopo para la inevitable aparición de su socio como competidor, ha sido un factor importante en la supervivencia de

su negocio en un mercado muy competitivo.

B) Un proveedor de Servicios Financieros Digitales importante (no de telecomunicaciones) sufrió un fraude de autoría por parte de uno de sus aliados. Contrató a los tres mayores operadores móviles (MNOs) del país para utilizar sus redes de comunicación, específicamente los canales SMS y USSD, y podía suministrar el servicio de dinero electrónico a cualquier cliente o corresponsal con una tarjeta SIM de cualquiera de ellos. Varios corresponsales comenzaron a reportar el mismo problema; su fondo de dinero electrónico estaba desapareciendo. En el curso de dos semanas esto pasó de un corresponsal por día a tres o cuatro, cada uno reportando pérdidas de varios cientos de dólares. Al examinar los estados de las transacciones de los corresponsales afectados alrededor del momento de los fraudes, y luego siguiendo las secuencias de las transacciones y cuentas involucradas, determinaron el medio por el cual se estaba perpetrando el fraude.

Se observó que todos los corresponsales afectados estaban utilizando corresponsales de teléfonos conectados a la misma MNO, y esto proporcionó la clave esencial. El fraude involucró a un empleado, en una función técnica en el MNO, con acceso a los sistemas de gestión de tarjetas SIM. Los estafadores habían desarrollado una estafa mediante la cual se recolectaba el PIN del corresponsal y se intercambiaba temporalmente la tarjeta SIM mientras se retiraban los fondos de la cuenta. Tan pronto como fue diagnosticada esta estafa, el socio MNO fue contactado y se explicó el problema. Presumiblemente, el MNO reforzó sus procedimientos de cambios de SIM, porque la estafa se detuvo en 24 horas y nunca se ha repetido.

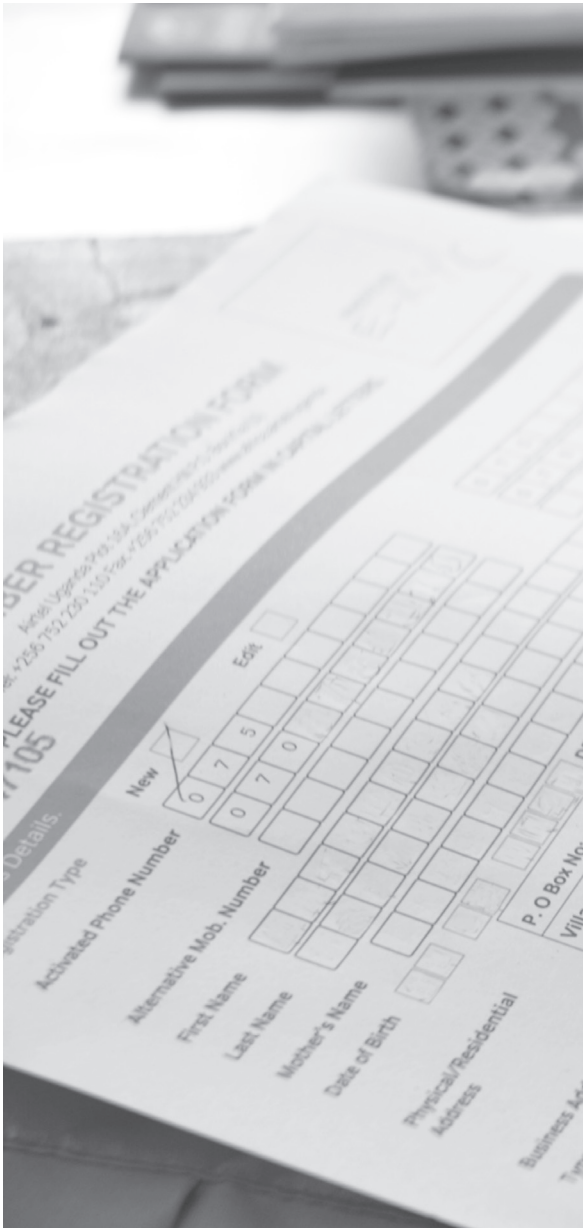
RIESGO SOCIETARIO - PREGUNTAS CLAVE

- ¿Tiene un contrato o Memorando de Entendimiento con su socio que incluye protecciones y planes de contingencia?
- ¿Tiene acuerdos de nivel de servicio con los corresponsales maestros y distribuidores?
- ¿Comparte los resultados esperados y KPIs con sus socios?
- ¿Tiene niveles de servicio técnico realistas y medibles acordados con sus socios?
- ¿Existe un proceso acordado de escalamiento técnico para resolver incidentes?

Resumen

Las diez categorías de riesgo descritas anteriormente son categorías amplias utilizadas para describir el riesgo de Servicios Financieros Digitales. En la base de datos de riesgos se encuentra una lista completa que incluye también una serie de subcategorías en la página 95. A medida que la industria de Servicios Financieros Digitales evoluciona, comenzarán a manifestarse muchos más riesgos potenciales y la tarea de identificar, entender y mitigar riesgos, será continua.

Ahora que se ha establecido un amplio entendimiento en la Parte I, y se han identificado en la Parte II los riesgos potenciales más comunes actualmente conocidos, las instituciones pueden pasar a desarrollar marcos de gestión de riesgo. La Parte III presenta instrucciones paso a paso sobre cómo configurar e implementar un marco.




Customer Form
FIRST NAME*
KATUSHIME
LAST NAME*
EDVINAH
GENDER*
Plot/Street Name & No:
Nationality
Recommendation from village chairperson/LC
Voter Registration Card
Employee ID/Letter from company
Passport (Compulsory for

03_

Parte III

Marco de Gestión de Riesgo Aplicado

En la parte anterior del manual, describimos e ilustramos los principales riesgos en la implementación de Servicios Financieros Digitales. En esta parte, tomaremos los conceptos del marco de gestión de riesgo descrito en la Parte I y conduciremos al lector por un proceso paso a paso del ciclo de gestión de riesgo. Comienza con establecer contexto, pasa a la identificación de riesgo, evaluación, y desarrollo de la estrategia de riesgo, y luego concluye con monitoreo y revisión.

Hay varias fuentes bibliográficas sobre el proceso de implementación de un marco de gestión de riesgo. La GSMA también ha publicado un conjunto de herramientas de gestión de riesgo, que utiliza un formato basado en Excel para guiar a los MNOs en los riesgos de dinero electrónico[13]. Este manual se basa en cierta forma en los estándares ISO 31000 de la industria y empresariales para la gestión de riesgo. Se ha adaptado y adecuado para la gestión de riesgos específicos de Servicios Financieros Digitales. El proceso comienza con la definición del equipo del proyecto y el establecimiento de objetivos y niveles de riesgo aceptables. Luego, se identifican y articulan todos los riesgos posibles. La evaluación de los riesgos se realiza mediante métodos cualitativos o cuantitativos para evaluar la probabilidad y el impacto potencial del riesgo. La evaluación permite a las instituciones priorizar los riesgos e identificar cuáles pueden ser tolerados, transferidos, terminados o requerir el desarrollo de una estrategia de tratamiento (cubierta en la Sección 4). Por último, se implementa el marco y se llevan a cabo revisiones periódicas, devolviéndose a la etapa de planificación e identificación para asegurar que sea siempre oportuno y refleje con precisión los riesgos enfrentados. Utilizando el Proceso de Gestión de Riesgo de ISO 31000 descrito en la Parte I, existen cinco secciones para desarrollar marcos de gestión de riesgo, como se muestra en la figura 7.

[13] Risk Management Toolkit, GSMA & Consult Hyperion, 2015 (https://www.gsma.com/mobilefordevelopment/programme/mobile-money/managing-risk-in-mobile-money-a-new-comprehensive-risk-toolkit)

Figura 7: Proceso de Gestión de Riesgo

Las secciones a continuación describen las actividades y áreas de foco en cada uno de los pasos del diagrama anterior.

Cuadro 11

Creación de una Unidad de Gestión de Riesgo

Mientras que muchas organizaciones más grandes tienen algún tipo de soporte en gestión de riesgo a nivel de grupo, Tigo Pesa Tanzania es una de las pocas compañías operativas locales con un equipo dedicado de gestión de riesgo en el país, encargado de prevenir, detectar y mitigar cualquier riesgo potencial. El equipo de gestión de riesgo se creó en 2012, dos años después del lanzamiento de Tigo Pesa, con el nombramiento de un Gerente de Finanzas y Riesgo de Servicios Financieros Digitales, reportando tanto al jefe de división como al director financiero de Servicios Financieros Digitales del grupo Millicom. Desde entonces, el equipo ha crecido a cinco personas que desempeñan una serie de funciones para proteger el negocio:

***Procesos y Controles** - responsable de asegurar que los procesos de negocio estén disponibles para todas las actividades de Tigo Pesa, y que éstas sean revisadas regularmente y actualizadas cuando sea necesario. También controla el acceso de entrada a los sistemas Tigo Pesa.*

***Prevención del Fraude** - Estas actividades se dividen en dos tipos: el fraude interno y el fraude de cara al cliente. El fraude interno potencial es controlado por una combinación de procedimientos de negocios; análisis de datos para descubrir cualquier actividad inusual; y el monitoreo de la interacción del personal con los sistemas para identificar comportamientos sospechosos. La mayor parte de la actividad consiste en detectar y mitigar el fraude de cara al cliente. Por ejemplo, hubo una creciente incidencia de clientes enviando dinero a números erróneos y los destinatarios alegaban fraudulentamente que el dinero era suyo. Impulsando el desarrollo de una nueva función para confirmar el nombre del destinatario durante las transacciones, el equipo logró reducir este tipo de fraude en un impresionante 60 por ciento.*

***Integridad de Plataforma y Aseguramiento de Proyectos** - cualquier cambio en la tecnología, sea un ajuste menor o una nueva funcionalidad importante, debe ser evaluado y aprobado por el equipo de riesgo. Se requiere un enfoque práctico para cualquier cambio y debe estar involucrado desde el inicio del proceso de desarrollo.*

***Cumplimiento de las normas** - es responsabilidad del equipo proporcionar informes específicos y cualquier otra información solicitada por el banco central, y evaluar y aplicar cualquier cambio en los informes u operaciones de negocios requeridos cuando las regulaciones cambian. Un miembro del equipo actúa como el oficial de informes anti-lavado de dinero.*

El equipo de gestión de riesgo está sujeto a revisiones periódicas por gerentes de Servicios Financieros Digitales de otros miembros del grupo; auditoría interna por el grupo Millicom; y auditoría externa por Ernst & Young.

Sección 1: Establecer Contexto

El objetivo del proceso de planificación de la gestión de riesgo es desarrollar la estrategia general de gestión de riesgo para el Servicios Financieros Digitales y decidir cómo se ejecutará y cómo se integrará en el plan general de implementación. El proceso de planificación comienza con la creación de un equipo que luego desarrolla el cronograma, los costos y el esquema del plan de gestión de riesgo, la metodología, y el proceso y las plantillas, que se utilizarán en el desarrollo del marco de gestión de riesgo.

Paso 1: Definir equipo de riesgo

El equipo estará integrado por varios funcionarios y partes interesadas, que serán responsables del éxito de los SFD, y proporcionarán antecedentes contrastados y complementarios para asegurarse que el marco de gestión de riesgo abarque una lista exhaustiva y un análisis de los riesgos potenciales y las estrategias de mitigación asociadas. El equipo debe incluir a miembros de los departamentos de gestión de riesgo, gestión de canales de SFD, ventas y marketing, TI, finanzas, control interno y cumplimiento, administración, así como expertos externos, consultores o facilitadores.

Tabla 1: Ejemplo de Equipo de Riesgo

Nombre	Título	Departamental	Detalles de Contacto
	Gerente de Riesgo	Banca de Corresponsales/Dinero Electrónico	
	Jefe de Banca de Corresponsales/ Dinero Electrónico	Banca de Corresponsales/Dinero Electrónico	
	Gerente de Distribución	Banca de Corresponsales/Dinero Electrónico	
	Gerente de Producto	Banca de Corresponsales/Dinero Electrónico	
	Jefe de TI	TI	
	Gerente de Marketing	Marketing	
	Gerente de Call Center	Atención al Cliente	
	Oficial Regulatorio	Cumplimiento	
	Gerente Financiero	Finanzas	
	Oficial de Investigación de Fraudes	Finanzas	

Paso 2: Definir roles y responsabilidades

El equipo de proyecto multidisciplinario es el principal responsable de ensamblar la evaluación y el marco de la gestión de riesgo. El equipo estará dirigido por un gerente de riesgo, quien idealmente también deberá estar en la evaluación de riesgos y en la administración de otros proyectos, para garantizar una gestión de riesgo coherente en toda la organización. Los roles de cada miembro del equipo deben estar claramente definidos y articulados en el proceso de planificación desde un principio y registrados en el plan del proyecto.

Las responsabilidades del gerente de riesgo incluyen:

- Solicitar apoyo de la alta dirección para el marco de gestión de riesgo
- Determinar los niveles aceptables de riesgo, consultando a las partes interesadas
- Elaborar y aprobar el plan de gestión de riesgo
- Promover el proceso de gestión de riesgo
- Facilita la comunicación
- Aprobar las respuestas al riesgo cuando sea necesario
- Informar periódicamente el estado del riesgo a la administración y a los principales interesados

Tabla 2: Ejemplo de Roles y Responsabilidades del Equipo de Riesgo

Nombre	Título	Dirigir o Soporte
	Gerente de Riesgo	Dirigir
	Jefe de Banca de Corresponsales/Dinero Electrónico	Dirigir
	Gerente de Distribución	Soporte
	Gerente de Producto	Soporte
	Jefe de TI	Soporte
	Gerente de Marketing	Soporte
	Gerente de Call Center	Soporte
	Oficial Regulatorio	Soporte
	Gerente Financiero	Soporte
	Oficial de Investigación de Fraudes	Soporte

Paso 3: Definir cronograma y presupuesto para desarrollo

El calendario del marco de gestión de riesgo será decidido por el equipo de planificación e incluirá fechas de inicio y finalización para cada fase, hitos clave y entregables. Los plazos también deben incluir intervalos acordados para la reevaluación del marco de gestión de riesgo.

Puede ser necesario asignar un presupuesto para el desarrollo del marco de gestión de riesgo, si se espera que las actividades incluyan la recopilación externa de datos, la contratación de consultores y facilitadores, o los costos de reuniones externas. Los presupuestos también pueden incluir fondos de contingencia para pérdidas potenciales basados en el análisis cuantitativo de la fase de evaluación del riesgo.

Tabla 3: Ejemplo de Cronograma y Presupuesto de Marco de Riesgo

Nombre	Fecha de Inicio	Fecha Final	Presupuesto Estimado
Identificación del Riesgo	Semana 1	Semana 8	
Revisión de la Publicación	Semana 1	Semana 1	
Revisión Histórica	Semana 2	Semana 2	
Evaluación Actual	Semana 3	Semana 6	$15.000 para consultor externo para asesoría técnica
Lluvia de ideas	Semana 7	Semana 8	$6.000 para facilitador
Evaluación del Riesgo	Semana 9	Semana 12	
Asignar probabilidad	Semana 9	Semana 10	$10.000 para consultor externo para asesoría técnica
Asignar impacto	Semana 9	Semana 10	$10.000 para consultor externo para asesoría técnica
Priorización de riesgos	Semana 10	Semana 10	$10.000 para consultor externo para asesoría técnica
Desarrollo de la Estrategia de Riesgo	Semana 11	Semana 12	
Desarrollar estrategia de tratamiento de riesgo	Semana 11	Semana 12	$10.000 para consultor externo para asesoría técnica
Desarrollar respuesta táctica al riesgo	Semana 11	Semana 12	$10.000 para consultor externo para asesoría técnica
Definir KRIs	Semana 11	Semana 12	$10.000 para consultor externo para asesoría técnica
Revisión Administrativa de Marco de Riesgo	Semana 13	Semana 14	$10.000 para consultor externo para asesoría técnica
Revisión del Marco	Cada 6 Meses		

Paso 4: Crear un plan

La planificación del desarrollo del marco de gestión de riesgo incluirá el desarrollo de procesos, esquemas, metodologías, definiciones y plantillas aprobadas por todos los miembros del equipo de riesgo.

Proceso: Describe el proceso que se utilizará para llevar a cabo el desarrollo del marco de gestión de riesgo y cómo se integrará en el negocio general de Servicios Financieros Digitales.

Esquema: Durante el proceso de planificación, el equipo de planificación desarrollará un esquema del marco de gestión de riesgo. Ver la página 93 para una lista de control para desarrollar un marco de gestión de riesgo.

Metodología: La metodología descrita en el esquema del plan identificará los medios para realizar las evaluaciones cualitativas y cuantitativas de riesgo, evaluación y análisis, clasificación de riesgo, y documentando en el registro de riesgo con los tratamientos asociados. El esquema de la metodología también describirá los medios a través de los cuales la organización decidirá si acaba con el riesgo, trata el riesgo, tolera el riesgo o transfiere el riesgo.

Definiciones: Las definiciones descritas en el marco de gestión de riesgo serán un glosario de términos para que el equipo trabaje bajo definiciones comunes de riesgo.

Plantillas: El esquema incluirá plantillas acordadas, que se utilizarán en todo el desarrollo del marco de gestión de riesgo. Las plantillas deben incluir el registro de riesgo como se describe a continuación, plantillas para sesiones de lluvia de ideas que ayudan en la identificación de riesgos, análisis de riesgo y evaluación de riesgo. La plantilla del marco de gestión de riesgo también se incluirá en el esquema del plan de gestión de riesgo.

Paso 5: Establecer Niveles de Tolerancia al Riesgo

Durante el proceso de planificación, el equipo de riesgo establecerá los niveles de tolerancia al riesgo de la institución, tanto en términos de niveles cuantitativos de pérdidas, como de niveles cualitativos de tolerancia. Los valores cuantitativos de las pérdidas potenciales se pueden estimar para la mayoría de los riesgos identificados mediante el proceso de evaluación de riesgo descrito a continuación. El equipo de riesgo establecerá el nivel de tolerancia, de tal forma que cualquier riesgo identificado con una pérdida potencial por encima del umbral deberá ser evitado o transferido o si está por debajo del umbral inferior, entonces el riesgo será aceptado. Por ejemplo, una institución puede decidir que cualquier riesgo con un impacto potencial de menos de $10,000 será aceptado, entre $10.000 y $ 100.000 será mitigado y de más de $100.000 será evitado o transferido.

Las pérdidas financieras debidas al fraude deben tener cierto grado de aceptación, ya que la implementación de políticas de riesgo para erradicar completamente las pérdidas sería más costosa que aceptar algunos niveles de fraude. Una vez acordado, el nivel aceptable de pérdidas por fraude debe presupuestarse e incluirse en las proyecciones y utilizarse como Indicador de Riesgo Clave para medir el desempeño. El punto de referencia de la industria para las pérdidas por fraude manejables es de siete puntos básicos del volumen total de transacciones, o un 0,07 por ciento.

La clasificación cualitativa descrita a continuación también puede utilizarse para establecer niveles de tolerancia al riesgo tales como aquellos riesgos identificados con un puntaje cualitativo de 1 - 5: Aceptar Riesgo, 6 - 12: Controlar Riesgo y 13 - 25: Evitar o Transferir. Es posible que existan otras políticas cualitativas de tolerancia al riesgo que la institución desee instituir, como la tolerancia cero para actividades ilegales o violaciones regulatorias.

Sección 2: Identificar Riesgo

El proceso de identificación de riesgos tiene como objetivo determinar todos los riesgos conocidos para el SFD. Sin embargo, como es imposible identificar todos los riesgos potenciales, se debe usar un proceso iterativo para realizar reevaluaciones periódicamente. La identificación del riesgo debe hacerse tan pronto como sea posible en el desarrollo del SFD, para permitir el máximo tiempo posible el desarrollo de las respuestas al riesgo. Sin embargo, cuanto antes se lleve a cabo el proceso de identificación, menos certeza tendrá la organización sobre la probabilidad esperada y el impacto del riesgo. El proceso de identificación de riesgos puede incluir diferentes metodologías para la identificación y debe incluir un espectro completo de riesgos para un Servicio Financiero Digital, como se ha descrito anteriormente.

Cuadro 12

Gestión de Riesgo Centrada en el Cliente

El mayor riesgo para cualquier estrategia de negocios es que los clientes no adopten el servicio en los números previstos. Tales problemas se asocian a menudo con un diseño de producto deficiente o debido a un desajuste entre las ubicaciones del cliente y de los corresponsales. Los clientes rara vez cierran una cuenta. Simplemente retiran sus fondos. Este riesgo empresarial debe entenderse a través de la relación adecuada con los clientes, a menudo gestionado por el call center o por medio de entrevistas periódicas que identifican las razones por las que no están utilizando el servicio, y estos hallazgos se agregan all registro de riesgos.

Paso 1: Investigar recursos de la industria

Se recomienda comenzar revisando las publicaciones para identificar los riesgos que son aplicables y con los que se identifica su institución. Hay una gran variedad de recursos disponibles (en inglés) que son específicos a diferentes tipos de instituciones o de riesgos específicos de Servicios Financieros Digitales, tales como:

- Risk Management Toolkit, GSMA & Consult Hyperion, 2015 (https://www.gsma.com/mobilefordevelopment/programme/mobile-money/managing-risk-in-mobile-money-a-new-comprehensive-risk-toolkit)
- MMU Managing the Risk of Fraud in Mobile Money, GSMA, 2012 (http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobile-money.pdf)
- Mobile Financial Services Risk Matrix, USAID and Booz Allen Hamilton, 2010 (https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilefinancialservicesriskmatrix100723.pdf)
- Bank Agents: Risk Management, Mitigation, and Supervision, CGAP, 2011 (http://www.cgap.org/publications/bank-agents-risk-management-mitigation-and-supervision)
- Digital Financial Services Risk Assessment For Microfinance Institutions, A Pocket Guide, AFI, 2014 (https://lextonblog.files.wordpress.com/2014/09/dfs_risk_guide_sept_2014_final.pdf)
- Mobile Financial Services Technology Risks, AFI, 2013 (http://www.afi-global.org/sites/default/files/pdfimages/AFI_MFSWG_guidelinenote_TechRisks.pdf)
- Fraud in Mobile Financial Services, Mudiri, MicroSave, 2012 (http://www.microsave.net/resource/fraud_in_mobile_financial_services#.VmWI9E10xes)
- Risk Management in Mobile Money, Lake, IFC, 2013 (http://www.ifc.org/wps/wcm/connect/37a0868042366698d8220ae0dc33b630b/Tool+7.1.+Risk+Management.pdf?MOD=AJPERES)

Además, en la sección Base de Datos de Riesgo de esta publicación, se incluye una lista exhaustiva de riesgos potenciales y se puede utilizar como referencia.

Paso 2: Revisión histórica

El proceso de identificación de riesgos comenzará con una visión retrospectiva del riesgo, teniendo en cuenta los riesgos tolerados, tratados o realizados a lo largo de los ciclos de vida de otros proyectos, incluyendo las implementaciones anteriores de productos y canales de la propia institución u otras, dentro del mercado. La revisión histórica se llevará a cabo a través de la investigación secundaria de la documentación interna de gestión de riesgo, así como fuentes externas, como los contactos de la industria y los medios de comunicación.

Paso 3: Evaluaciones de estado actual

La evaluación actual del desarrollo de Servicios Financieros Digitales revisa críticamente el estado de la implementación, para entender qué riesgos tienen más probabilidades de existir. La evaluación de la implementación incluirá un análisis del modelo financiero actual, especificaciones de producto, modelo de negocio, desarrollo tecnológico, aprobaciones regulatorias, análisis de competidores e investigación de mercados. Utilizando las categorías de riesgo descritas anteriormente, el equipo de riesgo puede comenzar a conformar la larga lista de riesgos potenciales. Muchos riesgos empezarán a surgir a medida que el equipo explora las definiciones de productos, la estrategia de corresponsales y distribución, los contratos de corresponsales, los contratos de socios tecnológicos, las directrices reglamentarias locales, las especificaciones tecnológicas, los manuales de procedimientos operativos, las proyecciones financieras, las investigaciones de mercado u otros documentos que están disponibles para su revisión. Teniendo en cuenta las categorías de riesgo, también se puede pedir al equipo que identifique todos los posibles riesgos que reconocen como relevantes para sus áreas de operaciones. En esta etapa, es importante enumerar todos los riesgos que sea posible, sin juzgar su importancia.

Paso 4: Luvia de ideas

Para complementar las evaluaciones históricas y actuales, las técnicas de creatividad pueden utilizarse para sesiones de lluvia de ideas que pueden incluir expertos externos o facilitadores.

Paso 5: Documentar todos los riesgos identificados en el registro de riesgo

Este es el primer paso en el desarrollo de un registro de riesgo. Todos los riesgos identificados deben ser registrados incluyendo nombre, descripción y propietario, así como cualquier nota sobre las respuestas preliminares al riesgo que surgen durante la fase de identificación. En esta etapa, la lista pretende ser lo más exhaustiva posible. Durante la etapa de evaluación, los riesgos se clasificarán y categorizarán para decidir la importancia relativa.

Tabla 4: Ejemplo de la Etapa de Identificación de Riesgo para el Riesgo Estratégico de Servicios Financieros Digitales

Tipo de Riesgo: Riesgo Estratégico				
Nombre	*Descripción*	*Causa*	*Efecto*	*Dueño*
Los Servicios Financieros Digitales no logran alcanzar la sostenibilidad en el plazo designado	Los Servicios Financieros Digitales no cumplen los objetivos de ingresos y gastos en un plazo determinado	Mala oferta de productos, mala gestión de los canales, mala gestión de los recursos, malas previsiones	Resulta en ingresos netos y retorno de la inversión negativos	Jefe de Banca de Corresponsales/Dinero Electrónico
El proveedor no entiende completamente su mercado objetivo para Servicios Financieros Digitales	Entendimiento incorrecto de las necesidades del cliente y de los recursos disponibles	Mal desarrollo de la estrategia, mala investigación de mercados, malas pruebas del producto o canal con los consumidores	Conduce al desarrollo de productos inapropiados, y mala adopción y uso	Jefe de Marketing
El proveedor no invierte completamente en los recursos necesarios para alcanzar los objetivos	No hay recursos suficientes de personal de apoyo de ventas	Las necesidades de inversión a largo plazo del canal de SFD no se entienden ni son apreciadas por parte de la administración y la Junta	El proveedor no puede cumplir con los objetivos de vinculación de corresponsales, por lo que no se alcanzan los objetivos de ingresos y no se logra la sostenibilidad.	Jefe de Ventas
Competencia	Los competidores están ganando cuota de mercado	Competidores que ofrecen un servicio superior o precios más bajos	Los clientes migran a otros proveedores	Jefe de Banca de Corresponsales/Dinero Electrónico

Sección 3: Analizar y Evaluar

Una vez identificados todos los riesgos, el proceso de análisis puede realizarse para evaluarlos y priorizarlos. Los métodos para el análisis más utilizados son los cualitativos, tales como el desarrollo de un sistema de scoring y clasificación, como se describe a continuación:

Cualitativo

El análisis cualitativo permite comenzar a clasificar la importancia de los riesgos identificados y arranca con la evaluación de características y prioridades, basadas en métricas precalificadas definidas durante el proceso de planificación de riesgo. El análisis cualitativo se basa en el proceso de identificación de riesgos para definir el riesgo y evaluar las causas y los impactos. Los riesgos pueden clasificarse según la fuente o causa, o por impacto, para facilitar el desarrollo de respuestas al riesgo durante el análisis cualitativo. El resultado final de un análisis cualitativo será la definición del riesgo, la probabilidad y el impacto potencial. Por ejemplo, al riesgo que los competidores ganen cuota de mercado se le da una probabilidad de 3 basada en el ejemplo ficticio de una institución financiera en un entorno altamente competitivo, con bajas barreras de entrada y un impacto potencial de 3, basado en algunas pérdidas en los ingresos financieros, pero no de pérdidas totales, ya que la lealtad del cliente es alta para esta institución en particular.

Los pasos para el análisis cualitativo se describen a continuación:

Paso 1: Asignar probabilidad e impacto

Para cada riesgo identificado, se debe realizar una evaluación cualitativa de probabilidad e impacto. El impacto es la pérdida potencial si se realiza el riesgo. Esto podría ser, pérdida financiera, pérdida de reputación o penalidades legales o reglamentarias. El impacto se puede medir en una escala de 1-5, siendo 1 el más bajo y 5 el más alto. Una medición de 1 representa un impacto insignificante, 2 es bajo, 3 es moderado, 4 es alto y 5 es extremo.

La probabilidad es la probabilidad asumida que el evento ocurrirá. También se asigna en una escala de 1 a 5, siendo 1 una posibilidad remota, 2 improbable, 3 posible, 4 probable y 5 casi seguro que ocurrirá el evento. Luego se cuantifica una calificación de riesgo multiplicando la clasificación asignada tanto a la probabilidad como al impacto para producir una puntuación combinada para un riesgo particular.

Paso 2: Análisis de riesgos

El análisis de riesgo es la documentación escrita para el registro de riesgos que incluye un análisis de las causas y efectos del riesgo; descripción del motivo por el que la probabilidad y el impacto se asignaron como tales; cualquier riesgo secundario; prioridad; marco de tiempo de cuándo pueden ocurrir; y posibles formas para tratar el mismo.

Priorización de Riesgo

Paso 3: Calificar los riesgos basándose en riesgos cualitativos y cuantitativos

Los riesgos ahora pueden ser priorizados, basados en el impacto potencial y la probabilidad. Utilizando la metodología de clasificación cualitativa, los riesgos con la mayor probabilidad combinada y la puntuación de impacto serán los más altos, y los que tengan la puntuación combinada más baja serán los más bajos. Si se utiliza la metodología cuantitativa, las que tengan el mayor valor R serán clasificadas como el riesgo más alto. La clasificación de los riesgos por prioridad permitirá al equipo del proyecto trabajar hacia estrategias de riesgo trabajando primero en los más importantes.

Paso 4: Decidir cuáles riesgos merecen respuestas de tratamiento

Usando la puntuación cuantitativa, la institución ahora puede decidir si tolerar, tratar, transferir o terminar el riesgo. Se pueden utilizar umbrales de puntaje tales como: 1 - 5: Aceptar Riesgo, 6 - 12: Controlar Riesgo y 13 - 25: Evitar o Transferir.

Figura 8: Matriz de clasificación de riesgo cualitativo

	Impacto				
Probabilidad	*Despreciable (1)*	*Bajo (2)*	*Moderado (3)*	*Alta (4)*	*Extremo (5)*
Cierto (5)	5	10	15	20	25
Probable (4)	4	8	12	16	20
Posible (3)	2	6	9	12	15
Improbable (2)	2	4	6	8	10
Remoto (1)	1	2	3	4	5

Una vez terminado el análisis, los riesgos se deben clasificar por tipo o prioridad, y deben documentarse en el registro de riesgo.

Tabla 5: Ejemplo de la Etapa de Evaluación de Riesgo para el Riesgo Estratégico de Servicios Financieros Digitales

Nombre	Descripción	Causa	Efecto	Dueño	Probabilidad (1-5)	Impacto (1-5)	Score combinado	Clasificación
Los SFD no logran alcanzar la sostenibilidad en el plazo designado	Los Servicios Financieros Digitales no cumplen los objetivos de ingresos y gastos en un plazo determinado	Mala oferta de productos, mala gestión de los canales, mala gestión de los recursos, malas previsiones	Resulta en ingresos netos y retorno de la inversión negativos.	Jefe de Banca de Corresponsales/ Dinero Electrónico	2	3	6	#2
El proveedor no entiende completamente su mercado objetivo para SFD	Un entendimiento incorrecto de las necesidades del cliente y recursos disponibles	Mal desarrollo de la estrategia, mala investigación de mercados, malas pruebas del producto o canal con los consumidores	Conduce al desarrollo de productos inapropiados y mala adopción y uso	Jefe de Marketing	1	2	2	#4
El proveedor no invierte completamente en los recursos necesarios para alcanzar los objetivos.	No hay recursos suficientes de personal de apoyo de ventas	La inversión a largo plazo del canal de Servicios Financieros Digitales no es entendida ni apreciada por la dirección y la Junta.	El proveedor no puede cumplir con los objetivos de vinculación y activación de clientes, por lo que no se alcanzan los objetivos de ingresos y no se logra la sostenibilidad.	Jefe de Ventas	1	3	3	#3
Competencia	Los competidores están ganando cuota de mercado	Competidores ofrecen un servicio superior o precios más bajos.	Los clientes migran a otros proveedores	Jefe de Banca de Corresponsales/ Dinero Electrónico	3	3	9	#1

Sección 4: Estrategias de Riesgo

En esta etapa del proceso, todos los riesgos deberán haberse evaluado y clasificado en función de la probabilidad y el impacto. Con base en los umbrales de aceptación de riesgos establecidos en el proceso de planificación, el equipo del proyecto ahora podrá identificar qué riesgos serán tolerados, tratados, transferidos o terminados. Los riesgos con baja probabilidad y bajo impacto son propensos a ser tolerados y no se requiere ninguna acción adicional. Para aquellos riesgos que requieren tratamiento, transferencia o terminación, se debe desarrollar una estrategia.

Paso 1: Desarrollar estrategia de interrupción de riesgos

La terminación del riesgo se realiza en los niveles más altos de probabilidad e impacto combinados. Implica tomar las medidas necesarias para asegurar que la amenaza no pueda ocurrir o no pueda tener un efecto significativo en el proyecto. El espectro de estrategias de terminación de riesgo incluye una cancelación completa de la implementación de Servicios Financieros Digitales, o cambiar los fundamentos de la estrategia del negocio, redefinir especificaciones del producto o estrategias de administración de corresponsales.

Paso 2: Desarrollar estrategia de transferencia de riesgo

Las estrategias de transferencia de riesgos se aplican cuando el riesgo puede transferirse a un tercero que esté mejor posicionado para hacer frente a una amenaza particular. Se requieren acuerdos con un tercero que defina claramente qué parte cubren las responsabilidades de la otra parte. Un ejemplo de una estrategia de transferencia de riesgo, se refiere al robo del efectivo del corresponsal en las instalaciones del corresponsal. Este riesgo puede ser transferido a través de la compra de un seguro de robo, ya sea en nombre del corresponsal, o como requisito para que los corresponsales compren un seguro para ellos mismos como parte del contrato del corresponsal.

Paso 3: Desarrollar estrategia de tratamiento de riesgo

El desarrollo de la estrategia de tratamiento de riesgos será una de las mayores tareas realizadas por el equipo del proyecto de gestión de riesgo. Decidir sobre estrategias de tratamiento puede requerir concesiones y arreglos, ya que algunas respuestas propuestas pueden ser mutuamente excluyentes o contraproducentes. Por ejemplo, mitigar el riesgo de retrasos excesivos en el lanzamiento de un servicio podría costar dinero, creando así nuevos riesgos al aumentar la presión sobre el presupuesto. El desarrollo de la estrategia de tratamiento de riesgos también debe tener una visión integral de todas las respuestas propuestas y asegurarse que son coherentes.

El tratamiento de riesgos puede incluir políticas o acciones que reduzcan la probabilidad o el impacto del riesgo específico, reduciendo así su puntuación a un rango aceptable, antes de que comience el proyecto; o una aplicación incremental de la estrategia de tratamiento, que se implementa cuando el riesgo se hace mayor. Las estrategias de tratamiento de riesgos también pueden incluir estrategias de respuesta sobre cómo controlar el daño sólo si se realiza el riesgo.

En general, las estrategias de tratamiento deben ser apropiadas, oportunas, rentables, viables, alcanzables, acordadas, asignadas y aceptadas. En esta etapa del proceso es importante involucrar a cualquier recurso de operaciones relevante para asegurar que el riesgo esté siendo abordado desde un enfoque práctico de abajo hacia arriba para prevenir la creación de estrategias inadecuadas o inviables. Cualquier estrategia de tratamiento de riesgo propuesta debe cumplir los siguientes criterios:

- Estar alineados con los valores de la organización, los objetivos del plan de negocio de los SFD y las expectativas de la gerencia;
- Deber ser técnicamente viable;
- El equipo del proyecto o los dueños de los riesgos deben tener la capacidad y los recursos para llevar a cabo las acciones requeridas;
- Lograr un equilibrio entre la reducción del impacto del riesgo y la capacidad de cumplir con los objetivos del proyecto.

Se requieren estrategias de tratamiento de riesgos para cubrir todos los riesgos expuestos. Se pueden usar múltiples estrategias para asegurar que no haya exposición residual como se muestra en la Figura 6 a continuación.

Figura 9: Pasos para desarrollar estrategias de mitigación del riesgo

Fuente: Project Management Institute: Practice Standard for Project Risk Management

Paso 4: Desarrollar respuesta táctica para tratamiento del riesgo

Una vez que se han desarrollado las estrategias de tratamiento de riesgo, también se necesita desarrollar una respuesta táctica y orientada a la acción, para cada estrategia. Las respuestas tácticas deben integrarse en la documentación de Servicios Financieros Digitales, como es el plan de negocios o los planes de trabajo.

Paso 5: Desarrollar Indicador Clave de Riesgo

La detección de la ocurrencia de un evento puede realizarse a través del monitoreo de los Indicadores de Riesgo Clave asociados con cada riesgo identificado. La sección Base de Datos de Riesgo, que se encuentra en el capítulo de Herramientas de este manual, tiene ejemplos de KRIs apropiados que se utilizarán para medir y detectar la ocurrencia de eventos. La gerencia y el comité de riesgodeben desarrollar y acordar parámetros aceptables de KRI para permitir que los encargados del proyecto continúen con procedimientos del escalamiento, cuando y donde las alertas son disparadas por incumplimiento de KRIs. Los parámetros y límites se deben establecer por la función de riesgo o comité de riesgo de la Junta. En general, son un reflejo de la tolerancia al riesgo de la institución.

Paso 6: Documentar estrategias de riesgo en registro

Por último, las estrategias de riesgo deben ser documentadas en el registro junto con la información previamente registrada para cada riesgo identificado.

Tabla 6: Ejemplo de la Etapa de Desarrollo de la Estrategia de Riesgo para el Riesgo Estratégico de SFD

Utilizando los umbrales de puntaje de:

Nivel de Riesgo	1 - 5	6 - 12	13 - 25
Acción	Tolerar	Tratar	Transferir o Finalizar

Para el riesgo identificado en la Tabla 5, los riesgos clasificados 3 y 4 pueden ser tolerados ya que tienen una puntuación combinada de menos de 5. Los riesgos 1 y 2 requerirán una estrategia de tratamiento porque caen en el umbral de control con puntajes entre 6 y 12.

Riesgo Estratégico #1:

Categoría del riesgo:	Riesgo Estratégico
Categoría Secundaria:	Riesgo Financiero
Nombre:	Competencia
Descripción:	Los competidores están ganando cuota de mercado
Dueño:	Jefe de Marketing
Causa:	Competidores que ofrecen un servicio superior o precios más bajos
Efecto:	Los clientes migran a otros proveedores
Probabilidad:	3 de 5
Impacto:	3 de 5
Estrategia de Riesgo:	Tratar
Estrategia de Tratamiento:	• Realizar investigaciones para entender la oferta de los competidores, sus fortalezas y debilidades • Supervisar los registros de los call centers, respecto a las quejas sobre los niveles de servicio • Promociones para mantener a los clientes comprometidos y activos • Venta cruzada de otros productos y servicios para crear permanencia del cliente
Respuesta Táctica de Tratamiento:	• Reevaluar diseño de producto y canal, precios y estructuras de comisiones • Realizar estudios para entender mejor la demanda del mercado y desarrollar una propuesta de valor renovada
Indicador Clave de Riesgo:	% Cuota de Mercado

Riesgo Estratégico #2:

Categoría del riesgo:	Riesgo Estratégico
Categoría Secundaria:	Riesgo Reputacional / Financiero
Nombre:	El SFD no logran alcanzar la sostenibilidad en el plazo designado
Descripción	Los SFD no cumplen las metas de ingresos y gastos, lo cual resulta en ingresos y retorno de la inversión negativos
Dueño:	Jefe de Servicios Financieros Digitales
Causa:	Mal diseño del producto o del canal, demanda del mercado y/o competencia mal entendidos
Efecto:	Pérdida de inversión
Probabilidad:	2 de 5
Impacto:	3 de 5
Estrategia de Riesgo:	Tratar
Estrategia de Tratamiento:	• Utilizar la investigación de mercados y benchmarks de la industria para establecer supuestos • Asegurar que las metas son realistas y están alineadas con los KPIs • Asegurar que hay suficientes recursos (personas / fondos) asignados para alcanzar los objetivos • Monitorear el desempeño y actualizar la estrategia según sea necesario
Respuesta Táctica de Tratamiento:	• Iterar el modelo financiero a medida que avanza la implementación • Reevaluar las estructuras de precios y comisiones • Realizar estudios de mercado para entender la demanda del mercado • Realizar actividades promocionales para estimular la adopción
Indicador Clave de Riesgo:	• Ingresos netos • Clientes activos • Transacciones por cliente • Corresponsales activos • Clientes por corresponsal • Tasa de interés del fondo de dinero electrónico

Sección 5: Monitorear y Revisar

La eficacia del marco de gestión de riesgo depende de lo bien que se implemente. La implementación incluye iniciar el trabajo sobre las respuestas tácticas tratadas en la Sección 4, así como revisiones periódicas y reevaluaciones. A medida que los Servicios Financieros Digitales maduran y evolucionan, aparecerán nuevos riesgos, y la probabilidad y el impacto de los riesgos previamente identificados cambiará.

El marco de gestión de riesgo y el registro de riesgo son documentos vivos. El equipo del proyecto decidirá sobre los intervalos de informes y reevaluación al inicio del desarrollo del marco de gestión de riesgo. Se recomienda que la información sobre el riesgo se realice trimestralmente y se lleve a cabo una revaluación completa anualmente.

Paso 1: Reevaluación de Riesgo

Además de la revisión periódica, puede ser necesario realizar una reevaluación si se produce alguna de las siguientes situaciones:

- Ocurrencia de un evento importante o inesperado;
- Un cambio fundamental en el plan de negocios o estrategia de gestión de Servicios Financieros Digitales;
- Se ofrece un nuevo tipo de servicio a través de los Servicios Financieros Digitales;
- Fin de la fase de implementación.

Paso 2: Seguimiento a riesgos durante un período

Para cada período informado, cada riesgo será reportado como:

- No ocurrió
- Ocurrido y plan de contingencia implementado
- Ocurrió y tuvo impacto en el proyecto (tiempo, costo y calidad)

Además de informar sobre el registro de riesgos existente, también se debe informar si se han observado riesgos nuevos o previamente no identificados, y la efectividad de las estrategias de riesgo, o cualquier cambio en la causa y efecto de los riesgos dentro del registro. También es muy útil hacer seguimiento al perfil de riesgo de los riesgos claves a lo largo del tiempo, ya que las circunstancias cambiantes (incluyendo la implementación de estrategias de prevención y mitigación de riesgos) pueden hacer que el riesgo de que ocurra un evento específico, sea más o menos probable o cambiar su impacto potencial.

Resumen

Con el fin de implementar con éxito una estrategia de Servicios Financieros Digitales, es necesaria una estructura estandarizada para la construcción de un marco de gestión de riesgo, con el objetivo de apoyar y mantener las operaciones. El proceso comienza con el establecimiento del contexto, incluyendo la construcción del equipo y conseguir plena aceptación de la alta gerencia y la Junta. La parte más importante del desarrollo del marco es la identificación del riesgo, la evaluación y el desarrollo de la estrategia de tratamiento. Un grupo amplio de personas con antecedentes diversos debe participar en el proceso de identificación de riesgos. Las revisiones administrativas, revisiones históricas y las revisiones de los aspectos actuales del proyecto, pueden usarse para dilucidar todos los posibles riesgos asociados con la implementación de Servicios Financieros Digitales. Una vez identificadas, pueden utilizarse metodologías de evaluación apropiadas y coherentes para evaluar y clasificar la prioridad del riesgo identificado. El desarrollo de estrategias de tratamiento incluye decidir si tolerar, tratar, transferir o terminar el riesgo, y desarrollar la estrategia apropiada para hacerlo. Una vez terminado, el marco de gestión de riesgo puede ser monitoreado y revisado. Es muy importante que el marco de riesgo sea un documento vivo y se utilice para informar en forma activa sobre la ocurrencia de riesgos, así como para revisarlo y actualizarlo periódicamente o al ocurrir un evento importante.

04_

PARTE IV

Insights y Herramientas

Lecciones Aprendidas

La mayoría de las instituciones entrevistadas en nuestra investigación, tenían algún tipo de marco de gestión de riesgo para su negocio principal que se había extendido a los Servicios Financieros Digitales. Las implicaciones respecto a la forma en la que los SFD cambian el perfil de riesgo, reduciendo algunos pero agregando nuevos riesgos pasivos potenciales, son entendidos por algunos, mientras que otros no están seguros de cómo reaccionar. Hay una necesidad creciente de orientación acerca de la gestión de riesgo en Servicios Financieros Digitales que sea relevante y esté al alcance de todo tipo de proveedores.
Las lecciones clave extraídas de nuestra investigación y las entrevistas con una variedad de proveedores se resumen en las siguientes observaciones. Lo más importante es que es necesario contar con marcos integrales de gestión de riesgo.

A medida que los Servicios Financieros Digitales siguen creciendo y ampliándose alrededor del mundo y se extiende la gama de servicios disponibles, se vuelven más vulnerables a riesgos imprevistos o nuevos. Un mayor conocimiento público de los servicios, y un mayor volumen y valor de las transacciones, pueden atraer la atención desde lugares y personas no deseados. Para proteger a estas empresas nuevas y en crecimiento, sus clientes y sus aliados (tales como los corresponsales), existe una clara necesidad que la mayoría de los proveedores de Servicios Financieros Digitales mejoren el conocimiento, el enfoque y la implementación de la gestión de riesgo. Mientras que una minoría ha desarrollado estrategias efectivas de tratamiento de riesgo, muchos proveedores de Servicios Financieros Digitales actualmente tienen un enfoque superficial, con poco o ningún tratamiento de riesgo establecido.

Los registros de riesgo han sido creados por algunos proveedores de Servicios Financieros Digitales, pero no está claro que éstos sean ampliamente utilizados en el funcionamiento del negocio. En general, parece haber una limitada comprensión y conciencia[14] de cómo implementarlos. Los registros se limitan típicamente a riesgos que podrían resultar en pérdidas financieras inmediatas, como fraude o cuestiones técnicas, y no cubren riesgos más amplios y profundos, tales como riesgos estratégicos, riesgo reputacional, riesgos cibernéticos, riesgo societario o riesgos políticos. Su creación se suele considerar como el objetivo final (calmar a los auditores o los comités de gobernanza), en lugar del inicio de un proceso continuo para reducir los riesgos de las organizaciones. Por último, no suelen estar clara o críticamente vinculadas a la consecución de los objetivos.

[14] En preparación para esta publicación, la IFC entrevistó a una serie de proveedores de Servicios Financieros Digitales, proveedores de tecnología, ONGs y otras organizaciones relacionadas.

1 Los riesgos de gestión de tecnología, estratégicos y de corresponsales, pueden conducir a riesgo reputacional

Si los clientes no pueden acceder a su dinero cuando lo necesitan, existe un riesgo reputacional potencial que puede conducir a la reducción de la adopción de clientes, la disminución de las tasas de actividad y cuentas inactivas;todo lo cual causará grandes pérdidas a un proveedor al no poder cumplir con las metas establecidas en su plan de negocio. Cuando esto sucede, hay repercusiones aún más graves si las juntas directivas y la gerencia pierden confianza y reducen los presupuestos o reorientan los recursos empresariales, y se depende de estrategias alternativas (distintas a Servicios Financieros Digitales) para impulsar el crecimiento de los clientes y los ingresos. Por lo tanto, es de suma importancia que la experiencia del cliente sea perfecta, con un servicio al cliente superior y precios competitivos. La tecnología, la estrategia y el riesgo de gestión de los corresponsales juegan un papel importante en la prestación de un servicio al cliente superior, e incluyen:

- Productos que satisfacen las necesidades de los clientes
- Diseño de canal que satisface las necesidades de los clientes
- Precios competitivos
- Las cuentas se pueden abrir donde los corresponsales, y el cliente idealmente debe poder tener acceso inmediato a las mismas
- Los clientes también pueden acceder a sus cuentas a través de otros canales si es necesario, como sucursales y cajeros automáticos
- Call centers con suficiente personal bien capacitado
- Múltiples puntos de atención al cliente, incluyendo call centers, así como correo electrónico, SMS, personal de ventas itinerante y personal de sucursales capacitado
- Tecnología que siempre está funcionando, es decir, conectividad de datos y voz disponibles; servicio de software disponible; dispositivo de hardware es operable; y no hay retrasos o fallos de transacción durante cualquier punto de la comunicación
- Recibos de SMS precisos y oportunos
- Los clientes siempre son reembolsados por actividades fraudulentas
- Las tarifas son fáciles de entender
- Los menús son fáciles de seguir
- Los corresponsales están siempre disponibles y tienen liquidez
- Los corresponsales están bien capacitados para atender a los clientes
- Los corresponsales tienen una marca clara y consistente

2 El fraude puede tener un gran impacto en la reputación

El fraude puede causar pérdidas financieras directas como resultado del retiro no autorizado de fondos o la creación no autorizada de dinero electrónico. Adicionalmente, el impacto total del fraude puede extenderse más. Cuando se hace pública, se sabe que la actividad fraudulenta reduce la confianza del consumidor en los Servicios Financieros Digitales, así como los servicios básicos del proveedor, tales como los negocios de voz del MNO o la banca personal. Los problemas de confianza de los consumidores también pueden afectar a otros proveedores y afectar al mercado en su conjunto. Por esta razón, se han producido varios incidentes de fraude

importantes con pérdidas asociadas, que los proveedores han impedido que se hagan públicas. Otros no han mantenido sus pérdidas en secreto, en detrimento tanto de sus Servicios Financieros Digitales, como de su actividad principal. Una institución implementó una estrategia de mitigación que consistía en ir a la prensa enseguida se daba un caso de fraude, con la esperanza que minimizaría el daño a la reputación, pero la sensación, visto en retrospectiva, es que esto solo llamó la atención sobre el tema y asustó a los clientes. Todavía existe desacuerdo entre los proveedores sobre la mejor manera de manejar grandes casos de fraude. Debido al daño potencial que el fraude puede infligir a todo el mercado de Servicios Financieros Digitales, se puede defender la idea que la industria comparta mejor las experiencias y lecciones aprendidas. Sin embargo, no se debe subestimar el reto de convencer a los proveedores a que cooperen, cuando también son competidores en Servicios Financieros Digitales y en otras áreas.

3 La utilidad del call center

La utilidad del call center es de amplio alcance, mucho más allá de la meta principal de resolver las necesidades de los clientes. Los call center pueden utilizarse para la educación del cliente, la retroalimentación de los clientes y la mejora del valor de marca de la institución. Las horas de servicio del call center deben extenderse a las noches y fines de semana para atender el alto volumen de llamadas cuando los clientes tienen más probabilidades de realizar transacciones y no pueden ir a una sucursal o centro de servicio. Debe haber un proceso para alertar y actualizar al personal del call center respecto de cualquier problema del sistema para que puedan tranquilizar a los clientes preocupados que llaman. Los call centers también pueden utilizarse con fines de gestión de riesgo, mediante la utilización de registros de call center para identificar los riesgos potenciales de los SFD, así como para vigilar los principales indicadores de riesgo.

Una vez que se llevan los problemas a un call center, las instituciones deben apuntar a resolver la mayoría de estos en la primera llamada. Cualquier demora adicional, o requerir llamadas adicionales, reducirá la confianza en el servicio y tendrá riesgos reputacionales y posibles pérdidas financieras.

4 Los procesos de conciliación y liquidación deficientes dejan a las instituciones abiertas a pérdidas potenciales

La liquidación y la conciliación es un proceso dispendioso que puede tener impactos significativos en los costos operacionales, así como reducir la confianza del cliente si las transacciones terminan en cuentas transitorias durante periodos de tiempo significativos. Por ejemplo, los reembolsos de transacciones de débito sin desembolso, pueden llevar hasta una semana, dejando a los clientes frustrados y pobres en efectivo. La conciliación diaria automática se recomienda no sólo para reducir el número de transacciones transitorias, sino también como una herramienta útil en la detección temprana de fraudes.

5 Hay que elegir cuidadosamente a los socios y luego hacerlos responsables

Por ejemplo los socios pueden ir donde otros proveedores que colaboran en productos o servicios conjuntos, o proveedores que proporcionan servicios de administración de tecnología o de corresponsales. En el contexto de los productos conjuntos, existe un fuerte riesgo estratégico si existe una alta dependencia a un solo socio; el socio puede no tener acuerdos de exclusividad, y puede estar utilizando la sociedad para aprender y replicar el servicio por su cuenta.

Se debe ingresar a cualquier sociedad solo después de una minuciosa debida diligencia y discusiones amplias sobre roles y responsabilidades. Los acuerdos societarios pueden ser en forma de contratos, memorandos de entendimiento entre proveedores o acuerdos de nivel de servicio con proveedores. Los memorandos de entendimiento y los acuerdos de nivel de servicio deben definir claramente los productos de cada lado, las rutas de escalamiento de fallos, la disponibilidad de servicios, los costos, las condiciones de pago, los derechos de propiedad intelectual y los acuerdos de confidencialidad. Para el socio más pequeño, el elemento más crítico de dichas sociedades es la protección, y la claridad en el acuerdo societario en cuanto al tiempo y modo en que los socios pueden entrar en competencia unos con otros. Los acuerdos bien pensados pueden contribuir, en gran medida, a proteger a una institución contra la incapacidad para suministrar o la falta de cumplimiento por parte de los socios. Sin embargo, vale la pena señalar que los acuerdos no siempre pueden garantizar la rendición de cuentas. Si el socio es muy grande y más poderoso, es posible que no pueda hacerle rendir cuentas, o si el socio es muy pequeño, simplemente puede no tener la capacidad de cumplir con los requisitos establecidos en los acuerdos. En la mayoría de los casos, es prudente evitar la exclusividad. Para la prestación de servicios técnicos, se deben buscar proveedores de canales múltiples siempre que sea posible.

Conclusiones

Este manual proporciona orientación para el tipo de riesgos que se pueden encontrar en el despliegue de una estrategia de Servicios Financieros Digitales. Muchos de los estudios de caso apuntan a la importancia primordial del riesgo estratégico, el riesgo que la estrategia no alcance sus objetivos debido al despliegue de servicios inapropiados, la mala tecnología, el comportamiento del cliente no alineado con los modelos iniciales o la evolución imprevista del mercado. Siempre es arriesgado proporcionar una lista de riesgos, y posiblemente más aún, el proporcionar una lista de riesgos futuros, pero ya están surgiendo una serie de tendencias que probablemente moldearán la evolución de la gestión de riesgo en Servicios Financieros Digitales.

- Uno de los riesgos más importantes está relacionado con la velocidad de la innovación y el cambio disruptivo de las estrategias de canal de Servicios Financieros Digitales existentes que pueden hacer que una estrategia de Servicios Financieros Digitales sea redundante antes que la tecnología esté completamente implementada. La tasa de cambio en la tecnología y las plataformas no tiene precedentes. No sólo los proveedores de servicios necesitan determinar qué plataformas soportar, sino que los requisitos de los clientes cambian rápidamente. Un banco en Mozambique desplegó dispositivos POS en los taxis; dos años más tarde, Uber estaba atendiendo el mismo mercado en siete de las ciudades más grandes de África con teléfonos inteligentes y facturación directa a tarjetas de crédito.
- Con el rápido aumento en el uso de teléfonos inteligentes, cada vez más despliegues de Servicios Financieros Digitales dependerán del teléfono inteligente del cliente o del corresponsal/comerciante. Esto debería reducir algunas de las dificultades que los operadores han experimentado con la gestión de la tecnología POS y con las limitaciones de SMS y USSD. Las instituciones financieras que deseen desarrollar una estrategia de Servicios Financieros Digitales tendrán que desarrollar los conocimientos técnicos sobre cómo gestionar dichos riesgos.
- En mercados como Kenia, donde la banca de corresponsales ha tenido éxito, los comerciantes ahora tienen un número desconcertante de dispositivos POS y teléfonos sobre los que manejan transacciones para un número creciente de instituciones. Por lo tanto, es probable que la banca de corresponsales evolucione de un servicio en el que cada banco busque habilitar al mayor número posible de corresponsales, a una situación en la cual cualquier comerciante pueda manejar un depósito o retiro en un solo dispositivo para cualquier banco o MNO, siempre que se hayan vinculado a un conjunto de reglas estándar.

Esto de nuevo cambiará la dinámica competitiva. Algunas instituciones se especializan en servicios de corresponsales, mientras que otras se centrarán en los servicios al cliente y utilizarán los servicios de banca de corresponsales suministrados por otros.

- Es probable que la regulación de los servicios habilitados para Servicios Financieros Digitales, tales como el dinero electrónico y banca de corresponsales, aumente y también cambie la dinámica competitiva. En un número creciente de jurisdicciones los reguladores están comenzando a exigir la interoperabilidad entre los servicios de pago, incluyendo dinero electrónico, así como impedendo que los proveedores firmen acuerdos de exclusividad con los corresponsales.
- Aunque el dinero en efectivo sigue siendo popular en todos los mercados del mundo, a medida que disminuyen los costos de transacciones electrónicas, habrá una reducción gradual en la necesidad de servicios de depósito/ retiro de efectivo, los cuales deben ser tenidos en cuenta en la estrategia de Servicios Financieros Digitales. A largo plazo, a medida que disminuya la dependencia en el efectivo, algunos comerciantes verán disminuir sus ventas en efectivo y, por lo tanto, serán menos capaces de soportar los requisitos de liquidez en efectivo de los servicios de banca de corresponsales.

Ningún proveedor de Servicios Financieros Digitales podrá escaparse de los riesgos asociados con la implementación de tecnología y modelos de negocios nuevos. Sin embargo, los estudios de caso han puesto de manifiesto, cómo es posible gestionar estos nuevos riesgos, con el fin de alcanzar los objetivos de negocio en favor del crecimiento de la inclusión financiera.

Herramientas

Lista de Control de Gestión de Riesgo

Arquitectura de riesgo

- Declaración producida que establece las responsabilidades de riesgo y enumera los asuntos basados en riesgo reservados a la Junta Directiva
- Responsabilidades de gestión de riesgo
- Se han adoptado disposiciones para garantizar la disponibilidad de asesoría competente y adecuada sobre los riesgos y los controles
- Existe una cultura consciente de riesgo dentro de la organización y las acciones están a la mano para mejorar el nivel de madurez del riesgo
- Se han identificado y validado las fuentes de aseguramiento de riesgo para la Junta Directiva

Estrategia de riesgo

- Se produce una política de gestión de riesgo que describe el apetito de riesgo, la cultura y filosofía de riesgo
- Dependencias clave para el éxito identificadas, junto con los asuntos que deben ser evitados
- Objetivos de negocio validados y los supuestos que sustentan esos objetivos probados
- Los riesgos importantes a los que se enfrenta la organización identificados, junto con los controles críticos requeridos
- Plan de acción de gestión de riesgo establecido, que incluye el uso de indicadores clave de riesgo según corresponda
- Se identificaron y proporcionaron los recursos necesarios para apoyar las actividades de gestión de riesgo

Protocolos de riesgo

- Se identificó y adoptó un marco adecuado de gestión de riesgo, con las modificaciones oportunas
- Las evaluaciones de riesgos adecuadas y suficientes se completaron, y los resultados se registraron de una manera apropiada
- Procedimientos para incluir el riesgo como parte de la toma de decisiones de negocios establecidos e implementados
- Detalles de las respuestas de riesgo requeridas registradas, junto con arreglos para rastrear las recomendaciones de mejora del riesgo
- Procedimientos de notificación de incidentes establecidos para facilitar la identificación de tendencias de riesgo, junto con procedimientos de escalamiento de riesgos
- Planes de continuidad de negocio y planes de recuperación de desastres, establecidos y probados regularmente
- Disposición establecida para auditar la eficiencia y la eficacia de los controles existentes para riesgos significativos
- Disposiciones en vigor para la notificación obligatoria de riesgos, incluyendo informes sobre al menos lo siguiente:
  - » Apetito, tolerancia y restricciones al riesgo
  - » Arquitectura de riesgo y procedimientos de escalamiento de riesgos
  - » La cultura consciente del riesgo actualmente en vigor
  - » Arreglos y protocolos de evaluación de riesgos
  - » Riesgo significativos e indicadores clave de riesgo
  - » Controles críticos y debilidades de control
  - » Fuentes de aseguramiento disponibles para la Junta

Fuente: Enterprise Risk Management (ERM) and the requirements of ISO 31000, AIRMIC, Alarm, IRM: 2010

Plantilla de Registro de Riesgo

Categoría del riesgo:	Seleccione una de las siguientes: Estratégico, Regulatorio, Operacional, Tecnológico, Financiero, Político, Fraude, Gestión de Corresponsales, Reputacional o de Socios
Categoría Secundaria:	Elija uno o más entre: Estratégico, Regulatorio, Operacional, Tecnológico, Financiero, Político, Fraude, Gestión de Corresponsales, Reputacional o de Socios
Nombre:	Nombre del riesgo
Descripción:	Breve descripción del riesgo, para describir con precisión puede requerir una breve referencia a causa y efecto
Dueño:	Persona responsable de monitorear el riesgo e implementar estrategias de tratamiento
Causa:	La razón por la que ocurre el evento
Efecto:	El impacto que tiene el riesgo si se realiza
Probabilidad:	La probabilidad de que ocurra el riesgo. Puede ser clasificado en una escala de 1 a 5 o asignado un porcentaje de 0 - 100%
Impacto:	Las pérdidas potenciales si el evento ocurriera. Puede clasificarse en una escala de 1 a 5 o asignar un valor de los costos reales de realización del riesgo
Estrategia de Riesgo:	Seleccione una de las siguientes: Tolerar, Tratar, Transferir o Terminar
Estrategia de Tratamiento:	Implicación política de la institución para controlar el riesgo antes, durante o después de la ocurrencia del evento
Respuesta Táctica de Tratamiento:	Acciones específicas a tomar en caso de ocurrencia de evento
Indicador Clave de Riesgo:	Indicador utilizado como alerta temprana de que el potencial de los efectos adversos de un riesgo pueden ocurrir
Estado actual:	Seleccione una de las siguientes: No ha ocurrido, Ocurrió y se trató, Ocurrió con impacto

Base de Datos de Riesgo

Riesgo[15]	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Riesgo Estratégico				
Los Servicios Financieros Digitales no logran alcanzar la sostenibilidad en el plazo designado.	El Servicio Financiero Digital no cumple metas de ingresos y gastos y resulta en ingresos y retorno de la inversión negativos.	Cualquiera	Utilizar la investigación de mercados y benchmarks de la industria para establecer supuestos. Iterar el modelo financiero a medida que avanza la implementación. Asegurar que las metas se difundan y están alineadas con los KPIs. Monitorear el desempeño y actualizar la estrategia según sea necesario.	Ingresos netos Clientes activos Transacciones por cliente Corresponsales activos Transacciones generadoras de ingresos Intereses devengados sobre encaje
El proveedor no entiende completamente su mercado objetivo para Servicios Financieros Digitales.	Una comprensión incorrecta del cliente conduce al desarrollo de productos y canales no adecuados para el cliente objetivo.	Cualquiera	Utilizar estudios de mercado para desarrollar las especificaciones del producto, el diseño del canal y decidir interfaces tecnológicas apropiadas. Supervisar la adopción y activación de clientes. Utilizar discusiones de grupos focales, registros de call center y retroalimentación de corresponsales para informar el diseño de Servicios Financieros Digitales. Lecciones aprendidas en otros mercados.	Clientes activos vs. clientes registrados Corresponsales activos vs. corresponsales registrados Transacciones por cliente
El proveedor no invierte completamente en los recursos necesarios para alcanzar los objetivos.	La dotación de personal y el marketing son insuficientes y el proveedor no puede cumplir con los objetivos de vinculación y activación de clientes.	Cualquiera	Asegurar que se asignen recursos desde el inicio para la dotación de personal y el marketing basado en los benchmarks de la industria y los costos locales del personal y las actividades de marketing. Comprometer los recursos durante todo el período hasta que se alcance la sostenibilidad o se revise la estrategia.	Gastos de personal reales y como % de los costos totales Gastos reales de marketing y como % de los costos totales
Des-priorización de productos o canales de Servicios Financieros Digitales	El mal desempeño conduce a la des-priorización de los Servicios Financieros Digitales y la organización se reorienta en torno a prioridades competitivas.	Cualquiera	Resolver los principales problemas dentro del departamento de Servicios Financieros Digitales (por ejemplo, riesgos tecnológicos, reputacionales u operacionales). Realizar estudios de mercado para identificar las necesidades de los clientes frente al servicio ofrecido.	Ingresos netos Clientes activos Corresponsales activos
Competencia	Los competidores están ganando cuota de mercado debido a un servicio superior o precios más bajos.	Cualquiera	Mejorar la calidad de servicio a través de corresponsales y call center. Reevaluar las estructuras de precios y comisiones. Reevaluar las características del producto.	Cuota de mercado de clientes activos Cuota de mercado de transacciones

[15] Propios de los autores, así como procedentes de:
Mobile Financial Services Risk Matrix, USAID, 2010
Fraud in Mobile Financial Services, Mudiri, MicroSave
Mobile Financial Services Technology Risks, Alliance for Financial Inclusion (AFI), 2013
Risk Management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money Operators, Lake, IFC, 2013
Digital Financial Services Risk Assessment for Microfinance Institutions: A Pocket Guide, The Digital Financial Services Working Group, 2014
Risk Management Case Studies, Fidelity Bank, Kopo Kopo, FINCA DRC and Tigo Tanzania, IFC & Genesis, 2015

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Canibalización de clientes	Sucursales y corresponsales cazando mutuamente sus clientes bancarios para satisfacer sus propios KPIs.	Banco de IMF	Desarrollar KPIs conjuntos para prevenir operaciones en silos.	Clientes atendidos a través de corresponsales vs. sucursales Servicios ofrecidos a través de corresponsales vs sucursales
La amenaza competitiva del socio	Socio compitiendo directamente con el proveedor para vincular comerciantes, corresponsales o clientes, resultando en tasas de crecimiento más lento o pérdida de clientes.	Cualquiera	MOU con socios para definir exclusividad y propiedad del cliente. Proporcionar un servicio de calidad a los clientes y corresponsales. Diversificar la dependencia del socio utilizando múltiples socios. Campañas de marketing y sensibilización. Investigación de mercados para diferenciadores adicionales e innovaciones de producto. Desarrollar estrategias de marketing conjunto.	Cuota de mercado de clientes activos Cuota de mercado de transacciones
Falta de interoperabilidad de la red impide la transacción del cliente con la parte deseada.	Redes de circuito cerrado sin capacidad para transferir fondos entre los titulares de cuentas de redes de pago de diferentes proveedores de cuentas debido a la falta de interoperabilidad.	Cualquiera	Integrar a otros proveedores y permitir a los clientes mover fondos entre las partes y realizar transacciones fuera de la red.	Volumen de transacción P2P Volúmenes totales de transacción
La interoperabilidad aumenta la rotación.	El desarrollo de sistemas interoperables con socios puede conducir a la pérdida de clientes empresariales centrales debido a que ya no necesitan ser su cliente para acceder a sus servicios.	Cualquiera, pero principalmente MNOs	Monitorear las transacciones durante la fase piloto para conocer las tendencias en el movimiento de efectivo y el comportamiento del cliente. Campañas conjuntas de marketing. Incentivos para impulsar la retención de clientes.	Cuota de mercado de clientes activos Cuota de mercado de Transacciones Actividad del cliente
Riesgo de persona clave	La dirección, fundadores o miembros de la Junta directiva salen de la organización, lo cual tiene un impacto directo en la sostenibilidad o lleva a la des-priorización de los Servicios Financieros Digitales.	Cualquiera	Implementar el enfoque en equipo, en los proyectos. Para cada cargo, tenga un sustituto en espera. Asegurar el intercambio de aprendizajes e información.	Ingresos netos Presupuestos totales vs. gastos del proyecto.
Riesgo Financiero				
El proveedor pierde fondos del cliente debido al fallo del banco fiduciario.	El banco fiduciario se vuelve insolvente, las cuentas en fideicomiso que no están legalmente segregadas del patrimonio general de activos bancarios disponible para satisfacer a los acreedores, pueden ser llevadas al proceso de bancarrota, y se bloquea el acceso a las mismas.	MNO	Identificar el banco fiduciario a través de una debida diligencia adecuada para determinar su estabilidad financiera. Los fondos fiduciarios que posean el valor de los artículos en tránsito están legalmente segregados de los activos propios del fideicomisario en quiebra. Las cuentas fiduciarias son divisibles y transferibles. Diversificación de depósitos en múltiples bancos.	Suficiencia de capital de banco fiduciario ROE y ROA del banco fiduciario

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Ajuste de activos - pasivos	Los clientes de Servicios Financieros Digitales pueden ser más propensos a hacer pequeños depósitos a corto plazo en comparación con otros clientes bancarios, lo que significa que el proveedor es tiene menos capacidad para intermediar fondos a fuentes de ingresos más rentables a largo plazo.	Bancos, IMFs	Diversificar el servicio para agregar capacidades de ahorro, así como préstamos a corto plazo. Incentivar depósitos a largo plazo a través de cuentas con intereses.	Saldo promedio en cuenta Número de transacciones de depósito y de retiro por mes por cliente
Riesgo de crédito de los clientes	Debido a la nueva estructura de distribución, los clientes pueden sentir una disminución en la obligación de pagar los préstamos debido a que ya no tienen una relación directa con el proveedor.	Bancos, IMFs	Vigilar de cerca los patrones de comportamiento del cliente. Desarrollar sistemas para alertar a los oficiales de crédito cuando los préstamos no son reembolsados a tiempo. Incentivar a los corresponsales para recaudar amortizaciones de préstamos similares a las estructuras de incentivos para los oficiales de crédito.	Cartera en Riesgo
Riesgo de crédito de corresponsales y comerciantes	No amortización de préstamos concedidos a corresponsales o comerciantes.	Cualquiera	Desarrollar políticas de riesgo crediticio, procedimientos de diligencia debida de préstamos y diversificar el riesgo de crédito. Implementar reservas para pérdidas por préstamos basadas en antigüedad de la cartera. Utilizar algoritmos para validar las aprobaciones de préstamos y monitorear el desempeño en curso del préstamo.	Cartera en Riesgo
Riesgo Cambiario	La devaluación de la moneda local aumenta los costos y devalúa los activos.	Cualquiera	Coberturas a préstamos en moneda extranjera	Tasas de Cambio
Riesgo de liquidación	El riesgo de que una parte no entregue fondos a otra parte en el momento de la liquidación	Cualquiera	Utilizar sistemas de liquidación bruta en tiempo real para transferencias bancarias. Para los MNOs, acuerdos bilaterales para controlar la liquidación.	Número transacciones en cuentas transitorias Tiempo necesario para conciliar y liquidar transacciones en cuentas transitorias
Riesgo Tecnológico				
Incumplimiento de la cuenta de cliente o corresponsal	Se viola la cuenta de cliente o corresponsal y se obtiene acceso a las credenciales de seguridad, la información de la cuenta o el historial de transacciones, lo que podría resultar en pérdida de fondos, procesamiento de transacciones ilícitas o robo de identidad. Se puede tener acceso a la información de la cuenta del cliente de manera inapropiada a través de: Historia de SMS Mala encripción de WAP Scripting entre sitios de sesiones USSD Acceso o uso no autorizado por el personal o corresponsales del proveedor	Cualquiera	Implementar controles para reducir la probabilidad de una liberación no autorizada o robo de información personal, mediante encripción, autenticación de doble factor y derechos de usuario en niveles.	Algoritmos para detectar comportamientos sospechosos Registros de escalamiento del call center

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
El cliente no puede acceder a la cuenta debido a la falta de disponibilidad del sistema y/o falla de la transacción.	El cliente no puede acceder a la cuenta a través de la aplicación o corresponsal debido a: La red móvil no está disponible El sistema del proveedor está sufriendo interrupciones temporales del sistema.	Cualquiera	El proveedor debe probar la disponibilidad de transacciones de punto a punto de forma periódica. Todas las interfaces de transacciones están definidas con límites claros de terminación, permitiendo así procedimientos claros de reversión en caso de incertidumbre. Acuerdos de nivel de servicio con proveedores y socios del sistema, y sanciones por incumplimiento Procesos acordados de escalamiento para resolver problemas. Actualizaciones del sistema. Utilizar USSD como respaldo a un POS habilitado con 3G para reducir la dependencia en la conectividad de datos	Tasa de éxito de transacciones de punto a punto
Malware	Los virus, troyanos o gusanos infectan archivos, obtienen acceso remoto, instalan software malicioso para robar datos, realizan transacciones no autorizadas o bloquean el uso autorizado.	Cualquiera	Utilizar una combinación de software antivirus, fire walls, sistemas de detección de intrusiones, servidores proxy, contenido web, filtros de adjuntos de correo electrónico y técnicas de encripción de datos. Desarrollar procedimientos para que el personal, corresponsales y clientes denuncien actividades sospechosas.	Informes de ataques exitosos en el servicio
Repetición de transacciones por la red	Los MNOs a menudo tienen solicitudes de reintento automático para entregar un SMS a un destino si no se tiene éxito en el primer intento. Cuando se utilizan en transacciones de dinero electrónico, algunos sistemas pueden interpretar esto como solicitudes de transacciones múltiples.	Cualquiera usando aplicaciones SMS	Deshabilitar peticiones de reintento. Utilizar recibos de SMS para las transacciones de los clientes con el objetivo de supervisar si hay duplicados	Informes del sistema sobre transacciones duplicadas
Retrasos de transacciones	Las demoras del sistema pueden causar retrasos en las transacciones o recibir recibos de SMS.	Cualquiera	Limitar la capacidad del sistema para reintentar las transacciones. Educar a los corresponsales y clientes para hacer revisiones de saldo si no reciben una confirmación vía SMS inmediatamente.	Quejas de transacciones duplicadas Llamadas a atención al cliente sobre SMS no recibidos
Fallos de hardware	Los dispositivos POS fallan debido a la mala construcción o incapacidad para conectarse al software	Banco, IMF o Proveedor de Servicios de Pago	Acuerdo de nivel de servicio con proveedores de hardware, incluyendo sanciones por incumplimiento. Acuerdo de mantenimiento con el proveedor de hardware.	Tasa de fallos de la transacción Tasa de fallos de POS
Pérdida de datos	Falla del almacenamiento principal y de la instalación de respaldo (incluidos los sistemas basados en la nube), lo que resulta en la pérdida de registros de transacciones.	Cualquiera	Proporcionar bases de datos espejo, separadas para documentar todas las transacciones en tiempo real. Exporte la información de transacciones al almacenamiento con regularidad.	Registros de transacciones perdidos
Fallo de entorno de hosting	El sistema no está disponible debido a problemas técnicos con el entorno de hosting de Servicios Financieros Digitales	Cualquiera	Auditoría técnica y financiera regular del entorno de hosting y del proveedor. Uso de acuerdos de nivel de servicio con el proveedor de hosting yde almacenamiento. Uso del software cloud-watch para monitorear la salud del proveedor de la nube. Procedimientos documentados para fallos de servicio y recuperación de desastres.	Disponibilidad del sistema Número de interrupciones Tiempo necesario para recuperarse de las interrupciones

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Riesgo Regulatorio				
Los clientes potenciales no tienen una Identificación (ID) u otros requisitos de KYC	Al registrarse inicialmente para una cuenta, el cliente no puede proporcionar una identificación	Cualquiera	Campañas de educación al cliente para obteneruna identificación y los requisitos de KYC, antes de la vinculación de la cuenta. Lobbying regulatorio para permitir la reducción de requisitos y/o sustitutos de la ID	Sensibilización al cliente vs. vinculación de clientes Comentarios del corresponsal sobre clientes a los que se les niega vinculación
Impuestos de transacción	Los gobiernos deciden gravar las comisiones de transacción con el fin de aumentar los ingresos que podrían afectar negativamente la demanda de los clientes.	Cualquiera	Lobby al gobierno y formadores de opinión para evitar la tributación Tasas potencialmente más bajas (es decir, pagar todo o parte del impuesto en nombre de los clientes)	Reducción aguda o inexplicable de transacciones
El corresponsal no hace KYC de clientes en forma adecuada	Los corresponsales pueden no cumplir con los requisitos de KYC, ya que las comisiones están diseñadas para incentivar la apertura de cuentas y realizar transacciones.	Cualquiera	Educación de corresponsales. Alinear incentivos únicamente a los clientes registrados correctamente. Cuando los reglamentos lo permitan, abrir cuentas de nivel uno con KYC reducido hasta que se pueda recopilar toda la información Comprador secreto. Sanciones por incumplimiento.	Porcentaje de registros de clientes rechazados por el proveedor de Servicios Financieros Digitales
Cambios en las regulaciones	El regulador cambia las leyes que ya no son favorables a las operaciones de Servicios Financieros Digitales o impiden que los proveedores obtengan licencias.	Cualquiera	Construir canales de alineación y comunicación con los reguladores.	Comunicación formal de los cambios regulatorios inminentes Quejas del regulador por incumplimiento
Falta de cumplimiento	El Proveedor no cumple con las leyes y regulaciones aplicables resultando en multas, intervención regulatoria y, en última instancia, pérdida de la licencia.	Cualquiera	El departamento de cumplimiento garantiza el cumplimiento total de las leyes regulatorias. Monitorear cualquier plan para cambiar las regulaciones aplicables y proporcionar comentarios al regulador. Asegurarse que el sistema se actualiza para cumplir con los cambios previstos en la regulación.	Informes de auditoría interna, carta de gerencia de auditoría externa Cumplimiento normativo
Riesgo Político				
Incapacidad para acceder a cuentas o realizar transacciones.	La violencia post-electoral, desórdenes civiles, guerra o actividad terrorista perturban las operaciones comerciales normales.	Cualquiera	Aplicar un plan de interrupción del servicio para los corresponsales y personal Planeación de Continuidad de Negocio Plan de comunicación.	Informar el número de horas o días sin servicio Comparar el tiempo de inactividad con los principales competidores
Riesgo de Corresponsales				
Falta de disponibilidad de corresponsales	Los clientes no pueden acceder a fondos ni realizar transacciones debido a la falta de corresponsales cercanos o los corresponsales existentes son inaccesibles debido a filas excesivas.	Cualquiera	Realizar campañas de vinculación de corresponsales en cercanías de corresponsales activos sobrecargados. Asegúrese de que la cobertura de corresponsales sea adecuada en densidad.	Number of customers Número de clientes por corresponsal. Tasas de actividad de corresponsales y de clientes

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Falta de liquidez del corresponsal	El cliente no puede realizar transacción de retiro o depósito porque el corresponsal no tiene suficiente dinero en efectivo o dinero electrónico.	Cualquiera	Uso de corresponsales y súper-corresponsales para la liquidez. Utilizar registros del call center para identificar corresponsales problemáticos y trabajar con ellos para resolver problemas de liquidez. Desarrollar corresponsales en conjunto con la vinculación de clientes con el objetivo de garantizar incentivos adecuados para gestionar las necesidades del cliente. Informes para identificar corresponsales que no cumplen con los requisitos de liquidez. Alertas manuales/automatizadas a los corresponsales cuando su encaje de dinero electrónico se está agotando. Prefinanciar los requisitos de capital de los corresponsales a través de préstamos o alianzas con instituciones de crédito. Compradores secretos y buena gestión de corresponsales.	Monitorear los saldos de dinero electrónico del corresponsal Número de quejas de clientes sobre liquidez en efectivo
Robo por parte de corresponsales	Corresponsal es robado	Cualquiera	Requerir/recomendar que los corresponsales compren seguro de robos. Educar a los corresponsales a no mantener cantidades excesivas de dinero en efectivo en los locales. Realizar comprobaciones de antecedentes de los empleados potenciales del corresponsal, o sugerir que los corresponsales lo hagan. Los corresponsales llevan a cabo conciliaciones diarias de transacciones, encaje y saldos de cuenta. Exigir la proximidad del corresponsal a la policía. Seguridad física para efectivo a través de cajas fuertes, cabinas protegidas, etc.	Hacer seguimiento y documentar el robo a corresponsales por área, hora del día, naturaleza del robo
Inactividad del corresponsal	El proveedor no identifica, entrena y administra adecuadamente a los corresponsales y/o hay clientes insuficientes para mantener a los corresponsales activos.	Cualquiera	Desarrollar corresponsales en conjunto con la vinculación de clientes. Monitorear las tasas de actividad de los corresponsales y aumentar la educación y el monitoreo de los corresponsales de bajo desempeño. Sistemas para alertar e informar la detección temprana de corresponsales inactivos. Cese de negocios con corresponsales constantemente inactivos. Revisar las estructuras de incentivos y precios para garantizar la idoneidad.	Tasa de actividad del corresponsal
Error por parte de corresponsales	Errores de captura de datos, errores de digitación, errores tipográficos, etc. hechos por el corresponsal o el personal que resultan en registros o transacciones imprecisas.	Cualquiera	Proporcionar búsqueda de número de teléfono para verificar nombre de cuenta durante el procesamiento de transacciones. Potencialmente, requerir digitar datos clave dos veces para confirmar. Entrenamiento del corresponsal ya sea propietario/operador y al personal del corresponsal. Call center de corresponsales para reversiones y consultas. Unidad de procesamiento de back-office para verificar detalles de KYC.	Tasa de reversión de transacciones Rechazo de vinculación de cuenta

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Riesgo de solvencia del corresponsal	La incapacidad de un corresponsal de pagar sus pasivos y resulta en la insolvencia y el cierre.	Cualquiera	Diligencia debida del corresponsal para seleccionar sólo corresponsales acreditados y estables. Proceso para eliminar branding y hardware de Servicios Financieros Digitales del local de un corresponsal que está fallando.	Tasas de cierre de corresponsales
Mala calidad de la experiencia del cliente en los corresponsales	El personal del corresponsal que atienda a los clientes puede no haber sido entrenado por el proveedor y tener una mala comprensión del servicio.	Cualquiera	Re-entrenamiento habitual para el corresponsal y todo el personal. Centro de llamadas para consultas del corresponsal. Compradores secretos y buena gestión de corresponsales	Tasa de actividad del cliente Quejas de clientes
Banca de corresponsales	Branding de corresponsales inconsistente debido a la eliminación por el corresponsal/ otros dotadores de material promocional o incapacidad de instalar branding debido a la presencia de otros materiales de branding.	Cualquiera	Asegúrese de que existe un acuerdo contractual con los corresponsales para tener un estándar mínimo de branding en todos los puntos de venta de corresponsales. Soporte de ventas para comprobar branding y la disponibilidad de otros materiales durante las visitas regulares. Comprador secreto.	Registros de incumplimiento por parte de los administradores de corresponsales
Caso de negocios de corresponsales	Riesgo que los corresponsales no tengan suficientes clientes o comisiones para mantener las operaciones.	Cualquiera	Incentivos de corresponsales bien estructurados. Despliegue estratégico de corresponsales con clientes y territorio adecuados. Comisión para el corresponsal por la vinculación de nuevas cuentas que impulsar la penetración a nuevos clientes. Apoyo a corresponsales, a través de oficiales de corresponsalía y call center, y capacitación.	Tasa de actividad del corresponsal
Riesgo de Fraude				
Cliente Defraudado por una parte externa				
Identidad robada	La identidad del cliente es robada y se utiliza para abrir una cuenta o para realizar transacciones fraudulentas.	Cualquiera	Considere el uso de dispositivos biométricos para reducir el fraude. Adopción de políticas y procedimientos para mejorar la detección del fraude. Utilizar los PIN y realice la educación del cliente sobre la protección del PIN. Buenas políticas de restablecimiento de PIN para impedir la actividad fraudulenta. Recogida rápida de documentación original del corresponsal o personal de apertura de cuentas. Idealmente obtener documentación electrónica que se puede transmitir al proveedor de inmediato. Verificación del carácter de los corresponsales durante el proceso de nombramiento.	Registros de incumplimiento por parte de los administradores de corresponsales

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Suplantación del proveedor o corresponsal	Un individuo se presenta como empleado o corresponsal del proveedor y acepta depósitos o logra acceso no autorizado a cuentas de clientes para llevar a cabo actividades fraudulentas.	Cualquiera	Educar a los clientes para que reciban una confirmación por SMS antes de entregar dinero en efectivo. Campañas de educación del cliente para identificar corresponsales válidos y mantener el PIN en secreto. Call centers para reclamaciones de clientes. Liberar escalamiento del cliente y el proceso de retroalimentación para reportar casos de fraude y activar la sensibilización del mercado sobre el fraude. Reconciliaciones diarias de pagos y recibos contra sistemas internos. Marca de corresponsal clara y consistente.	Registros de incumplimiento por parte de los administradores de corresponsales
Phishing	Los estafadores se presentan como representantes oficiales de corresponsales o proveedores para obtener acceso a PINs, capacidades de cuentas, registros de transacciones o saldos de cuentas de corresponsales o clientes.	Cualquiera	Minimizar la información reportada en los informes de transacciones sólo a lo que es absolutamente necesario. Solicitar a los clientes que denuncien cualquier amenaza y fraude a las autoridades policiales. Campañas de concienciación para educar a los corresponsales y clientes sobre la seguridad de las cuentas y mantener secretos el PIN, etc. Desarrollar procedimientos y directrices claros para la identificación, comunicación y gestión del fraude.	Registros de incumplimiento por parte de los administradores de corresponsales
Cambio de SIM	La tarjeta SIM de un cliente (o corresponsal) se cambia por una nueva sin autorización. El titular de la tarjeta SIM puede acceder a la cuenta del cliente y realizar transacciones sin su conocimiento.	Cualquiera que utilice Dispositivos Móviles	Documentar un proceso claro de intercambio de SIMs que limita a las personas/organizaciones que pueden realizar intercambios de SIM y establecer límites de tiempo entre el momento en que se realiza el intercambio de SIM y el momento en que se implementa. Mantener un registro de los cambios realizados a través de informes.	Registros de incumplimiento por parte de los administradores de corresponsales
Fraude de comprobates	Los comprobantes y códigos de transacción que se generan para permitir pagos a los comerciantes para bienes predefinidos o para retiros de efectivo, son robados y utilizados sin autorización.	Cualquiera	Desarrollar procesos claros que definan la generación de soportes, plazos de vencimiento y notificaciones al vencimiento. Los soportes no deben ser visibles para nadie, excepto para el destinatario y, cuando se extravía, el destinatario puede notificar al negocio y obtener los nuevos reeditados directamente. Preferentemente, en el caso de clientes no registrados, deben registrarse antes de acceder a los fondos.	Quejas de clientes
Cliente defraudado por el corresponsal				
Cuotas no autorizadas	El corresponsal puede cobrar excesivamente o cobrar una tarifa de efectivo adicional no autorizada al consumidor.	Cualquiera	Los proveedores usan contratos claros que revelan completamente todos los cargos que se cobrarán, adaptados a las diversas situaciones de los clientes, incluyendo diferentes idiomas y analfabetismo. Los cargos de servicio están claramente publicados en la ubicación de cada corresponsal. Divulgaciones razonablemente comprensibles para todos los grupos de clientes.	Quejas de clientes

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
El corresponsal recibe dinero del cliente, pero no realiza la transacción	El corresponsal recibe fondos de un usuario del servicio, pero dirige mal los fondos para beneficio propio del corresponsal.	Cualquiera	Campañas de educación al cliente para que verifiquen que la transacción se ha producido, antes de salir de las instalaciones del corresponsal. Call centers para reclamaciones de clientes. Políticas y procedimientos para el mal uso de los fondos de los clientes, incluyendo sanciones y cierre del corresponsal.	Quejas de clientes
El corresponsal paga en efectivo que resulta ser falsificado	El corresponsal puede utilizar pagos en efectivo para distribuir moneda falsa o puede pagar moneda falsa recibida de clientes sin darse cuenta de que es falsa.	Cualquiera	Exigir a los corresponsales que usen detectores de falsificación para asegurarse que no recogen fondos falsos de manera errónea. Poner las herramientas a disposición de los clientes en las tiendas de corresponsales. Campañas de educación al cliente. Políticas y procedimientos para el mal uso de los fondos de los clientes, incluyendo sanciones y cierre del corresponsal.	Quejas de clientes
Acceso no autorizado al PIN de los clientes	Los corresponsales acceden al PIN del cliente y lo utilizan para retirar fondos. Debido a la escasa alfabetización del cliente, el cliente puede compartir PIN con los corresponsales de sin problema.	Cualquiera	Desarrollar un proceso exhaustivo de debida diligencia en el proceso de contratación de corresponsales, con el fin de minimizar la contratación de corresponsales con mala reputación o aquellos que puedan cometer fraude. Llevar a cabo una sensibilización periódica y planeada del consumidor y del mercado, sobre la seguridad del PIN, para desincentivar el intercambio de PIN. Asegurarse que la documentación pertinente de la campaña también se encuentre en todos los puntos de venta. Educar al cliente en que debecambiar su PIN cuando lo recibe y mantener confidencial siempre. Formación de clientes sobre cómo realizar transacciones de forma segura.	Quejas de clientes
Retiros fraccionados	Los corresponsales obligan a los clientes a dividir los retiros en una serie de pequeñas transacciones con el fin de generar mayores comisiones porcliente y mayores comisiones por corresponsal.	Cualquiera	Utilizar las herramientas de análisis de datos para marcar transacciones sospechosas. Desarrollar un proceso exhaustivo de debida diligencia en el proceso de contratación de corresponsales con el objetivo de minimizar la contratación de corresponsales con mala reputación o aquellos que puedan cometer fraude. Llevar a cabo actividades de cliente secreto y auditorías de canales. Políticas y procedimientos para el mal uso de los fondos de los clientes, incluyendo sanciones y cierre del corresponsal.	Transacciones duplicadas Quejas de clientes
Cliente defraudado por el personal interno del proveedor				
Los empleados vinculan números móviles erróneos a las cuentas bancarias	Complicidad entre los empleados y los estafadores para vincular los números móviles de los estafadores a las cuentas de los clientes, facilitando el retiro de fondos de las cuentas.	Cualquiera	Mantener cuentas separadas de recibos y desembolsos para limitar la exposición de los clientes al fraude. Para las cuentas vinculadas a carteras, asegúrese que los clientes firmen la autorización para la vinculación de la cuenta. Utilizar confirmació vía de SMS para notificar a los clientes de la vinculación. Auditoría bancaria de cuentas vinculadas.	Quejas de clientes

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Reversión ilegal de pagos / transferencias de clientes	Empleados confabulan con la parte que paga y revierten los pagos de los clientes de manera ilegal.	Cualquiera	Utilizar confirmación vía SMS para notificar a los clientes de las transacciones. Asegurar procedimientos de separación de funciones para toda reversión. Crear informes para supervisar el comportamiento sospechoso del cliente y del personal.	Informes de actividad sospechosos Quejas de clientes
Transferencias ilegales desde cuentas móviles	Transferencias ilegales por parte de empleados, desde cuentas de clientes a cuentas falsas o cuentas de estafadores	Cualquiera	Utilizar confirmación vía SMS para notificar a los clientes sobre las transacciones Asegurar procedimientos de separación de funciones para toda reversión. Crear informes para supervisar el comportamiento sospechoso del cliente y del personal.	Informes de actividad sospechosos Quejas de clientes
Corresponsal defraudado por el cliente				
Corresponsal recibe efectivo que resulta falso	El falsificador fabrica billetes falsos, los deposita en una cuenta a través de un corresponsal, y luego retira moneda válida de otro corresponsal.	Cualquiera	Los corresponsales utilizan herramientas de detección de falsificaciones. Educación de corresponsales. Call center para corresponsal. Compradores secretos y buena gestión de corresponsales.	Quejas del corresponsal
Acceso no autorizado al dispositivo del corresponsal.	Los clientes tienen acceso a las herramientas de transacción del corresponsal para realizar transacciones fraudulentas.	Cualquiera	Exigir a los corresponsales que mantengan un teléfono comercial y una tarjeta SIM independientessi utilizan teléfonos móviles, y emplear buenas prácticas de administración de teléfonos. Restringir las tarjetas SIM de los dispositivos sólo para realizar actividades relacionadas con Servicios Financieros Digitales. Límite de llamadas al dispositivo transaccional que se originen desde unos pocos números preautorizados por el proveedor. El corresponsal llama al Call para informar sobre el fraude. Utilizar autenticación de doble factor, para habilitar las transacciones en línea, Cada persona del corresponsal debe tener acceso y contraseña únicos. Si los empleados son despedidos, se deben inhabilitar sus contraseñas.	Quejas del corresponsal
Solicitudes de reversión de una transacción válida por parte del cliente.	El cliente solicita un retiro. Luego el cliente niega el recibo y solicita al proveedor que reverse la transacción.	Cualquiera	Un proceso claro para gestionar el rechazo y asegurar que se cuiden los intereses de todas las partes implicadas. La transacción puede ser revertida, negada o puesta en espera hasta que se complete una investigación. Educar al corresponsal para que informe sobre comportamientos sospechosos del cliente.	Niveles altos de receptor que se niegan a permitir reversiones
Corresponsal defraudado por el personal interno				
Empleado del proveedor defrauda al corresponsal	Un empleado del proveedor utiliza el acceso no autorizado a las cuentas del corresponsal, con el fin de manipular saldos o realizar transacciones en su propio beneficio.	Cualquiera	Llevar a cabo verificaciones de antecedentes de los empleados potenciales del proveedor. Limitar el acceso del personal a las cuentas del corresponsal. Utiliar recibos de SMS para transacciones de corresponsal. Entrenar a los corresponsales en mantener secretos los detalles de PIN / login.	Quejas del corresponsal

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Fraude de comisión instantánea	Para los modelos que pagan comisión inmediata, los dueños del negocio encuentran difícil reconciliar comisiones ganadas porque se confunden con otras transacciones. Los empleados aprovechan esta mezcla para defraudar a sus empleadores.	Cualquiera	Proporcionar información digital para facilitar la conciliación de transacciones, efectivo y fondo de dinero electrónico. Incorporar pagos de comisiones a corresponsales después de un período de tiempo programado, preferiblemente mensual. Debe generarse un informe periódicamente, especificando la comisión ganada, el modo de pago y cualquier número de referencia para el pago.	Quejas del corresponsal
Funcionario del corresponsal defrauda a los corresponsales	Los corresponsales dan sus PINs al personal del proveedor, dándoles acceso completo a la cuenta del corresponsal.	Cualquiera	Educar a los corresponsales para que mantengan el PIN confidencial. Para acceder a los fondos en el dispositivo el funcionario del corresponsal solo tiene derechos según el rol y no derechos de inicio de sesión.	Quejas del corresponsal
Corresponsal defraudado por el corresponsal maestro				
Retiro no autorizado de fondos o comisiones del corresponsal	Los corresponsales maestros llevan a cabo retiros no autorizados del fondo de las cuentas del corresponsal o deducen la comisión.	Cualquiera	Contratos y directrices detallados para el funcionamiento de los corresponsales maestros en relación con las obligaciones, dotación de personal y requisitos para la vinculación de corresponsales. Aplicar directrices sobre el reparto de comisiones entre los corresponsales maestros y los corresponsales. Proporcionar a los corresponsales foros de retroalimentación adecuados, incluyendo líneas telefónicas, direcciones de correo electrónico y foros para recibir comentarios. Declaraciones detalladas de la comisión del corresponsal para la conciliación del corresponsal	Quejas del corresponsal
Proveedor defraudado por el cliente				
Desembolsos erróneos	Los clientes reciben depósitos de fondos erróneos, retiran fondos, y cierran cuentas antes que los fondos puedan ser congelados y devueltos.	Cualquiera	Las organizaciones deben desarrollar un proceso claro para el desembolso de fondos con el fin de minimizar los errores. Proceso integral que cubre la identificación, el monitoreo, la comunicación y la gestión del fraude. Conciliaciones diarias de pagos y recibos, contra sistemas internos.	Quejas de clientes
Provider defrauded by agent				
Depósitos divididos	Los corresponsales dividen los depósitos en una serie de pequeñas transacciones con el fin de generar mayores comisiones a costa del proveedor.	Cualquiera	Utilizar las herramientas de análisis de datos para marcar transacciones sospechosas. Desarrollar un proceso exhaustivo de debida diligencia para la contratación de corresponsales con el fin de minimizar la contratación de corresponsales con mala reputación o aquellos que puedan cometer fraude. Llevar a cabo las actividades de comprador secreto y buenas prácticas gestión de corresponsales. Educación de los corresponsales. Call center para que los clientes denuncien actividades sospechosas. Aplicación de sanciones por mala gestión de corresponsales y cierre de corresponsales.	Informes de transacciones sospechosas

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Depósitos directos	Los corresponsales depositan fondos directamente en la cuenta de un destinatario, en lugar de hacerlo a la cuenta del cliente para que haga una transacción P2P, con el fin de evitar los gastos de transacción.	Cualquiera	Llevar a cabo campañas de educación al consumidor para generar concientización sobre estos tipos de fraude. Analizar y revisar regularmente las estructuras de comisiones de los corresponsales para detectar cualquier anomalía y abordarlas. Comprador secreto para detectar incidencias de la voluntad del corresponsal de cometer fraude. Utilizar los datos de la red GSM para identificar la ubicación del cliente y del corresponsal con el objetivo de asegurarse que la transacción se está llevando a cabo en la misma ubicación.	Informes de transacciones sospechosas
Vinculación de cuentas falsas	Los corresponsales registran cuentas falsas o clientes sin la documentación completa de KYC, para ganar comisión.	Cualquiera	Comisión de vinculación del cliente que se reparte entre la vinculación y la primera transacción. Los departamentos de procesamiento y cumplimiento verifican KYC. La comisión pagada únicamente sobre cuentas con KYC completo.	Tasas de rechazo de vinculación de cuentas
Proveedor defraudado por una parte externa				
Hacking	Una parte externa invade el sistema para obtener acceso a las cuentas del proveedor para realizar transacciones fraudulentas o para robar datos.	Cualquiera	Fire walls, encripción, derechos de acceso basados en roles, etc. Conciliación diaria de la cuenta.	IResultados de auditoría de TI
Proveedor defraudado por personal interno				
Cuentas fantasma	Un empleado utiliza el acceso no autorizado para crear cuentas falsas con depósitos falsos. La complicidad con los estafadores les permite retirar fondos del corresponsal.	Cualquiera	Conciliación diaria de la cuenta. Personal de investigación y capacitación. Políticas y procedimientos adecuados para investigar actividades sospechosas.	Auditoría interna Resultados de auditoría de TI
Riesgo Operacional				
Variaciones en la conciliación y cuentas	Riesgo de que el valor real en cuentas en el fideicomiso sea diferente a la cantidad reflejada en el sistema. Riesgo de que las transacciones fuera de la red (por ejemplo, retiro de cajeros automáticos, pago de facturas) no se concilien con las cuentas internas.	Cualquiera	Para MNOs: integrar el sistema en las cuentas bancarias para que todos los cambios en la cuenta principal se reflejen automáticamente. Use cuentas separadas para los ingresos de la empresa y el desembolso de la comisión. Informes de varianza de fin de día gestionados y firmados por administrador empresarial adecuado. Función robusta de autoridad de aprobador y verificador del sistema. Conciliación diaria en proveedor y corresponsal. Políticas internas y procedimientos sólidos para la conciliación de transacciones en cuentas de orden.	% de transacciones en cuentas transitorias % de variación al final del día
El cliente es incapaz de disputar una transacción o cargo en cuenta.	Los clientes no pueden resolver conflictos con un proveedor de cuentas y el recurso ante organismos gubernamentales o autoridades regulatorias para dirimir disputas es débil o inexistente.	Cualquiera	Procesos eficientes de solución de controversias. Los call center cuentan con personal y capacitación adecuados con políticas de escalamiento claras para la resolución de conflictos. Normas de servicio claras y publicadas	Tasas de solución de call center

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Tarjeta SIM o teléfono móvil perdidos	El cliente no puede realizar transacciones debido a la pérdida de tarjeta de débito o tarjeta SIM.	Cualquiera	Políticas de sustitución de tarjetas. Call center para informes y resolución de problemas. Formación de corresponsales para proporcionar un servicio al cliente de primer nivel.	Tasas de sustitución de tarjetas Tasa de restablecimiento del PIN
Falta de manuales operativos y procesos de negocio	Los manuales de operación están incompletos, carecen de los procesos de excepción y no se actualizan regularmente, lo que resulta en que se sigan procedimientos inadecuados de operación	Cualquiera	Revisar el manual de operación en relación con la lista de procedimientos que se están llevando a cabo. Agregar cualquier procedimiento que falte, actualizando los procedimientos existentes según sea necesario y agregando los casos de uso de excepciones a todos. Asegúrese que los departamentos pertinentes firmen cada proceso Crear listas de verificación de procesos y asegurar que todos los procesos han sido documentados y actualizados si es necesario, y circulados al personal relevante.	Auditoría interna Revisiones de Riesgo y Cumplimiento Tiempo tomado para resolver disputas
Falta de auditorías operativas	Los procedimientos operativos actuales no están optimizados con respecto a la conciliación y procesamiento de ingresos.	Cualquiera	Es necesario realizar auditorías de riesgos para identificar problemas y garantizar la eficiencia e integridad operativas.	Auditoría interna Revisiones de Riesgo y Cumplimiento
Reestablecimiento de PINs	Los procedimientos de restablecimiento de PINs prolongados o complicados producen una mala experiencia del cliente	Cualquiera	Políticas eficaces para los procedimientos de restablecimiento de PIN	Tiempo tomado para resolver restablecimientos de PINs
Débito sin desembolso (DWD)	Cuando un cajero automático debita una cuenta de un cliente, pero no dispensa el efectivo correspondiente causando retrasos en el reembolso al cliente.	Cualquiera usando tarjetas habilitadas para cajeros automáticos	Profundizar en las relaciones con los sistemas de liquidación interbancaria para las transacciones fuera de la red. Mejorar los procedimientos operativos para las resoluciones. Aumentar los recursos humanos dedicados a la resolución de disputas. Actualizar cajeros automáticos.	Número de incidentes
Falta de controles internos, informes internos y monitoreo de datos	No hay procedimientos para supervisar la actividad del corresponsal, empleado o cliente. Incumplimiento potencial a los requisitos reglamentarios.	Cualquiera	Implementar controles internos para monitorear la actividad transaccional y de la entidad, a través de reportes internos y monitoreo de datos.	Auditoría interna Revisiones de Riesgo y Cumplimiento
Procesos de conciliación	Falta de procedimientos eficaces de conciliación que crean atrasos	Cualquiera	Tener procesos de conciliación eficientes claramente definidos que sean idealmente automatizados.	% de montos no conciliados Tiempo de conciliación
Errores de entrada de datos	Errores de entrada de datos, errores tipográficos, errores de digitación realizados por el personal del proveedor de back office.	Cualquiera	Utilizar separación de funciones para realizar tareas. Separación de funciones	Controles de conciliación Auditoría interna

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Riesgo de alianzas				
Dificultades de relación entre los propietarios del servicio - que conducen a la interrupción del servicio (por ejemplo, en colaboraciones entre IFs, MNOs, proveedores y/o otros proveedores de servicios)	Problemas graves de relaciones dentro del consorcio de proveedores, resulta en, falta de disponibilidad del servicio para los clientes.	Cualquiera	Memorando de Entendimiento detallado con roles, responsabilidades y propuesta de valor claramente definidos para cada parte en la alianza. Acuerdos contractuales claros para la continuidad del servicio durante las disputas.	Resultados de la auditoría interna Resultados de la auditoría de TI
Falta de fiabilidad de los socios	Los socios no cumplen con las expectativas y los resultados de los acuerdos.	Cualquiera	Llevar a cabo la debida diligencia en los socios. Utilizar contratos de garantía de rendimiento cuando el pago se efectúa al firmarse. Aplicar sanciones de no conformidad.	Resultados de la auditoría interna
Los sistemas de socios están inactivos	El tiempo de inactividad de los sistemas de aliados interrumpe el servicio.	Cualquiera	Informar a los corresponsales / clientes a través de SMS cuando haya tiempos de inactividad del sistema, según corresponda. Aprovechar las líneas de atención al cliente. Utilizar acuerdos de nivel de servicio (SLA) para que los socios garanticen el tiempo de actividad del servicio y apliquen multas por incumplimiento. Desarrollar socios de respaldo para repartir el riesgo.	Resultados de auditoría de TI
Riesgo Reputacional				
Fraude	El fraude generalizado disuade la confianza del cliente y crea riesgo de reputación para el proveedor y el mercado como un todo.	Cualquiera	Limitar la exposición al fraude. Estrategia de comunicación proactiva y prudente para gestionar la exposición al fraude.	Pérdidas por fraude
Fallos en las transacciones	Los fallos de las transacciones afectan la confianza en la organización y reducen la actividad y la retención del cliente.	Cualquiera	Mejorar la tecnología y el rendimiento. Imponer SLAs con proveedores y socios. Campañas de educación y marketing del cliente.	Fallos en las transacciones
Conectividad MNO	Los corresponsales ubicados en áreas de baja conectividad interrumpen el acceso de los clientes a los servicios, dejando a los clientes frustrados y reduciendo la confianza en el proveedor.	Banco, IMF y Proveedor de Servicios de Pago	Desarrollar mejores relaciones con los MNO para mejorar la calidad del servicio. Utilizar dispositivos SIM duales con los dos MNOs más fuertes en cada área en particular.	Volumen de transacciones en geografías específicas
Mala experiencia del cliente	Mala atención al cliente, resolución inoportuna de incidentes, incapacidad de contactar al proveedor.	Cualquiera	Proceso de resolución de incidentes y matriz de escalamiento establecida. Servicio de atención al cliente con recursos suficientes	Hora para contestar llamadas % de llamadas no contestadas Tasa de resolución de llamadas
Riesgo de marca debido a las alianzas	Los socios no agregan valor a la marca del proveedor, e incluso pueden perjudicar a la marca por mala reputación o calidad de servicio.	Cualquiera	Comunicación con el cliente y campaña publicitaria para desarrollar marca. Desarrollar múltiples alianzas para reducir el impacto de una relación en particular.	Informes de prensa sobre marcas de socios

Glosario

TÉRMINO	DEFINICIÓN
Interfaz de Programación de Aplicaciones (API, por sus siglas en inglés)	Un método para especificar un componente de software en términos de sus operaciones destacando un conjunto de funcionalidades que son independientes de su respectiva implementación. Las API se utilizan para la integración en tiempo real al Sistema de Core Bancario /MIS, que especifican cómo dos sistemas diferentes pueden comunicarse entre sí a través del intercambio de 'mensajes'. Existen varios tipos diferentes de API, incluidas las basadas en la Web, la comunicación TCP e integración directa en una base de datos, o APIs propietarias escritas para sistemas específicos.
Banca de corresponsales	Servicios bancarios, a menudo limitados, realizados por un corresponsal.
Banca electrónica	El suministro de productos y servicios bancarios a través de canales de distribución electrónicos.
Banca móvil	El uso de un teléfono móvil para acceder a los servicios bancarios convencionales. Esto abarca tanto los servicios transaccionales, como los no transaccionalescomo la visualización de información financiera y la ejecución de transacciones financieras.
Billeteras electrónicas	Una cuenta de dinero electrónico que pertenece a un cliente de Servicios Financieros Digitales y a la que se accede a través de un teléfono móvil.
Cajero Automático (ATM)	Un dispositivo electrónico de telecomunicaciones que permite a los clientes de una institución financiera, realizar transacciones financieras sin la necesidad de un cajero humano, auxiliar o cajero de banco. Los cajeros automáticos identifican a los clientes a través de una tarjeta magnética o basada en un chip, y la autenticación ocurre después que el cliente ingresa un número PIN. La mayoría de los cajeros automáticos están conectados a redes interbancarias para permitir a los clientes acceder a máquinas que no pertenecen directamente a su banco, aunque también existen algunos sistemas de circuito cerrado. Los cajeros automáticos están conectados a un host o controlador ATM usando un módem, una línea arrendada o ADSL.
Call center	Una oficina centralizada utilizada para recibir o transmitir un gran volumen de solicitudes telefónicas. En este contexto, además de manejar las quejas y consultas de los clientes, también se utiliza como un canal de distribución alternativo para mejorar el alcance y atraer nuevos clientes a través de varias campañas promocionales.
Canal	El punto de acceso del cliente a un Proveedor de Servicios Financieros, es decir, con quien o que interactúa el cliente para acceder a un servicio financiero o producto.
Canales de Distribución Alternativos (CDAs)	Canales que amplían el alcance de los servicios financieros más allá de la rama tradicional. Estos incluyen cajeros automáticos, banca por Internet, banca móvil, billeteras electrónicas, algunos servicios de tarjeta/dispositivo POS y servicios de conseción de crédito.
Comerciante	Una persona o negocio que proporciona bienes o servicios a un cliente a cambio de pago.
Conozca a su Cliente [Know Your Customer] (KYC)	Reglas relacionadas con la ALA/CFT que obligan a los proveedores a llevar a cabo procedimientos para identificar a un cliente y que evalúan el valor de la información para detectar, supervisar y reportar actividades sospechosas.
Corresponsal	Una persona o negocio contratado para procesar las transacciones de los usuarios. Los más importantes son depósitos y retiros (es decir, el cargue de valor efectivo en el sistema de dinero electrónico, y luego convertirlo de nuevo); en muchos casos, los corresponsales registran nuevos clientes también. Los corresponsales suelen ganar comisiones por realizar estos servicios. También suelen ofrecer un servicio de atención al cliente de primera línea, como enseñar a los nuevos usuarios a realizar transacciones desde su teléfono. Por lo general, los corresponsales llevarán a cabo otro tipo de negocios, además del de dinero electrónico. Los corresponsales a veces estarán limitados por la regulación, pero los comerciantes a pequeña escala, las instituciones de microfinanzas, las cadenas de tiendas y las sucursales bancarias sirven como corresponsales en algunos mercados. Algunos participantes de la industria prefieren los términos 'comerciante' o 'minorista' para evitar ciertas connotaciones legales del término 'corresponsal', ya que se utiliza en otras industrias. (GSMA, 2014)
Corresponsal Maestro	Una persona o negocio que compra dinero electrónico de un proveedor de Servicios Financieros Digitales al por mayor y luego lo revende a corresponsales, quienes a su vez lo venden a los usuarios. (A diferencia de un súper-corresponsal, los corresponsales maestros son responsables de gestionar los requisitos de liquidez en efectivo y de valor electrónico de un determinado grupo de corresponsales.)

Dinero electrónico	El dinero electrónicoes el valor almacenado en billeteras virtuales o tarjetas. Por lo general, el valor total del dinero electrónico emitido es igualado por los fondos mantenidos en una o más cuentas bancarias y normalmente se mantienen en fideicomiso, de modo que incluso si el proveedor del servicio de billeteras móviles electrónicas fallara, los usuarios podrían recuperar el valor total almacenado en sus cuentas.
Evaluación de Riesgo	El proceso de identificación, evaluación y desarrollo de estrategia de mitigación de riesgos.
Gestión de Riesgo Empresarial (ERM)	El proceso de planificación, organización, dirección y control de las actividades de una organización con el fin de minimizar los efectos del riesgo sobre el capital y las ganancias de una organización.
Indicador Clave de Riesgo (KRI)	Un Indicador Clave de Riesgo es una medida usada para indicar el grado de riesgo de una actividad. Se diferencia de un Indicador Clave de Desempeño (KPI) en que este último se entiende como una medida de lo bien que se está haciendo algo, mientras que el primero indica lo perjudicial que puede ser algo si se produce y lo probable que es que ocurra.
Institución Financiera (IF)	Un proveedor de servicios financieros, incluyendo cooperativas de ahorro y crédito, bancos, instituciones financieras no bancarias, instituciones de microfinanzas y proveedores de servicios financieros móviles.
Instituciones Microfinancieras (IMF)	Una institución financiera especializada en servicios bancarios para grupos de bajos ingresos, pequeñas empresas o individuos.
ISO 31000	Directrices ISO establecidas para la implementación de la Gestión de Riesgo Empresarial (ERM).
Lucha contra el Lavado de Activos/Lucha contra el Financiamiento del Terrorismo (ALA/CFT)	ALA/CFT son controles legales aplicados al sector financiero para ayudar a prevenir, detectar y reportar actividades de lavado de dinero. Los controles ALA/CFT incluyen montos máximos que pueden ser retenidos en una cuenta o transferidos entre cuentas en cualquier transacción, o en cualquier día dado. También incluye la información financiera obligatoria de KYC para todas las transacciones de más de $10,000, incluyendo la declaración de la fuente de los fondos, así como la razón de la transferencia.
Marco de Gestión de Riesgo	Un conjunto integral de políticas que apuntan a reducir el Impacto de los riesgos asociados a Servicios Financieros Digitales. El marco es la culminación de todos los procesos de planeación y evaluación e incluye el registro de riesgo como su pieza y documento de trabajo principal.
Operador de Red Móvil (MNO)	Una empresa que tiene una licencia expedida por el gobierno para proporcionar servicios de telecomunicaciones a través de dispositivos móviles.
Punto de Venta (POS)	Dispositivo electrónico utilizado para procesar pagos con tarjeta en el punto en el que un cliente hace un pago al comerciante a cambio de bienes y servicios. El dispositivo POS es un dispositivo de hardware (fijo o móvil) que ejecuta software para facilitar la transacción. Originalmente eran dispositivos o PC, pero cada vez más incluyen teléfonos móviles, teléfonos inteligentes y tabletas.
Registro de riesgos (Matriz de Riesgo)	La base de datos central de los riesgos identificados, junto con sus descripciones, causas, efectos y políticas, ya sea para tolerar, tratar, transferir o terminar.
Servicio de dinero electrónico/servicio financiero móvil (MFS)	Un Servicio Financiero Digital que se suministra mediante la emisión de cuentas virtuales contra una sola cuenta bancaria agrupada, como billeteras electrónicas a las que se accede mediante un teléfono móvil. La mayoría de los proveedores de dinero electrónico son MNO o Proveedores de Servicios de Pago.
Servicio de Mensajes Cortos (SMS)	Un canal de comunicación que 'almacena y reenvía', que implica el uso de la red de telecomunicaciones y el protocolo SMPP para enviar una cantidad limitada de texto de un teléfono a otro o de uno a muchos teléfonos.
Servicio Suplementario de Datos no Estructurados (USSD)	Protocolo utilizado por los dispositivos móviles GSM para comunicarse con los computadores/red del proveedor de servicios. Este canal está soportado por todos los teléfonos GSM, permitiendo una sesión interactiva consistente en un intercambio de mensajes en dos direcciones basado en un menú de aplicación definido.
Servicios Financieros Digitales (SFD)	El uso de medios digitales para ofrecer servicios financieros. Incluye todas las ofertas de móviles, tarjetas, POS y comercio electrónico entregadas a los clientes a través de redes de corresponsales.
Súper-Corresponsal	Un negocio, a veces un banco, que compra dinero electrónico de un proveedor de Servicios Financieros Digitales al por mayor y luego lo revende a los corresponsales, que a su vez lo venden a los usuarios.
Teléfono inteligente	Un teléfono móvil que tiene la capacidad de procesamiento para realizar muchas de las funciones de un computador, que normalmente tiene una pantalla relativamente grande y un sistema operativo capaz de ejecutar un conjunto de aplicaciones complejo, con acceso a Internet. Además del servicio de voz digital, los teléfonos inteligentes modernos ofrecen mensajes de texto, correo electrónico, navegación por Internet, cámara fija y de vídeo, un reproductor de MP3 y reproducción de vídeo con capacidades de transferencia de datos / GPS integradas.

Referencias

1. Risk Management Toolkit, GSMA & Consult Hyperion, 2015 (https://www.gsma.com/mobilefordevelopment/programme/mobile-money/managing-risk-in-mobile-money-a-new-comprehensive-risk-toolkit)

2. MMU Managing the Risk of Fraud in Mobile Money, GSMA, 2012 (http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobile-money.pdf)

3. Mobile Financial Services Risk Matrix, USAID and Booz Allen Hamilton, 2010 (http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilefinancialservicesriskmatrix100723.pdf)

4. Bank Agents: Risk Management, Mitigation, and Supervision, CGAP, 2011 (http://www.cgap.org/publications/bank-agents-risk-management-mitigation-and-supervision)

5. Digital Financial Services Risk Assessment For Microfinance Institutions, A Pocket Guide, AFI, 2014 (https://lextonblog.files.wordpress.com/2014/09/dfs_risk_guide_sept_2014_final.pdf)

6. Mobile Financial Services Technology Risks, AFI, 2013 (http://www.afi-global.org/sites/default/files/pdfimages/AFI_MFSWG_guidelinenote_TechRisks.pdf)

7. Fraud in Mobile Financial Services, Mudiri, Microsave, 2012 (http://www.microsave.net/resource/fraud_in_mobile_financial_services#.VmWI9E10xes)

8. Risk Management in Mobile Money, Lake, IFC, 2013 (http://www.ifc.org/wps/wcm/connect/37a086804236698d8220ae0dc33b630b/Tool+7.1.+Risk+Management.pdf?MOD=AJPERES)

9. Enterprise Risk Management (ERM) and the requirements of ISO 31000, AIRMIC, Alarm, IRM, 2010 (https://www.theirm.org/media/886062/ISO3100_doc.pdf)

Lesley Denyes

Lesley es Especialista en Servicios Financieros Digitales del IFC. Ha trabajado en el sector más de quince años, específicamente en las áreas de modelamiento de negocios, análisis financiero, banca móvil, planificación estratégica, desarrollo de productos y gestión del canales en Asia y África Subsahariana. Lesley ha trabajado con bancos comerciales, operadores de redes móviles, proveedores de servicios de pago, instituciones de investigación, desarrolladores de apps móviles, ONGs, y compañías de consultoría para llegar a hogares de bajos ingresos por medio de la tecnología y la Banca sin sucursales. Lesley tiene sede en Toronto, Canadá, y posee un BSc en Economía Cuantitativa de la Universidad Dalhousie, Canadá, y un MBA del Edinburgh Business School, del Reino Unido.

Susie Lonie

Susie pasó tres años en Kenia creando y operando el servicio de pagos móviles M-PESA, después de lo cual facilitó su lanzamiento en varios otros mercados incluyendo Tanzania, Suráfrica e India. En 2010, Susie fue co-ganadora del Economic Innovation Award for Social and Economic Innovation por su trabajo en M-PESA. Se convirtió en consultora independiente en Servicios Financieros Digitales en 2011 y trabaja con bancos, MNOs, y otros clientes en todos los aspectos del suministro de servicios financieros a los desbancarizados en mercados emergentes, incluyendo dinero electrónico, banca de corresponsales, transferencias internacionales de dinero, e interoperabilidad. Susie trabaja en estrategia de Servicios Financieros Digitales, evaluación financiera, diseño de productos y requerimientos funcionales, operaciones, gestión de corresponsales, evaluaciones de riesgo, evaluaciones de investigación, y ventas y marketing. Sus títulos son en Ingeniería Química de Edinburgo y Manchester, Reino Unido.

The Partnership for Financial Inclusion

The Partnership for Financial Inclusion es una iniciativa conjunta de $ 37.4 millones de la IFC y Mastercard Foundation para expandir las microfinanzas y avanzar los servicios financieros móviles en el África subsahariana. La Asociación también recibe el apoyo de la Fundación Bill & Melinda Gates y del Banco de Desarrollo de Austria (OeEB, Oesterreichische Entwicklungsbank.AG). Trabaja con instituciones microfinancieras, bancos, operadores de redes móviles y proveedores de servicios de pago en todo el continente para probar modelos de negocios innovadores para la inclusión financiera. El programa tiene un componente fuerte de intercambio de información. Este manual es el segundo en una serie de manuales acerca de cómo hacer una implementación exitosa de servicios financieros digitales, es una de muchas publicaciones de la Alianza. Para mayor información y acceso a todos los informes, por favor visite www.ifc.org/financialinclusionafrica

Acerca de IFC

La IFC, miembro del Grupo del Banco Mundial, es la institución global de desarrollo más grande y centrada exclusivamente en el sector privado. Trabajando con más de 2.000 negocios mundialmente, utilizamos nuestro capital, conocimiento experto, e influencia, para generar oportunidades donde más se necesitan. En el año fiscal 2015, nuestras inversiones a largo plazo en países en desarrollo subieron a casi $18 billones, ayudando al sector privado a jugar un papel esencial en el esfuerzo global de acabar con la pobreza extrema e impulsar la prosperidad compartida. Para mayor información, visite www.ifc.org

Acerca de Mastercard Foundation

Mastercard Foundation trabaja con organizaciones visionarias para proveer mayor acceso a la educación, capacitación técnica y servicios financieros para las personas que vivien en pobreza, primordialmente en África. Como una de las fundaciones independientes más grandes, su trabajo es guiado por su misión de avanzar el conocimiento y promover la inclusión financiera para aliviar la pobreza. Con sede en Toronto, Canadá, su independencia fue establecida por MasterCard cuando se creó la Fundación en 2006. Para mayor información y para registrarse para el boletín de la Fundación, por favor visite www.mastercardfdn.org.

Este manual es uno de los tres manuales sobre Servicios Financieros Digitales publicados por The Partnership for Financial Inclusion, una iniciativa conjunta de la IFC y Mastercard Foundation para fomentar la expansión de la inclusión financiera. Los otros dos manuales están disponibles a solicitud desde IFC o para descargar desde el sitio web de la Alianza: www.ifc.org/financialinclusionafrica:

El **Manual de Canales de Distribución Alternativos y Tecnología** ofrece una guía práctica, paso a paso, para desarrollar canales de distribución alternativos que vinculan opciones de tecnología con el proceso general del negocio.

El **Manual de Análisis de Datos y Servicios Financieros Digitales** ofrece a los proveedores de servicios financieros, una perspectiva general del potencial que los datos y el análisis de datos representan para la inclusión financiera en cuanto a la mejora de la eficiencia a nivel operativo y la eficacia en el desarrollo de producto y marketing; al mismo tiempo que aumenta el alcance a través de métodos innovadores basados en datos.

DETALLES DE CONTACTO

Anna Koblanck

IFC, África Subsahariana

akoblanck@ifc.org

www.ifc.org/financialinclusionafrica

2016

mastercard foundation

IFC International Finance Corporation WORLD BANK GROUP