Tecnologías Emergentes
Informe Oficial de ISACA
sobre tecnologías emergentes
Noviembre de 2011

ISACA®
Trust in, and value from, information systems

Pagos mediante dispositivos móviles: cuestiones relacionadas con los riesgos, la seguridad y el aseguramiento

Resumen
Los pagos mediante dispositivos móviles como medio para efectuar transacciones financieras surgieron hace diez años, aproximadamente. La adopción de este medio fue lenta debido a la naturaleza de la tecnología móvil que soporta este concepto. Sin embargo, los importantes adelantos producidos recientemente en el plano tecnológico han convertido esta área en una de las de mayor crecimiento dentro del sector de los servicios financieros. Los medios de pago basados en servicios y mensajes de texto, así como las comunicaciones mediante dispositivos de proximidad, están surgiendo en todo el mundo. El uso generalizado de teléfonos inteligentes y la comodidad que los dispositivos móviles ofrecen al consumidor, a través de prestaciones que exceden la mera comunicación, son los principales factores que impulsan un renovado y creciente interés en la realización de pagos mediante este tipo de dispositivos. Además, los adelantos en las técnicas de seguridad de software y hardware han posibilitado la realización de transacciones financieras confiables a través de estos dispositivos. Este Informe Oficial examina el estado actual y la naturaleza del mercado de pagos mediante dispositivos móviles, así como algunas de las tecnologías relevantes que lo permiten, y analiza las cuestiones pertinentes en materia de riesgos, seguridad y aseguramiento que los profesionales de seguridad y auditoría deberían tener en cuenta al desarrollar y evaluar los servicios de pago mediante dispositivo móvil.

ISACA®

Con 95.000 miembros en 160 países, ISACA (*www.isaca.org*) es un proveedor líder global de conocimiento, certificaciones, comunidad profesional, promoción y educación en materia de aseguramiento y seguridad de los sistemas de información (IS), gobierno corporativo y gestión de TI, riesgos relacionados con las TI y cumplimiento de las normas. Fundada en 1969, ISACA, una organización independiente sin ánimo de lucro, auspicia conferencias internacionales, publica *ISACA® Journal* y desarrolla normas internacionales de control y auditoría para los sistemas de información, lo que ayuda a sus miembros a asegurar el valor y la confianza en los sistemas de información. También desarrolla y certifica destrezas y conocimientos en TI a través de la internacionalmente reconocida Certified Information Systems Auditor® (Auditor Certificado en Sistemas de Información) (CISA®), Certified Information Security Manager® (Administrador Certificado en Seguridad de la Información) (CISM®), Certified in the Governance of Enterprise IT® (Certificado en el Gobierno de Tecnologías de la Información Corporativa) (CGEIT®) y Certified in Risk and Information Systems Control™ (Certificado en Riesgo y Control de Sistemas de Información) (CRISC™). ISACA actualiza continuamente COBIT®, lo que ayuda a los profesionales y líderes empresariales a cumplir con sus responsabilidades de gestión y gobierno de las TI, particularmente en las áreas de aseguramiento, seguridad, riesgo y control, y así aportar valor al negocio.

Cláusula de exención de responsabilidad

ISACA ha diseñado y creado *Pagos mediante dispositivos móviles: cuestiones relacionadas con los riesgos, la seguridad y el aseguramiento* ("La Obra", en adelante), principalmente como un recurso educativo para los profesionales de gobierno, seguridad y aseguramiento. ISACA no garantiza que el uso de cualquier componente de "La Obra" asegure un resultado exitoso. "La Obra" no debería ser considerada como incluyente de toda la información, procedimientos y pruebas apropiadas ni tampoco como excluyente de otra información, procedimientos y pruebas que se aplican razonablemente para obtener los mismos resultados. Para determinar la conveniencia de cualquier información específica, procedimiento o prueba, los profesionales de gobierno y aseguramiento deberían aplicar su propio criterio profesional a las circunstancias específicas presentadas por los sistemas particulares o por el entorno de tecnología de la información.

Reserva de derechos

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE. UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *info@isaca.org*
Página de Internet: *www.isaca.org*

Pagos mediante dispositivos móviles: cuestiones relacionadas con los riesgos, la seguridad y el aseguramiento

Agradecimientos

ISACA desea agradecer a:

Equipo de desarrollo del proyecto
Nikolaos Zacharopoulos, CISA, CISSP, Geniki Bank, Grecia, Presidente
Milthon Chávez, Ph.D., CISA, CISM, CGEIT, CRISC, ISO27000LA, CIFI, MCH Consultoría Integral/C.I.R.O., EE. UU.
Mohamad Hammoud, Path Solutions, Kuwait
Cristian Pigulea, CISA, Endava Romania SRL, Rumania
Dionysios Travlos, CISA, Grecia
Peter Van Mol, CISA, Atos Worldlinenv, Bélgica
Gautam Vora, CISA, TDK Corporation, EE. UU.
Mahmoud Yassin, CISA, CRISC, CISSP, ITIL, PMP, National Bank of Abu Dhabi (NBAD), EAU

Revisores expertos
Prashantsinh V. Jethwa, CISSP, CBCI, RBS Group, Inglaterra
Fundile Ntuli, MCSSA, Ubank, Sudáfrica
Hari Ramamurthy, CISA, CGEIT, ACA, Leading System Consultants Inc., Canadá

Consejo de dirección de ISACA
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (jubilado), EE. UU., Presidente Internacional
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grecia, Vicepresidente
Gregory T. Grocholski, CISA, The Dow Chemical Co., EE. UU., Vicepresidente
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Gobierno de Queensland, Australia, Vicepresidente
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vicepresidente
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, EE. UU., Vicepresidente
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vicepresidente
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (jubilado), EE. UU., ex Presidente Internacional
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Federación Rusa, ex Presidente Internacional
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, UK, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Bélgica, Director

Comité de Conocimiento
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Bélgica, Presidente
Michael A. Berardi Jr., CISA, CGEIT, Nestle USA, EE. UU.
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapur
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, EE. UU.
Jon Singleton, CISA, FCA, Auditor General de Manitoba (jubilado), Canadá
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, Francia

Comité de Orientación y Prácticas
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, EE. UU., Presidente
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, 6 Sigma, Quest Software, España
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, EE. UU.
Yongdeok Kim, CISA, IBM Korea Inc., Corea
Perry Menezes, CISM, CRISC, Deutsche Bank, EE. UU.
Mario Micallef, CGEIT, CPAA, FIA, Consultor en GRC, Malta
Salomon Rico, CISA, CISM, CGEIT, Deloitte, México
Nikolaos Zacharopoulos, CISA, CISSP, Geniki Bank, Grecia

Agradecimientos *(continuación)*

Afiliados y patrocinadores de ISACA y el IT Governance Institute® (ITGI®)
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association (ISSA)
Institute of Management Accountants Inc.
Capítulos de ISACA
ITGI Francia
ITGI Japón
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School
ASI System Integration
Hewlett-Packard
IBM
SOAProjects Inc.
Symantec Corp.
TruArx Inc.

Introducción: ¿Qué son los pagos mediante dispositivos móviles?

Los dispositivos móviles han cambiado la forma de hacer negocios y la vida cotidiana en materia de comunicaciones, y posiblemente estén modificando ahora el modo en que se realizan las transacciones financieras de todo tipo. El uso de dispositivos móviles —en particular, el de los teléfonos móviles— se ha generalizado y los consumidores están cada vez más familiarizados con el empleo de teléfonos móviles para efectuar diversas operaciones, como la realización de transacciones financieras "seguras" a través de un sitio web de servicios bancarios.[1] Una nueva oportunidad está surgiendo para los proveedores de servicios y comerciantes: el uso del teléfono móvil a modo de "cartera" móvil. Teniendo en cuenta el éxito que han tenido los servicios de contenidos para móviles, como los tonos de llamada, juegos y demás aplicaciones, resulta cada vez más evidente que los consumidores están dispuestos a utilizar el teléfono móvil para efectuar pagos. Los teléfonos móviles también presentan una oportunidad sin precedentes para la expansión de la actividad financiera en los países en vías de desarrollo, donde suele haber una mayor cantidad de usuarios de telefonía que titulares de cuentas bancarias.

Definición y características distintivas

El concepto de pago mediante dispositivos móviles se define como:

> *Pago de productos o servicios entre dos partes para el que cumple una función clave el uso de un dispositivo móvil (por ejemplo, un teléfono móvil).*

El concepto de pago mediante dispositivos móviles se define como: Pago de productos o servicios entre dos partes para el que cumple una función clave el uso de un dispositivo móvil (por ejemplo, un teléfono móvil).

El pago mediante dispositivos móviles se aplica, fundamentalmente, a las transacciones efectuadas entre consumidores y comerciantes por la compra directa de bienes y servicios, ya sea a través de una cuenta o de un punto de venta (Point of Sale, POS).

Los pagos mediante dispositivos móviles pueden dividirse en dos categorías, según la tecnología utilizada: por proximidad o remotos. Estas modalidades determinan la naturaleza del modelo de servicio de pago, la propuesta de valor tanto para el consumidor como para el comerciante, y las tecnologías y consideraciones de infraestructura pertinentes para la realización del tipo de pagos mediante dispositivos móviles. La **figura 1** ofrece una visión general de estos dos tipos de pago.

Figura 1: Tipos de pagos mediante dispositivos móviles

Tipo	Tecnología empleada	Adopción a nivel mundial
Pago por proximidad El pago por proximidad suele hacer referencia a los pagos efectuados "sin contacto" ("contactless"), en los que la credencial de pago se almacena en el dispositivo móvil y se transmite de forma inalámbrica ("Over The Air", OTA), mediante el empleo de tecnología NFC (Near Field Communication), a un terminal de pago dedicado y compatible. En otras palabras, el dispositivo móvil actúa como una tarjeta de pago "sin contacto" y se convierte, de este modo, en una nueva modalidad de pago. El pago mediante tecnología "sin contacto" también se puede efectuar de forma remota; por ejemplo, es posible realizar una compra en línea pasando el dispositivo móvil por un lector de NFC "sin contacto" conectado a un ordenador personal (PC).	El consumidor utiliza el teléfono móvil en la tienda para efectuar el pago de bienes o servicios mediante el uso de un lector "sin contacto", o a través de métodos basados en mensajes de texto o en un número de identificación personal (PIN), que emplean la tecnología de comunicación de corto alcance (NFC)[2] para establecer una comunicación entre el dispositivo del consumidor, el operador del sistema de pago y el comerciante minorista en la tienda. Dado que todos los dispositivos móviles compatibles con la tecnología NFC pueden enviar y recibir datos, los teléfonos que emplean esta tecnología también pueden actuar como lectores de tarjetas. Se trata de una tecnología estrechamente alineada con el uso de medios informáticos confiables, como las tarjetas de módulos de identidad del suscriptor (SIM) y los módulos de plataforma segura (TPM).	Los sistemas basados en tecnología NFC se están utilizando o evaluando en Europa Occidental, los Estados Unidos, Canadá y Japón, entre otras regiones. También están obteniendo una aceptación cada vez más amplia en los países en vías de desarrollo, donde se los utiliza especialmente para efectuar transacciones mediante tarjetas "sin contacto". Entre las instalaciones de este tipo se destacan: ExpressPay™ de American Express, Discover® Network Zip℠, MasterCard® PayPass™, y Visa® payWave™ y Speedpass™. En julio de 2011, PayPal™ lanzó un nuevo modelo de pago con tecnología NFC. Se trata de una variante del modelo eWallet® en la que PayPal actúa como intermediario transparente en una transacción de pago de persona a persona (P2P), permitiendo que dos usuarios de dispositivos con tecnología NFC y plataforma Android™ efectúen una operación de pago al acercar un dispositivo al otro.

[1] Los servicios bancarios móviles consisten en el uso de dispositivos móviles, principalmente teléfonos inteligentes, para acceder a servicios bancarios y financieros tradicionales, fundamentalmente operaciones bancarias e inversiones. Está orientado a transacción y focalizado en las transacciones entre los bancos y sus clientes. El dispositivo móvil se utiliza más como medio de comunicación que como instrumento de pago (por ejemplo, para acceder a servicios bancarios ofrecidos en la web mediante el uso de un explorador en un teléfono inteligente).

[2] NFC es un estándar de radiofrecuencia que se utiliza para transferir datos a distancias de hasta 10 centímetros (3,9 pulgadas).

Figura 1: Tipos de pago mediante dispositivos móviles *(continuación)*

Tipo	Tecnología empleada	Adopción a nivel mundial
Pago remoto El pago remoto cubre los pagos efectuados a través de un explorador ("browser") web móvil o de una aplicación residente en un teléfono inteligente (smartphone), utilizando el teléfono móvil como dispositivo para autenticar de forma remota la información personal almacenada. Las soluciones de pago remoto también se pueden emplear para realizar transacciones presenciales y con máquinas expendedoras.	El consumidor utiliza el teléfono móvil junto con un servicio de mensajería de red, como el servicio de mensajes cortos de texto (SMS)[3] o el servicio suplementario de datos no estructurados (USSD)[4], para pagar servicios o contenido digital. Los mensajes pueden utilizarse en sí mismos para iniciar o autorizar un pago, o, en algunas situaciones, como unidad monetaria o de cambio. Para transacciones de bajo importe como la compra de tonos de llamada o cuando se utilizan soluciones de autenticación de contenido móvil basadas en el número de identificación del suscriptor del móvil (MSIDN), la facturación se lleva a cabo a través de la factura de teléfono del usuario. Las transacciones con importes más altos pueden ser procesadas mediante la utilización de diversos enfoques técnicos, como: • Pago con tarjeta de crédito/débito, introduciendo la información del usuario a través de una interfaz de protocolo de aplicación inalámbrica (WAP) segura. • Pago con eWallet/pago basado en una cuenta con saldo almacenado a través de una interfaz WAP segura. En este caso, la tarjeta del usuario y la información de la cuenta bancaria son almacenadas en modo seguro en el dispositivo móvil del usuario. Se emplea un sistema de autenticación mediante PIN junto con un método de transmisión a través de canales de respuesta de voz interactiva (IVR), WAP, SMS y USSD. • activación segura del cliente por parte del proveedor de servicios, y la habilitación confiable del enlace entre el MSIDN y el número de tarjeta son requisitos esenciales.	Los sistemas de SMS y USSD se están utilizando ampliamente en África y en regiones de Medio Oriente donde existe una elevada concentración de dispositivos móviles, grandes comunidades migratorias y una escasa penetración de servicios bancarios. Estos servicios de mensajes se emplean con distintos fines, como la realización de pagos a comerciantes, el envío de dinero fuera del país y el pago de los salarios de los trabajadores emigrantes. Una aplicación generalizada de este tipo de pago mediante dispositivo móvile es la compra de tonos de llamada, juegos y otros artículos a través de SMS con tarifa especial ("premium"). Hasta ahora, esta modalidad de pago se empleaba, habitualmente, para pequeños importes (micropagos).

Actualmente, las partes interesadas no han separado claramente los roles en el ecosistema de pago mediante dispositivos móviles. Las instituciones financieras y los operadores de redes móviles (Mobile Network Operator, MNO) están compitiendo para constituirse en la entidad que gestione la cuenta del cliente y reciba la porción más grande de los pagos. En un entorno tan poco claro ha surgido una nueva clasificación basada en el tipo de entidad que gestiona la cuenta del cliente: bancarizada ("bank-centric") y no bancarizada ("nonbank-centric").

En el modelo bancarizado, la cuenta del cliente es gestionada por un banco. Las cuestiones relacionadas con temas como la responsabilidad, las medidas contra el lavado de dinero, el monitoreo de las transacciones para la detección de fraudes y el cumplimiento con las normas se rigen por las leyes y normas pertinentes que regulan la actividad bancaria en el ámbito local, nacional e internacional. Cuando se inicia una operación de pago, el banco del consumidor debe autorizar la transacción. Las redes de pago utilizadas son las tradicionales, como Visa y MasterCard, y las principales diferencias radican en los extremos de la transacción.

En el modelo no bancarizado, la cuenta del cliente es gestionada por organizaciones no financieras (por ejemplo, un MNO o un servicio de pago prestado a través de terceros, como PayPal). En este caso, surgen una serie de cuestiones importantes respecto del marco normativo, la seguridad e incluso la participación en los beneficios/utilidades. Por ejemplo, ¿qué entidad se ocupará de regular estos servicios: el organismo nacional competente en materia de telecomunicaciones o el banco nacional que corresponda?

[3] El SMS es un servicio de envío de mensajes de texto a través de un teléfono, de la web o de sistemas de comunicaciones móviles, que utiliza protocolos de comunicaciones estandarizados (sistema global de comunicaciones móviles/servicio general de radiocomunicaciones por paquetes [GSM/GPRS] y acceso múltiple por división de código [CDMA]) para permitir el intercambio de mensajes de texto cortos entre líneas de telefonía fija o teléfonos móviles.

[4] USSD es un protocolo utilizado por los teléfonos móviles con GSM para establecer comunicaciones con las computadoras de los proveedores de servicios.

En la Unión Europea (UE), especialmente, la flexibilización de las restricciones impuestas a los operadores de pago está modificando el panorama de los pagos mediante dispositivos móviles en toda Europa. Específicamente, una serie de nuevos actores (operadores de telefonía móvil, grandes almacenes, etc.) serán oficialmente reconocidos como proveedores de servicios de pago (PSP) aunque no sean una entidad crediticia tradicional (tal como la define la directiva de la Unión Europea 2000/12/CE) y se les permitirá operar en competencia directa con las instituciones financieras/crediticias tradicionales, en tanto cumplan con los requerimientos establecidos en la directiva. En concreto, podrán actuar como emisores de dinero electrónico (EMI)[5] o como PSP.[6] Podrán ofrecer ciertos servicios, como depósitos en efectivo, retirada de efectivo, débitos directos, transferencias de crédito, pagos iniciados con una tarjeta o dispositivo de pago similar y crédito (por un plazo máximo de 12 meses). Muchas de las compañías que compiten por la prestación de estos servicios —desde gigantes de la industria de Internet, como PayPal y Google™, hasta las nuevas empresas, como Crandy, Luup o Tunz—, ya poseen licencias para operar como emisoras de dinero electrónico en Europa. Algunos operadores de telecomunicaciones que ya han obtenido una licencia para ofrecer servicios bancarios, como Mobilkom en Austria, disponen de una filial de tipo financiera o se han asociado con PSP o bancos. Hasta ahora, ninguna de las iniciativas mencionadas anteriormente parece haber sido imitada en el resto del mundo.

Todo indica que el modelo de pago bancarizado con tecnología NFC es el más utilizado en la actualidad, razón por la cual el presente artículo se centrará en este modelo. Si bien se están empleando algunos sistemas de pago no bancarizados, la adopción de esos sistemas no ha sido tan amplia. En este contexto, el presente artículo pone de relieve, con fines ilustrativos, las características y los riesgos de los pagos no bancarizados, haciendo especial hincapié en las cuestiones relacionadas con los sistemas de proximidad y bancarizados que utilizan tecnología NFC, para ampliar el análisis.

Ecosistema de los pagos mediante dispositivos móviles

El ecosistema de los pagos mediante dispositivos móviles se compone de los siguientes actores:
- Consumidores
- Proveedores de servicios financieros (FSP)
- Proveedores de servicios de pago (PSP)
- Proveedores de servicios (comerciantes), incluidos los proveedores de contenido
- Proveedores de servicios de red (NSP)
- Fabricantes de dispositivos
- Entidades reguladoras
- Organismos de normalización y Confederaciones Industriales.
- Compañías dedicadas a la gestión de servicios confiables (TSM)
- Desarrolladores de aplicaciones

Estos actores pueden adoptar diversas formas: instituciones financieras, redes de tarjetas de débito/crédito, organizaciones que prestan servicios de compensación/liquidación, proveedores de soluciones de software, procesadores de pagos a cargo de terceros, MNO/operadores de servicios inalámbricos, fabricantes de aparatos telefónicos/chips, clientes y comerciantes. Los diversos actores pugnan por obtener parte de los ingresos en el nuevo ecosistema, donde las instituciones financieras, las redes de tarjetas de débito/crédito y los MNO compiten entre sí para desempeñar el rol de FSP y NSP, y para recibir los beneficios/las utilidades correspondientes a los cargos abonados en cada transacción. El pago mediante dispositivos móviles mediante tecnología sin contacto es una aplicación entre otras muchas. En el siguiente párrafo, se presenta una perspectiva general de los principales actores del ecosistema de la tecnología NFC, y del rol que estos podrían desempeñar en un futuro cercano.

Los diversos actores pugnan por obtener su parte de los ingresos en el nuevo ecosistema, donde las instituciones financieras, las redes de tarjetas de débito/crédito y los MNO compiten para desempeñar el rol de FSP y NSP y por los cargos asociados a las transacciones.

A continuación se ofrecen algunos ejemplos de las propuestas de valor para los diversos actores:

- **Operadores de telefonía móvil**: el pago mediante dispositivos móviles a través de tecnología sin contacto proporciona un medio para añadir valor a sus ofertas comerciales con nuevos servicios que, potencialmente, les permitirán incrementar el promedio de ingresos por usuario (ARPU) a través de nuevas y diferentes fuentes de ingresos, como la aplicación de cargos por transacción, el alquiler de espacios en los teléfonos o tarjetas SIM, el tráfico de datos (principalmente inalámbrico [Over The Air, OTA]), la gestión de aplicaciones de los proveedores de servicios y la prestación de servicios financieros.

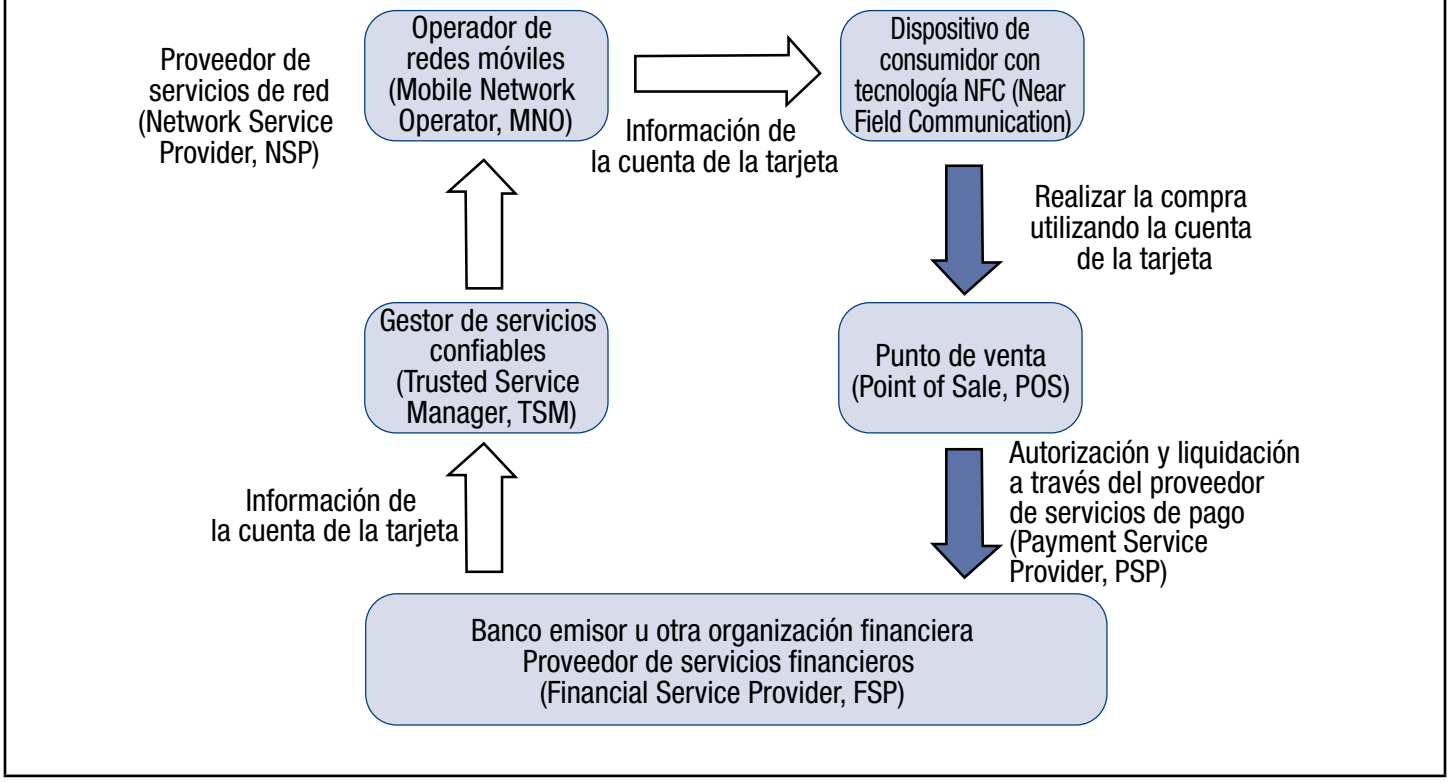
[5] Emisor de dinero electrónico: El candidato debe tener una licencia para operar como emisor de dinero electrónico, según lo definido en la directiva 2000/46/CE, que le permita gestionar pagos por importes bajos, basados en una cuenta en línea con saldo almacenado.
[6] Proveedor de servicios de pago: El candidato debe tener el estatus de institución de pago (PI), tal como la define el artículo 6 de la directiva de la Unión Europea sobre servicios de pago en el mercado interno, adoptada en abril de 2007.

- **Bancos**: el pago mediante dispositivos móviles a través de tecnología sin contacto reducirá el manejo de efectivo (para micropagos) y los costos de la emisión de tarjetas plásticas (para macropagos). También permite ampliar la oferta de servicios interactivos vinculados con los servicios bancarios en línea, tales como concesión de crédito en el punto de compra.
- **Comerciantes**: el pago mediante tecnología sin contacto permite reducir el tiempo empleado en cada transacción y, a su vez, generar más transacciones, especialmente para micropagos, y también reducen el manejo de efectivo. Los pagos mediante dispositivos móviles a través de tecnología sin contacto también podrían presentar nuevas oportunidades para desarrollar programas de fidelidad, particularmente mediante el uso de cupones electrónicos que podrían almacenarse en el teléfono y consumirse en la caja al pasar el teléfono por un lector.
- **Operadores de transporte**: muchos operadores de sistemas de transporte ya han comenzado a ofrecer tarjetas con tecnología sin contacto para ser utilizadas en sus redes. Dado que la infraestructura ya está implementada, el sector del transporte es el más adecuado para lanzar nuevos servicios móviles con tecnología sin contacto a gran escala. La introducción de un ticket electrónico ("e-ticket") en el teléfono móvil permite obtener una mayor satisfacción del cliente, al simplificar los viajes diarios. A su vez, la sustitución de los tickets y de las tarjetas para tecnología sin contacto por aplicaciones que empleen esta clase de tecnología y se puedan descargar en el teléfono reducirá considerablemente los costos de la emisión de tickets.
- **Proveedores de entradas**: ahora, los organizadores de eventos, los museos y los cines que venden entradas a través de Internet o de una red móvil pueden enviar las entradas directamente al comprador desde un teléfono con tecnología NFC. De este modo, la compra de entradas se puede realizar en mucho menos tiempo y desde cualquier lugar. Además, los compradores pueden acceder rápidamente al evento al llegar, sin hacer largas filas o colas. Los organizadores de eventos también pueden utilizar estas aplicaciones para ofrecer una mayor variedad de servicios interactivos, como proporcionar información adicional sobre el evento.

Aunque es evidente que el potencial de la modalidad de pago mediante dispositivos móviles a través de tecnología sin contacto es relevante para todos los implicados, existen dudas respecto del modelo de negocio y del modo de compartir el valor.

Para contextualizar y desarrollar con mayor amplitud los puntos mencionados anteriormente, se analizará en el presente artículo el ciclo de vida de un pago mediante dispositivo móvil bancarizado con tecnología NFC, que se ilustra en la **figura 2**.

Figura 2: Ciclo de vida de un pago mediante dispositivo móvil, bancarizado, con tecnología NFC



El diagrama ilustra los distintos actores que participan en una operación bancarizada de pago mediante dispositivo móvil. También muestra el flujo de la información que abarca: a) el suministro de información sobre la cuenta de pago del consumidor desde la institución financiera emisora al teléfono (personalización del dispositivo) y b) la autorización del pago mediante dispositivo móvil a través de tecnología NFC de proximidad a través de una red de proveedores de tipo PSP existente. Las flechas azules señalan las transacciones relacionadas con el pago, mientras que las flechas blancas denotan acciones relacionadas con la personalización de la aplicación. También se supone, en esta figura y en el modelo de transacción con tecnología NFC, que el dispositivo móvil del usuario que contiene el chip de NFC es una plataforma confiable, es decir, utiliza un módulo de plataforma confiable (TPM) que se ajusta a la definición y a las especificaciones de Trusted Computing Group (TCG).

Un nuevo actor que se incorpora al modelo NFC es el gestor de servicios confiables (Trusted Service manager, TSM). La TSM es una entidad externa confiable que podría ocuparse (potencialmente) de gestionar el despliegue de las aplicaciones móviles. Tal como se ilustra en la **figura 2**, el ciclo de vida de un pago mediante dispositivo móvil con la intervención de una TSM comprendería lo siguiente:

- Una institución financiera prepara los datos de la cuenta y envía la información de la cuenta de pago a una TSM.
- La TSM entrega la información de la cuenta de pago del consumidor, por vía inalámbrica (OTA) y a través de la red móvil al elemento seguro del teléfono móvil.
- Una vez que la cuenta de pago está en el teléfono, el consumidor puede utilizarlo como tarjeta de pago virtual en comercios que acepten pagos con operaciones de crédito y débito mediante tecnología sin contacto.
- En este caso, los pagos se procesan a través de las actuales redes financieras, con créditos y débitos en las cuentas correspondientes.
- La red de operadores de servicios móviles solo se utiliza durante la personalización del dispositivo. La TSM también se ocupa del ciclo de vida del dispositivo, ya que administra la federación de datos de las cuentas de los clientes entre sus teléfonos móviles y desactiva el chip NFC en caso de robo.

A nivel mundial, ya se encuentran disponibles pagos mediante dispositivos móviles , contemplando las modalidades de pago por proximidad y remoto así como el uso de modelos de transacciones bancarizadas y no bancarizadas. La **figura 3** proporciona una imagen de los tipos de servicios de pago mediante dispositivos móviles que actualmente se ofrecen y que son representativos de la evolución del ecosistema de pagos mediante dispositivos móviles.

Figura 3: Servicios de pago mediante dispositivos móviles

Tipo de proveedor de servicios	Servicios-ejemplos
Híbrido-colaborativo	• Safaricom y Vodafone (África) lanzaron M-PESA, un servicio de pago por SMS dirigido a abonados no bancarizados y con servicios prepago de telefonía móvil en Kenia. • Google Checkout™ (EE. UU.): sociedad entre Google y Sprint®, Citi®, MasterCard y FirstData®.
Operador de redes móviles (MNO)	• Paybox de MobilkomAustria: sistema basado en SMS que también incluye un sistema NFC para la compra de pasajes de transporte a través de dispositivos móviles. • NTT DoCoMo, Inc. (Japón): servicio de “cartera” móvil Osaifu-Keitai®.
Servicios de pago independientes	• Obopay™, Inc. (EE. UU.): compañía que presta servicios de pago mediante dispositivos móviles de tipo P2P, ofreciendo a los usuarios de dispositivos móviles la posibilidad de enviar y recibir dinero a través de sus teléfonos mediante el uso de un explorador (“browser”) web móvil o de SMS. • PayPal Mobile™ (EE. UU.): sistema que permite utilizar la web y el servicio de SMS mediante la introducción de un PIN para realizar pagos a través de una cuenta de PayPal. • Western Union®: aplicación móvil que permite realizar transferencias de dinero en modalidad P2P entre la cuenta bancaria del emisor y la tarjeta de débito de Western Union que posee el destinatario. • e-Transfer de Interac, Inc. (Canadá): permite enviar dinero directamente desde una cuenta bancaria y recibirlo en otra utilizando los “servicios bancarios móviles” o en línea que alguna de las instituciones financieras autorizadas suministra, sin revelar ningún dato personal ni proporcionar información financiera.

Cada parte percibe de forma diferente sus responsabilidades y obligaciones, por lo que el ecosistema necesita un plan de acción que identifique las infraestructuras y funcionalidades necesarias para respaldar los contextos de las transacciones y, como aspecto más importante, conseguir el éxito requerirá colaboración e interoperabilidad entre industrias que nunca han trabajado conjuntamente ni han utilizado un entorno compartido.

Un punto clave a tener en cuenta es que cada parte percibe de forma diferente sus responsabilidades y obligaciones, por lo que el ecosistema necesita un plan de acción que identifique las infraestructuras y funcionalidades necesarias para respaldar los contextos de las transacciones y, como aspecto más importante, conseguir el éxito requerirá colaboración e interoperabilidad entre industrias que nunca han trabajado conjuntamente ni han utilizado un entorno compartido.

Beneficios de Negocio y Desafíos.

La llegada del pago mediante dispositivos móviles presenta diversos beneficios, tanto desde la perspectiva del negocio como del consumidor. Estos incluyen:

- **Rapidez y comodidad para el cliente** Los clientes no necesitan llevar consigo dinero en efectivo ni utilizar tarjetas de crédito.
- **Se obtiene cobertura con una adecuada relación costo/efectividad en zonas rurales donde no opera ninguna institución financiera.** De hecho, las cifras registradas recientemente en las Filipinas demuestran que una transacción típica realizada en la sucursal de un banco tiene un costo de US $2,50 para el banco, mientras que el costo de una transacción de pago mediante dispositivo móvil se reduce a US $0,50 (según un informe realizado en 2007 por *The Asian Banker*).
- **La capacidad de enviar dinero al extranjero a través de servicios de pago mediante dispositivos móviles de persona a persona (P2P).** Con una cantidad estimada de 191 millones de trabajadores emigrantes en el mundo, y con un negocio potencial para el envío de dinero a nivel internacional de US $257 mil millones en 2005 (según datos de la ONU y del Banco Mundial, respectivamente), la transferencia internacional de fondos a través de teléfonos móviles constituye una oportunidad importante para los operadores de servicios móviles.
- **La "cartera" móvil puede concentrar muchas tarjetas.** Esto elimina la necesidad de tarjetas físicas y proporciona un mismo tipo de dispositivo para todas las aplicaciones con NFC (transporte, compra de productos, etc.).
- **Autenticación mejorada a través del servicio basado en el uso de un PIN.** Esto proporciona una capa de seguridad mejorada.
- **Existe una oportunidad para acceder a gran parte de la población mundial sin necesidad de realizar grandes inversiones en tecnología.** Los teléfonos móviles están más extendidos que las cuentas bancarias, particularmente en las zonas rurales.
- **Los comerciantes y clientes no necesitan dinero en efectivo.** Esto reduce el riesgo al manejar y trsnsferir dinero en efectivo, especialmente en entornos volátiles o de alto riesgo.
- **Se reduce la cantidad requerida de datos almacenados para cubrir los requerimientos de cumplimiento normativo.**
- **Las capacidades de los teléfonos inteligentes, como la geolocalización y la conexión a Internet, pueden ser utilizados para mejorar la seguridad de las transacciones y las capacidades de detección de fraudes.** Además, la combinación de las dos tecnologías mencionadas anteriormente puede crear un nuevo tipo de marketing, el "geomarketing", que le permite al comerciante utilizar la geolocalización y los datos del pago mediante dispositivos móviles para construir un perfil del cliente y ofrecer una experiencia personalizada.
- **El robo de un teléfono móvil es más fácil de advertir que el de una tarjeta de crédito.** Los consumidores suelen ser más cuidadosos con sus teléfonos móviles que con sus tarjetas de crédito, porque los teléfonos son dispositivos multifuncionales son utilizados con más frecuencia.
- **Los pagos mediante dispositivos móviles abren el mercado a los profesionales y a los comerciantes de segmentos más pequeños que no poseen terminales de puntos de venta (POS).** Es una alternativa más económica que la inversión en hardware para aceptar pagos electrónicos. En la actualidad este es un aspecto emergente de los pagos mediante dispositivos móviles, que podría convertirse con el tiempo en un factor clave para la venta de esta tecnología.
- **El uso de teléfonos inteligentes contrarresta los métodos de robo de información que se emplean en muchos de los casos de fraude con tarjetas.** También ofrecen protección contra el robo de información de las tarjetas (denominado "pickpocketing electrónico") equipadas con etiquetas de identificación por radiofrecuencia (RFID).
- **La funcionalidad de "pasar la tarjeta" de forma remota (remote swipe) está disponible en muchos de los teléfonos inteligentes y tabletas con pantalla táctil ("tablet"), bien por defecto o mediante una aplicación.** Esto ofrece protección de la información personal y financiera del usuario en caso de pérdida o robo del dispositivo móvil.

Existen algunos desafíos y consideraciones sobre la relación coste/valor cuando se plantea el uso de servicios de pago mediante dispositivos móviles. Estos incluyen acuerdos sobre el modelo de negocio que se empleará para la participación en los ingresos y la propiedad del cliente, los costos de la reestructuración necesaria para ofrecer servicios de pago mediante dispositivos móviles (como la implementación de tecnología NFC) y las incertidumbres del marco normativo actual.

Asuntos relacionados con los riesgos y la seguridad

Históricamente, los estafadores han tenido como objetivo los distintos instrumentos de pago y es probable que los pagos mediante dispositivos móviles lo sean también; por lo tanto, es necesario realizar un análisis inicial y adoptar contramedidas destinadas a mitigar los riesgos de esta arma de doble filo. Desde la perspectiva de los pagos mediante dispositivos móviles, los riesgos se pueden clasificar como tradicionales o emergentes. Los riesgos tradicionales afectan a la denegación o el robo de servicios y la pérdida de ingresos, reputación de la marca y base de clientes, mientras que el riesgo emergente comprende el uso del sistema de pago mediante dispositivos móviles para lavado de dinero y financiación de actividades terroristas.

Los riesgos tradicionales afectan a la denegación o el robo de servicios y la pérdida de ingresos, reputación de la marca y base de clientes, mientras que el riesgo emergente comprende el uso del sistema de pago mediante dispositivos móviles para lavado de dinero y financiaciópn de actividades terroristas.

Dado que el modelo bancarizado con tecnología NFC es el más utilizado en la actualidad, el riesgo emergente actualmente excede el alcance de este informe y, por consiguiente, el análisis se centrará en las cuestiones relacionados con los riesgos tradicionales. Para un debate sobre el lavado de dinero y la financiación de actividades terroristas, y sobre las estrategias para reducir este riesgo, una excelente fuente es el documento publicado por el Banco Mundial con el siguiente título: "Integrity in Mobile Financial Services: Measures for Mitigating Risk From Money Laundering and Terrorist Financing"[7] (Integridad de los servicios financieros móviles: medidas para mitigar el riesgo de lavado de dinero y financiación de actividades terroristas).

Los riesgos que afrontan quienes intervienen en el ecosistema de los pagos mediante dispositivos móviles dependen del rol de las entidades usuario, proveedor de redes o comunicaciones, o proveedor de servicios de pago. Algunas entidades, como los MNO, pueden desempeñar dos de estos roles simultáneamente. La **figura 4** proporciona una imagen de los tipos de amenazas y riesgos que pueden entrar en juego entre los actores principales que intervienen en el entorno de los pagos mediante dispositivos móviles.

Figura 4: Riesgos de los pagos mediante dispositivos móviles

Tipo de Objetivo	Vulnerabilidad	Amenaza	Riesgo	Contramedidas
Usuario	Transmisión inalámbrica (OTA) entre el teléfono y el punto de venta (POS) (lector de NFC)	Interceptación de tráfico	Robo de identidad, divulgación de información, ataques por repetición	Módulo de plataforma confiable (TPM), protocolos seguros, encriptación
Usuario	Instalación inadvertida de software malintencionado en el teléfono móvil del usuario	Aplicación descargada que intercepta los datos de autenticación	Robo de parámetros de autenticación, divulgación de información, repudio de transacciones	Autenticación del usuario (PIN) y de la aplicación (firma digital por una entidad externa confiable), TPM
Usuario	Ausencia de autenticación de dos factores	Enmascaramiento del usuario	Transacciones fraudulentas, responsabilidades del proveedor	Autenticación de dos factores
Usuario	Cambio o sustitución del teléfono móvil	Complejidad en la configuración y el establecimiento de parámetros	Escasa adopción de la tecnología; "seguridad por ofuscación de código" ("security by obscurity").	Interfaz de usuario simplificada, establecimiento de parámetros en TPM por una entidad confiable
Usuario	Capacidades de conexión a Internet y geolocalización en teléfonos inteligentes	Software malintencionado (malware) en dispositivo móvil; controles deficientes para la protección de datos en comercio/procesador de pagos	Divulgación de datos y violación de la privacidad; obtención del perfil de comportamiento del usuario	Control de las características de geolocalización por el usuario, protección criptográfica de la privacidad, módulo de plataforma confiable, control de autorizaciones y contabilidad
Proveedor de servicios	Sistema de punto de venta (POS) acepta transmisiones inalámbricas (OTA)	Entidad malintencionada que satura el sistema POS con solicitudes sin sentido	Denegación de servicio (DoS)	Filtrado de solicitudes en el lector en función de la geometría relativa dispositivo móvil –lector.
Proveedor de servicios	Dispositivos de POS están instalados en el local del comerciante.	Ataques enmascarados; manipulación de los puntos de venta (POS)	Robo de servicios, repetición, modificación de mensajes	Investigación del proveedor de POS, autenticadores de mensajes, control de autorizaciones y contabilidad
Proveedor de servicios	Carencia de gestión de derechos digitales (Digital Rights Managemeent, DRM) en el dispositivo móvil	Distribución ilegal de contenido (tonos de llamada, videos, juegos, etc.) por parte del usuario del dispositivo móvil	Robo de contenido, piratería digital, riesgo para el proveedor por violación de derechos digitales, pérdida de ingresos del proveedor de contenido o del comerciante	Incorporación de procesos de DRM en el diseño de TPM del teléfono inteligente, DRM con soporte criptográfico
Proveedor de servicios	Debilidad de la encriptación del Sistema Global de Comunicaciones Móviles (GSM) para la transmisión OTA; datos de SMS en texto legible en la red móvil	Modificación de mensajes, repetición de transacciones, evasión de controles de fraude	Robo de servicios o de contenido, pérdida de ingresos, transferencia ilegal de fondos	Protocolos criptográficos fuertes, autenticadores de mensajes SMS, encriptación

[7] Chatain, P.; et al.; "Integrity in Mobile Phone Financial Services—Measures for Mitigating Risks from Money Laundering and Terrorist Financing", documento de trabajo n.º 146 del Banco Mundial, Banco Mundial, Washington D.C., EE.ºUU., 2008, http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf

Estrategias para afrontar los riesgos

Los pagos mediante dispositivos móviles presentan nuevas oportunidades y nuevos riesgos. La transacción de pago mediante dispositivos móviles puede estar más expuesta a los riesgos, porque son muchos los actores que intervienen conjuntamente en la implementación del servicio de pago. Esta situación podría agravarse si la prestación de servicios importantes se externalizara en entidades externas no reguladas, sin criterios claros respecto de la rendición de cuentas y la supervisión, o que operaran desde el exterior. Este entorno de transacción con múltiples actores propicia la explotación por parte de estafadores, a través de ataques tanto tecnológicos como sociológicos, si no se establecen los adecuados mecanismos de protección y controles sobre la responsabilidad en todo el ecosistema de los pagos mediante dispositivos móviles. Con una planificación minuciosa que comprenda a todos los actores, procesos y tecnologías que intervienen, habrá posibilidades de lograr que la seguridad sea un componente intrínseco de todos los sistemas de pagos mediante dispositivos móviles.

Los proveedores de servicios financieros, de pago y de red (FSP, PSP y NSP, respectivamente) deberían implementar las salvaguardias adecuadas así como programas de gobierno de la seguridad y la privacidad. La ausencia de un marco normativo claro no debería ser utilizado como excusa por una organización para adoptar una actitud pasiva. Existe un riesgo de uso indebido por parte de usuarios autorizados, como el lavado de dinero, así como el riesgo de uso ilegal. Esta última situación puede requerir un respaldo de nuevas leyes que garanticen una protección adecuada. Cada una de las organizaciones que participa en la cadena de de datos de las transacciones debería aplicar controles positivos y fuertes para proteger los datos que se encuentran bajo su custodia.

Una de las preocupaciones fundamentales consiste en determinar con la mayor certeza posible que la persona que está realizando una transacción es efectivamente el usuario autorizado o registrado para llevarla a cabo. El uso de la autenticación de dos factores permitirá ofrecerle al consumidor una protección más eficaz de su identidad y un mayor grado de aseguramiento de la identidad al comerciante. En el caso de las transacciones bancarizadas con tecnología NFC, la protección contra la realización de transacciones por usuarios no autorizados o con teléfonos móviles falsos se puede lograr mediante el uso de valores de verificación de tarjetas (Card Verification Value, CVV) dinámicos. Los teléfonos móviles que pueden contener chips de NFC admiten CVV dinámicos, a diferencia de las tarjetas con bandas magnéticas, en las que se emplean CVV estáticos. Por lo tanto, cuando se utilice un teléfono móvil falso, este presentará un CVV incorrecto, la transacción no se procesará y, de este modo, se protegerá tanto al consumidor como al proveedor de servicios o comerciante. El mismo nivel de aseguramiento implementado en relación con el consumidor se debería establecer respecto del comerciante. Deberían emplearse técnicas análogas a los métodos de nivel de conector seguro (SSL) para garantizar que solo los POS o proveedores de servicios legítimos puedan interactuar con los teléfonos móviles. Estos puntos son representativos de una serie más amplia de cuestiones relacionadas con la fiabilidad de las identidades y credenciales, tanto en el sistema de pagos mediante dispositivos móviles como en el comercio vinculado a la telefonía móvil en general. Estas cuestiones y las estrategias que podrían adoptarse para abordarlas se analizan, por ejemplo, en la publicación realizada por la Casa Blanca en 2010 sobre la estrategia nacional de los Estados Unidos para identidades confiables en el ciberespacio.[8]

Otro de los factores importantes que se debe tener en cuenta es la clasificación de la información durante la transmisión y el almacenamiento de datos en los diversos nodos. Las organizaciones deberían identificar los datos considerados personales y sensibles, y deberían asegurar que están implementados los mecanismos adecuados. En lo que respecta a los datos financieros, un aspecto muy importante (además de la encriptación) es el tema de la integridad de los datos. Las organizaciones deberían tener esto en cuenta. Si los datos de los pagos mediante dispositivos móviles se usaran para prestar servicios de marketing, se podría acusar a las organizaciones de emplear prácticas comerciales desleales al utilizar los datos de los clientes con fines no especificados en los avisos que reciben.

Es igualmente importante considerar los sistemas POS en la modalidad de pago por proximidad. Las organizaciones deberían asegurarse de que las entidades externas con las que interactúan implementen proyectos eficaces en materia de gobierno de la seguridad. Además, debería dedicarse atención específica a la gestión de servicios confiables (TSM), que se ocupa de "personalizar" el chip compatible con la TSM en el dispositivo móvil suministrado por el proveedor. En ese entorno de colaboración con plataformas cruzadas, el programa de control de riesgos de una organización debería abordar específicamente la gestión de servicios prestados por terceros.

El Modelo de negocio de ISACA para la seguridad de la información (BMIS) y los marcos de referencia COBIT y Risk IT ofrecen enfoques útiles que las empresas podrían emplear al analizar e implementar las medidas necesarias en relación con las personas, los procesos, la tecnología y los cambios requeridos en la organización para adoptar un sistema de pagos mediante dispositivos móviles. El BMIS puede ayudar a la organización para abordar el contexto y la protección de los datos de los pagos mediante dispositivos móviles dentro de la organización. Los marcos COBIT y Risk IT pueden ser utilizados por una empresa para asegurar que se establecerá un proceso eficaz de control y reducción de riesgos en relación con el uso, la obtención y el gobierno de la información de los pagos mediante dispositivos móviles, no solo dentro de la organización, sino también para la gestión de los riesgos derivados de las relaciones con entidades externas.

[8] "National Strategy for Trusted Identities in Cyberspace—Enhancing Online Choice, Efficiency, Security and Privacy", Casa Blanca, EE.ºUU., abril de 2010, *www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf*

Por último, así como una cadena solo es tan fuerte como su eslabón más débil, se debería prestar especial atención al punto de origen de una transacción mediante dispositivo móvil: el dispositivo del cliente y el usuario. Se debería instruir a los usuarios para que conozcan los riesgos involucrados. Los fabricantes de dispositivos móviles deberían colaborar con la industria de instrumentos de pago en el desarrollo de plataformas que garanticen no solo un entorno seguro para la realización de transacciones mediante dispositivo móvil, sino también la interoperabilidad entre los distintos modelos de teléfonos inteligentes, ya que los usuarios suelen cambiar o actualizar sus teléfonos móviles a menudo. La prestación ininterrumpida de servicios seguros e interoperables es fundamental para garantizar el éxito de los pagos mediante dispositivos móviles.

En el artículo *Securing Mobile Devices* (Securización de los dispositivos móviles), publicado por ISACA (2010), se analizan muchos de estos puntos en el contexto del uso de dispositivos móviles.

En este nuevo ecosistema, además, se deberían aprovechar los mecanismos de control que los bancos han desarrollado durante muchos años. El uso de estos controles, combinado con la aplicación de contramedidas tecnológicas y la información obtenida a través de las transacciones con dispositivos móviles —como la geolocalización—, puede aumentar la confianza en que las transacciones no son fraudulentas. No obstante, las transacciones también deberían segmentarse por importe de compra, ubicación y categoría de comerciante, y los riesgos deberían ser gestionados de acuerdo las mismas.

Cuestiones relacionadas con el gobierno y los cambios

La adopción de sistemas de pago mediante dispositivos móviles exigirá la implementación de cambios en los modelos y procesos de negocio, así como en las infraestructuras tecnológicas subyacentes. Se deberían diseñar y supervisar programas de formación y nuevos controles internos. Uno de los principales factores que impulsan la adopción de servicios de pago mediante dispositivos móviles es el modelo de negocio que aporta valor a todos los actores que intervienen en el ecosistema. Los modelos de negocio pueden ser bancarizados, centrados en los operadores de telefonía móvil, centrados en los proveedores de servicios independientes o híbridos/colaborativos. Tal como se apuntó anteriormente, esta publicación analiza los aspectos del ecosistema de los pagos mediante dispositivos móviles que corresponden al modelo bancarizado.

La adopción de sistemas de pago mediante dispositivos móviles exigirá cambios en los modelos y procesos de negocio, así como en las infraestructuras tecnológicas subyacentes.

Desde la perspectiva de un modelo de negocio que comprenda actividades de negocio a negocio (B2B) y de negocio a consumidor (B2C), se deberá proporcionar un acceso equitativo a los segmentos de consumidores para los actores que intervienen en el sistema de pago mediante dispositivos móviles, y una adecuada protección y privacidad del cliente. Una gestión de relaciones con los clientes (CRM) razonable requerirá informarles, de forma adecuada y oportuna, sobre los riesgos, las responsabilidades y las obligaciones asociadas con las transacciones mediante dispositivo móvil, identificar los recursos de los que dispondrán los clientes, y establecer procedimientos relacionados con el manejo de las quejas tanto para las transacciones efectuadas a nivel interno y con plataformas cruzadas como para las transacciones en las que intervengan varias organizaciones.

Se deberán introducir modificaciones en las redes existentes o desarrollar nuevas estructuras de redes para proporcionar una interoperabilidad ininterrumpida entre los actores que intervienen en el ecosistema de los pagos mediante dispositivos móviles, teniendo en cuenta que muchos de esos actores nunca tuvieron una interacción directa anteriormente.

Dada la singularidad de los pagos mediante dispositivos móviles, no bastará con aplicar contramedidas individualmente en una organización, y se deberá prestar especial atención a las relaciones entre las distintas organizaciones que integran el ecosistema de los pagos mediante dispositivos móviles. Hasta ahora, por ejemplo, las tarjetas de pago habían sido controladas por una organización o institución financiera. Ahora, la información de las tarjetas se almacena en chips (por ejemplo, en tarjetas SIM), que se pueden transferir de un dispositivo a otro. Y los clientes cambian sus teléfonos móviles, los pierden y compran en distintos proveedores, que no son controlados por los bancos. Esta situación exige el establecimiento de una nueva entidad para gestionar los chips incontrolados y para asegurar una distribución confiable de la información de las tarjetas de pago.

Una posible solución para mitigar las amenazas que afectan los pagos mediante dispositivos móviles consiste en la implementación de una arquitectura TSM que posibilite la colaboración más allá de los límites técnicos y comerciales, para aportar el núcleo de un ecosistema seguro de pagos mediante dispositivos móviles. Este enfoque está siendo evaluado activamente por algunos de los bancos nacionales, en forma conjunta con operadores de redes y comunidades de comerciantes.

Una posible solución para contrarrestar las amenazas que afectan los pagos mediante dispositivos móviles consiste en desplegar una arquitectura TSM que posibilite la colaboración más allá de las fronteras tecnológicas y de negocio, para aportar el núcleo de un ecosistema seguro de pagos mediante dispositivos móviles.

En una infraestructura basada en TSM, la compañía dedicada a la gestión de servicios confiables actuaría como un intermediario neutral para supervisar los requerimientos comerciales y operacionales para el dspliegue de los pagos mediante dispositivos móviles a gran escala. Sus funciones deberían incluir temas como la gestión de las reglas de negocio y de las operaciones de autenticación, el suministro de conectividad entre los MNO y los proveedores de servicios, garantizando la seguridad en todas las etapas del proceso, aportando la gestión del ciclo de vida de las aplicaciones para los MNO, los teléfonos y los clientes, y la atención al cliente en todas las etapas del proceso. Algunas advertencias al usar este enfoque son el hecho de que la entidad dedicada a la TSM no participaría realmente en los procesos de las transacciones realizadas mediante tecnología NFC sin contacto, ya que las transacciones se procesarían a través de los canales de pago existentes y la TSM proporcionaría una autenticación segura en un extremo de la red, antes de que se produzca la transmisión a través de los canales existentes.

Consideraciones sobre aseguramiento

Al examinar el ecosistema de los pagos mediante dispositivos móviles, los roles que desempeñan los distintos actores y la naturaleza de las transacciones realizadas, se puede concluir que el método más conveniente para determinar los criterios de aseguramiento que deberían aplicarse (y el contexto en el que deberían aplicarse) consiste en evaluar dos niveles o grados de aseguramiento. El enfoque que deba adoptarse en materia de aseguramiento de los servicios de pago mediante dispositivos móviles dependerá de los roles implicados. Específicamente, ésto puede conseguirse:

- Analizando minuciosamente el comportamiento de los proveedores de servicios que se ocupan de manejar dinero así como ofrecer servicios de pago (PayPal, Western Union, Google Checkout y los sistemas de lotería, entre otros) para determinar el cumplimiento normativo de las operaciones bancarias.
- Aplicando modelos de auditoría estándar y normas que regulen los sistemas de pago asociados con la compra de bienes y servicios (MNO, autoridades de sistemas de transporte y comerciantes minoristas).

El profesional a cargo del aseguramiento debería tener en cuenta los siguientes aspectos al analizar el desempeño de las organizaciones que prestan servicios de pago mediante dispositivos móviles:

- La conveniencia de utilizar el marco COBIT de ISACA con los proveedores de servicios y terceros, ya que dicho marco proporciona una base sólida para la gestión de riesgos, el cumplimiento normativo, y la protección y el uso adecuados de la información suministrada al efectuar pagos mediante dispositivos móviles. El documento de ISACA *Mobile Computing Security Audit/Assurance Program* (Programa de aseguramiento/auditoría de seguridad de los sistemas informáticos con tecnología móvil) ofrece un dominio de COBIT sumamente útil y referencias cruzadas a procesos que se pueden adaptar específicamente a las condiciones de seguridad de los pagos mediante dispositivos móviles, y al entorno y contexto de las auditorías.
- Asegurar el cumplimiento de las regulaciones pertinentes que rigen tanto el sector de los instrumentos de pago como la industria de las telecomunicaciones, dado que esta nueva modalidad de pago corresponde, lógicamente, a ambas categorías.
- La relación contractual entre la organización y la entidad dedicada a la TSM, especialmente las representaciones y obligaciones de aseguramiento mutuo.
- Los puntos de transferencia confiables del proceso de la transacción de pago mediante dispositivo móvil y cómo éstas son protegidas para garantizar la fiabilidad de todo el proceso, desde el inicio de la transacción por parte del consumidor hasta la realización de la compra, el pago y la liquidación.
- La protección de la privacidad y la integridad de los datos de la transacción, y los detalles de la cuenta correspondiente a los datos del cliente.
- Formación para concienciar a los miembros de la organización respecto de los nuevos riesgos y responsabilidades que supone el manejo de los pagos mediante dispositivos móviles en el nuevo ecosistema.

Conclusiones

El mercado de los pagos mediante dispositivos móviles es un sector que está sufriendo una importante transformación y ofrece perspectivas prometedoras tanto para los consumidores como para los proveedores, teniendo en cuenta que el uso de servicios móviles basados en la tecnología de los teléfonos inteligentes se está extendiendo en todo el mundo. Algunos de los puntos clave de especial interés para los profesionales a cargo de la seguridad y el aseguramiento, basados en el estado actual y las perspectivas futuras de los pagos mediante dispositivos móviles, son los siguientes:

- **Se están creando modelos competitivos y colaborativos para la prestación de servicios de pago mediante dispositivos móviles**. Recientemente, diversas compañías han establecido sociedades: tal es el caso de la asociación entre Google y Sprint, Citi, MasterCard y FirstData; y el anuncio de que Visa ha adquirido Fundamo™, la plataforma que respalda las soluciones de pago mediante dispositivos móviles en más de 40 países. Estas operaciones en las que intervienen distintas empresas y plataformas serán necesarias para lograr la consolidación del sistema de pago mediante dispositivos móviles y exigirán la introducción de cambios en los modelos de negocio, seguridad y aseguramiento existentes, además de la modificación o creación de nuevas normas que regulen la interoperabilidad.
- **La seguridad y la privacidad, al igual que la comodidad, son factores clave desde la perspectiva del consumidor.**
- **Se deberá exigir la aplicación de estrictas medidas de aseguramiento a entidades independientes confiables, así como el desarrollo de, y la adhesión a, mejores prácticas de negocios dentro del ecosistema de los pagos mediante dispositivos móviles para fomentar el uso extensivo de este sistema entre los consumidores.** Será necesario presentar casos de negocio convincentes, que impulsen a las empresas a realizar las reestructuraciones necesarias para implementar las tecnologías de pago mediante dispositivos móviles, como la tecnología NFC.
- **En este momento, el futuro es prometedor y tentador, pero incierto.**

Recursos adicionales y retroalimentación
Visite *www.isaca.org/mobile_payments* para obtener recursos adicionales y utilizar la función de retroalimentación para aportar sus comentarios y sugerencias sobre este documento. Su opinión es muy importante en el desarrollo de las guías de ISACA para sus miembros, y es muy valorada.