Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Tema

Seguridad en Medios de Pagos Electrónicos en la Argentina

Título

Medidas de Seguridad aplicadas al Dinero Electrónico en la Argentina

Subtítulo

Proyecto de Norma: "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con el Dinero Electrónico en la Argentina"

Autor: Ing. Gastón Alejandro Cordero
Tutor: Graciela Pataro
Año 2018
Cohorte 2015

DECLARACIÓN JURADA DE ORIGEN DE LOS CONTENIDOS

Por medio de la presente el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Firmado,

Cordero, Gastón Alejandro
DNI: 31.583.761

RESUMEN

En las últimas décadas el avance de la tecnología y el uso de dispositivos móviles se ha hecho masivo en la sociedad, y de esto los actores del sistema financiero deben sacar provecho y poder definir nuevos modelos de negocios.

La unión de estos dos hechos ofrece una oportunidad para desarrollar nuevas formas de hacer llegar los servicios financieros a la población utilizando tecnologías móviles. A su vez, las tasas de suscriptores móviles a lo largo de la región latinoamericana continúan creciendo y se espera que alcancen a casi el 60% de la población total para 2020. Los servicios de dinero móvil, que permitirían a las personas no bancarizadas utilizar teléfonos móviles para realizar y recibir pagos, y que se basan en una red de puntos de transacción fuera de las sucursales bancarias, son una fuerte herramienta para profundizar el acceso financiero en los mercados en desarrollo. Los servicios de dinero móvil pueden ser ofrecidos por una gran cantidad de proveedores que pueden ser compañías telefónicas, entidades financieras y terceras partes, todos los cuales desempeñan un rol fundamental en el desarrollo de un saludable ecosistema financiero digital.

El presente trabajo cuenta de una primera parte, en la cual se realizó un análisis de las distintas implementaciones en el mundo de los modelos de negocios y de regulaciones acerca del dinero electrónico y los diferentes medios de pago. Y luego de una segunda parte, en donde se definieron lineamientos de seguridad para crear un marco regulatorio en la implementación del dinero electrónico y su aplicación para el pago de servicios a través de teléfonos móviles.

ÍNDICE

PRÓLOGO ..... **- 4 -**

NÓMINA DE ABREVIATURAS ..... **- 5 -**

CAPÍTULO I. MARCO TEÓRICO ..... **- 6 -**

I.I CONCEPTOS GENERALES ..... - 6 -
I.II MODELOS DE NEGOCIO ..... - 8 -
I.III PRINCIPALES AMENAZAS ..... - 9 -

CAPÍTULO II. SERVICIOS OFRECIDOS Y MARCO REGULATORIO EN EL MUNDO ..... **- 18 -**

CAPÍTULO III. REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN Y CONTROL DE LOS RIESGOS RELACIONADOS CON EL DINERO ELECTRÓNICO ..... **- 25 -**

CONCLUSIONES ..... **- 37 -**

ANEXO I – INVESTIGACIÓN SOBRE SERVICIOS OFRECIDOS Y MARCO REGULATORIO EN EL MUNDO ..... **- 39 -**

SUDÁFRICA ..... - 39 -
ECUADOR ..... - 41 -
FILIPINAS ..... - 45 -
BRASIL ..... - 47 -
REPÚBLICA DE KENIA ..... - 49 -
UNIÓN EUROPEA ..... - 51 -
ARGENTINA ..... - 54 -

REFERENCIAS ..... **- 58 -**

PRÓLOGO

El presente trabajo cuenta de una primera parte, en la cual se realizó un análisis de las distintas implementaciones en el mundo de los modelos de negocios y de regulaciones acerca del dinero electrónico y los diferentes medios de pago. Y luego de una segunda parte, en donde se definieron lineamientos para crear un marco regulatorio en la implementación del dinero electrónico y su aplicación para el pago de servicios a través de teléfonos móviles.

El dinero electrónico es un medio de pago que se puede utilizar para realizar pagos móviles, que se definen como aquellos en los que utiliza el teléfono móvil, u otro dispositivo similar de telecomunicaciones para, como mínimo, iniciar una orden de pago y, potencialmente, también para transferir fondos. Asimismo, los pagos móviles pueden liquidarse en cuentas bancarias, lo que se conoce como banca móvil.

NÓMINA DE ABREVIATURAS

BCE: Banco Central Europeo.

CVV: Código valor de verificación.

DE: Dinero Electrónico.

EDE: Emisores de dinero electrónico.

GSM: Sistema Global para Móviles.

NFC: Comunicación de campo cercano.

PAN: Número de cuenta principal

POS: Terminal punto de venta.

PSP: Proveedores de servicio de pago.

SMS: Servicio de mensajes cortos.

USSD: Datos de Servicio Suplementario no Estructurados.

CAPÍTULO I. MARCO TEÓRICO

I.I Conceptos Generales

¿Qué es el dinero electrónico?

Según Wikipedia, el dinero electrónico (también conocido como e-money, efectivo electrónico, moneda electrónica, dinero digital, efectivo digital o moneda digital) se refiere a dinero que se intercambia sólo de forma electrónica, a través de la utilización de una red de ordenadores, internet y sistemas de valores digitalmente almacenados. [1]

Según la Unión Europea, el dinero electrónico se define como el valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor, se emite al recibo de fondos con el propósito de efectuar operaciones de pago, y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico (DE). [2] Además, el Banco Central Europeo (BCE) agrega una definición dentro del contexto del dinero electrónico, definiendo a la moneda virtual como un "tipo de dinero no regulado, digital, que se emite y controla normalmente por sus desarrolladores, y utilizado y aceptado entre los miembros de una comunidad virtual específica". [3]

Según el Banco Central de Ecuador, definimos al dinero electrónico como el valor monetario equivalente al valor expresado en la moneda de curso legal del país que:

a) Se almacena e intercambia únicamente a través de dispositivos electrónicos, móviles, electromecánicos, fijos, tarjetas inteligentes, computadoras y otros, producto del avance tecnológico;
b) Es aceptado con poder liberatorio ilimitado y de libre circulación, reconocido como medio de pago por todos los Agentes Económicos en el Ecuador y para el pago de obligaciones públicas de conformidad con las normas que dicte el Organismo Regulatorio Competente;
c) Es convertible en efectivo a valor nominal; y,

d) Es emitido privativamente por el Banco Central del Ecuador sobre la base de las políticas y Regulaciones que expida el Organismo Regulatorio Competente y por ende se registra en el pasivo de la Institución. [4]

Podemos realizar diferentes clasificaciones del DE, si lo miramos desde quién es el encargado de emitirlo se puede dividir en:

- Dinero electrónico bancario: emitido por entidad financiera,
- Dinero electrónico no bancario: emitido por una organización especializada en el rubro, no financiera.

Por otro lado, si lo clasificamos prestando atención en el momento que se produce el pago, se puede diferenciar en:

- Medios de prepago: en estos como primer paso se debe transferir a la cuenta una cierta cantidad de dinero poder realizar transacciones. Luego dicha cantidad se puede gastar cuando se desee y no es necesario contar con banco (dinero off line). Por ejemplo, las tarjetas prepagas;
- Medios de pago inmediato: (dinero on line) es necesario contar con un servicio bancario (red o banca electrónica) para llevar a cabo el pago de una transacción con terceros (comercio o tienda online);
- Medios de pago diferido: el pago se realiza por el importe gastado durante un determinado período de tiempo. Por ejemplo, las tarjetas de crédito.

En función del soporte que utilizan se pueden diferenciar:

- Dinero software: es dinero electrónico almacenado bajo un formato software. No interviene ningún otro soporte físico que una computadora;
- Dinero unido a tarjetas: se corresponde a las tarjetas de plástico, las mismas tienen un poder real de compra y el usuario pagará por su adquisición en función de la modalidad de la tarjeta. También, se incluyen a las tarjetas prepagas;[5]
- Dinero móvil: es el dinero electrónico que es soportado por los teléfonos móviles. Abarcan a los monederos móviles y la banca móvil.

¿Qué es el dinero móvil?

Es dinero electrónico que tiene como soporte al teléfono móvil. Incluye a los **monederos móviles** (no asociados a una cuenta bancaria) y la **banca móvil** (asociada a una cuenta bancaria).

I.II Modelos de Negocio

De estudio acerca de las implementaciones de dinero electrónico en el mundo, se puede realizar una clasificación de los modelos de negocio, entre los que se destacan:

1) Centrado en el Banco Central de un país

En este modelo el Banco Central es el que emite, gestiona y administra el sistema de dinero electrónico. Las operaciones de crédito/débito pueden ser sobre una cuenta bancaria o monedero electrónico. Por ejemplo: se encuentra el modelo aplicado en el Ecuador, en donde el principal actor del sistema es el banco central del país.

2) Administrado por una institución privada

La institución es la que maneja el proceso de principio a fin, usando una plataforma propietaria. Las operaciones de crédito/débito pueden ser sobre una cuenta bancaria o monedero electrónico (utilizando una cuenta virtual no bancaria). Por ejemplo: la plataforma de pago M-PESA creada en el país de Kenia.

3) Alianza

Existe una colaboración entre una entidad bancaria, la cual es la autorizada para emitir el dinero electrónico, y una empresa privada, la cual brinda la infraestructura para que el sistema funcione. En general las empresas son operadores de telecomunicaciones. Por ejemplo, en Sudáfrica el MTN Mobile Money, es una alianza entre la empresa de telecomunicaciones MTN y el banco Standard.

I.III Principales amenazas

El uso de teléfonos móviles para realizar el pago de bienes y servicios crea un cambio de paradigma hacia pagos únicamente digitales. Los cuales han sido impulsados por consumidores que desean realizar compras en tiendas minoristas o transferir fondos utilizando su "billetera digital" móvil. Para la mayoría de los consumidores, la posibilidad de pagar por celular ofrece una mayor comodidad que llevar una billetera tradicional con múltiples tarjetas de crédito y débito. En función de esto, como primer punto del trabajo analizaremos y tipificaremos las posibles amenazas a las cuales se está enfrentando cuando se quiere realizar una operación a través de un teléfono móvil, y los vectores de ataque de los principales componentes del ecosistema de pagos móviles, estos son:

1. Amenazas a los usuarios de aplicaciones de pagos móviles.
2. Amenazas a los dispositivos móviles.
3. Amenazas a las aplicaciones de pagos móviles y de billeteras electrónicas.
4. Amenazas a los comerciantes.
5. Amenazas a proveedores de servicios de pago (PSP).
6. Amenazas a bancos / instituciones financieras.
7. Amenazas a proveedores de la red de pago.
8. Amenazas a los emisores de tarjetas.
9. Amenazas a los proveedores de aplicaciones de pago móvil.

1. Amenazas a los usuarios de aplicaciones de pagos móviles:

1.1. Phishing e ingeniería social:

En la actualidad los teléfonos móviles están siendo utilizados para cuestiones personales y laborales, por eso están recopilando una gran cantidad de información del cliente, lo que puede ayudar a llevar a cabo sofisticados ataques. Estos ataques se dirigen al usuario mediante correos electrónicos (phishing) e ingeniería social que explotan diferentes canales de comunicación (por ejemplo, teléfono, correo electrónico, SMS)

y datos sobre el usuario disponible en el dominio público (por ejemplo, sitios de redes sociales, motores de búsqueda). Los datos buscados por los atacantes que usan ingeniería social a menudo son datos de tarjetas de crédito y datos personales que el usuario conoce. La tarjeta de crédito / débito robada o los datos de la tarjeta prepaga (por ejemplo, PAN, CVV, fecha de vencimiento de la tarjeta) pueden ser comercializados (por ejemplo, venderse en foros de mercado clandestinos) o utilizarse para pagos fraudulentos. Los datos personales robados del usuario de pagos móviles (por ejemplo, nombre, apellido, fecha de nacimiento, información de contacto como dirección de envío de facturación, correos electrónicos, números de teléfono) se pueden usar para los ataques de suplantación y para el robo de identidad.

1.2. Instalación de aplicaciones fraudulentas y malware:

Los atacantes buscan formas de instalar malware en el dispositivo móvil mediante phishing / ingeniería social para que una víctima abra un archivo adjunto malicioso en un correo electrónico y por ejemplo redirija al usuario a una URL maliciosa. Otra forma de instalar un malware son los puntos de acceso WiFi inseguros (por ejemplo, las conexiones utilizadas en las cafeterías) que podrían permitir que un atacante acceda al dispositivo móvil. También existe la posibilidad de un ataque de suplantación de red, en la que se puede configurar un sitio web falso para "autenticar" a los usuarios y, de esta manera, recopilar datos que luego pueden usarse para los próximos pasos del ataque. No es raro ver a muchas personas usar el mismo nombre de usuario y contraseña para múltiples servicios diferentes, incluso para una aplicación de pago móvil.

2. Amenazas a los dispositivos móviles: accesos no autorizados, pérdida o robo del dispositivo.

2.1. Acceso no autorizado a un dispositivo móvil perdido o robado:

Un ataque directo ocurre cuando el atacante tiene posesión de un dispositivo que el usuario ha perdido o que ha sido robado. Los ataques más probables consisten en intentos de eludir cualquier PIN o bloqueos de

huellas dactilares. Un atacante en posesión del dispositivo puede intentar utilizar herramientas forenses de código abierto o comerciales que destraben el sistema operativo del dispositivo y obtengan acceso de usuario root al sistema de archivos para robar los datos instalados en el dispositivo.

2.2. Instalación de malware en el dispositivo:

Dichos ataques son realizados mediante la carga de malware en aplicaciones legítimas, que al momento de ser descargadas de las distintas tiendas online por los usuarios facilitan la instalación del malware en el dispositivo.

3. Amenazas a las aplicaciones de pagos móviles y de billeteras electrónicas:

3.1. Ingeniería inversa del código fuente de la aplicación:

Con frecuencia, la ingeniería inversa del binario es el primer puerto de escala para un atacante que busca obtener una comprensión de la aplicación de pago para explotar vulnerabilidades tales como contraseñas codificadas y claves de cifrado, así como para crear vectores de ataque específicos de la aplicación.

3.2. Manipular la aplicación de pago móvil:

Un atacante puede elegir una puerta trasera de una aplicación de pago móvil para capturar los datos de inicio de sesión y enviarlos a un servidor controlado por un atacante. Haría esto descargando la aplicación legítima de la tienda, desempacándola, parchando las rutinas relevantes y luego reempaquetando y cargando nuevamente la aplicación en la tienda. Dada la proliferación de cientos de tiendas de aplicaciones que ofrecen tales aplicaciones, esta es una amenaza muy real en los dispositivos móviles.

3.3. Explotación de vulnerabilidades de aplicaciones de pago móvil:

Pueden permitir a los atacantes robar cualquier información sensible almacenada por la aplicación (por ejemplo, detalles de la cuenta personal del usuario y datos de la tarjeta de crédito), la autenticación débil puede permitir que un atacante obtenga acceso no autorizado al dispositivo.

Por otro lado, el acceso no autorizado a una funcionalidad de la aplicación de pagos móviles puede producirse debido a la explotación de las API utilizadas para las funciones de compras en la aplicación que permiten a un atacante realizar transacciones fraudulentas. Además, el fraude es posible con cuentas bancarias y de tarjetas de crédito robadas. Un estafador también podría explotar las debilidades en el proceso de registro para agregar otro dispositivo móvil al perfil del usuario para realizar compras fraudulentas.

3.4. Instalación de rootkits / malware:

Los rootkits son un vector de amenaza significativo y también se pueden aprovechar para monitorear y secuestrar / manipular llamadas de API directamente desde / hacia el extremo de la API de pago móvil y manipular variables en tránsito, por ejemplo, montos de pago.

3.5. Permisos de acceso al sistema operativo móvil:

Los sistemas operativos de los dispositivos móviles pueden dar acceso a ciertos recursos con el permiso del usuario. Incluso si una aplicación determinada no es maliciosa, la posesión de ciertos permisos podría dar acceso a datos confidenciales o ser utilizada por otra aplicación para elevar el acceso.

4. Amenazas a los comerciantes: malware de Punto de Venta (POS), Man-in-the-Middle y ataques de repetición.

4.1. Malware en terminal POS (contactless):

Se refieren a la carga de malware en las terminales POS, las cuales explotan las vulnerabilidades de seguridad en el comerciante, como el uso

de acceso de escritorio remoto inseguro a los servidores POS. Una vez que el malware POS está instalado en el terminal POS (contactless), el atacante puede configurarlo para robar de forma remota los datos de pago que se procesan a través de los lectores de tarjetas que pueden incluir también datos de tarjetas de banda magnética e información de los chips de las tarjetas de crédito.

4.2. Ataques Man in the middle contra las terminales POS (conctactless) y las conexiones con el servidor POS:

Los ataques son posibles mediante la explotación de vulnerabilidades, como por ejemplo, la falta de seguridad del canal de comunicación utilizado en el punto de venta, la no utilización de canales seguros (SSL / TLS) entre el terminal POS y el servidor POS.

4.3. Ataques de retransmisión contra terminal POS habilitado para NFC:

Un ataque conocido contra la interfaz NFC es el ataque de retransmisión. El software de retransmisión instalado en el teléfono de la víctima puede transmitir comandos y respuestas entre el elemento seguro y un emulador de tarjeta (que se instala como proxy en el dispositivo móvil POS) a través de una red inalámbrica.

5. Amenazas a los proveedores de servicios de pago (PSP):

5.1. Sistemas de pago comprometidos:

Los PSP proporcionan terminales POS sin contacto para pagos móviles (por ejemplo, terminales POS habilitados para NFC) así como servicios de pago para comerciantes mediante el procesamiento de datos de diferentes canales incluyendo pagos con tarjetas, pagos en línea y móviles (sin contacto).

Las plataformas de pago representan un objetivo interesante para los atacantes que buscan comprometer los datos de pago en tránsito de los comerciantes a los diferentes bancos adquirentes. Los atacantes podrían intentar explotar las vulnerabilidades del software que se encuentran en los

terminales POS que los PSP brindan a los comerciantes, en el software de los servidores POS y en los servicios de pagos que se brindan en la plataforma.

5.2. Compromiso de conectividad de datos:

Los atacantes pueden intentar explotar conexiones inseguras (por ejemplo, falta de conexiones seguras en protocolos como SSL / TLS, VPN) para realizar ataques como Man-in-the-middle para falsificar datos confidenciales en tránsito desde sistemas alojados en comercios a la plataforma de pago que se encuentra en los diferentes PSP.

6. **Amenazas a bancos / instituciones financieras:** Son las posibles amenazas y ataques contra los bancos / instituciones financieras que procesan pagos móviles.

6.1. Sistemas de procesamiento de pagos comprometidos:

Los servicios de procesamiento de pagos son probablemente los objetivos principales de los atacantes que buscan obtener grandes cantidades de datos del titular de la tarjeta, ya que los compradores envían solicitudes de autorización de pago y reciben autorizaciones a través de la red de pago. Los atacantes podrían tratar de comprometer los servidores de procesamiento de pagos del banco adquirente desde el interior de la red explotando el acceso no autorizado a las pasarelas de pago, así como remotamente mediante la instalación de puertas traseras y herramientas de acceso remoto a través de la infección de malware de los servidores alojados en la red.

6.2. Compromiso de conectividad de datos:

Los atacantes podrían intentar explotar conexiones punto a punto inseguras (por ejemplo, configuraciones erróneas, vulnerabilidades en conexiones) entre los bancos y los vendedores.

6.3. Repudio de la autorización del pago:

El objetivo de los ataques es repudiar una autorización de pago de un emisor, estos se pueden lograr explotando fallas de diseño en la implementación de los servicios de procesamiento de pagos. Por ejemplo, no utilizar la autenticación del canal o las firmas digitales para validar las aprobaciones de autorización y el proceso de verificación de pagos a través de un canal independiente desde el canal de la red de pago donde se reciben estas autorizaciones.

7. Amenazas a los proveedores de la red de pago:

7.1. Compromiso de los proveedores de servicio de Token (PST)

Para incrementar la seguridad de los pagos móviles muchos proveedores utilizan la tecnología de Tokenización. Este proceso consiste en reemplazar el número de una tarjeta de crédito (número PAN) por un valor llamado “Token”, el cual es usado durante la transacción de pagos manteniendo seguro el número de la tarjeta en todo el proceso. A menudo, estos tokens solo se pueden usar en un dominio específico, como, el sitio web o el canal en línea de un comerciante, lo que limita aún más el riesgo.

El Proveedor de Servicio de Token (PST) es una entidad que genera y administra los tokens en el ecosistema de pagos móviles. Los PST mapean el número de tarjeta original con el token de pagos y los almacenan de forma segura. Además, ofrecen servicios de eliminación (recuperación del PAN desde un token) y validación de integridad de datos.

Si un proveedor de servicios de tokens se viera comprometido, los atacantes probablemente tratarían de obtener las tablas Tokens que proporcionan el token a PAN, CVV y fechas de vencimiento.

7.2. Denegación de servicios de pagos

Los ataques dirigidos a la disponibilidad de servicios alojados en la red de pago tendrán un impacto en la autorización de pagos móviles y posiblemente también en pagos provenientes de otros canales (por ejemplo, el canal de tarjetas) que también utilizan estos servicios.

8. Amenazas a los emisores de tarjetas:

8.1. Compromiso del proceso de autorización de pago:

Una de las principales amenazas para los emisores de tarjetas es a los procesos que validan los datos del titular de la tarjeta y emiten autorizaciones de pago al adquirente. Un atacante interno o un atacante externo que obtuvo acceso a servidores críticos puede intentar eludir los controles (por ejemplo, cambiando los límites de pago de las tarjetas comprometidas que ya están autorizadas y registradas para transacciones de pago móvil).

8.2. Confidencialidad de los datos del titular de la tarjeta:

Las cuentas de crédito y débito que incluyen datos de cuentas bancarias almacenadas en los bancos emisores son un atractivo altamente apetecible para ataques por estafadores y ciberdelincuentes que intentan cometer fraudes con datos de tarjetas de crédito robadas a través de tarjetas falsas y reventa de datos de tarjetas de crédito robadas en el mercado negro.

9. Amenazas a los proveedores de aplicaciones de pago móvil:

9.1. Compromiso de los datos sensibles del titular de la tarjeta:

Los atacantes pueden dirigir su esfuerzo a la obtención de los datos de crédito / débito del titular de la tarjeta y a los datos personales del usuario almacenados por el proveedor del servicio de pago móvil. Esto puede ocurrir durante la transmisión de datos confidenciales del titular de la tarjeta desde el dispositivo móvil a los servidores, como durante el registro del servicio de aplicación de pago móvil con el emisor de la tarjeta.

9.2. Compromiso del perfil de usuario administrador:

Dado que la aplicación móvil tiene acceso a los servidores de pagos móviles, un atacante podría tratar de comprometer este acceso para cometer fraude, como por ejemplo:

a. realizar un acceso no autorizado con el perfil del usuario administrador en el proveedor de pago móvil (por ejemplo, a través de un dispositivo robado / perdido o mediante el acceso en línea a su cuenta);
b. cambiar los datos de contacto de la cuenta, correos electrónicos, números de teléfono, en otros datos.

9.3. Ataques de Denegación de Servicio (DDoS):

Los servicios de billetera digital, incluidos los servicios en la nube utilizados por los proveedores de pagos móviles, pueden ser atacados con DDoS por parte de atacantes que buscan interrumpir los servicios de pago móvil. Estos ataques pueden afectar las transacciones que requieren acceso en tiempo real por la aplicación de pago móvil a los servicios alojados en la nube, como para las inscripciones de las tarjetas de pago móvil.

CAPÍTULO II. SERVICIOS OFRECIDOS Y MARCO REGULATORIO EN EL MUNDO

En este capítulo se presenta a modo de resumen la investigación realizada sobre las distintas implementaciones en el mundo de los modelos de negocios y de regulaciones acerca del dinero y medios de pago electrónicos.

	Principales funcionalidades	**Principales actores que intervienen**	**Operaciones habilitadas**	**Marco regulatorio**
SUDÁFRICA	No requiere que los usuarios estén bancarizados. Apertura de cuenta sin el requisito de presencia física: los clientes pueden abrir cuentas de banca móvil suministrando datos desde lejos a través de un teléfono móvil. Utiliza una tecnología, que sirve de base a todos los teléfonos GSM, denominada "unstructured supplementary services data" (**USSD**).	Banco WIZZIT. WIZZkids: promocionan el producto y ayudan a los clientes no-bancarizados a abrir sus cuentas	Transferencias. Pagos. Retiros de efectivo. Carga de dinero.	En cuanto a la regulación, dado que ese país contempla al dinero electrónico dentro de los servicios bancarios, el Banco Central de Sudáfrica (BCS) es la entidad encargada de emitir la regulación relativa a dinero electrónico. El BCS aprueba la introducción de cualquier forma de moneda electrónica. En ese aspecto, se destaca que todos los participantes en el sistema de pagos móviles están regulados por el Banco Central.

ECUADOR	Apertura de cuentas virtuales a través de mensajes SMS, desde cualquier dispositivo móvil. No se requiere una cuenta en una entidad financiera. Protección con claves personalizadas. En cada operación requiere el ingreso de una clave Cada persona tiene asociada una única cuenta con su cedula de identidad y puede tener hasta 3 monederos móviles. Cada monedero está asociado con un número de teléfono móvil. El sistema funciona a través de la tecnología USSD. Si una persona pierde su teléfono puede bloquear la cuenta de dinero electrónico en cualquier momento llamando al contact center del Sistema. Puede ser canjeado por dinero físico en todo momento. La gente tiene acceso a este medio de pago, incluso en las áreas más alejadas donde no hay presencia del sistema financiero ni cobertura de Internet.	El Banco Central del Ecuador (BCE) es el Administrador del Sistema de Dinero Electrónico (SDE). Operadoras telefónicas fijas y móviles, operadores satelitales, operadores eléctricos, operadores TV, otros.	Transferencias. Pagos. Retiros de efectivo. Carga de dinero.	El BCE emitió la 005-2014-M “Normas para la Gestión de Dinero Electrónico”, la cual regulan el nuevo Sistema de Dinero Electrónico. En la misma se define al “dinero electrónico” como medio de pago electrónico denominado en dólares, gestionado exclusivamente por el Banco Central del Ecuador. Puede ser intercambiado únicamente a través de dispositivos electrónicos. El sistema, entre otros objetivos, busca eficiencia en los sistemas de pagos para promover y coadyuvar a la estabilidad económica del país. No se considera como dinero electrónico a valores monetarios almacenados electrónica o magnéticamente que constituyan instrumentos de prepago de bienes o de servicios exclusivamente en locales del emisor o por un círculo cerrado de agentes económicos

FILIPINAS	En diciembre de 2000 la operadora de telefonía móvil SMART Communications y el Banco de Oro de las Filipinas lanzaron el producto conocido como SMART Money. Está dirigido a la población de bajos ingresos con telefonía móvil prepagada y, ofrece una variedad de opciones de pago, consignación y recargo que vinculan el teléfono móvil del usuario a su cuenta bancaria, todo por medio de un mensaje de texto. Para realizar una compra se envía un mensaje de texto, indicando el valor y el número de la persona a la que se le está haciendo el pago. De esta manera, el sistema debita el valor correspondiente de la cuenta del comprador y, acredita en la cuenta del comerciante. Los compradores con tarjeta débito pueden hacer uso de ella de manera convencional para pagar en el comercio y, el valor será debitado de su cuenta bancaria. Por su lado, la operadora de telefonía móvil Globe Telecom, por medio de un acuerdo con varios bancos comerciales, introdujo al mercado en octubre de 2004 su producto G-cash, el cual al igual que SMART Money convierte el teléfono celular en billetera.	Operadora de telefonía móvil SMART Communications. Banco de Oro de las Filipinas. Operadora de telefonía móvil Globe Telecom.	Hacer depósitos y retiros de efectivo de las cuentas. Pagar en sitios de comercio que formen parte de la red. Transferir entre usuarios de la red: esta operación consiste en transferir dinero, por medio de un mensaje de texto, a otros usuarios.	Luego de varios años observando los productos de pago móvil del país, el Banco Central de Filipinas (BCF) reguló la emisión de dinero electrónico mediante la Circular “649” del año 2009. En la misma se definen 3 posibles tipos de emisores de dinero electrónico: Bancos, instituciones financieras no bancarias y agentes de transferencia de dinero (instituciones financieras no bancarias registradas por el BCF). Además, define también los principales requerimientos para los emisores de dinero electrónico cuyo incumplimiento está sujeto a penalizaciones, entre ellos: - Límite de valor mensual por cliente de PHP 100.000 (USD 2444,99). - El sistema tiene que ser capaz de poder monitorear las transacciones y poder conectar directamente el dinero emitido con los clientes.

BRASIL	Oi Paggo consiste en asociar una tarjeta de crédito Oi, emitida por el Banco do Brasil, al teléfono celular y permite comprar en negocios, por Internet, o en cualquier lugar, al igual que efectuar ventas a través de una comunicación entre el equipo y el puesto de venta. En el caso de compras, el usuario puede realizarlas por proximidad o en forma remota. El usuario informa su número de línea y es cargado por vendedor en el sistema (denominado “Máquina da Cielo”), el comprador, por su parte, digita una contraseña para confirmar el pago y recibe un mensaje de texto como recibo. Para las ventas, el vendedor solo necesita el chip “Oi” (prestador del servicio) en su celular para aceptar el cobro con tarjetas de crédito de las operaciones que realice, cuyo importe es acreditado en su cuenta en el día.	Banco do Brasil. Banco Central del Brasil (BCB).	Depósitos y extracciones. Ejecutar o facilitar la instrucción de pago relacionada a determinado servicio. Administrar las cuentas de pago. Emitir órdenes de pago. Registrar las aceptaciones de los citados medios de pago. Convertir moneda física en moneda electrónica y viceversa. Realizar otras actividades vinculadas la prestación de servicios de pago, que les asigne el BCB.	El 9/10/13 se promulgó la Ley 12.865/13 que regula, entre otros aspectos, los sistemas de pagos mediante celulares. La norma -apodada de “bancarización” también apunta a lograr la inclusión de más del 39 % de la población brasileña (unos 53 millones de personas) que actualmente se encuentra fuera del sistema bancario, de acuerdo con datos del Instituto de Investigación Económica Aplicada. La Ley estipula la figura de “instituciones de pago”, que podrán ofrecer servicios de pagos móviles, pero no así servicios financieros, que seguirán siendo facultad de bancos y otras instituciones financieras. Es decir, los operadores de telecomunicaciones podrán ofrecer pagos móviles, pero no podrán, por ejemplo, realizar préstamos de dinero.

REPÚBLICA DE KENIA	En este modelo no es necesario tener una cuenta bancaria para acceder a tener un servicio de dinero electrónico. Los servicios son ofrecidos por la empresa de telefonía móvil Safaricom, denominada M-Pesa (Pesa en swahilli es efectivo). El procedimiento para realizar una transacción persona a persona consiste en enviar un mensaje SMS o USSD hacia el servidor del Banco desde el menú de la aplicación, en dicho mensaje consta la información del monto a transferir y el número celular telefónico del equipo terminal destino, el integrador del Banco solicita se valide la operación a través de una contraseña asignada previamente a cada usuario; para finalmente, y una vez aceptado el password, comunicar a través del integrador tanto al usuario origen como al destino, el débito y la acreditación correspondientes.	Banco Central de Kenia. Banco Comercial de África. Empresa de telefonía móvil Safaricom.	Permite cargar el celular en cualquier momento y lugar. Facilita el pago de facturas de Persona a Negocio (P2B) por medio de los 350 socios encargados de esto. Provee acceso a cajeros automáticos en una red de más de 650 de ellos. Permite el pago de salarios. Transferencias de dinero al y del Reino Unido.	El Banco Central de Kenia colaboró y participó activamente en el crecimiento de M-Pesa, al autorizar en el 2006 el trabajo de M-Pesa como una entidad de comunicación y no una financiera. El Banco Central, no tiene ningún rol en la supervisión de proveedores de telefonía móvil, los cuales son autorizados por la Comisión de Comunicaciones de Kenia (CCK). El punto de contacto entre el Banco Central y los proveedores de servicios de telefonía móvil se da a través de las licencias que se brindan a los bancos comerciales que ofrecen una plataforma para servicios mediados por telefonía móvil.

UNIÓN EUROPEA	<u>BBVA</u> Para utilizar solo hay que descargarse la aplicación BBVA Wallet, y luego simplemente bastará con acercar el teléfono al terminal de pago Contactless y confirmar tu PIN. <u>Vodafone Wallet</u> La empresa de telefonía Vodafone ha lanzado la aplicación Vodafone Wallet y desde hace un tiempo ya permite pagar con el móvil con cualquier tarjeta Visa o Mastercard, de débito o crédito, independientemente de la entidad bancaria. Permite guardar y utilizar tarjetas bancarias en el móvil sin necesidad de disponer de ellas físicamente.	Banco Central Europeo. Banco central de cada país europeo. Banco BBVA. Banco de Dinamarca. Empresa de telefonía móvil Vodafone.	Permite realizar pagos sin contacto con sus celulares y elegir la tarjeta de crédito que se quiere usar. “Encender” y “apagar” las tarjetas cuando el usuario lo requiera, es decir, poner en funcionamiento o deshabilitar una tarjeta para realizar operaciones. Financiar pagos realizados con tarjetas. Transferencias.	En el año 2009 se emitió la Directiva 2009/110/CE la cual regula el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades. Las actividades que se permite realizar a las entidades de dinero electrónico incluyen el suministro de servicios de pago y la concesión de créditos en relación con dichos pagos.

ARGENTINA	<u>Red Link y Prisma:</u> Modalidades del Pago Electrónico Inmediato (PEI): • Botón de Pago: utilizado para la compra y venta de servicios a través de la web (e-commerce). • El Pos Móvil: es un dispositivo de seguridad (dongle) que se conecta a un teléfono móvil o Tablet, permitiendo el pago mediante una transferencia bancaria. • Billetera electrónica: permite enviar dinero entre personas a través de la web o mediante una aplicación en el celular, sin costo y con acreditación inmediata, hasta $8.060 por día. Para su utilización se debe bajar la aplicación al teléfono móvil, luego registrarse y por último se debe adherir el medio de pago (cuenta bancaria o tarjetas de débitos asociadas). <u>Naranja Mo / Monedero:</u> Es un monedero digital que se puede cargar dinero. <u>PIM:</u> Es una billetera móvil para personas no bancarizadas lanzado por el Banco Nación. Permite enviar y recibir dinero, y pagar servicios con el celular, sin necesidad de tarjeta de crédito ni cuenta bancaria. El comerciante que quiera cobrar deberá solicitar el pago a un teléfono celular. La otra persona envía el dinero ingresando su clave de cuatro dígitos y segundos más tarde ambas personas serán notificadas de la compra a través de un SMS.	Banco Central de la República Argentina (BCRA). Red Link. Prisma. Tarjeta Naranja. Monedero S.A. Nación Servicios.	<u>Red Link y Prisma:</u> Transferencias. Pagos. <u>PIM</u> Transferencias. Pagos. Retiros de efectivo. Carga de dinero. <u>Naranja Mo / Monedero</u> Transferencias. Pagos. Carga de dinero.	A partir de año 2016 el Banco Central de la República Argentina (BCRA) ha emitido distintas comunicaciones que intentan normar el desarrollo y utilización de pagos móviles. Se creó un nuevo canal de pago, a través del cual las entidades financieras deben ofrecer la modalidad de Pago Electrónico Inmediato (PEI), permitiendo realizar pagos a través del celular, tableta o computadora móvil, con débito y crédito en línea, en cualquier lugar a través de tres modalidades: el POS Móvil, Botón de Pago y Billetera Electrónica.

CAPÍTULO III. REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN Y CONTROL DE LOS RIESGOS RELACIONADOS CON EL DINERO ELECTRÓNICO

Luego de analizar como primer punto a las principales amenazas a las que se está expuesto al realizar pagos móviles y como segundo punto el estado de las distintas implementaciones del dinero electrónico en el mundo, el objetivo del presente trabajo final es desarrollar una serie de lineamientos que definan requisitos mínimos de seguridad y tecnología sobre la implementación del dinero electrónico en la Argentina:

1. Disposiciones generales.

1.1. Glosario de términos utilizados.

IMEI: (del inglés International Mobile Station Equipment Identity, identidad internacional de equipo móvil) es un código USSD pregrabado en los teléfonos móviles GSM. Este código identifica al aparato de forma exclusiva a nivel mundial, y es transmitido por el aparato a la red al conectarse a esta.

Identificación positiva: Comprende a los procesos de verificación y validación de la identidad que reducen la incertidumbre mediante el uso de técnicas complementarias a las habitualmente usadas en la presentación de credenciales o para la entrega o renovación de las mismas.

Se incluyen, a algunas de los siguientes métodos: verificación de la identidad de manera personal, mediante firma holográfica y presentación de documento de identidad, mediante serie de preguntas desafío de contexto variable, entre otros.

Autenticación: es un proceso que permite comprobar la identidad de una persona. La Autenticación fuerte, es un proceso basado en el uso de dos o más de los siguientes elementos, clasificados como conocimiento, posesión e inherencia:

i) algo que solo conoce el usuario, por ejemplo, una contraseña, código o número de identificación personal fijos;

ii) algo que solo posee el usuario, por ejemplo, token, tarjeta inteligente, teléfono móvil;

iii) algo que caracteriza al propio usuario, por ejemplo, una característica biométrica, como su huella dactilar. Además, los elementos seleccionados deben ser independientes entre sí; es decir, la violación de uno no debe comprometer la seguridad de los otros.

Terminal POS: son dispositivos que permiten la utilización de distintos medios de pago electrónico (Tarjetas de Débito/Crédito) para el pago de servicios u operaciones financieras que generen un débito o un crédito en las cuentas bancarias que el cliente posee con el emisor y que confirman tales operaciones mediante la comunicación local o remota con un centro de procesamiento de la entidad.

Técnicas de jailbreaking: son métodos utilizados para eludir las medidas de seguridad impuestas por los fabricantes de los teléfonos móviles y asi poder instalar, modificar y cambiar cualquier característica/servicio/aplicación del sistema operativo.

NFC: Es un sistema de comunicación de campo cercano utilizado para intercambiar información entre dos dispositivos. Ambos deben casi tocarse para poder llevar a cabo la acción. Pueden enviarse información entre sí o puede que solo uno de ellos la mande.

2. Condiciones para funcionar

2.1. Operaciones con dinero electrónico.

Las operaciones que pueden realizarse son:
a) Carga de dinero.
b) Descarga de dinero.
c) Pagos de servicios / Compra de bienes.

d) Transferencia de dinero entre cuentas propias y a terceros.
e) Consultas sobre saldos y transacciones.

2.2. Soportes para uso de dinero electrónico.

Los soportes mediante los cuales se puede hacer uso del dinero electrónico serán solo los Teléfonos móviles. Los mismos deberán contar con plataformas tecnológicas que permitan realizar transacciones en línea y de manera segura, entre los diferentes tipos de usuarios y participantes de la red de dinero electrónico. Para ello se deberán definir mecanismos de control del grado de exposición a potenciales riesgos inherentes al uso del dinero electrónico, considerando las amenazas y las vulnerabilidades asociadas al mismo, como por ejemplo: Amenazas a los usuarios (Phishing e ingeniería social, Instalación de aplicaciones fraudulentas y malware), amenazas a los dispositivos móviles (Acceso no autorizados), Amenazas a las aplicaciones de pagos móviles (Ingeniería inversa del código, Explotación de vulnerabilidades), Amenazas a bancos / instituciones financieras (Compromiso de conectividad de datos, Repudio de la autorización del pago), Amenazas a los proveedores de aplicaciones de pago móvil (Compromiso de los datos sensibles del titular de la tarjeta, Ataques de Denegación de Servicio (DDoS)).

2.3. Cuentas de dinero electrónico.

Se consideran “cuentas de dinero electrónico” a aquellas cuentas que los emisores de dinero electrónico ponen a disposición de personas, y que cumplen con las siguientes condiciones:

a) Son abiertas por personas nacionales o extranjeras residentes.
b) Solo puede ser utilizadas en la moneda nacional de la República Argentina.
c) Pueden estar asociadas a una cuenta bancaria de una entidad financiera o pueden ser cuentas independientes (cuentas virtuales) administradas por los emisores de dinero electrónico.

2.4. Transacciones

Para todas las transacciones que desean cursar por medio de los teléfonos móviles se deberán utilizar técnicas fuertes de autenticación del usuario, las cuales se detallan más adelante.

2.5. Adhesión al servicio de dinero electrónico

La suscripción a cuentas de dinero electrónico deberá ser a través de los emisores de dinero electrónico, y la cuenta deberá estar asociada al titular de la línea del teléfono móvil con la cual se desea operar. La adhesión a los soportes que se necesiten para su uso, debe realizarse con un mecanismo que utilice la identificación positiva del usuario. Se entiende por identificación positiva a la utilización de algunas de las siguientes técnicas:

- Cuestionarios predefinidos y que se pueda realizar una validación automática;
- Presentación de documentos de identidad emitidos por autoridad nacional;
- Comparación de firmas ológráficas.

Se debe garantizar que se suministre la información a los usuarios, la cual contenga detalles específicos relacionados con los servicios de dinero electrónico se contratarán. Estos deberían incluir como mínimo:

- información clara sobre cualquier requisito en términos de equipo móvil del cliente, software u otras herramientas necesarias (por ejemplo, software antivirus, firewalls);
- pautas para el uso correcto y seguro de los factores de autenticación;
- una descripción detallada del procedimiento de cada transacción habilitada;
- pautas para el uso correcto y seguro de todo el hardware y software proporcionado al usuario;

- el procedimiento a seguir en caso de pérdida o robo de las credenciales de seguridad o del hardware o software del cliente, incluido el dispositivo móvil;
- el procedimiento que debe seguir el cliente si cambia su número de teléfono o adquiere un nuevo dispositivo móvil.

3. Protección de Activos de Información

3.1. Definiciones Generales

Se deben implementar medidas de seguridad proporcionales con los riesgos identificados. Estas medidas deberían incorporar múltiples capas de seguridad, por lo que la falla de una línea de defensa se mitiga con la siguiente línea de defensa. Deben suponer que los dispositivos móviles están expuestos a vulnerabilidades de seguridad y se deberán tomar las medidas apropiadas al diseñar, desarrollar y mantener los servicios de pago móvil.

3.2. Gobierno

Se deberá crear un área que gestione la protección de los activos de información dentro de la estructura de los emisores de dinero electrónico, con el fin de establecer los mecanismos para la gestión y el control de la seguridad sobre el acceso lógico y físico a sus distintos ambientes tecnológicos y recursos de información relacionados con el dinero electrónico.

3.3 Políticas

Se deberán crear políticas de seguridad para establecer cuáles serán los lineamientos generales que se deben perseguir para cumplir los objetivos de seguridad de la información propuestos.

Las mismas deben abordar el diseño y la implementación adecuados y seguros de todos los componentes de los servicios de pago móvil. Además, deben tener en cuenta los riesgos derivados de la dependencia de terceros

(por ejemplo, fabricantes de dispositivos móviles, desarrolladores de aplicaciones) al diseñar e implementar su política de seguridad para dinero electrónico y pagos móviles.

Se deberán documentar adecuadamente, revisarse regularmente y ser aprobadas por las instancias superiores.

3.4 Análisis de riesgos

Se deberá realizar una gestión de riesgos de manera de poder identificar, evaluar y reducir los riesgos de TI relacionados con el dinero electrónico de forma continua. Los mismos se deberán centrar en la mitigación de los riesgos del dinero electrónico y aplicaciones de pagos móviles e identificar medidas que incluyan la detección de posibles daños a los datos y el fraude.

Los riesgos se revisarán en cada cambio que se introduzca en la aplicación móvil para identificar debilidades / brechas y vulnerabilidades de control. Estas revisiones de riesgos deberán ser continuas, teniendo en cuenta las amenazas emergentes y en evolución dirigidas al ecosistema de aplicaciones de pago móvil. Asimismo, deben estar detalladamente documentados.

3.5 Medidas mínimas de seguridad

3.5.1 Mecanismos de identificación y autenticación de usuarios

Todas las operaciones de dinero electrónico en la etapa de iniciación y aprobación, deberán utilizar una autenticación fuerte del usuario, es decir, utilizar la combinación de al menos dos factores de autenticación distintos.

Los factores de autenticación se pueden dividir en:

1) Algo que solo conoce el usuario, por ejemplo: contraseña, PIN, datos personales, entre otros.

2) Algo que solo el usuario tiene, por ejemplo: token, tarjeta magnética, teléfono móvil, entre otros.
3) Algo que caracteriza al propio usuario, por ejemplo: una característica biométrica, como su huella dactilar, reconocimiento facial, del iris, de la voz, entre otros.

Solo será permitido el almacenamiento de los valores de los factores de autenticación cuando estos se encuentren protegidos por mecanismos criptográficos (algoritmos de cifrado no menores a 3DES o AES) que impidan su conocimiento a terceros y solo con propósito de verificación automática de las credenciales presentadas por el usuario al operar con las cuentas de dinero electrónico.

Los factores de autenticación basados en “algo que solo conoce el usuario” y “algo que caracteriza al propio usuario” deben bloquearse luego de 3 (tres) intentos fallidos consecutivos de inicio de sesión. Luego se deberá realizar la autenticación positiva del usuario para el desbloqueo de la cuenta de dinero electrónico. Asimismo, se deben bloquear el acceso a las aplicaciones de pago móvil luego de no más de cinco intentos fallidos consecutivos de inicio de sesión, informar al usuario de la situación y realizar la autenticación positiva para el desbloqueo.

Características propias que deben tener cada factor:

“Algo que solo conoce el usuario”

Deben estar protegidos los valores del factor durante la generación, uso y transporte por algunas de las siguientes medidas de seguridad:
a. Cifrado no menor a 3DES ó AES.
b. Funciones de “hashing” no menor a SHA2.

En la implementación del factor mencionado se debe considerar:

- Los valores solo deben ser conocidos por sus propietarios durante su generación y uso;

- El cambio obligatorio de los valores en el primer inicio de sesión;
- Se debe tener un registro de los últimos 12 (doce) valores para que se evite su reutilización;
- La renovación de los valores debe ser personal o debe haber la mínima intervención de un operador durante el proceso;
- Los valores deben tener una longitud no menor a 8 (ocho) caracteres;
- Se debe controlar la composición de los valores, teniendo una complejidad tal que incluya al menos la combinación de tres de los siguientes atributos:
    - Letras minúsculas.
    - Letras mayúsculas.
    - Caracteres especiales.
    - Números.
    - No contener más de dos caracteres iguales y consecutivos.
- El intervalo de caducidad debe ser de 45 (cuarenta y cinco) días o al vencimiento del factor basado en “algo que tiene” asociado a la cuenta de dinero electrónico;
- La desconexión automática de la sesión en la aplicación/sistema/red por tiempo de inactividad a los 15 (quince) minutos;
- Se debe prevenir que los valores no estén asociados a datos personales públicos del cliente.

“Algo que solo el usuario tiene”

Los procesos de entrega, habilitación y rehabilitación del factor se deben realizar con previa identificación positiva del usuario. Asimismo, sólo podrán estar vinculados durante su uso a una única persona de forma individual e intransferible.

En el caso de las tarjetas magnéticas, deben contar con códigos de seguridad renovables diferentes en cada renovación. Si los mismos son de banda magnética, deben contar un código de verificación no visible (almacenado en la banda) y un código de verificación de la transacción

visible impreso en los mismos. En el caso que las mismas posean chip, deben contar con un mecanismo de autenticación dinámica y un cifrado de los datos almacenados en el circuito integrado.

"Algo que caracteriza al propio usuario"

Los datos biométricos utilizados en los procesos de autenticación y validación de los usuarios, se considerarán como datos personales, por lo cual se deben cumplimentar los requisitos previstos en la Ley 25.326 de Protección de Datos Personales (y modificatorias).

Deben estar protegidos durante la generación, uso y transporte por algunas de las siguientes medidas de seguridad:
a. Cifrado no menor a 3DES ó AES.
b. Funciones de "hashing" no menor a SHA2.

Por otro lado, la protección de dichos datos siempre se debe llevar a cabo con el deber de especificar la finalidad de su uso. Asimismo, para las situaciones que se solicite o se produzca la baja del usuario, sus datos deben eliminarse correctamente y se deberán presentar evidencias de ello.

3.5.2 Teléfono móvil

Se recomiendan que los usuarios de los dispositivos adopten las siguientes prácticas:

- Actualizar el sistema operativo regularmente, tan pronto como el proveedor del sistema operativo libere una actualización disponible;
- Tener implementado el bloqueo de dispositivo remoto y la limpieza remota de los datos vinculados con las cuentas de dinero electrónico (dichos procedimientos borran todos los datos del teléfono móvil, como las aplicaciones instaladas, las fotos y la información personal);
- No realizar ningún mecanismo para alterar el dispositivo con el propósito de obtener privilegios de administrador del mismo, utilizando algunas de las técnicas de jailbreaking.

En los casos que el usuario desee cambiar el operador de telefonía móvil o el teléfono con credenciales (por ejemplo, tarjeta SD, tarjeta SIM, etc.), la transferencia de dichas credenciales de usuario a los nuevos dispositivos / entorno debe llevarse a cabo de manera segura (por ejemplo, a través de agentes de confianza, servicios, etc.).

3.5.3 Aplicación de dinero electrónico para pagos móviles

Las aplicaciones utilizadas para brindar los servicios de dinero electrónico en dispositivos móviles deben garantizar la vinculación única entre la “aplicación”, el cliente y el dispositivo. Utilizando el identificador IMEI (International Mobile Station Equipment Identity) o código único de identificación del dispositivo, y un código de seguridad que solo conoce el usuario o identificación biométrica del mismo.

Al diseñar, desarrollar y mantener las aplicaciones, se deberán separar adecuadamente los entornos de tecnología de la información (por ejemplo, entornos de desarrollo, prueba y producción) y prestar especial atención a la adecuada segregación de funciones y derechos de acceso, incluida la implementación adecuada del principio de "menor privilegio".

Las aplicaciones deben alojarse en sitios que posean adecuadas medidas de seguridad acordes con la política de los emisores de dinero electrónico y estas deben ser informadas al consumidor de servicios de manera fehaciente. Se debe verificar regularmente que las mismas estén actualizadas con los parches de seguridad críticos.

El proceso de gestión de cambios de las aplicaciones, debe contar con estrictos mecanismos de control a lo largo de todo el ciclo de vida. Todos los cambios deben estar rigurosamente detallados y documentados. Asimismo, se deben efectuar auditorias frecuentes al proceso de gestión de control, con el fin de detectar posibles debilidades en el mismo.

Se deberá tener la capacidad de desactivar la aplicación de pago móvil en teléfonos que, por ejemplo, se han perdido, han sido robados o mal utilizados.

3.6 Monitoreo y control transaccional

Se deberán utilizar mecanismos de monitoreo de transacciones para prevenir, detectar y bloquear transacciones de pagos fraudulentas, sospechosas o de alto riesgo. Se deberán basar, por ejemplo, en reglas parametrizadas (como listas negras de datos potencialmente comprometidos o robados), velocidad de transacción atípica o datos de transacciones anormales (como transacciones realizadas en ubicaciones geográficamente distantes entre sí en un corto período de tiempo), etc. Tales sistemas también deberán detectar signos de infección de malware y escenarios conocidos de fraude.

Se deberá definir por cada usuario un perfil/patrón de comportamiento, en el cual estén determinados los límites y umbrales de uso, con el fin de poder detectar posibles comportamientos inesperados y así tomar acciones en función de las alertas detectadas.

3.7 Trazabilidad

Se deberá garantizar que los sistemas/aplicaciones/servicios por los cuales se cursen transacciones de pagos móviles, incorporen mecanismos de seguridad para el registro detallado de los datos de transacción, incluido el número secuencial de la transacción, fecha y hora, usuarios involucrados, los cambios de parametrización, el acceso a los datos, entre otros.

Se deberán implementar mecanismos para asegurar la no alteración de la fecha y hora de los servidores que dan soporte a la red de pagos móviles, como, por ejemplo, la utilización del protocolo NTP para sincronizar los relojes de tiempo de los equipos de una red de comunicaciones.

Se deberán tener archivos de registro robustos que permitan la recuperación de datos históricos, incluida una pista de auditoría completa de altas, modificaciones o borrado de transacciones.

3.8 Gestión de incidentes

Se deberá establecer un marco metodológico el cual permita llevar adelante la identificación, gestión, registro, comunicación y monitoreo de los incidentes de seguridad. Para ello, se deberán establecer adecuados mecanismos que permitan coordinar las actividades de detección, prevención y corrección, como así también el establecimiento de roles y responsabilidades. Se deberán considerar mínimamente las siguientes etapas:

- Detección;
- Análisis;
- Contención;
- Erradicación; y
- Recuperación.

A fin de contribuir en los procesos de análisis y mitigación del riesgo, se deberá contar con una base central de eventos e incidentes que contenga la identificación de las amenazas y los controles aplicados, permitiendo la supervisión continua y directa sobre el tratamiento de los incidentes de seguridad detectados.

Por otro lado, se deberán contar con mecanismos que permitan utilizar el conocimiento obtenido del análisis y resolución de incidentes en la disminución de la probabilidad e impacto de futuros incidentes.

CONCLUSIONES

En vista de que el marco regulatorio del mundo del dinero electrónico y pagos móviles se encuentra en proceso de desarrollo, es de vital importancia que se elaboren directrices para que todos los actores del ecosistema de pagos móviles (Emisores de tarjetas, Proveedores de servicios bancarios y/o aplicaciones, Administradores de redes de pago, Entidades financieras, Comerciantes y Usuarios) puedan aplicar controles de seguridad que, de implementarse, ayudarían a garantizar que las transacciones de pago estén protegidas contra las amenazas a las cuales se encuentran expuestas. En mi opinión la implementación de medidas de seguridad en todo el ciclo de vida de una transacción de pago móvil es un proceso global que debe abarcar a todos los actores antes mencionados. Y ante la pregunta ¿Es seguro pagar con un teléfono móvil?, afirmaría que sí, y les diría a los nuevos usuarios de servicios de pagos móviles que dejarán de creer que las nuevas formas de pago, como el pago con teléfonos móviles, son menos seguras que pagar en efectivo o con tarjeta.

Este trabajo tiene precisamente como objetivo principal definir las medidas mínimas que deben seguir los distintos actores que intervienen en un pago móvil, por ejemplo podemos mencionar:

- Consideraciones generales, de qué forma las aplicaciones y las transacciones se aseguran y confirman y como se identifica de forma segura al usuario;

- Para los clientes se definieron requerimientos para un uso seguro de los dispositivos y aplicaciones;

- Los proveedores deben asegurarse de que su sistema operativo se actualice periódicamente para solucionar cualquier problema de seguridad identificado, lo que puede poner en peligro la integridad, la confidencialidad o la disponibilidad del sistema o de los datos;

- Los desarrolladores de aplicaciones de pago móvil deberían proporcionar visibilidad a las medidas de seguridad aplicadas en la aplicación al ofrecerla a los clientes.

Las instituciones que quieran implementar nuevos medios de pagos, como los que se citan en el presente trabajo, no solo deberán implementar las medidas de seguridad mencionadas, sino que las deberán acompañar de un marco integral de gestión de la seguridad de la información. Con el fin de

abarcar todos los procesos y recursos que intervengan en el ecosistema de pagos móviles.

ANEXO I – INVESTIGACIÓN SOBRE SERVICIOS OFRECIDOS Y MARCO REGULATORIO EN EL MUNDO

SUDÁFRICA

WIZZIT es un concepto bancario, en base a telefonía celular, que tiene como objetivo brindar servicios a sudafricanos no-bancarizados o sub-bancarizados. El banco WIZZIT opera como una división del South African Bank de Athens Limited y posee licencia para captar depósitos. La marca y las operaciones son gestionadas de forma separada por un grupo de empresa independientes, con participación accionarial de otras entidades. El vínculo con un banco que le autoriza a gestionar y liquidar las operaciones, permite a Wizzit ofrecer a sus clientes acceso al sistema de pagos electrónicos. La iniciativa fue lanzada en noviembre del 2004, siendo la misión del banco hacer una diferencia en las vidas de personas no-bancarizadas. En la actualidad, ofrece servicios bancarios móviles, en base a telefonía celular, para distintos tipos de redes y tipo tarjeta SIM.

Sus principales características son:

• **No requiere que los usuarios tengan una cuenta bancaria** y es compatible con la nueva generación de teléfonos celulares, de baja funcionalidad, populares en las comunidades de bajos ingresos.

• Adicionalmente a realizar transacciones de celular a celular, a los titulares de cuentas WIZZIT se les otorga una tarjeta de débito Maestro, que puede ser utilizada en cualquier cajero automático o minorista.

• **Cobra tarifas por transacción celular**, que van desde 99c hasta un máximo de ZAR4.99, indistintamente del valor de la transacción.

• Utiliza una tecnología, que sirve de base a todos los teléfonos GSM, denominada “unstructured supplementary services data” (**USSD**). El tiempo de respuesta, para los servicios en base a USSD interactivo, es generalmente más rápido que el utilizado por “short message service” (SMS). USSD es también más barato que SMS.[6]

• Permite realizar operaciones con otras instituciones del sistema financiero gracias a que está interconectado con la Cámara de Compensación Interbancaria de Sudáfrica.

• **Para abrir una cuenta sólo se requiere copia del documento de identidad.** Se permitió la apertura de cuenta sin el requisito de presencia física: los clientes pueden abrir cuentas de banca móvil suministrando datos desde lejos a través de un teléfono móvil. Estos datos son validados contra una fuente externa de información. Para limitar el riesgo se establecieron topes en los montos de las transacciones permitidas en las cuentas abiertas bajo esta modalidad.

• Debido a que WIZZIT no tiene sucursales, los clientes abren sus cuentas a través de agentes de campo, denominados WIZZkids (Chicos WIZZ) que, anteriormente, eran miembros desempleados de comunidades locales. Los WIZZkids, promocionan el producto y ayudan a los clientes no-bancarizados a abrir sus cuentas.

En cuanto a la regulación, dado que ese país contempla al dinero electrónico dentro de los servicios bancarios, el Banco Central de Sudáfrica (BCS) es la entidad encargada de emitir la regulación relativa a dinero electrónico. El BCS aprueba la introducción de cualquier forma de moneda electrónica. En ese aspecto, se destaca que todos los participantes en el sistema de pagos móviles están regulados por el Banco Central. Entre otros temas se norman quiénes pueden prestar servicios de dinero electrónico (sólo los bancos), el manejo del dinero, los montos transados, etc.).

Las transacciones posibles son:

- Transferencias de dinero desde una cuenta WIZZIT, a titulares de cuenta de cualquier otro banco.
- Pagos (almacenes de ropa, electricidad, obligaciones y cualquier otra cuentacelular).

- Retiros de efectivo, de cualquier cajero automático alrededor del mundo, que muestre el signo Maestro.
- Carga de dinero.

ECUADOR

El Banco Central del Ecuador (BCE) cerró un acuerdo con las tres operadoras móviles (Movistar, Claro y CNT) para conectarlas a la plataforma única, provista por el consorcio Adexus- In Switch. Las personas interesadas pueden abrir sus cuentas virtuales a través de mensajes SMS, desde cualquier dispositivo móvil. El cliente posee una cuenta de dinero electrónico en el BCE y desde el teléfono se puede interactuar con dicha cuenta. Los dólares entregados para la carga tienen como respaldo los activos del BCE. (Billetes físicos, oro, depósitos de corto plazo en el exterior).

Características:

- No requiere internet ni tener un Smartphone.
- Funciona las 24 horas los 7 días de la semana.
- Funciona con todas las compañías telefónicas.
- Protección con claves personalizadas. En cada operación requiere el ingreso de una clave.
- Limites Transacciones hasta USD 9000 por personas físicas. Para limitar que las operaciones se usen en el mercado minorista. También con esto se disminuye el uso del sistema para Lavado de Dinero.
- En todo momento se puede descargar el dinero físico.

Actores:

1. Administrador del Sistema de Dinero Electrónico: El Banco Central del Ecuador es el responsable de, planificar, controlar, establecer normas de funcionamiento operativo y gestionar eficientemente el Sistema de Dinero Electrónico.
2. Entidades reguladoras: Son la Junta de Política y Regulación Monetaria y Financiera, Consejo Nacional de Telecomunicaciones, Secretaría

Nacional de Telecomunicaciones, Superintendencia de Telecomunicaciones, Superintendencia de Bancos, Superintendencia de Compañías Valores y Seguros, Superintendencia de Economía Popular y Solidaria, y la Superintendencia de Control del Poder de Mercado, en el ámbito de sus competencias.

3. Canales tecnológicos: Operadoras telefónicas fijas y móviles, operadores satelitales, operadores eléctricos, operadores TV, otros.
4. Macroagentes: son empresas, organizaciones e instituciones públicas y privadas; instituciones financieras; forman una red para atención al cliente y en donde los mismos pueden adquirir dinero móvil, utilizarlo o convertirlo en especies monetarias conforme los procedimientos que establecidos por el BCE. Todos poseen cuentas corrientes en el BCE.
5. Centros transaccionales: Todas las oficinas de atención de los Macroagentes, directas o corresponsales.
6. Usuarios: Son aquellas personas naturales o jurídicas, públicas o privadas, inscritas en el Sistema de Dinero Electrónico, que mantengan una CUENTA DE DINERO ELECTRÓNICO.

Tipos de cuentas:

Cuentas para personas físicas: cada persona tiene asociada una única cuenta de DE con su cedula de identidad y puede tener hasta 3 monederos móviles. Cada monedero está asociado con un número de teléfono móvil.
Cuentas para personas jurídicas: cada persona tiene asociada una única cuenta de DE con su cedula de identidad y puede tener ilimitados monederos móviles.

Seguridad:

El Banco Central del Ecuador utiliza estándares internacionales de seguridad. El Sistema de Dinero Electrónico funcionará a través de la tecnología USSD. Además, no almacena claves, la clave es propia del usuario y todos los procedimientos o transacciones requieren de la clave de seguridad del usuario para ser validadas. Si una persona pierde su teléfono puede bloquear la cuenta de dinero electrónico en cualquier momento llamando al contact center del Sistema. En función al Artículo 1 de la

Regulación 055-2014 emitida por el Directorio del Banco Central del Ecuador, se define al dinero electrónico como:

“ 1.1 DINERO ELECTRÓNICO.- Es el valor monetario equivalente al valor expresado en la moneda de curso legal del país que: a) Se almacena e intercambia únicamente a través de dispositivos electrónicos, móviles, electromecánicos, fijos, tarjetas inteligentes, computadoras y otros, producto del avance tecnológico; b) Es aceptado con poder liberatorio ilimitado y de libre circulación, reconocido como medio de pago por todos los Agentes Económicos en el Ecuador y para el pago de obligaciones públicas de conformidad con las normas que dicte el Organismo Regulatorio Competente; c) Es convertible en efectivo a valor nominal; y, d) Es emitido privativamente por el Banco Central del Ecuador sobre la base de las políticas y Regulaciones que expida el Organismo Regulatorio Competente y por ende se registra en el pasivo de la Institución.

1.2 NO CONSTITUYE DINERO ELECTRÓNICO a) Cualquier forma de depósito o captación detallada en los términos que constan en el artículo 51 de la Ley General de Instituciones del Sistema Financiero. b) Los valores monetarios almacenados en medios electrónicos o magnéticos que constituyan instrumentos de prepago de bienes o de servicios que puedan ser adquiridos exclusivamente en locales del emisor de los instrumentos, o sea aceptado como pago únicamente por un círculo cerrado de agentes económicos. Para tal efecto el emisor de este tipo de medio de pago electrónico deberá cumplir las disposiciones que al respecto emita el Directorio del Banco Central del Ecuador, en ejercicio de sus funciones que constan en el literal l) del artículo 60 de la Ley de Régimen Monetario y Banco del Estado.

1.3 SISTEMA DE DINERO ELECTRÓNICO (SDE).- Es el conjunto de operaciones, mecanismos y normativas que facilitan los flujos, almacenamiento y transferencias en tiempo real, entre los distintos Agentes Económicos, a través del uso de: dispositivos electrónicos, electromecánicos, móviles, fijos, tarjetas inteligentes, computadoras y otros que se incorporen producto del avance tecnológico. “

Por otro lado, definen al Monedero Electrónico como:

“MONEDERO ELECTRÓNICO (MOE). - Es el registro virtual asociado a una cuenta de Dinero Electrónico en la que constarán las transacciones efectuadas en el sistema mediante un dispositivo móvil u otros mecanismos definidos para su uso. Existirán tantos MOE como dispositivos tengan los USUARIOS. Así también cada MOE deberá estar asociado a una sola cuenta de dinero electrónico.”

Las características que tiene el modelo implementado en el Ecuador son:

- Es un medio de pago, como lo son las monedas fraccionarias emitidas por el BCE, las tarjetas de débito emitidas por los bancos, los cheques o las transferencias electrónicas.
- Permite realizar pagos en dólares de los Estados Unidos de América a través de teléfonos celulares sin la necesidad de contar con Internet ni con una cuenta en una entidad financiera.
- Evita cambiar billetes por monedas fraccionarias, ya que se puede pagar el precio exacto con precisión de hasta un centavo, sin la necesidad de buscar “sueltos”.
- Puede ser canjeado por dinero físico en todo momento.
- La gente tiene acceso a este medio de pago, incluso en las áreas más alejadas donde no hay presencia del sistema financiero ni cobertura de Internet.
- Las empresas facilitan sus transacciones y reducen sus costos.
- El Estado reduce sus gastos en reposición de especies monetarias deterioradas.
- El dinero electrónico está respaldado con activos del BCE.
- No se requiere una cuenta en una entidad financiera.
- No se deteriora, no pesa y evita cambiar billetes por monedas fraccionarias debido a que se puede pagar el precio exacto.
- El dinero electrónico es un medio seguro porque no requiere llevar dinero físico. Además, está protegido por un sistema de seguridad con claves personales, y tiene trazabilidad (se sabe de dónde viene y a dónde va).
- Está disponible a través de un dispositivo móvil celular.

- Su uso no implica cobro de altas tarifas, pues se trata de un servicio público, el cual permite la inclusión financiera.
- Al ser administrado por el BCE se garantiza la interoperabilidad. Es decir, puede acceder desde un teléfono de cualquier operadora, sin consumir saldo celular, ni mensajes. [4]

FILIPINAS

En diciembre de 2000 la operadora de telefonía móvil SMART Communications y el Banco de Oro de las Filipinas lanzaron el producto conocido como SMART Money. Está dirigido a la población de bajos ingresos con telefonía móvil prepagada y, ofrece una variedad de opciones de pago, consignación y recargo que vinculan el teléfono móvil del usuario a su cuenta bancaria, todo por medio de un mensaje de texto. El sistema ofrece dos alternativas de uso, una de banca móvil y otra de e-money (monedero electrónico). La banca móvil admite a los clientes hacer recargas, pago de facturas, transferir fondos a terceros que dispongan de una cuenta Smart, y otras operaciones que se podrían realizar a través de un cajero automático. En cambio, el e-money tiene asociado una tarjeta recargable válida para cualquier cajero automático o banco asociado, y puede ser usada para hacer cualquier pago en aquellos lugares donde acepten Mastercard.

Las personas interesadas en hacer uso del servicio de SMART Money deben registrarse solo una vez en el sistema SMART y, lo pueden hacer de dos maneras. La primera consiste en acercarse a una oficina SMART, donde deben llevar su teléfono móvil y tener su número de identificación nacional, también pueden hacerlo en el Banco. Por su lado, la operadora de telefonía móvil Globe Telecom, por medio de un acuerdo con varios bancos comerciales, introdujo al mercado en octubre de 2004 su producto G-cash, el cual al igual que SMART Money convierte el teléfono celular en billetera.

Las transacciones permitidas son:

- Hacer depósitos en la cuenta SMART: éstos se pueden realizar en una sucursal, en una oficina del Banco de Oro o en puntos de comercio autorizados que también hagan parte de la red de SMART Money. El

depósito se puede hacer por medio de la tarjeta débito si el usuario la posee, de lo contrario se debe llenar un recibo de consignación. En cualquier caso, el depositante debe mostrar su número de identificación.

- Realizar retiros, de la misma forma en que se hace el depósito. Ahora, los usuarios con tarjeta débito también pueden usarla en cajeros automáticos para hacer retiros de dinero.
- Pagar en sitios de comercio que formen parte de la red de SMART Money: el comprador envía un mensaje de texto, indicando el valor de la compra y el número de la persona a la que se le está haciendo el pago. De esta manera, el sistema debita el valor correspondiente de la cuenta del comprador y, acredita en la cuenta del comerciante. Los compradores con tarjeta débito pueden hacer uso de ella de manera convencional para pagar en el comercio y, el valor será debitado de su cuenta bancaria.
- Transferir entre usuarios de SMART Money: esta operación consiste en transferir dinero, por medio de un mensaje de texto, a otros usuarios de SMART Money. Con el envío de un mensaje de texto una persona puede transferir dinero a la cuenta SMART de otro usuario indicando la cantidad y la persona a la cual se le está haciendo la transferencia.
- Recargar tiempo al aire: teniendo en cuenta que el servicio SMART Money es para personas con telefonía móvil prepagada, los usuarios tienen la opción de recargar la tarjeta prepago o los minutos disponibles al mandar un mensaje de texto. La cantidad de dinero usada para recargar tiempo al aire se debita de la cuenta del usuario. Ahora, los clientes también pueden comprar tiempo al aire de comerciantes autorizados. Éste servicio es conocido cómo SMART Load, y reemplaza la tarjeta prepaga. El comerciante recibe efectivo o una transferencia monetaria, mediante un mensaje de texto del cliente y, a cambio el comerciante envía otro mensaje de texto al cliente en donde recarga los minutos al celular.[7]

Luego de varios años observando los productos de pago móvil del país, el Banco Central de Filipinas (BCF) reguló la emisión de dinero electrónico mediante la Circular “649” del año 2009. En la misma se definen 3 posibles tipos de emisores de dinero electrónico: Bancos, instituciones

financieras no bancarias y agentes de transferencia de dinero (instituciones financieras no bancarias registradas por el BCF).

Además, define también los principales requerimientos para los emisores de dinero electrónico cuyo incumplimiento está sujeto a penalizaciones, entre ellos:
- Límite de valor mensual por cliente de PHP 100.000 (USD 2444,99) independientemente del número de productos de que disponga.
- Sistema de mantenimiento de registros tanto del dinero electrónico emitido, como de la identidad de los clientes y sus balances. Además, el sistema tiene que ser capaz de poder monitorear las transacciones y poder conectar directamente el dinero emitido con los clientes.
- El dinero electrónico debe tener un valor nominal invariable. [8]

BRASIL

Oi Paggo consiste en asociar una tarjeta de crédito Oi, emitida por el Banco do Brasil, al teléfono celular y permite comprar en negocios, por Internet, o en cualquier lugar, al igual que efectuar ventas a través de una comunicación entre el equipo y el puesto de venta. Con este servicio, se proporciona un medio de pago de crédito con una factura independiente de la del teléfono celular, sin necesidad de que el cliente disponga de una cuenta bancaria ni de que el comerciante tenga instalado un TPV específico (POS). Sin embargo, al tratarse de un medio de pago de crédito, el proceso de registro está sujeto a un análisis de crédito (a partir de un comprobante de renta) y a una identificación mediante RG (registro general) y CPF (registro de personas físicas)

En el caso de compras, el usuario puede realizarlas por proximidad o en forma remota. El usuario informa su número de línea y es cargado por vendedor en el sistema (denominado “Máquina da Cielo”), el comprador, por su parte, digita una contraseña para confirmar el pago y recibe un mensaje de texto como recibo. Para las ventas, el vendedor solo necesita el chip “Oi” (prestador del servicio) en su celular para aceptar el cobro con tarjetas de crédito de las operaciones que realice, cuyo importe es acreditado en su

cuenta en el día. Este mecanismo se aplica tanto para comerciantes, taxistas o profesionales. Como puede apreciarse, esta modalidad no es un monedero electrónico, ya que otorga crédito a través de la tarjeta asociada. [9]

El 9/10/13 se promulgó la Ley 12.865/13 que regula, entre otros aspectos, los sistemas de pagos mediante celulares. La norma -apodada de "bancarización" también apunta a lograr la inclusión de más del 39 % de la población brasileña (unos 53 millones de personas) que actualmente se encuentra fuera del sistema bancario, de acuerdo con datos del Instituto de Investigación Económica Aplicada. [10]

La Ley estipula la figura de "instituciones de pago", que podrán ofrecer servicios de pagos móviles, pero no así servicios financieros, que seguirán siendo facultad de bancos y otras instituciones financieras. Es decir, los operadores de telecomunicaciones podrán ofrecer pagos móviles, pero no podrán, por ejemplo, realizar préstamos de dinero. Dentro de las operaciones permitidas por esta norma figuran:

- Depósitos y extracciones de recursos almacenados en la cuenta de pago.
- Ejecutar o facilitar la instrucción de pago relacionada a determinado servicio.
- Administrar las cuentas de pago.
- Emitir órdenes de pago.
- Registrar las aceptaciones de los citados medios de pago.
- Efectuar remesas de fondos.
- Convertir moneda física o escritural en moneda electrónica y viceversa, registrando su aceptación o administrando el uso de dinero electrónico;
- Realizar otras actividades vinculadas la prestación de servicios de pago, que les asigne el Banco Central del Brasil.

REPÚBLICA DE KENIA

En este modelo no es necesario tener una cuenta bancaria para acceder a tener un servicio de dinero electrónico. Los servicios son ofrecidos por la empresa de telefonía móvil Safaricom, denominada M-Pesa (Pesa en swahilli es efectivo). Este es un sistema de pago (en base a SMS) que utiliza dinero electrónico, permitiendo a cualquier tipo de usuario hacer pagos, recibirlos y recibir transferencias de móvil a móvil. Las transacciones se realizan en tiempo real y se reciben confirmaciones en SMS de la misma tanto para el emisor como para el receptor de la operación. La plataforma M-PESA cuenta con todas las seguridades relacionadas con prácticas de prevención de lavado de activos.

Para abrir una cuenta M-PESA el cliente necesita su documento de identificación, y el agente le entrega una nueva tarjeta SIM donde está cargada la aplicación de billetera móvil M-PESA. La red de agentes también se encuentra clasificada por varios niveles; desde súper agentes hasta sub agentes. Las diferentes jerarquías entre agentes, además, permite que el efectivo fluya desde agentes grandes hacia agentes pequeños cuyos puntos de atención están próximos a donde se encuentran los usuarios. De esta forma un agente pequeño no tiene que acercarse a una institución financiera para realizar un depósito, sino que puede realizarlo directamente ante un agente de mayor jerarquía y de esta forma comprar dinero móvil. [11] El dinero electrónico se crea cuando un usuario deposita efectivo en su cuenta de M Pesa. Esto lo puede hacer con cualquiera de los agentes, en una relación uno a uno. El agente podrá recibir estos depósitos, hasta que su balance de moneda electrónica quede en cero.

El procedimiento para realizar una transacción persona a persona consiste en enviar un mensaje SMS o USSD hacia el servidor del Banco desde el menú de la aplicación, en dicho mensaje consta la información del monto a transferir y el número celular telefónico del equipo terminal destino, el integrador del Banco solicita se valide la operación a través de una contraseña asignada previamente a cada usuario; para finalmente, y una vez

aceptado el password, comunicar a través del integrador tanto al usuario origen como al destino, el débito y la acreditación correspondientes. [12]

En noviembre del 2012, conjuntamente con el Banco Comercial de África lanzó M Shwari, una plataforma bancaria virtual, que se apoya en M-Pesa. M Shwari permite a los usuarios de M-Pesa a ahorrar y recibir créditos, de hasta 20000 KES (175 euros) por medio del celular.El desarrollo de M Pesa le ha permitido transformarse en una plataforma de pago que brinda los siguientes servicios:

- Permite ingresar y quitar dinero del sistema por medio de sus 78 mil agentes en todo el país.
- Facilita la transferencia Persona a Persona (P2P).
- Permite cargar el celular en cualquier momento y lugar.
- Facilita el pago de facturas de Persona a Negocio (P2B) por medio de los 350 socios encargados de esto.
- Provee acceso a cajeros automáticos en una red de más de 650 de ellos.
- Permite el pago de salarios.
- Tiene convenios con instituciones de microfinanzas para recibir el pago de los créditos.
- Transferencias de dinero al y del Reino Unido. Se pueden recibir ayudas sociales de algunas ONGs, entre ellas Oxfam y Concern.

Safaricom mantiene los depósitos de dinero de los usuarios depositados en varias cuentas bancarias agrupados en varios bancos, con el fin de mitigar algunos de los riesgos de cualquier banco en particular el colapso. El dinero en estas cuentas se mantiene en fideicomiso para el beneficio de los usuarios de M-Pesa y asegura que el dinero electrónico está totalmente respaldado por chelines. Esto significa que si Safaricom quebrara sus acreedores no tendrá ningún derecho sobre los depósitos de clientes. [13]

En cuanto al marco regulatorio, el Banco Central de Kenia colaboró y participó activamente en el crecimiento de M-Pesa, al en el 2006 autorizar el trabajo de M-Pesa como una entidad de comunicación y no una financiera. Safaricom ha logrado mantener a M-Pesa en esa línea, para de esta forma

evitar las complicaciones, logrando que su sistema no cobre interés, no usa los depósitos de los clientes o no participa de los créditos, y mantiene los fondos en un fideicomiso. El Banco Central, no tiene ningún rol en la supervisión de proveedores de telefonía móvil, los cuales son autorizados por la Comisión de Comunicaciones de Kenia (CCK). El punto de contacto entre el Banco Central y los proveedores de servicios de telefonía móvil se da a través de las licencias que se brindan a los bancos comerciales que ofrecen una plataforma para servicios mediados por telefonía móvil. [14]

UNIÓN EUROPEA

En el año 2009 se emitió la Directiva 2009/110/CE la cual regula el acceso a la actividad de las entidades de dinero electrónico y su ejercicio. Las actividades que se permite realizar a las entidades de dinero electrónico incluyen el suministro de servicios de pago y la concesión de créditos en relación con dichos pagos.

En general, la presente Directiva pretende:

- facilitar la creación de servicios nuevos, innovadores y seguros de dinero electrónico;
- ofrecer acceso al mercado a las nuevas empresas;
- fomentar la competencia eficaz entre los participantes en el mercado.

Las entidades cubiertas por la directiva de dinero electrónico incluyen bancos, entidades de dinero electrónico, el Banco Central Europeo y los bancos centrales nacionales. [15]

<u>Aspectos claves que plantea la normativa:</u>

- Ampliación del ámbito de aplicación, se extiende a todas las monedas y transacciones utilizadas en la Unión Europea.
- Autenticación reforzada, con la exigencia de comprobación de la identidad mediante al menos dos factores seguros e independientes cuando el usuario:
  a) Acceda a su cuenta de pago en línea.
  b) Inicie una operación de pago electrónico.

c) Realice, por un canal remoto, cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.

- Establecimiento de nuevos perfiles de proveedores de servicios de pago:
  a) Proveedores de Servicios de Iniciación de Pagos (PISP): que proporcionan la capacidad de iniciar una orden de pago, respecto una cuenta de pago abierta con otro proveedor de servicios de pago.

  b) Proveedores de Servicios de Información Sobre Cuentas (AISP): servicio en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago o bien en otro proveedor de servicios de pago, o en varios proveedores de servicios de pago.

- Incremento de la protección a los usuarios, exigiendo y controlando que los proveedores de servicios de pago desarrollen procedimientos adecuados y eficaces para la resolución de reclamos que permitan responder a las mismas en un plazo no superior a quince días hábiles.

- Limitación de la responsabilidad de los usuarios, hasta un máximo de 50 euros, por las pérdidas derivadas por operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado o robado.

- Mayor nivel de supervisión por parte de los organismos correspondientes, en materia de gestión de los riesgos operativos y de seguridad, con la obligatoriedad de comunicación por parte del proveedor de servicios de incidentes operativos o de seguridad graves. [16]

Algunos ejemplos de utilización de medios de pagos electrónico en Europa son:

BBVA Wallet

Se trata de un producto que el Banco BBVA de España lanzo en el año 2013, llegando a ser en la actualidad la app bancaria más descargada entre las de su clase. La posibilidad de “apagar” y “encender” las tarjetas, es una de las últimas incorporaciones, y permite que el usuario bloquee de manera temporal sus tarjetas. Asimismo, desde la misma se pueden solicitar nuevas tarjetas, determinar qué tipo de operaciones se pueden realizar con

cada una de ellas (sacar dinero, compras online, compras en el extranjero). De esta manera el teléfono se convierte en un control a distancia de las tarjetas.

Para utilizar solo hay que descargarse la aplicación BBVA Wallet, y luego simplemente bastará con acercar el teléfono al terminal de pago Contactless y confirmar tu PIN. [17]

Algunas de las funcionalidades que posee son:

- Pago a través de tecnología NFC y utilización de PIN de seguridad.
- Permite realizar pagos sin contacto con sus smartphones y elegir la tarjeta de crédito que se quiere usar.
- "Encender" y "apagar" las tarjetas cuando lo desee; en el caso de que un cliente pierda una tarjeta, puede bloquearla de manera temporal hasta que se asegure de la pérdida.
- Financiar pagos realizados con tarjetas desde la propia aplicación.
- A través de las notificaciones "push", el cliente puede obtener una copia del recibo en su terminal móvil en cuanto realiza una transacción, lo que dota a la aplicación de un nivel mayor de seguridad.

Vodafone Wallet

La empresa de telefonía Vodafone ha lanzado la aplicación Vodafone Wallet y desde hace un tiempo ya permite pagar con el móvil con cualquier tarjeta Visa o Mastercard, de débito o crédito, independientemente de la entidad bancaria española a la que pertenezca, una innovación hasta ahora inédita en España. Hasta el momento, todas las aplicaciones de pago por móvil que funcionan por ejemplo en España como la de La Caixa o la del BBVA solo son válidas con el banco que las comercializa. Vodafone Wallet da un paso adelante al prescindir de la entidad financiera, pudiendo almacenar hasta cinco tarjetas de crédito Visa o Mastercard. [18]

Su funcionamiento es simple: permite guardar y utilizar tarjetas bancarias en el móvil sin necesidad de disponer de ellas físicamente. De esta manera nos evitamos cargarlas encima, la posibilidad de perderlas, que nos las roben o tener que aprendernos los distintos códigos PIN para cada

una. Además, permite definir el nivel de seguridad que quieras con las tarjetas pudiendo configurarlas en modo manual para que siempre soliciten un PIN o bien en modo automático para que solo haya que introducir PIN para pagos superiores a 20€.

La aplicación permite pagos en cualquier comercio con terminal de pago sin contacto (contacless) equipado con tecnología NFC tan solo acercando el móvil al terminal. Otra diferencia de Vodafone Wallet es que el elemento de seguridad no se encuentra en la memoria del móvil como en otras aplicaciones, sino en el chip de la SIM. Esta facilidad permite a diferencia de otros servicios pagar incluso si el smartphone está apagado, en conversación, sin cobertura o sin batería. Todos los datos se guardan de forma encriptada en la SIM de tu teléfono y no viajan a través de la red a ningún sitio. [19]

ARGENTINA

En el caso de nuestro país existen diferentes implementaciones de pagos electrónicos, en donde la gran mayoría se encuentran implementadas por las entidades bancarias y las administradoras de redes de cajeros automáticos (Red Link y Prisma).

En relación a regulaciones existentes a los medios de pagos electrónicos, el Banco Central de la República Argentina (BCRA) ha emitido distintas comunicaciones que intentan normar el desarrollo y utilización de pagos móviles. Como primer medida, se definió un nuevo canal de pago, a través del cual las entidades financieras deben ofrecer la modalidad de Pago Electrónico Inmediato (PEI), permitiendo realizar pagos a través del celular, tableta o computadora móvil, con débito y crédito en línea, en cualquier lugar a través de tres modalidades: el POS Móvil y el Botón de Pago, modalidades orientadas a comercios y la Billetera Electrónica, más funcional para transferencias entre personas. El POS Móvil, es un dispositivo de seguridad que se conecta al teléfono móvil o tableta, que se utiliza para validar transacciones mediante la tarjeta de débito del pagador, permitiendo realizar el pago mediante transferencia inmediata. El Botón de pago, se utiliza para

comprar y vender bienes o servicios a través de internet y permite que los compradores puedan realizar sus operaciones en los comercios virtuales (e-commerce) a través de transferencias inmediatas con débito en las cuentas a la vista. Estos botones pueden incorporarse en la página web del comercio, integrarse con distintas redes sociales o enviarse por correo electrónico. Y por último, la Billetera Electrónica permite enviar dinero entre personas a través de internet o por una aplicación en el celular. Sólo se necesita la aplicación app al teléfono, y luego cargar por única vez los datos correspondientes a las cuentas bancarias o las tarjetas de débito asociadas de distintos bancos. [20]

Algunas de las aplicaciones son:

Red Link y Prisma

Link Celular y Banelco Móvil: son aplicaciones que se descargan en los teléfonos celulares, las cuales permiten realizar transferencias, pagos de impuestos y servicios públicos, consultas de saldos y de CBU, recargas de celulares, al igual que la recarga de la tarjeta SUBE, administrando sus cuentas por medio de la red a la que esté adherida su entidad financiera.

Modalidades del PEI:

- El Botón de Pago, es utilizado para la compra y venta de bienes o servicios a través de la web (ecommerce). En la actualidad, la red Prisma implemento el botón de pago “Todo Pago”, el cual es una herramienta que permite crear un botón para insertar en la página web, compartir en redes sociales y/o enviar por email.
- El Pos Móvil, como se mencionó antes es un dispositivo de seguridad (dongle) que se conecta a un teléfono móvil o Tablet, permitiendo el pago mediante una transferencia bancaria. Las implementaciones que se encuentran en el mercado son MPos de la red Prisma y Red Mob de la red Link.

- La Billetera electrónica permite enviar dinero entre personas a través de la web o mediante una aplicación en el celular, sin costo y con acreditación inmediata, hasta $8.060 por día. La implementación de Red Link es Vale y de Prisma es Todo Pago. Para su utilización se debe bajar la aplicación al teléfono móvil, luego registrarse y por último se debe adherir el medio de pago (cuenta bancaria o tarjetas de débitos asociadas). [21]

Naranja Mo

Es un servicio de Tarjeta Naranja (tarjeta de crédito nacida como un medio de pago local en la provincia de Córdoba y que luego fue adquirida por el Banco de Galicia y Buenos Aires S.A., dándole así un carácter nacional). Es un canal alternativo a los pagos móviles como un aumento personal de su límite de crédito y la posibilidad de extenderlo a otros usuarios, tengan o no la tarjeta de crédito. No constituye un monedero móvil dado que no hay adelanto de fondos, sino que se alimenta con cargo a la tarjeta de crédito.

Monedero On-line

Es un pionero en nuestro país en el campo de los pagos por lectura de códigos QR, que es operado por Monedero S.A., una subsidiaria de Visa Argentina S.A. También cuenta con un sistema de tags que son adheridos a un celular, billetera o llavero y utiliza un sistema de proximidad a un lector que permite deducir el dinero almacenado en la cuenta virtual.

PIM

El producto PIM es una billetera móvil para personas no bancarizadas lanzado por el Banco Nación. Permite enviar y recibir dinero, y pagar gastos con el celular, sin necesidad de tarjeta de crédito ni cuenta bancaria. Permite comprar en comercios adheridos y enviar plata de un celular a otro en cualquier lugar del país al instante, sin costo y con total seguridad, ya que la billetera está protegida por una clave personal de 4 números. El comerciante que quiera cobrar deberá solicitar el pago a un teléfono celular. La otra persona envía el dinero ingresando su clave de cuatro dígitos y segundos más tarde ambas personas serán notificadas de la compra a través de un SMS.

Su forma de carga es a través de Pago Fácil, Rapipago, cajeros Link y Banelco, Home Banking o PagoMisCuentas. Y también se puede retirar plata cargada en el celular PIM, a través de Pago Fácil, Rapipago y cajeros de la Red Link. [22]

REFERENCIAS

[1] Dinero Electrónico, Wikipedia. Del sitio https://es.wikipedia.org/wiki/Dinero_electr%C3%B3nico , consultado el 26/7/2016.

[2] Diario Oficial de la Unión Europea. DIRECTIVA 2009/110/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE LA UNIÓN EUROPEA de 16 de septiembre de 2009. Del sitio https://www.boe.es/doue/2009/267/L00007-00017.pdf, consultado el 01/05/2016

[3] Aproximación al Concepto Jurídico de Dinero Electrónico, Universitat de les Illes Balears Carretera de Valldemossa km. 7.5, Palma de Mallorca, 07122, Spain. Del sitio http://www.criptored.upm.es/guiateoria/gt_m081e.htm, consultado el 24/07/2016

[4] Codificación de regulaciones del Banco Central del Ecuador- Libro I Política monetaria-crediticia, Quito, 28 de febrero de 2014. Del sitio http://www.bce.fin.ec/documents/pdf/general/LibroI.pdf, consultado el 01/05/2016

[5] Todo lo que debería saber sobre el dinero electrónico, IESE, Revista de antiguos alumnos, junio de 2001, http://www.ee-iese.com/82/82pdf/afondo1.pdf,consultado el 27/5/2017.

[6] Innovaciones en Microfinanzas Rurales. WIZZIT Bank. Del sitio http://docplayer.es/1840602-Innovaciones-en-microfinanzas-rurales-wizzit-bank-wizzit-bank-innovaciones-en-microfinanzas-rurales-sudafrica-2008-fordfoundation.html, consultado el 03/03/2016.

[7] Mobile Money in the Philippines – The Market, the Models and Regulation. Del sitio http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/Philippines-Case-Study-v-X21-21.pdf , consultado el 05/10/2016.

[8] Directrices sobre la emisión de dinero electrónico y las operaciones de emisores de dinero electrónico en Filipinas. Del sitio http://www.bsp.gov.ph/downloads/Regulations/attachments/2009/c649.pdf , consultado el 05/11/2016.

[9] M-Banking: Oportunidades y barreras para el desarrollo de servicios financieros a través de tecnologías móviles en América Latina y el Caribe. Del sitio https://www.oecd.org/dev/americas/42825480.pdf, consultado el 01/12/2016.

[10] Ley 12.865/13 Pagos Móviles. Del sitio http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm, consultado el 07/11/2016.

[11] Mobile Payments Go Viral M-PESA in Kenya. Del sitio http://siteresources.worldbank.org/AFRICAEXT/Resources/258643-1271798012256/YAC_chpt_20.pdf, consultado el 02/02/2017

[12] Aspectos Jurídicos del Dinero Electrónico: Instrumento de Inclusión Financiera. Del sitio http://revistas.pucp.edu.pe/index.php/derechoysociedad/article/viewFile/15243/15711, consultado el 02/02/2017.

[13] El M-Pesa, la moneda telefónica de Kenya. Del sitio http://www.monedasocial.org/el-m-pesa-la-moneda-telefonica-de-kenya/, consultado el 03/02/2017

[14] Cómo facilitar las transferencias de dinero por telefonía móvil Posición adoptada por el Banco Central de Kenia frente al M-Pesa. Del sitio http://www.afi-global.org/sites/default/files/afi%20case%20study-spanish.pdf , consultado el 03/02/2017

[15] Actividad y supervisión prudencial de las entidades de dinero electrónico. Del sitio http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Ami0042, consultado el 06/05/2016.

[16] El impacto de la nueva directiva europea de servicios de pago. Del sitio https://nae.es/el-impacto-de-la-nueva-directiva-europea-de-servicios-de-pago, consultado el 01/08/2017.

[17] Adiós al 'cash': el pago móvil es una realidad. Del sitio https://www.bbva.com/es/adios-al-cash-el-pago-movil-es-una-realidad/, consultado el 01/08/2017.

[18] Vodafone libera el pago por móvil de los bancos. Del sitio https://elpais.com/economia/2015/11/27/actualidad/1448619809_764413.html , consultado el 15/10/2017.

[19] Aprende a utilizar Wallet y paga con tu móvil. Del sitio https://www.vodafoneteayuda.es/2014/01/aprende-a-utilizar-wallet-y-paga-con-tu-movil/, consultado el 15/10/2017.

[20] Nuevos Medios Electrónicos de Pago. Del sitio http://www.bcra.gob.ar/SistemasFinancierosYdePagos/Sistema_de_Pagos_PPM.asp, consultado el 16/10/2017.

[21] Nuevos Medios de Pago impulsados por el BCRA. Del sitio http://www.bcra.gov.ar/Pdfs/Medios_Pago/Nuevos_medios_de_pago_abril.pdf, consultado el 16/10/2017.

[22] Pim. Del sitio https://www.pim.com.ar/, consultado el 16/10/2017.