FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

ANÁLISIS DE TECNOLOGÍAS UTILIZADAS PARA LA SEGURIDAD EN LAS TRANSACCIONES DE LA BILLETERA MÓVIL EN EL PERÚ

PRESENTADO POR

STEPHANIE ROCÍO AGUIRRE GOYCOCHEA

KAROL KARINA GAMBOA CARDENAS

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO

DE COMPUTACIÓN Y SISTEMAS

LIMA – PERÚ

2016

USMP
UNIVERSIDAD DE SAN MARTIN DE PORRES

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

ANÁLISIS DE TECNOLOGÍAS UTILIZADAS PARA LA SEGURIDAD EN LAS TRANSACCIONES DE LA BILLETERA MÓVIL EN EL PERÚ

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

PRESENTADO POR

AGUIRRE GOYCOCHEA, STEPHANIE ROCÍO

GAMBOA CARDENAS, KAROL KARINA

LIMA – PERÚ

2016

Dedicatoria

A nuestros padres quienes siempre nos apoyaron en todo el transcurso de esta carrera, por su dedicación y ser nuestra fuente de motivación.

Agradecimiento

Expresamos nuestro agradecimiento a la universidad de San Martin de Porres por las facilidades que ha otorgado para llevar a cabo la presente investigación, a los profesores, compañeros, colegas que colaboraron con el desarrollo de esta tesis.

ÍNDICE

Lista de tablas

Lista de figuras

Página

Lista de anexos

RESUMEN

El presente trabajo de investigación tiene como objetivo principal, llegar a conocer la seguridad y las vulnerabilidades a las cuales podría estar expuesta la billetera móvil que se usa en el Perú, denominado BIM.

En la investigación realizada fue necesario conocer primero los antecedentes de la Billetera Móvil en el exterior y como se ha ido desarrollando tanto por el lado tecnológico como a nivel de seguridad con el propósito de realizar una investigación más objetiva en el análisis de la billetera móvil en el Perú, dando a conocer cuáles son los elementos que intervienen la arquitectura del BIM, en el proceso de afiliación y en el proceso realizar transacciones, así como las tecnologías que existen o que fueron usados en los casos de éxito de implementación de billetera móvil como en Filipinas y Kenia.

La metodología utilizada en la presente tesis está enfocada en la investigación científica utilizando el enfoque cualitativo y el método inductivo como parte de esta, se incluyen las evidencias, los entregables y finalmente esto permitirá formular la hipótesis y las conclusiones de esta investigación.

Como parte final de este resumen se puede concluir que no existen reglamentos relacionados a la tecnología USSD que utiliza el BIM del Perú, lo cual aumenta la vulnerabilidad de intercepción, interrupción y fabricación cuando se ejecute automáticamente el USSD en un sistema operativo Android. Adicionalmente existen vulnerabilidades al digitar la contraseña para confirmar una operación y por último se evidencio el desconocimiento de las medidas de seguridad por parte del usuario

Palabras claves: Seguridad, Vulnerabilidades, Billetera móvil, BIM.

ABSTRACT

This abstract has as main goal, get to know the security and vulnerabilities which would expose the mobile wallet used in Peru, called BIM.

In this investigation, it was necessary to know first the background of the Mobile wallet abroad and how it was developed as much as technological side and a level of security with purpose of carrying out an investigation more objective in the analysis of mobile memory in Perú, giving to kwow What are the elements involved in the BIM architecture, the process of affiliation and the process of making transactions, as well as the technologies that exist that were used in the successful cases of the implementation of mobile wallet as in the Philippines and Kenya.

The methodology used in the present thesis is focused on the scientific research using the qualitative approach and inductive method as part of this, including evidences, deliverables and finally this will allow formulating hypothesis and conclusions of this investigation.

As a final part in this summary, it can be concluded that there are not regulations related to USSD technology used by Peru's BIM, which increases the interception, interruption and fabrication vulnerability when the USSD is automatically run on an Android operating system. In addition there are vulnerabilities when entering the password to confirm an operation and finally it is evident the ignorance of the security measures by the user.

Keywords: Security, Vulnerabilities, Mobile wallet, BIM.

INTRODUCCIÓN

El uso del dinero electrónico ya se encuentra en actividad en el Perú, uno de ellos es el BIM que fue lanzado por la Asociación de Bancos (ASBANC) en el proyecto “Modelo Perú” con el objetivo de dejar atrás el concepto bancarización y dar paso al concepto de inclusión financiera y así llegar a zonas de menores recursos que no tengan una cuenta bancaria, sin la necesidad de tener saldo en el celular para acceder al BIM o de tener internet, datos o dinero en efectivo y sin ser necesario la presencia de personas para realizar la transacción. Se puede usar un celular inteligente así como un celular básico para acceder al Menú del BIM y realizar las transacciones. Estas características pueden ser más atractivas a la vista de los usuarios que se encuentren en lugares alejados de los Bancos pero también hay otro factor importante relacionado a cuan seguro es el aplicativo para realizar operaciones y con qué sistemas de seguridad cuenta y que tan informado está el usuario acerca de las vulnerabilidad de seguridad a las que podría estar expuesto y que podría hacer para disminuir el riesgo.

En algunos casos, el temor a lo desconocido tiene como efecto que el usuario tenga temor a usar un producto o aplicativo nuevo y mucho más si hay probabilidad que esté en juego su dinero. Pero cómo conocer si dicho producto nuevo alcanza las expectativas de seguridad que le brinden la suficiente confianza para realizar una transacción.

Para realizar una investigación más objetiva este trabajo recurre a los inicios de la Billetera móvil y cómo fue evolucionando a través del tiempo, siendo necesario conocer que tecnologías usan o cuáles son las más usadas en el exterior y así tener un punto de comparación con la tecnología utilizada en el BIM, luego se realiza un análisis de cómo interactúa el BIM con los demás medios con los que interactúa como son los operadores móviles con los que tiene convenios así como las Entidad Bancarias respaldadas por la SBS; con el fin de poder conocer los elementos que intervienen y analizar las posibles vulnerabilidades a las que podría estar expuesto la billetera móvil en el Perú, llegando así al planteamiento de la hipótesis.

La presente tesis está estructurada en 3 capítulos, en el primero se da a conocer el marco teórico, en él se muestra los antecedentes de la Billetera móvil en Asia, Europa, Norteamérica, Sudamérica y como nació el BIM en el Perú, las etapas y alcance del Modelo Perú y los demás elementos que interactúan en el entorno del funcionamiento del BIM. Este capítulo también contiene la ISO 17799, 27001, 27002, la ley N° 29985, Normas emitidas por la SBS, también se da a conocer la metodología de la investigación científica utilizada siguiendo el método inductivo y por último definiendo términos básicos para tener claros los conceptos que serán un apoyo para el desarrollo de los demás capítulos. En el segundo, se presenta la metodología con dos puntos importantes uno son los materiales que fueron necesarios para la investigación y el otro es el método utilizado en el desarrollo de la investigación el cual se sustenta bajo la metodología inductiva como parte del método cualitativo dividiéndolo en 4 fases (observación, análisis, clasificación y formulación del enunciado) para que sea más didáctica la compresión y en base al alcance de la presente tesis luego se hace una trazabilidad de los objetivos específicos vs las 4 fases del método cualitativo, también se indican los entregables por cada fase. En el tercer capítulo se realiza el desarrollo de toda la investigación realizando un análisis con la información obtenida en el capítulo 1 y utilizando la metodología descrita en el capítulo 2; en este capítulo se realiza un estudio de la percepción respecto al uso de la billetera móvil basada en una encuesta realizada a las personas que viven en Lima Metropolitana, con una muestra de 50 personas para poder conocer si tienen conocimiento de la BIM, medidas de seguridad al realizar una operación así como de los riesgos a los cuales puede estar sometido, otro punto importante que también se desarrolla es la identificación de Normas de seguridad y tecnologías existentes en el Perú así como la evaluación de las vulnerabilidad a la cual puede estar expuesto el uso de la billetera móvil en el Perú. Para finalizar la tesis se formula la hipótesis y se propone algunas tecnologías que pueden reducir las vulnerabilidades en el uso del BIM.

1. Planteamiento del problema

Limitada información de las vulnerabilidades asociadas a las tecnologías usadas en la billetera móvil en el Perú.

- Pocos estudios de percepción respecto al uso de la billetera móvil.
- Poca Identificación de las normas de seguridad y tecnologías existentes en el Perú
- Desconocimiento de la vulnerabilidad a la cual puede estar expuesto el uso de la billetera móvil en el Perú

2. Objetivos

2.1 Objetivo general

Identificar las vulnerabilidades asociadas a la tecnología y la seguridad utilizada en la billetera móvil.

2.2 Objetivos específicos

- Realizar un estudio de percepción respecto al uso de la billetera móvil.
- Identificar las normas de seguridad y tecnologías existentes en el Perú.
- Evaluar la vulnerabilidad a la cual puede estar expuesta el uso de la billetera móvil en el Perú.
- Proponer las tecnologías que reduzcan las vulnerabilidades en el uso de la billetera móvil.

3. Justificación

En Perú el uso de la billetera móvil recién se comenzó a utilizar en el año 2015, actualmente ya son 3 bancos los que están utilizando la billetera móvil, pero el uso de este medio electrónico de pago ya existe en el mercado exterior desde la década de los 90s.y sigue siendo un caso de éxito. Pero también ha habido casos de fracasos por los cuales ha motivado a realizar un análisis de las tecnologías que actualmente se están utilizando para evitar posibles robos de información y password al momento de realizar una transacción con la billetera móvil y así poder tener nuevas alternativas a utilizar para prevenir riesgos futuros debido a que en el Perú recién ha comenzado su auge por lo cual esta tesis puede ayudar a prevenir problemas futuros que se pueden

presentar en las transacciones en el uso de la billetera móvil, ya que este proyecto pueda tener un arraigo seguro en el país como en los países que tuvo éxito.

4. Limitación

Actualmente no se cuenta con encuestas relacionadas al BIM que se haya realizado en todo el Perú.

No hay mucha información publicada en cuanto a la tecnología del BIM como si lo hay en otras billeteras móviles que se usaron en otros países.

Además no se encuentra información acerca de las vulnerabilidades a las cuales se puede presentar el BIM

5. Alcances

Esta tesis abarca la primera fase del Modelo Perú**,** las leyes, normas e ISO que se analizarán respecto a la billetera móvil son las que se encuentran relacionadas con la primera fase del Modelo Perú, fase que se encuentra actualmente en funcionamiento.

En cuanto a la encuesta, se realizó en varios puntos de Lima metropolitana, lo cual se sugiere que se realice una encuesta a nivel macro para poder continuar con los estudios de esta investigación

CAPÍTULO I
MARCO TEÓRICO

1.1. Antecedentes

Para el diario “El universo” (El universo, 2014) el dinero electrónico en varios países del mundo y Latinoamérica se ha constituido en una importante herramienta que promueve la inclusión financiera de la población caracterizada por tener ingresos bajos aunque el concepto del uso de sistemas de moneda no basados en moneda física tiene una larga historia (Hollow, 2012), es en la actualidad que la tecnología para apoyar este tipo de sistemas se ha vuelto ampliamente disponibles. Con el incremento acelerado de la cantidad de teléfonos celulares, el comercio móvil tiende a convertirse en el tipo de comercio electrónico de masa popular. Cuji (2014, p.13) afirma que existe un complejo ecosistema en donde intervienen más de un actor, como el operador de red móvil, consumidor, comerciantes, bancos, emisores de tarjetas entre otros.

Se afirma que al igual que los teléfonos celulares, el uso de tarjetas de crédito se incrementan cada año y la facilidad de obtenerla en muchos países motiva la idea de tener un sistema de pago a través de un teléfono celular (Espinosa, 2009).

Las personas interactúan cada vez más con los servicios de comercio digitales de muchos proveedores diferentes y de muchas maneras diferentes. Para reducir esta complejidad, los consumidores necesitan un enfoque sencillo y coherente para la organización de comprobantes digitales, programas de fidelización, tarjetas de pago, tickets y otros artículos. Una billetera móvil puede satisfacer esa necesidad .Una billetera móvil está diseñado para agregar y gestionar servicios de comercio móvil, el apoyo a las tarjetas de pago, billetes, tarjetas de fidelización, recibos, comprobantes y otros artículos que se pueden encontrar en una cartera convencional. Así como permitir al usuario gestionar una amplia cartera de comercio digital,

servicios de comercio digital, billeteras móviles suelen estar diseñados para permitir al usuario gestionar información de forma segura (GSMA, 2016).

Luego del análisis de los beneficios que puede brindar la billetera móvil se evidencia de lo siguiente:

Para la revista Dinero en Movimiento (2014):

> El dinero electrónico y la billetera móvil no son el futuro, son el presente, este sistema es un mecanismo de inclusión que permite llegar donde no existen las agencias bancarias, ya que basta con la señal del celular. La billetera móvil ofrece a las personas que nunca tenido una cuenta bancaria no solo la opción de tener su dinero a buen recaudo, sino también acceder a préstamos y créditos, usando como respaldo el récord de movimientos de su dinero electrónico
>
> Se estima que entre el 25 y el 30% de la población económicamente activa no está bancarizada, básicamente esto ha sucedido por razones de infraestructura. (s/p)

El análisis de la billetera móvil en otros países es vital pues ayuda a no empezar desde cero sino partiendo de experiencias vividas en otros países evitando cometer los mismos errores.

1.1.1. Asia

La industria móvil asiática siempre ha estado a la vanguardia de la tecnología y desde los años 90 comenzó con sus sistemas de pagos móviles utilizando métodos sin contacto.

- Japón: Osaifui-Keitai, JCB Mobile Wallet
- Corea del Sur: SK Smart Mobile Wallet, KT MOCA
- Singapur: mWallet, M1 NFC Service
- Hong Kong: Citi Wallet.
- India: Loop Mobile mWallet.
- Afganistán: M-PAISA

1.1.2. Europa

La industria móvil europea constituye una de las más avanzadas siempre a la vanguardia en el desarrollo de nuevos servicios. La industria móvil en Europa ha evolucionado más allá de la prestación de servicios de voz y datos básicos.

- Alemania: MyWallet.
- Turquía: Cep-T.
- Rumania: NETOPIA mobilPay
- Reino Unido: QuickTap, Pingit, Moneto.
- Francia: Orange Cash.
- España: Vodafone Wallet.

1.1.3. Norteamérica

En el continente Norteamericano, la Billetera Móvil ha demostrado un gran desarrollo y aceptación. Aunque el mayor desarrollo se presenta en Estados Unidos; en los países de México y Canadá, también se puede encontrar algunos modelos de Billetera Móvil.

- Estados Unidos: ISIS Mobile Wallet, Google Wallet, Us Bank Mobile Wallet, Western Union Mobile Wallet, Vantiv Mobile Wallet, Apriva, Blaze Mobile Wallet, C-Sam Mobile Wallet, Cat Mobile Wallet, CorPay Mobile Wallet, FIS Mobile Suite, Fon Wallet, Griftango MGift, Kuapay Mobile Wallet.
- Canadá: Omnego Mobile Wallet, PayMobile, Rogers Mobile Wallet.

1.1.4. Sudamérica

Cuji (2014, p18) asegura que el continente sudamericano está compuesto por países en vías de desarrollo y caracterizados en muchos casos por los notables niveles de pobreza. Este es uno de los motivos por los que el desarrollo tecnológico y el aporte en cuanto a innovación por parte de los

países sudamericanos, es reducido. Sin embargo, Sudamérica se presenta como un escenario ideal para el desarrollo de los pagos móviles.

(IATAI, 2015) la primera billetera móvil en Latinoamérica llegó a Colombia con ALLEGRA, la plataforma que soporta tecnológicamente aplicación móvil de Asobancaria, cuenta con la primera billetera para el almacenamiento de datos de las tarjetas de crédito aprobada por Apple en Latinoamérica. Esta billetera maneja un sistema de autenticación por huella y por token en los servidores de Cybersource, Visa, similar al sistema Apple Pay en Estados Unidos. Asobancaria, a través de Allegra es la organización en Latinoamérica en brindar esta solución que está revolucionando los sistemas de medios de pago en el mundo.

1.1.5. Perú

Actualmente en el Perú ya son nueve las entidades que se han suscrito a los convenios comerciales con las empresas operadores de telefonía móvil, es decir, que ya están habilitadas para realizar el servicio de billetera móvil, según indicó Osiptel. En detalle son: el Banco de Crédito del Perú, BBVA Banco Continental, Interbank, Banco Financiero del Perú, Banco GNB Perú, Crediscotia, Financiera Credinka, Gmoney y la Caja Municipal de Ahorro y Crédito de Sullana, representadas por la empresa Pagos Digitales Peruanos.

En tanto, las empresas operadoras de telecomunicaciones que en el lanzamiento del también denominado dinero electrónico son Telefónica del Perú, América Móvil y Entel Perú -en el futuro lo hará Bitel-. Si bien la noticia de la llegada de la billetera móvil ya se ha comentado, es importante conocer algunos alcances de la misma.

(Asbanc, 2016) sustenta que, en principio, todos aquellos que tengan un celular podrán – sin necesidad de contar con una cuenta bancaria – depositar, transferir y retirar dinero. Esta es una revolución en la manera de cómo aparecerá el nuevo consumidor que no necesita tarjetas ni créditos pre-aprobados o cualquier otra oferta para poder gestionar dinero.

La aplicación que permitirá este tipo de transferencias se llama BIM, pero aún queda por determinar lo riesgos a los que pueden estar expuestos los usuarios al utilizar el BIM.

1.2. Bases teóricas

En esta sección se detallaran puntos acerca de la billetera móvil en cuanto a su significado, el alcance del Modelo Perú así como los elementos que intervienen en el entorno del BIM.

1.2.1. Billetera móvil

La billetera móvil es uno de los medios de pago del dinero electrónico, conocido también como Mobile Wallet, m-Wallet, Billetera Móvil-BIM. Entre las definiciones dadas por algunas asociaciones y/o organizaciones a nivel mundial son:

1.2.1.1 EPC1: dispositivo móvil, posee información personal identificación, imágenes, documentos- del dueño de la billetera y contiene instrumentos de pago - tarjetas de prepago, crédito y débito - además puede contener información relacionada con firmas y certificados digitales, tarjetas de fidelización, transporte, tickets. (European Payments Council, 2014)

1.2.1.2 GSMA2:Para Neil Daly(2010):

Global System Mobile Association define a la billetera móvil como Un repositorio que contiene los datos del consumidor suficientes para facilitar una transacción financiera desde un teléfono móvil, y la inteligencia aplicable para traducir una instrucción del consumidor a través de un teléfono móvil o de una aplicación, en un mensaje que una institución financiera puede usar para debitar o acreditar una cuenta bancaria o un instrumento de pago(s/p)

1.2.1.3 ITU3, en su reporte denominado “Mobile Money” clasifica a la billetera móvil como una forma de pagos de proximidad C2B/B2C, mencionando también que es uno de los tipos más comunes de

tipos de servicio del dinero móvil “m-money”, es un menú en el teléfono móvil el cual permite el acceso a los diferentes instrumentos de pago e información de la cuenta de pago (International Telecommunication Union, 2013).

Si se define a la billetera móvil en términos de usabilidad se podría decir que es un tipo de dinero electrónico que permite a cualquier persona depositar, transferir y retirar dinero desde cualquier teléfono celular, sin necesidad de contar con una cuenta bancaria, un teléfono inteligente, acceso a Internet, ni saldo (RPP noticias, 2016). También permite realizar pagos de servicios y Pago de productos los cuales todavía no están habilitados en Perú.

1.2.2. Billetera móvil en el Perú

RPP noticias (2016) emitió un reportaje el 16 de febrero del 2016 donde se lanzó al mercado peruano la billetera móvil, la herramienta billetera móvil (BIM) permite a cualquier persona depositar, transferir y retirar dinero desde cualquier teléfono celular, sin necesidad de contar con una cuenta bancaria, un teléfono inteligente, acceso a Internet, ni saldo.

La participación e integración entre todos los actores, entidades bancarias operadores y usuarios, afirma Aguirre (2014), hace que el Modelo Perú sea único en el mundo.

La República (2013) asegura que no es necesaria una cuenta bancaria porque la billetera móvil maneja una cuenta transaccional cuyas principales características es que el saldo no puede ser superior a dos mil soles en todo momento y que es de libre disponibilidad. Los puntos de recaudación del dinero para la billetera se llaman agentes BIM o agentes corresponsales BIM, y están ubicados en bodegas, supermercados y kioscos.

Es probable que se haya escuchado hablar de la billetera móvil, pero muy pocos saben cómo se originó. Por lo cual se brinda más detalle de los inicios de la billetera móvil en el Perú.

1.2.2.1 Modelo Perú

BIM responde a la primera etapa del llamado Modelo Perú el cual está conformado por 3 etapas, orientado a lograr procesos de inclusión financiera a partir del desarrollo del canal digital a través de teléfonos móviles (en particular de gama baja).

a) Primera etapa

La primera, es el desarrollo de un canal digital que opere desde cualquier teléfono móvil (en equipos básicos, pre pago e incluso sin saldo). Se trata de tomar ventaja de la simplicidad que el canal electrónico de pagos ofrece para que sea consecuentemente, de fácil uso (adopción) para los usuarios finales. Para lograr poner dinero y transar con él desde y hacia teléfonos móviles, es necesario trabajar de manera conjunta con las instituciones de dos industrias clave para el desarrollo de BIM en Perú: la industria financiera y la de telecomunicaciones, logrando que una de las más importantes características de BIM sea la interoperabilidad, tanto entre los 34 emisores financieros enlazados a Modelo Perú, como entre compañías de telecomunicaciones, tres de las cuatro compañías en el país.

Para lograr que BIM salga al mercado, los reguladores (Superintendencia de Banca, Seguros y AFP, Banco Central de Reserva del Perú, y el Organismo Supervisor de Inversión Privada en Telecomunicaciones, OSIPTEL) han jugado un papel central, adaptando y creando regulaciones sobre la base de la Ley de Dinero Electrónico para facilitar el proceso.

Las aprobaciones de los contratos se realizaron en el marco de las atribuciones asignadas a Osiptel por la Ley de Dinero Electrónico - N°29985 - (RPP noticias, 2016).

b) Segunda etapa

En esta etapa tiene por objetivo desarrollar un ecosistema de pagos digitales, donde BIM pueda ser utilizado como parte de la vida cotidiana de las personas, ya sea en instituciones que remuneren a sus trabajadores

mediante BIM, o en las compras y pagos que requieran los usuarios en pequeñas ciudades alejadas del sistema financiero o en áreas remotas del Perú (Trivelli & Pinto, 2016).

c) Tercera etapa

En esta etapa, Trivelli et al. (2016) afirman que está relacionada con el desarrollo de un ecosistema de pagos digitales que permitirá a las entidades financieras crear nuevos productos y servicios financieros para estos nuevos clientes lo cual forma parte de la tercera etapa.

1.2.3. Elementos que interviene en el entorno del BIM

En este punto se procederá a describir los pasos que son necesarios para poder acceder al BIM así como todos los elementos que interactúan en el entorno del BIM como son las entidades financieras, los operadores, las operaciones que te permite realizar el BIM, los límites que existen entre los montos a transferir, las tarifas y empresas emisoras de divisa electrónica en el Perú.

1.2.3.1 Acceso a la Billetera Móvil - BIM

No hay costos de afiliación. Para poder abrir el BIM se necesita ser mayor de edad y contar con un celular. Desde este terminal móvil que no necesita ser un Smartphone ni contar con saldo, se debe marcar el *838# y digitar el número de DNI o carné de extranjería, seguido del número que aparece luego del guion, tal como figura en la esquina derecha del DNI.

Luego, se pedirá generar una clave secreta de cuatro números y aceptar los términos y condiciones del BIM. En la pantalla se debe elegir la entidad financiera que respaldará el BIM (El comercio, 2016).

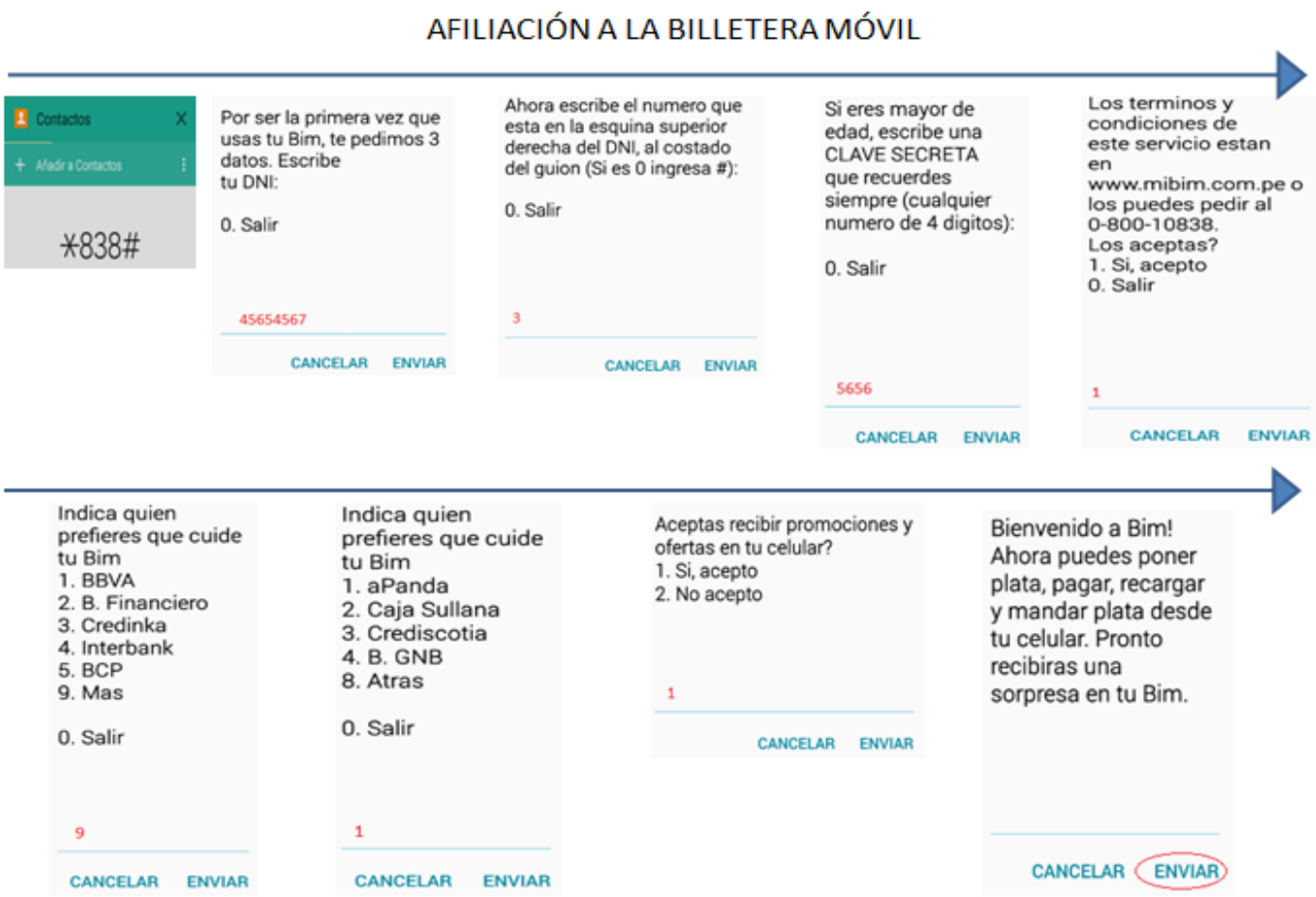


Figura 1: Afiliación a la Billetera Móvil
Fuente: Propia

1.2.3.2 Entidades financieras

De acuerdo a lo informado por Asbanc “Asociación de Bancos del Perú” son nueve las entidades que se han suscrito a los convenios comerciales con las empresas operadores de telefonía móvil.

Asbanc(2016) confirmó que entre las entidades financieras que están habilitadas para realizar el servicio de la Billetera Móvil se encuentran:

- Banco de Crédito del Perú.
- BBVA Banco Continental.
- Interbank.
- Banco Financiero del Perú.
- Banco GNB Perú.
- Crediscotia.
- Financiera Credinka.
- Gmoney (aPanda).
- Crédito de Sullana.

1.2.3.3 Operadoras móviles afiliadas

Hasta el momento, Entel, Movistar y Claro están afiliados al BIM. Próximamente se sumará Bitel.

1.2.3.4 Operaciones permitidas

La Republica.pe (2016) entrevista a Carolina Trivelli, gerente de Pagos Digitales Peruanos (PDP), empresa a cargo del proyecto de dinero electrónico, donde detalló que actualmente se pueden efectuar cuatro operaciones – Primera fase del modelo Perú -.

a) Pagos

En la primera etapa solo está habilitado el pago a TECSUP. Donde es necesario tener el número de DNI del alumno.

b) Recarga de celular

Para la recarga del Celular por el momento solo es posible con el operador Movistar. Conforme se vuelva más amigable esta plataforma para el usuario, se incorporarán progresivamente nuevas funcionalidades. Para "poner" y "sacar" plata solo debe acercarse a alguno de los 6 mil agentes corresponsales identificados como puntos BIM.

c) Envío de dinero (Mandar Plata).

Para enviar dinero desde el celular, se debe marcar *838# y se debe digitar la opción 3. Luego se debe ingresar el número de celular de la persona a la que se desea enviar el dinero, el monto, confirmar el costo e ingresar tu clave secreta y confirmar el monto.

d) Retiro de dinero (Sacar Plata)

Para retirar tu dinero o una transferencia, se debe acudir a un agente BIM, y se debe brindar el número de celular, luego desde el equipo móvil se debe ingresar la clave secreta y confirmar el monto.

e) Poner plata en tu BIM

Para tener dinero en la billetera móvil, se debe acudir a uno de los 4000 agentes identificados con la marca BIM, darle tu número de celular y el dinero. Se recibirá un mensaje de texto confirmando la operación.

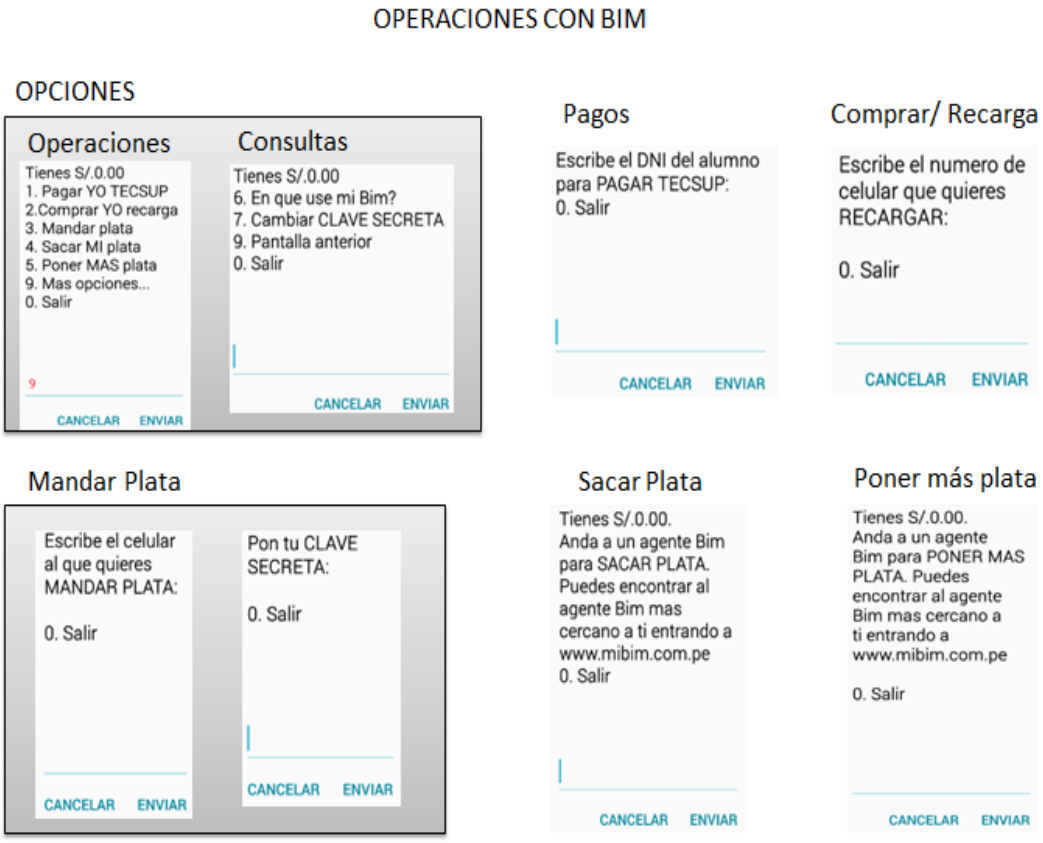


Figura 2: Operaciones con BIM
Fuente: Propia

f) Montos a transferir

La República (2016) afirma que este sistema está orientado a efectuar pequeñas transacciones. A través de la billetera móvil se pueden hacer operaciones de hasta S/6.000 mensuales (entre poner, mandar, recibir, sacar y recargar dinero). Las operaciones no podrán superar los S/999 por vez, donde el usuario debe mantener un saldo máximo de S/. 2.000 en su billetera móvil, según regulación de la SBS.

1.2.3.5 Tarifas

Tarifas de acceso según las normas aprobadas, los emisores de dinero electrónico serán quienes establezcan los precios finales por los servicios financieros que ofrezcan, lo que incluirá el costo por el uso de las redes de telefonía móvil de las empresas operadoras.

Por ahora, a través de la billetera móvil se podrán hacer envíos y depósitos de dinero en soles (con costo desde los S/0,50) y comprar recargas. También se podrán revisar las operaciones hechas a través de este sistema.

BANCO FINANCIERO

PRODUCTO:	CUENTA DE BILLETERA MÓVIL
FECHA DE ACTUALIZACIÓN:	23.02.2016
BANCA:	PERSONA NATURAL

CONCEPTO	TARIFAS						OBSERVACIONES
	EN MN			EN M.E.			
	Tasa.	min	max	Tasa	min	max	
Afiliación y activación de BIM							Gratis
Poner plata (Depósitos)							Gratis
Sacar plata (Retiros)							
Hasta S/. 300.00			S/. 1.50				
Más de S/. 300.00			S/. 2.50				
Mandar plata (Transferencias)							
Hasta S/. 100.00			S/. 0.50				
De S/. 101.00 - S/.500.00			S/. 1.50				
De S/. 501.00 - S/.999.00			S/. 2.00				

Notas:

(1) El cobro de las comisiones se realizará sobre el saldo disponible de la cuenta. Las comisiones son cobradas e informadas al usuario del producto Billetera Móvil al momento de realizar la transacción.

(2) El producto Billetera Móvil no contempla cobrar comisión alguna por las transacciones no financieras (afiliación, activación, consulta de saldos, consulta de últimos movimientos, cambio de clave) ni por las transacciones de conversión de dinero electrónico (poner plata).

(3) Puede realizar sus operaciones en cualquier agente autorizado del Banco Financiero.

(*) La empresa tiene la obligación de difundir información de conformidad con la Ley N° 28587 y el Reglamento de Transparencia de información y Disposiciones aplicables a la contratación con Usuarios del Sistema Financiero, aprobado mediante Resolución SBS N° 8181-2012.

Figura 3: Tarifario BIM
Fuente: Propia

1.2.3.6 Empresas emisores de divisa electrónica en el Perú

La República (2013) informa que según la ley del dinero electrónico, todos los interesados en emitir divisas virtuales deben conformarse como “Empresas Emisoras de Dinero Electrónico” (EEDE), cuya función primordial es la emisión de dinero electrónico, sin poder conceder créditos con cargo a los fondos recibidos. Las compañías que están trabajando con billeteras móviles deberán incluirse en el registro de EEDE y operar bajo el ámbito de la Superintendencia Nacional de Banca, Seguros y AFPs.

En el Perú existen diversas entidades emisoras de divisas como GMoney y Wanda que lanzaron un piloto de billetera móvil en el País, GMoney se expandió por el norte mientras que Wanda se asoció con el Banco de Crédito del Perú y Movistar.

a) GMoney

A finales de noviembre del año 2012, la empresa GMoney convirtió un importante corredor comercial de la región Lambayeque en el terreno de pruebas de su sistema de billetera móvil.

En la ruta que va desde la ciudad de Chiclayo hasta Olmos la empresa ha establecido desde noviembre del 2012 puntos para ofrecer el servicio de dinero electrónico bajo el ecosistema de persona a persona (P2P), el primero de su tipo en operar en el Perú, permitiendo tanto el envío de remesas como el intercambio de dinero, también está utilizando el sistema de pagos móviles en su ecosistema B2B, de negocio a negocio, para manejar la recaudación de la venta del diario La República con distribuidores del norteños.

El sistema de GMoney tiene la particularidad de no usar el SMS para realizar las transacciones, sino la tecnología USSD. Y aunque su mecanismo de funcionamiento es similar, el sistema USSD se diferencia principalmente del mensaje de texto no solo en la mayor rapidez para el envío de datos lo que se

conoce como servicio de telefonía en tiempo real, sino también en que la comunicación no deja ningún tipo de registro y recurre a un menú sencillo e intuitivo.

b) WANDA

La República (2013) emite un reportaje sobre Wanda, una empresa asociada con el Banco de Crédito del Perú y Movistar que ha comenzado a hacer pruebas piloto de su sistema de billetera móvil. Monet, por su parte, es un servicio que exige la descarga de una aplicación en teléfonos con soporte Java, ya sean celulares convencionales o Smartphones, y trabaja tanto con Movistar como con Claro. Monet permite hacer giros, transferir fondos y pagar servicios.

Las dos principales emisoras de dinero electrónico en Perú por el momento son Monet y BIM, que funcionan como intermediarias y brindan servicio de información acerca de este proceso. (Business School, 2015).

Monet, a diferencia de BIM, ofrece pago de servicios a terceros, aunque aún no ha publicado su tarifario y su servicio está a punto de lanzarse (Business School, 2015).

1.2.1. Fallas reportadas hasta el momento utilizando la billetera móvil en el Perú

La Republica.pe (2016):

> Como la billetera móvil empezó a ser utilizado a mitad de febrero de este año 2016, no se encontró noticias de suplantación de identidad relacionado directamente con el uso de la billetera móvil. Pero sí hay casos de suplantación de identidad respecto a celulares utilizados de manera ilícita los cuales han sido reportados en la página oficial de Osiptel y en el diario La República, lo cual podría tener un impacto negativo en el BIM en el caso que persista o se incremente la suplantación de identidad. Se pudieron identificar las suplantaciones gracias a la campaña de Osiptel

donde los usuarios podían llamar a las líneas de telefonía móvil que tienen a su nombre, es decir los usuarios podían conocer el número de líneas móviles que poseen a su nombre, en prevención que estas sean utilizadas de manera ilícita. En el año 2015 se habían reportado más de 100 mil líneas telefónicas cuestionadas por su plantación de identidad. En el caso que se presenten fallas en las transacciones del dinero electrónico, las entidades financieras no se responsabilizarían(s/p).

1.2.2. Tecnologías usadas en la billetera móvil

1.2.2.1 Kenia

El caso más emblemático de este modelo (SMS) es M-PESA de Kenia. El servicio fue diseñado por los operadores móviles Safaricom y Vodafone para un piloto el año 2006, seguido del lanzamiento comercial el 2007. M-PESA surge en el contexto de una población con muy baja bancarización y un fuerte desarrollo de medios de pago informales. Consiste en la instalación de un código en la tarjeta SIM de cualquier tipo de teléfono - tradicionales y smartphones - que permite utilizarlo como medio prepago, cuya carga de dinero se hace directamente en agentes autorizados o bien mediante la trasferencia electrónica de fondos entre clientes que posean una de estas cuentas móviles. Actualmente M-PESA tiene más de 14 millones de clientes y 32 mil agentes autorizados para efectuar las recargas.

Para el lanzamiento de este proyecto, Safaricom trabajó en conjunto con el Banco Central de Kenia (“BCK”) con el objeto de estructurar un modelo que cumpliera los estándares necesarios. No se creó un marco regulatorio por adelantado, sino que el BCK autorizó a Safaricom a operar M-Pesa como un sistema de pago fuera del ámbito de la ley de bancos, sujeto a ciertas restricciones. Así, los fondos de los clientes de Safaricom deben ser depositados en instituciones financieras reguladas; los intereses obtenidos de los saldos de las cuentas de los clientes deben ser depositados en un fondo sin fines de lucro a la espera de determinar

su destino, sin estar autorizado Safaricom a beneficiase de los mismos; se establecen límites a los montos depositados en cada cuenta individual (US$750, aproximadamente) y al tamaño de cada transferencia (US$530, aproximadamente), con el objeto de prevenir actividades de lavado de dinero y disminuir el riesgo de cada cliente en caso de insolvencia; entre otros. Posteriormente en el año 2008, a solicitud del Ministerio de Hacienda, Safaricom fue auditado por el BCK con el objeto de evaluar la seguridad, integridad y eficiencia del sistema. En términos generales, y además de ciertas recomendaciones, la auditoría determinó que el sistema era seguro y que cumplía con objetivos de inclusión financiera. Finalmente, en el año 2011 se dictó una ley que incluye todos los sistemas de pago (incluyendo los pagos móviles) y cuyo objeto es fortalecer el rol supervisor y regulador del BCK sobre los mismos y sus proveedores, estableciendo normas relativas a las facultades regulatorias y de inspección de dicho organismo, requerimientos de información, insolvencia, publicidad engañosa, entre otras.(Gobierno de Chile, 2013)

1.2.2.2 Filipinas

Otro caso emblemático del uso de SMS para transferencia de dinero y que es un caso exitoso es GCASH de Filipinas, servicio ofrecido por Gxchange, una filial del operador móvil Globe Telecom. GCASH ofrece el servicio de enviar y recibir dinero entre los usuarios del mismo sistema, mediante agentes minoristas, encargados de efectuar las operaciones de ingreso y salida de dinero. Las primeras regulaciones de Filipinas relativas a los servicios bancarios electrónicos en general son del año 2000, al amparo de las cuales se crearon alianzas entre compañías de telecomunicaciones y bancos para prestar esta clase de servicios. En el caso específico de GCASH, el Banco Central de Filipinas (“BCF”) reconoció a Gxchange como “agente de remesas” el año 2005, aprobando su producto y estableciendo requisitos de seguridad, lavado de dinero, protección al consumidor, entre otros. Al igual que el caso de Kenia, este reconocimiento fue fruto del trabajo conjunto entre el proveedor y la autoridad.

Con posterioridad, el BCF emitió diversas regulaciones relativas al lavado de dinero, gestión de riesgo y protección a clientes, para en el 2009 emitir la circular, sobre dinero electrónico, autorizando a entidades bancarias y no bancarias para emitirlo, estableciendo requisitos prudenciales, de seguridad, acerca de límites a las transacciones, información y conocimiento de los clientes, entre otros.(Gobierno de Chile, 2013)

1.2.2.3 Perú

La tecnología que maneja el BIM a diferencia de Filipinas y Kenia es USSD para realizar las transacciones y SMS para el envío de mensajes informativos, donde el componente principal de la arquitectura del BIM fue tomado de la solución brindada por la empresa Ericsson (Pagos Digitales Peruanos, 2016).

La Asociación de Bancos eligió a Ericsson para proveer la solución tecnológica que permita el inicio de esta plataforma desde mediados del 2015. SemanaEconomica.com (2015) afirma que el rol de Ericsson será el desarrollo de la solución tecnológica que viabilice la plataforma y su operación para el 2015 con servicios con altos estándares de calidad y seguridad.

En el desarrollo del BIM, también intervino Glenbrook, consultora encargada de determinar un modelo de gobernanza ideal para el óptimo desarrollo de las iniciativas de pagos digitales. Ericsson Wallet Platform (EWP) de la Compañía Ericsson, según los expertos brindan una función principal la cual es adaptada respondiendo así al nombre del BIM (Pagos Digitales Peruanos, 2016).

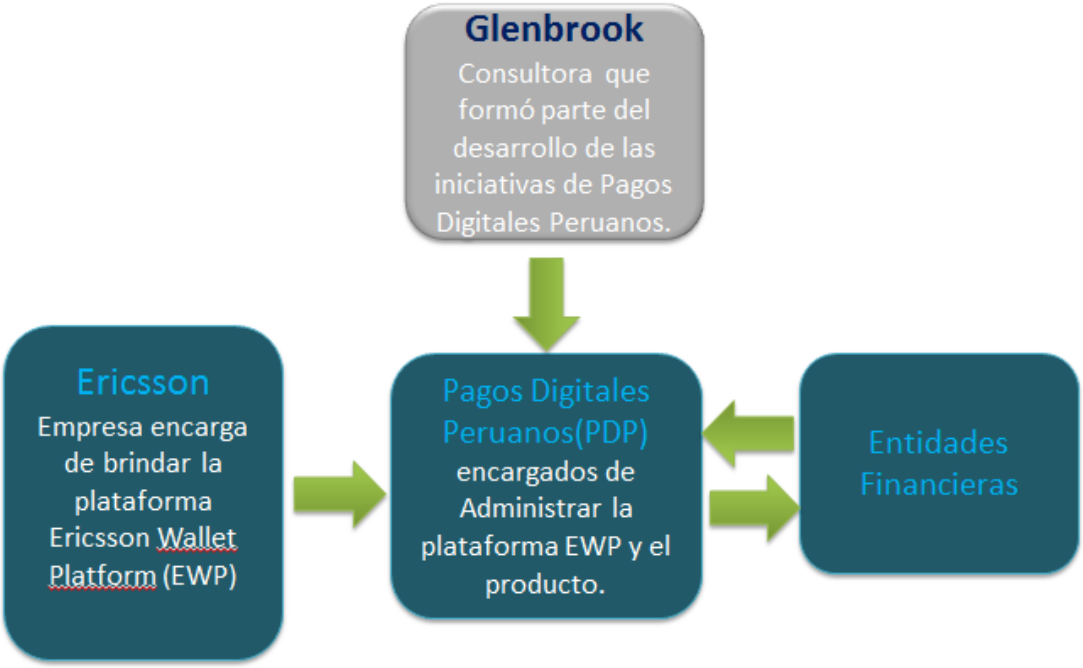


Figura 4: Gráfico de las entidades que participan en la comunicación del BIM
Fuente: Propia

1.2.3. Vulnerabilidades en los servicios financieros móviles

Es necesario conocer el significado de una vulnerabilidad y un riesgo para poder analizar la influencia en los servicios financieros móviles, de tal manera que en la etapa de desarrollo se pueda relacionar las posibles vulnerabilidades a las que podría estar expuesto el BIM.

Alberts (2003):

> El término amenaza puede definirse como la indicación de un potencial evento no deseado. El término vulnerabilidad se puede definir como debilidades de seguridad que pueden resultar en acciones no autorizadas. La literatura, las define como: "debilidades en las políticas organizacionales o prácticas que pueden resultar en acciones no autorizadas". Asimismo sugiere la literatura que las amenazas y vulnerabilidades debe presentarse juntas para poder causar algún daño (s/p).

En todo proceso existe el factor llamado “riesgo”, pues como su definición lo establece: es la posibilidad de que ocurra un evento y afecte adversamente el logro de objetivos. El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad.(Auditool, 2016)

Figura 5: Esquema general para el análisis de las vulnerabilidades
Fuente: Propia

Luego de haber relacionado las amenazas, vulnerabilidades y riesgos, se procederá a describir las amenazas a las cuales que pueden estar expuestos los servicios financieros móviles.

Las amenazas que a continuación se van a describir han sido tomadas de un estudio que realizó el Grupo de Trabajo de Servicios Financieros Móviles – MFSWG- (Alliance for Financial Innclusion, 2013).

1.2.2.4 Amenaza de Modificación: Infección por software malicioso (malware) móvil (riesgo)

Los ataques de software malicioso son comunes en el entorno PC y se espera que pronto se extiendan a los dispositivos móviles de manera repentina. Los ataques de software malicioso en teléfonos celulares pueden ocurrir de las siguientes maneras:

- Los virus/troyanos/gusanos del software malicioso pueden diseminarse vía Bluetooth y MMS.
- El software malicioso puede manipular al usuario al enviar un mensaje SMS.
- El software malicioso puede infectar archivos.

- Los atacantes pueden obtener acceso remoto a los teléfonos celulares al propagar software malicioso.
- Cuando se descarga, el software malicioso puede cambiar los íconos y las aplicaciones del sistema.
- El software malicioso puede instalar funciones y aplicaciones no operativas.
- El software malicioso es un canal útil que puede utilizarse para instalar otros programas maliciosos.
- El software malicioso puede robar datos o información que capture el usuario y bloquear el uso de las tarjetas de memoria.

1.2.2.5 Amenaza de Revelación: Legibilidad de información financiera crítica de los clientes vía SMS (riesgo)

La legibilidad resulta una gran inquietud cuando se utilizan SMS para tener acceso a cuentas y recibir notificaciones sobre actividades previas. Los SMS se transmiten y reciben en texto simple y dicho protocolo no utiliza ninguna técnica de cifrado. En los casos de robo del dispositivo y software malicioso, los usuarios no autorizados pueden tener acceso total a la cuenta de un cliente.

1.2.2.6 Amenaza de Revelación: Exposición de datos críticos debido a cifrado no seguro de extremo a extremo (riesgo)

El Protocolo de Aplicaciones Inalámbricas (WAP por sus siglas en inglés) es una aplicación estándar que permite que los teléfonos móviles tengan acceso a la Internet. Los teléfonos celulares con tecnología WAP utilizan navegadores similares a los que utilizan las computadoras, aunque tienen modificaciones para adecuarse a las restricciones de dichos teléfonos.

El WAP utiliza el mismo enfoque estratificado que el TCP-IP. Un sitio web normal basado en la computadora permite a los usuarios tener acceso a internet mediante el uso del HTML del protocolo de la capa de aplicación. Asimismo, los consumidores que cuentan con teléfonos móviles con tecnología WAP pueden

tener acceso al mismo sitio web utilizando sus teléfonos por medio del protocolo WML (Lenguaje de Marcado Inalámbrico), que es una capa de aplicación del WAP. La única diferencia entre los dos es el tamaño y resolución de la visualización ya que el sitio web se convierte para atender las restricciones del teléfono móvil. Por lo tanto, las transmisiones no cifradas son vulnerables a quedar expuestas a partes no autorizadas.

1.2.2.7 Amenaza de Interrupción: Falta de disponibilidad del canal de comunicaciones debido a ataques de denegación de servicio (riesgo)

Los ataques de denegación de servicio (DOS, por sus siglas en inglés) hacen que un recurso computacional no esté disponible mediante la saturación o el consumo del recurso del componente. El objetivo más común de los ataques DOS son los servidores y bases de datos, que también pueden afectar las redes móviles, debido a que tanto el entorno con cables como el inalámbrico utilizan la misma infraestructura.

1.2.2.8 Amenaza de Interceptación: Ataque por secuencias de comandos entre páginas web (cross-scripting attack) en USSD (riesgo)

El protocolo de comunicación USSD (Unstructured Supplementary Service Data) permite una transmisión de datos más rápida en comparación con el SMS. A diferencia del SMS, el USSD utiliza una conexión directa entre el remitente y el destinatario. Es un canal de comunicación orientado a la sesión, donde la aplicación USSD se utiliza como interfaz entre el proveedor de telecomunicaciones y la cuenta bancaria del cliente. El USSD también puede manejarse utilizando aplicaciones basadas en la web, por lo que es propenso a ataques por secuencias de comandos entre páginas web. En dichos ataques, un usuario malicioso explota la vulnerabilidad de la aplicación basada en la web instalada en el teléfono móvil del usuario para manipular operaciones al inyectar

una secuencia de comandos Java o SQL a fin de robarla información crítica del usuario. También puede llevar a cabo actos maliciosos en la base de datos, tomar la sesión activa de otro usuario y conectar a usuarios a servidores maliciosos.

La presente lista de riesgos no pretende ser exhaustiva, pero ilustra los tipos de riesgos que cualquier oferta de servicios debe manejar. Tomando en cuenta dichos riesgos, ahora se enfocará los principios de la gestión de riesgos y supervisión que los entes reguladores deben conocer.

1.3. ISO 17799

En toda organización que haga uso de las tecnologías de información se recomienda implementar buenas prácticas de seguridad, pues en muchas ocasiones el no seguir un proceso de implementación adecuado como el que establece el ISO 17799 puede generar huecos por la misma complejidad de las organizaciones, en ese sentido, aumenta la posibilidad de riesgos en la información.

Este estándar internacional de alto nivel para la administración de la seguridad de la información, fue publicado por la ISO (International Organization for Standarization) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones.

El ISO 17799, al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática:

- Confidencialidad. Asegurar que únicamente personal autorizado tenga acceso a la información.
- Integridad. Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.
- Disponibilidad. Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación; no obstante, dependiendo de la naturaleza y metas de las organizaciones, éstas mostrarán especial énfasis en algún dominio o área del estándar ISO 17799.

El objetivo de la seguridad de los datos es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad.

Como todo buen estándar, el ISO 17799 da la pauta en la definición sobre cuáles metodologías, normas o estándares técnicos pueden ser aplicados en el sistema de administración de la seguridad de la información, se puede entender que estos estándares son auxiliares y serán aplicados en algún momento al implementar el mismo.

La aplicación de un marco de referencia de seguridad basado en el ISO 17799 proporciona beneficios a toda organización que lo implemente, al garantizar la existencia de una serie de procesos que permiten evaluar, mantener y administrar la seguridad de la información.
Las políticas, estándares locales y los procedimientos se encuentran adaptados a las necesidades de la organización debido a que el proceso mismo de su elaboración integra mecanismos de control y por último, la certificación permite a las organizaciones demostrar el estado de la seguridad de la información, situación que resulta muy importante en aquellos convenios o contratos con terceras organizaciones que establecen como requisito contractual la certificación BS7799.

1.3.1. Antecedentes

Es importante entender los principios y objetivos que dan vida al ISO 17799, así como los beneficios que cualquier organización, incluyendo las instituciones públicas, privadas y ambientes educativos pueden adquirir al implementarlo en sus prácticas de seguridad de la información.

El estándar de seguridad de la información ISO 17799, descendiente del BS 7799 – Information Security Management Standard – de la BSI (British Standard Institute) que publicó su primera versión en Inglaterra en 1995, con actualizaciones realizadas en 1998 y 1999, consiste de dos partes:

- Parte 1**:** Código de prácticas.
- Parte2**:** Especificaciones del sistema de administración de seguridad de la información

Por la necesidad generalizada de contar con un estándar de carácter internacional que permitiera reconocer o validar el marco de referencia de seguridad aplicado por las organizaciones, se elaboró el estándar ISO17799:2000, basado principalmente en la primera parte del BS 7799 conocida como Código de Prácticas (BS 7799 Part 1: Code of Practice).

1.3.2. Los controles del ISO 17799

El éxito de la implementación del estándar de seguridad ISO 17799 requiere de una serie de procedimientos donde, inicialmente, el análisis de riesgos identificará los activos de la información y las amenazas a las cuales se encuentra expuesta.

El análisis de riesgos guiará en la correcta selección de los controles que apliquen a la organización; este proceso se conoce en la jerga del estándar como Statement of Applicability, que es la definición de los controles que aplican a la

organización con objeto de proporcionar niveles prácticos de seguridad de la información y medir el cumplimiento de los mismos.
A continuación, se describirán cada una de las diez áreas de seguridad con el objeto de esclarecer los objetivos de estos controles.

1.3.2.1 Políticas de seguridad

El estándar define como obligatorias las políticas de seguridad documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

1.3.2.2 Seguridad organizacional

Establece el marco formal de seguridad que debe integrar una organización, tales como un foro de administración de la seguridad de la información, un contacto oficial de seguridad (Information System Security Officer – ISSO), revisiones externas a la infraestructura de seguridad y controles a los servicios de outsourcing, entre otros aspectos.

1.3.2.3 Clasificación y control de activos

El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

1.3.2.4 Seguridad del personal

Contrario a lo que uno se puede imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información.

El objetivo de esta área del estándar es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras

responsabilidades por parte del personal en materia de seguridad de la información.

1.3.2.5 Seguridad física y de entorno

Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

1.3.2.6 Comunicaciones y administración de operaciones

Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

1.3.2.7 Control de acceso

Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

1.3.2.8 Desarrollo de sistemas y mantenimiento

La organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

1.3.2.9 Continuidad de las operaciones de la organización

El sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

1.3.2.10 Requerimientos legales

La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

Cada una de las áreas establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle (Universidad Nacional Autónoma de México, 02-05).

1.4. ISO 27001

ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

1.4.1. Estructura

Esta norma se encuentra dividida en dos partes; la primera se compone de 10 puntos entre los cuales se encuentran:

- Objeto y campo de aplicación: Especifica la finalidad de la norma y su uso dentro de una organización.
- Referencias normativas.
- Término y definiciones: Los términos y definiciones usados se basan en la norma ISO/IEC 27000.
- Contexto de la organización: Se busca determinar las necesidades y expectativas dentro y fuera de la organización que afecten directa o indirectamente al sistema de gestión de la seguridad de la información. Adicional a esto, se debe determinar el alcance.
- Liderazgo: Habla sobre la importancia de la alta dirección y su compromiso con el sistema de gestión, estableciendo políticas, asegurando la integración de los requisitos del sistema de seguridad en los procesos de la organización, así como los recursos necesarios para su implementación y operatividad.
- Planificación: Se deben valorar, analizar y evaluar los riesgos de seguridad de acuerdo a los criterios de aceptación de riesgos, adicional mente se debe dar un tratamiento a los riesgos de la seguridad de la información. Los objetivos y los planes para logar dichos objetivos también se deben definir en este punto.
- Soporte: Se trata sobre los recursos destinados por la organización, la competencia de personal, la toma de conciencia por parte de las partes interesadas, la importancia sobre la comunicación en la organización. La importancia de la información documentada, también se trata en este punto.
- Operación: El cómo se debe planificar y controlar la operación, así como la valoración de los riesgos y su tratamiento.
- Evaluación de desempeño: Debido a la importancia del ciclo PHVA (Planificar, Hacer, Verificar, Actuar), se debe realizar un seguimiento, medición, análisis y evaluación del sistema de gestión de la información.
- Mejora: Habla sobre el tratamiento de las no conformidades, las acciones correctivas y a mejora continua.

La segunda establece los objetivos de control y los controles de referencia. Ver Anexo 1.

1.4.2. Beneficios que aporta este a los objetivos de la organización

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

Las organizaciones que simplemente cumplen la norma ISO/IEC 27001 o las recomendaciones de la norma del código profesional, ISO/IEC 27002 no logran estas ventajas.

1.4.3. Implantación

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al sistema de gestión de la seguridad de la información elegido. En general, es recomendable la ayuda de consultores externos.

Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos por ejemplo en España la conocida LOPD y sus normas de desarrollo, siendo el más importante el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica de Protección de Datos) o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática generalmente ingenieros o ingenieros técnicos en Informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información que hayan realizado un curso de implantador de SGSI

1.5. ISO 27002

El Estándar Internacional ISO/IEC 27002 nace bajo la coordinación de dos organizaciones:

ISO: International Organization for Standardization.

IEC: International Electrotechnical Commission.

ISO e IEC han establecido un comité técnico conjunto denominado ISO/IEC JTC1 (ISO/IEC Joint Technical Committee). Este comité trata con todos los asuntos de tecnología de información. La mayoría del trabajo de ISO/IEC JTC1 es hecho por subcomités que tratan con un campo o área en particular. Específicamente el subcomité SC 27 es el que se encarga de las técnicas de seguridad de las tecnologías de información, que es en esencia de lo que trata el Estándar Internacional ISO/IEC 27002 antiguamente llamado ISO/IEC 17799, pero a partir de julio de 2007, adoptó un nuevo esquema de numeración y actualmente es ISO/IEC 27002.

El ISO/IEC 27002 se refiere a una serie de aspectos sobre la seguridad de las tecnologías de información, entre los que se destacan los siguientes puntos:

1.5.1. Evaluación de los riesgos de seguridad

Se deben identificar, cuantificar y priorizar los riesgos.

1.5.2. Política de seguridad

Debe haber políticas organizacionales claras y bien definidas que regulen el trabajo que se estará realizando en materia de seguridad de la información.

1.5.3. Aspectos organizativos de la seguridad de la información

Cómo se trabajará en la seguridad de la información organizativamente, tanto de manera interna, empleados o personal de la organización, como de forma externa o con respecto a terceros: clientes, proveedores, etc.

1.5.4. Gestión de activos

Se debe tener un completo y actualizado inventario de los activos, su clasificación, quiénes son responsables por los activos, etc.

1.5.5. Seguridad ligada a los recursos humanos

Especificar las responsabilidades del personal o recursos humanos de una organización, así como los límites que cada uno de ellos tiene con respecto al acceso y manipulación de la información.

1.5.6. Seguridad física y ambiental

Consiste en tener una infraestructura física (instalaciones) y ambiental (temperaturas adecuadas, condiciones ideales de operación ideales) adecuadas de modo que no pongan en riesgo la seguridad de la información.

1.5.7. Gestión de comunicaciones y operaciones

Asegurar la operación correcta de cada uno de los procesos, incluyendo las comunicaciones y operaciones que se dan en la organización. Esto también incluye la separación entre los ambientes de desarrollo, de prueba y de operación, para evitar problemas operacionales.

1.5.8. Control de acceso

Deben existir medidas adecuadas que controlen el acceso a determinada información, únicamente a las personas que están autorizadas para hacerlo, utilizando autenticaciones, contraseñas, y métodos seguros para controlar el acceso a la información.

1.5.9. Adquisición, desarrollo y mantenimiento de los sistemas de información

Consiste en tomar medidas adecuadas para adquirir nuevos sistemas (no aceptar sistemas que no cumplan con los requisitos de calidad adecuados), haciendo también un eficiente desarrollo y mantenimiento de los sistemas.

1.5.10. Gestión de incidentes en la seguridad de la información

Los incidentes se pueden dar tarde o temprano, y la organización debe contar con registros y bitácoras para identificar a los causantes y responsables de los incidentes, recopilar evidencias, aprender de los errores para no volverlos a cometer, etc.

1.5.11. Gestión de la continuidad del negocio

Se deben tener planes y medidas para hacerle frente a los incidentes, de modo que el negocio pueda continuar en marcha gracias a medidas alternativas para que un incidente no detenga las operaciones por tiempos prolongados, que no se pierda información, que no se estanquen o detengan las ventas o negocios, etc.

1.5.12. Cumplimiento

Debe darse el debido cumplimiento a los requisitos legales, como derechos de propiedad intelectual, derecho a la confidencialidad de cierta información, control de auditorías, etc.

1.6. Ley N° 29985

Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera.

1.6.1. Objeto de la ley

El objeto de la presente Ley es regular la emisión de dinero electrónico, determinar las empresas autorizadas a emitirlo y establecer el marco regulatorio y de supervisión de las Empresas Emisoras de Dinero Electrónico. La emisión de dinero electrónico comprende las operaciones de emisión propiamente dicha de dinero electrónico, reconversión a efectivo, transferencias, pagos y cualquier movimiento u operación relacionada con el valor monetario del que disponga el titular y necesaria para las mismas.

Para ver el reglamento a más detalle de la Ley N° 29985 ir al Anexo 2.

1.7. Normas emitidas por la SBS

1.7.1 Reglamento de operaciones con dinero electrónico Resolución SBS Nº 6283-2013

Esta norma establece las operaciones que pueden realizarse con dinero electrónico, tales como la conversión y reconversión, pagos (persona a persona, persona a negocio, negocio a persona, persona a gobierno, gobierno a persona), transferencias, entre otras.

Estas operaciones se podrán realizar a través de teléfonos móviles, tarjetas prepago o cualquier otro equipo o dispositivo electrónico que cumpla los fines establecidos en la Ley de Dinero Electrónico.

El reglamento también establece el concepto de “cuentas de dinero electrónico simplificadas”, y las define como aquellas que los emisores de dinero electrónico ponen a disposición de personas. *Ver Anexo 3.*

1.7.2 Reglamento de las EDDE: Resolución SBS Nº 6284-2013

Establece el marco normativo para las EEDE, el cual comprende disposiciones aplicables respecto a la constitución, funcionamiento y capital mínimo de estas empresas, así como las operaciones permitidas, medidas prudenciales (límites, patrimonio efectivo, gestión de riesgos, etc.), entre otras.

En ese sentido, se contempla como una de las medidas prudenciales el que las EEDE deban contar con un patrimonio efectivo no menor al 2% del total del dinero electrónico en circulación.

Adicionalmente, se establece un proceso de adecuación para las empresas que, al momento de entrada en vigencia de este reglamento, se encuentren operando y cumplan con las características para ser consideradas como EEDE. Ver Anexo 4.

1.7.3 Reglamento de uso de cajeros automáticos y cajeros corresponsales: Resolución SBS Nº 6285-2013

Propone un nuevo reglamento de apertura, conversión, traslado o cierre de oficinas, uso de locales compartidos, uso de cajeros automáticos y cajeros corresponsales, que permite a los cajeros corresponsales lleven a cabo operaciones en nombre de los emisores de dinero electrónico. *Ver Anexo 5*.

1.8. Investigación científica

Todo el proceso de la investigación es indispensable pues cada una de sus distintas etapas aporta un elemento básico para el estudio, sin embargo, el punto crucial es el planteamiento del problema pues de él depende la formulación de los objetivos, la hipótesis, la justificación del trabajo, el marco teórico y el método de investigación, prácticamente toda la investigación.

En la siguiente figura en espiral que se usa esquematiza el proceso de investigación que evoluciona desde aspectos muy específicos y se expande hacia aspectos más complejos en una creciente integración de las partes de todo el proceso.

Figura 6: Diagrama del proceso de investigación en espiral
Fuente: (Roberto Hernández Sampieri, 2010)

La investigación científica es en esencia como cualquier tipo de investigación, solo que más rigurosa, organizada y se lleva a cabo cuidadosamente. Como siempre señaló Fred N. Kerlinger: es sistemática, empírica y critica. Esto aplica tanto a estudios cuantitativos, cualitativos 0 mixtos. Que sea "sistemática" implica que hay una disciplina para realizar la investigación científica y que no se dejan los hechos a la casualidad. Que sea "empírica" denota que se recolectan y analizan datos. Que sea "critica" quiere decir que se evalúa y mejora de manera constante. Puede ser más o menos controlada, más o menos flexible o abierta, más o menos estructurada, en particular bajo el enfoque cualitativo, pero nunca caótica y sin método. La investigación puede cumplir dos propósitos

fundamentales: a) producir conocimiento y teorías (investigación básica) y b) resolver problemas prácticos (investigación aplicada). Gracias a estos dos tipos de investigación la humanidad ha evolucionado. La investigación es la herramienta para conocer el entorno y su carácter es universal.

La investigación científica se concibe como un conjunto de procesos sistemáticos y empíricos que se aplican al estudio de un fenómeno; es dinámica, cambiante y evolutiva. Se puede manifestar de tres formas: cuantitativa, cualitativa y mixta. Esta última implica combinar las dos primeras. Cada una es importante, valiosa y respetable por igual.

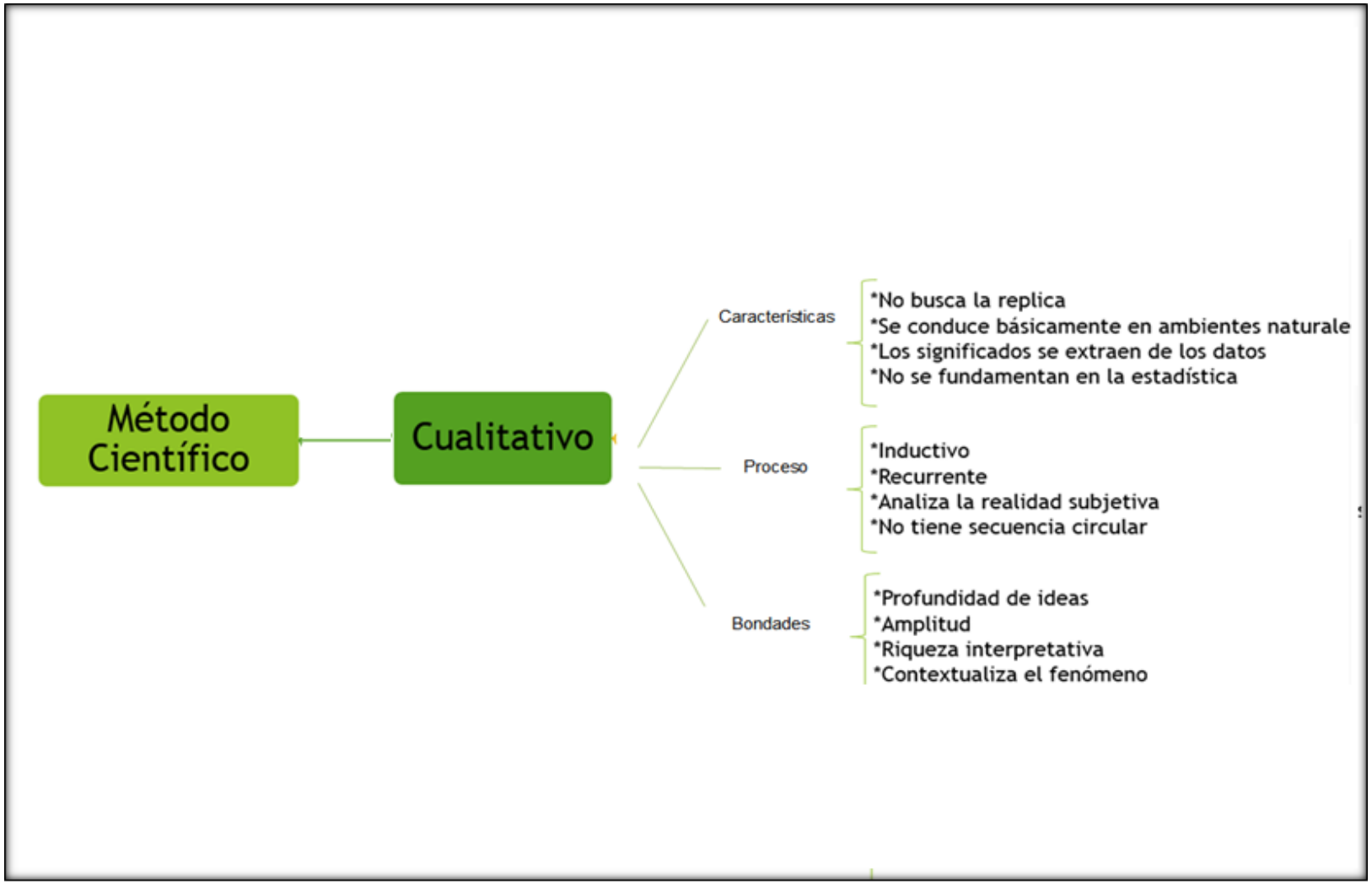


Figura 7: Diagrama del método científico
Fuente: Propia

1.8.1. Enfoque cuantitativo

Usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías.

1.8.2. Enfoque cualitativo

Utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación.

Tabla 1: Diferencia del método cualitativo vs método cuantitativo

Definiciones	Enfoque cuantitativo	Enfoque cualitativo
Objetividad	Busca ser objetivo	Admite subjetividad
Metas de la investigación	Describir, explicar y predecir los fenómenos (causalidad). Generar y probar teorías	Describir, comprender e interpretar los fenómenos, a través de las percepciones y significados producidos por las experiencias de los participantes
Lógica	Se aplica la lógica deductiva. De lo general a lo particular [de las leyes y teoría a los datos).	Se aplica la lógica inductiva. De lo particular a lo general (de los datos a las generalizaciones -no estadísticas- y la teoría).
Lógica Relación entre ciencias físicas /naturales y sociales	Las ciencias físicas/naturales y las sociales son una unidad. A las ciencias sociales pueden aplicárseles los principios de las ciencias naturales.	Las ciencias físicas/naturales y las sociales son diferentes. No se aplican los mismos principios.
Posición personal del investigador	Neutral. El investigador "hace a un lado" sus propios valores y creencias. La posición del investigador es "imparcial", intenta asegurar procedimientos rigurosos y "objetivos" de recolección y análisis de los datos, así como evitar que sus sesgos y tendencias influyan en los resultados.	Explicita. El investigador reconoce sus propios valores y creencias, incluso son parte del estudio.
Interacción física entre el investigador y el fenómeno	Distanciada, separada.	Próxima, suele haber contacto
Interacción psicológica entre el investigador y el fenómeno	Distanciada, lejana, neutral, sin involucramiento.	Cercana, próxima, empática con involucramiento.

Papel de los fenómenos estudiados (objetos. seres vivos, etc.)	Los papeles son más bien pasivos.	Los papeles son más bien activos.
Relación entre el investigador y el fenómeno estudiado	De independencia y neutralidad, no se afectan. Se separan	De interdependencia, se influyen. No se separan.
Planteamiento del problema	Delimitado, acotado, especifico. Poco flexible.	Abierto, libre, no es delimitado o acotado. Muy flexible.
Uso de la teoría	La teoría se utiliza para ajustar sus postulados al mundo empírico.	La teoría es un marco de referencia.
Generación de teoría	La teoría es generada a partir de comparar la investigación previa con los resultados del estudio. De hecho, estos son una extensión de los estudios previos	La teoría no se fundamenta en estudios anteriores, sino que Se genera o construye a partir de los datos empíricos obtenidos y analizados

Fuente: Propia

El método inductivo es parte del enfoque cualitativo, a veces referido como investigación naturalista, fenomenológica, interpretativa o etnográfica, es una especie de "paraguas" en el cual se incluye una variedad de concepciones, visiones, técnicas y estudios no cuantitativos (Grinnell, 1997). Sus características más relevantes son: EI investigador plantea un problema, pero no sigue un proceso claramente definido. Sus planteamientos no son tan específicos como en el enfoque cuantitativo. Se utiliza primero para descubrir y refinar preguntas de investigación (Grinnell, 1997). Bajo la búsqueda cualitativa, en lugar de iniciar con una teoría particular y luego "voltear" al mundo empírico para confirmar si esta es apoyada por los hechos, el investigador comienza examinando el mundo social y en este proceso desarrolla una teoría coherente con 10 que observa que ocurre -con frecuencia denominada teoría fundamentada (Esterberg, 2002)-. Dicho de otra forma, las investigaciones cualitativas se fundamentan más en un proceso inductivo (explorar y describir, y luego generar perspectivas teóricas). Van de lo particular a lo general. Por ejemplo, en un típico estudio cualitativo, el investigador entrevista a una persona, analiza los datos que obtuvo y saca algunas conclusiones; posteriormente, entrevista a otra persona, analiza esta nueva información y revisa sus resultados y conclusiones; del mismo modo, efectúa y analiza más entrevistas para comprender lo que busca. Es decir,

procede caso por caso, dato por dato, hasta llegar a una perspectiva más general.

1.9. Método inductivo

El método inductivo o inductivismo es aquel método científico que obtiene conclusiones generales a partir de premisas particulares. Se trata del método científico más usual, en el que pueden distinguirse cuatro pasos esenciales: la observación de los hechos para su registro; la clasificación y el estudio de estos hechos; la derivación inductiva que parte de los hechos y permite llegar a una generalización; y la contrastación.

Esto supone que, tras una primera etapa de observación, análisis y clasificación de los hechos, se logra postular una hipótesis que brinda una solución al problema planteado. Una forma de llevar a cabo el método inductivo es proponer, mediante diversas observaciones de los sucesos u objetos en estado natural, una conclusión que resulte general para todos los eventos de la misma clase.

En concreto, se puede establecer que este citado método se caracteriza por varias cosas y entre ellas está el hecho de que al razonar lo que hace quien lo utiliza es ir de lo particular a lo general o bien de una parte concreta al todo del que forma parte.

De la misma forma es importante subrayar el hecho de que este método que se está abordando se sustenta en una serie de enunciados que son los que le da sentido. Así, se puede establecer que existen tres tipos diferentes de ellos: los llamados observacionales que son aquellos que hacen referencia a un hecho que es evidente, los particulares que están en relación a un hecho muy concreto, y finalmente los universales. Estos últimos son los que se producen como consecuencia o como derivación de un proceso de investigación y destacan porque están probados empíricamente.

El razonamiento inductivo puede ser completo, en este caso se acerca debido a que sus conclusiones no brindan más datos que los aportados por las

premisas o incompleto (la conclusión trasciende a los datos aportados por la premisa; a medida que hay más datos, habrá una mayor probabilidad de verdad. La verdad de las premisas, de todos modos, no asegura que la conclusión sea verdadera).

1.10. Definición de términos básicos

Tabla 2: Definición de términos básicos

Términos	Definición
Asbanc	Asociación de Bancos del Perú.
Asobancaria	Asobancaria es la asociación representativa del sector financiero Colombiano. Está integrada por los bancos comerciales nacionales y extranjeros, públicos y privados, las más significativas corporaciones financieras e instituciones oficiales especiales.
aPanda	Es una Billetera Electrónica, que funciona del modo "pre-pago" y opera a través de una plataforma tecnológica que permite realizar transacciones en tiempo real (en línea), de manera segura, y no requiere que los celulares tengan ninguna aplicación preinstalada, ni utiliza el saldo del celular para hacer transacciones. Sólo se utiliza el teclado para seleccionar opciones y responder a las solicitudes del sistema. No hace uso de Internet ni consume el saldo del cliente.
Apple Pay	Apple Pay es un pago por móvil y la cartera digital de servicios por Apple Inc. que permite realizar pagos utilizando el iPhone 6, 6 Plus, y más tarde, Apple Watch -Compatible (iPhone 5 y modelos posteriores), IPadAir 2, iPad Pro y Mini iPad 3 y posteriores. Apple Pay no requiere de Apple Pay específicas de pago sin contacto terminales, y puede trabajar con terminales sin contacto existentes.
BCF	Banco Central de Filipinas
BCK	Banco Central de Kenia
BIM	Billetera Móvil.
Comercio Móvil	Es el uso de un dispositivo móvil en el proceso de pago, proceso de compra y venta de bienes y servicios a través de dispositivos inalámbricos como el teléfono celular, llamado Mobile commerce o M-commerce.
Cybersource	CyberSource es una tarjeta de crédito de pago del sistema de comercio electrónico empresa de gestión. Los clientes que procesan

	los pagos en línea, agilizan el fraude en línea de gestión, y simplifican la seguridad de los pagos.
EEDE	Empresas Emisoras de Dinero Electrónico
GMoney S.A.	Es una empresa peruana de propiedad del Grupo La República, creada con la finalidad de brindar servicios de emisión de dinero electrónico a través de soportes tecnológicos, como lo son los teléfonos celulares.
Ontología	La ontología es una rama de la metafísica que estudia lo que hay. Intenta responder preguntas generales como: ¿Qué es la materia? ¿Qué es un proceso? ¿Qué es el espacio-tiempo? ¿Hay propiedades emergentes? ¿Se ajustan todos los eventos a alguna(s) ley(es)? ¿Hay especies naturales? ¿Qué hace real a un objeto? ¿Hay causas finales? ¿Es real el azar? Además, la ontología estudia la manera en que se relacionan las entidades que existen.1 Por ejemplo, la relación entre un universal (rojo) y un particular que "lo tiene" (esta manzana), o la relación entre un acto (Sócrates bebió la cicuta) y sus participantes (Sócrates y la cicuta).
Operador de red móvil:	Son compañías telefónicas que proveen servicios de telefonía para clientes.
PDP	Pagos Digitales Peruanos
Servicios de comercio digitales	El comercio digital o comercio electrónico, también conocido como e-commerce (electronic commerce en inglés) consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas. Originalmente el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el Intercambio electrónico de datos, sin embargo con el advenimiento de la Internet y la World Wide Web a mediados de los años 90 comenzó a referirse principalmente a la venta de bienes y servicios a través de Internet, usando como forma de pago medios electrónicos, tales como las tarjetas de crédito.
Tarjeta de Fidelización	Una tarjeta de fidelización o fidelidad, que también se conoce como tarjeta de beneficios y descuentos o tarjeta de puntos, es el soporte físico de programas que ofrecen bonificaciones (descuentos, premios etc.) al titular cuando consume productos de la empresa emisora de la tarjeta.

	Una tarjeta de fidelidad posibilita el acceso a beneficios especialmente diseñados para los titulares, que pueden gozar sin coste alguno de los beneficios que otorgan a sus socios los establecimientos afiliados (restaurantes, discotecas, hoteles, agencia de viajes, tiendas, cines) que participan en el programa. Es una tarjeta electrónica emitida por determinados fabricantes, cadenas de distribución o empresas de servicios que la entregan gratuitamente a sus clientes. Este tipo de tarjetas permiten a los usuarios la acumulación de puntos en función de los consumos realizados en los establecimientos del emisor.
Token	Un token deseguridad (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación. Los tokens electrónicos tienen un tamaño pequeño que permiten ser llevados cómodamente en el bolsillo o la cartera y su diseño permite llevarlos en un llavero. Los tokens electrónicos se usan para almacenar claves criptográficas como firmas digitales o datos biométricos, como las huellas digitales. Algunos diseños se hacen a prueba de alteraciones, otros pueden incluir teclados para la entrada de un PIN. Existen muchos tipos de token. Están los bien conocidos generadores de contraseñas dinámicas "OTP" (One Time Password) y la que comúnmente se denominan tokens USB, los cuales permiten almacenar contraseñas y certificados y, además, llevar la identidad digital de la persona.
USSD	Acrónimo de Unstructured Supplementary Service Data, Servicio Suplementario de Datos no Estructurados en inglés) es un servicio para el envío de datos a través de móviles GSM, al igual que el SMS.

Fuente: Propia

CAPÍTULO II
METODOLOGÍA

2.1. Materiales

Los materiales que se han utilizado para la presente tesis son los que se describen en la siguiente tabla.

Tabla 3: Descripción de Herramientas

Software	Versión	Descripción
Atlas.ti	7	Herramienta utilizada para descubrir y analizar datos y así evaluar las variables que resultaron de ese análisis
MS-Word	2013	Herramienta de Microsoft Office que permitirá crear documentos de texto requeridos para la gestión y ejecución del proyecto y producto.
MS-Excel	2013	Herramienta de Microsoft Office que permitirá crear documentos de cálculos, encuestas y reportes planos requeridos para la ejecución del proyecto
MS-Power Point	2013	Herramienta de Microsoft Office que permitirá crear las presentaciones (como el alcance, avances, etc.) realizadas en toda la ejecución del proyecto.
ScreenHunter	Libre	Herramienta que permitirá capturar pantallas y compartirla ya sea en un documento u otro medio.
VISIO	2013	Herramienta que permite graficar los diversos modelos de la tesis.
Software	Versión	Descripción
GMAIL	Libre	Se utilizara Gmail para la comunicación con Correos electrónico.
Drive	Libre	Herramienta para compartir información en línea y almacenamiento de datos en la nube.
Zotero	Libre	Herramienta web que sirve como repositorio en donde se almacenan las referencias la Tesis.
Equipo		Descripción
Computadoras personales		Se utilizara las computadoras personales. Req. Mínimos : • Procesador Intel core i5 • Memoria RAM 8gb

- disco duro 500gb

Fuente: Propia

2.2. Métodos

Como se menciona anteriormente la estrategia que se utilizará en el desarrollo del proyecto se sustenta bajo la metodología inductiva como parte del método cualitativo.

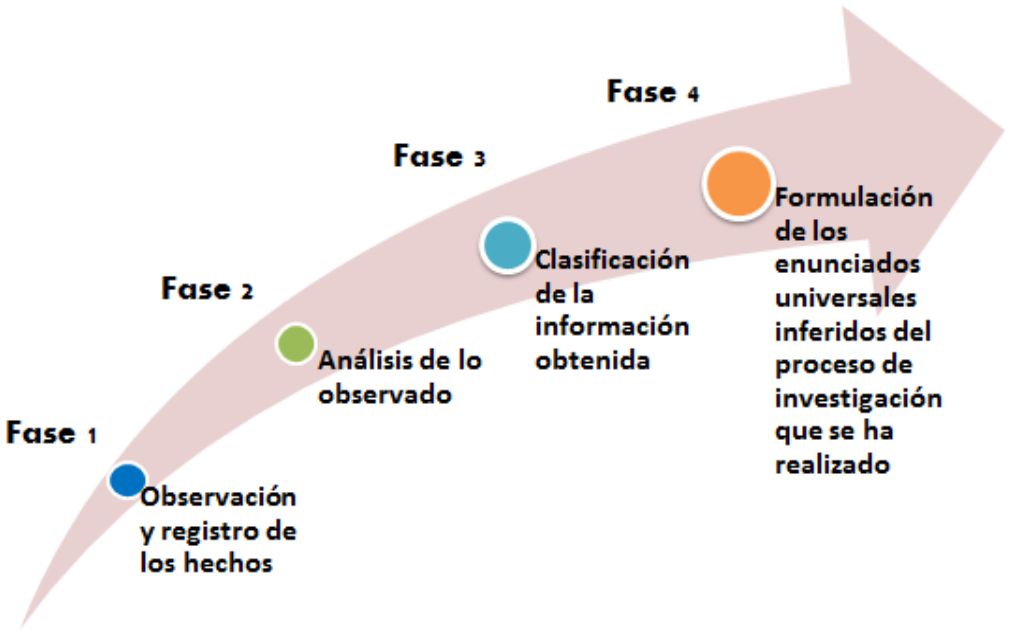


Figura 8: Fases del método inductivo
Fuente: Propia

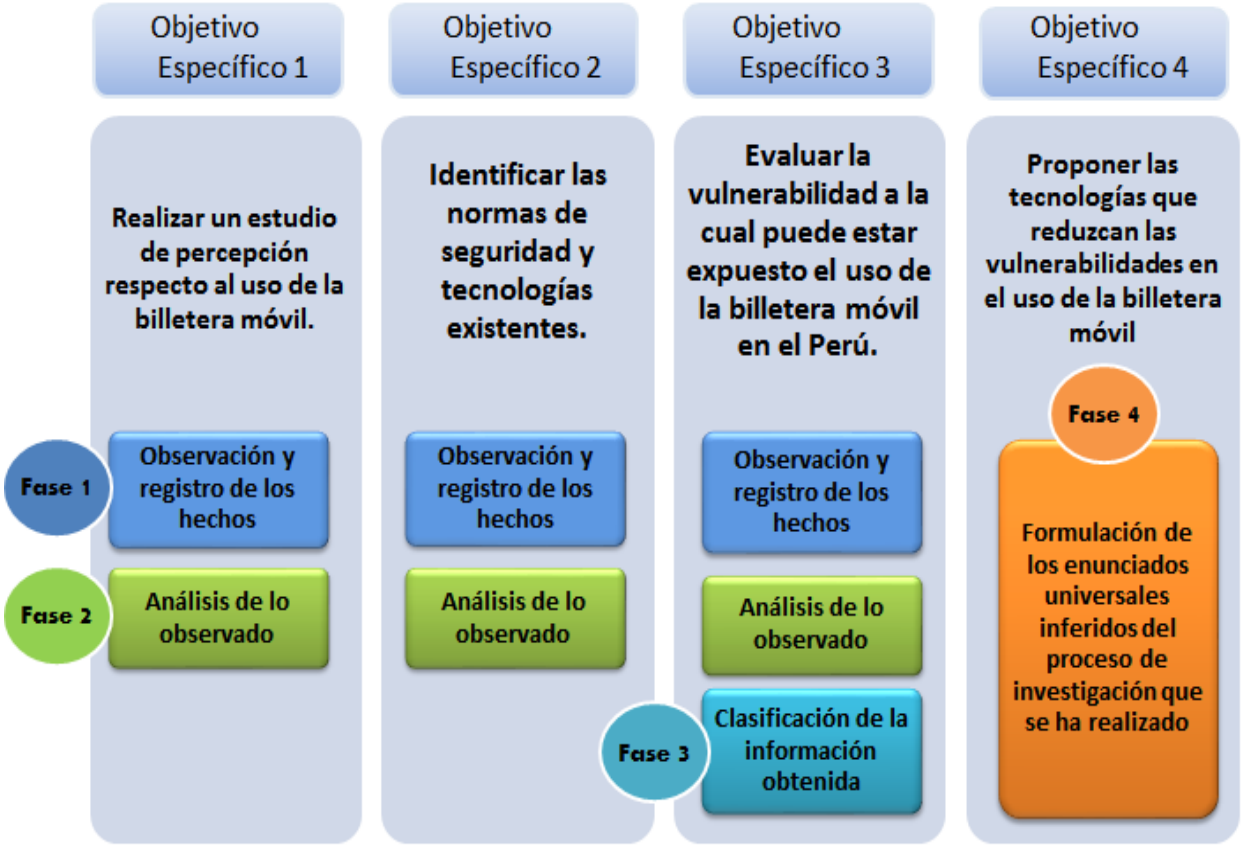


Figura 9: Objetivos específicos vs fases del método inductivo
Fuente: Propia

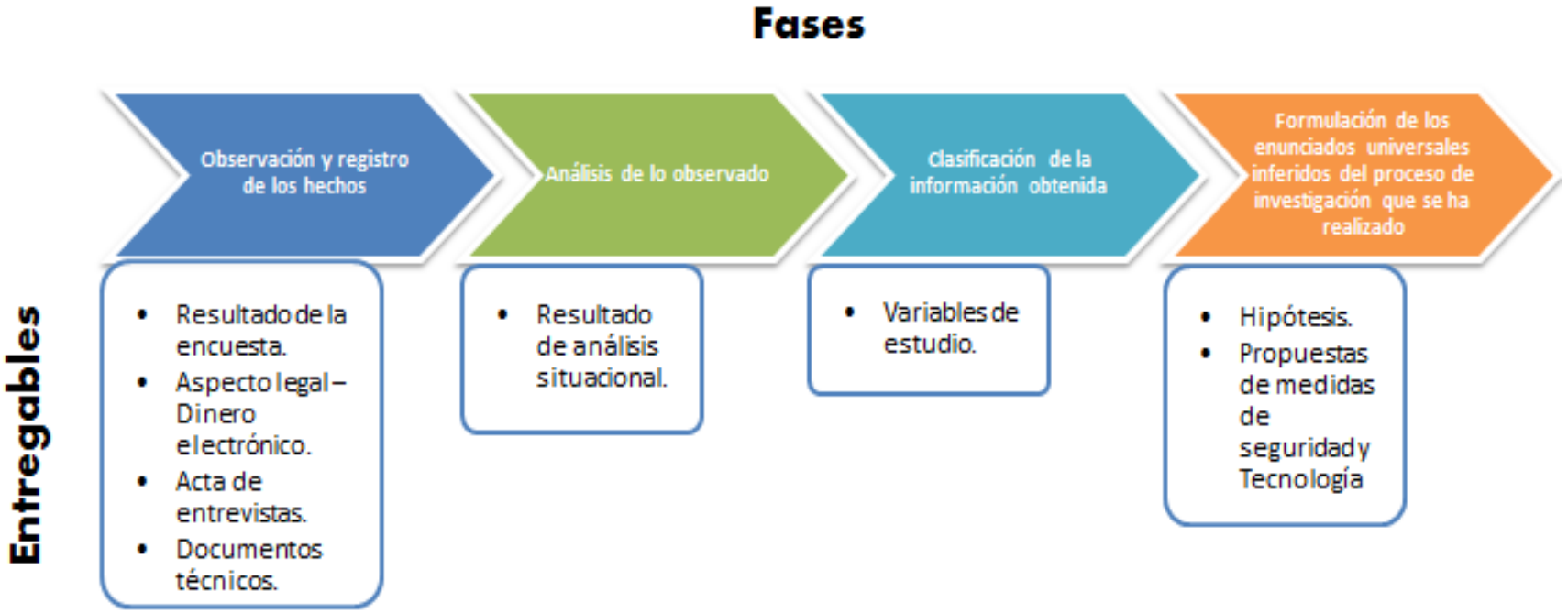


Figura 10: Trazabilidad del método inductivo vs entregables
Fuente: Propia

2.2.1. Fases del método inductivo

A continuación se describirán las Fases del método inductivo con sus respectivos inputs, procesos, y outputs para tener un mapeo claro de lo que se realiza en cada fase.

2.2.1.1 Fase 1: Observación y registro de los hechos.

En esta fase se procede a registrar toda la información recopilada como parte de la observación, esta fase cuenta con tres sub-fases:

- Descripción de los hechos.
- Interpretación del investigador.
- Interpretación de los sujetos estudiados.

Teniendo como input los documentos: Encuestas, ISO – Leyes y normas, entrevistas y documentos recopilados, para luego del proceso obtener como salida los documentos: Resultados de las encuestas, aspecto legal del dinero electrónico, acta de entrevista y por último los documentos técnicos

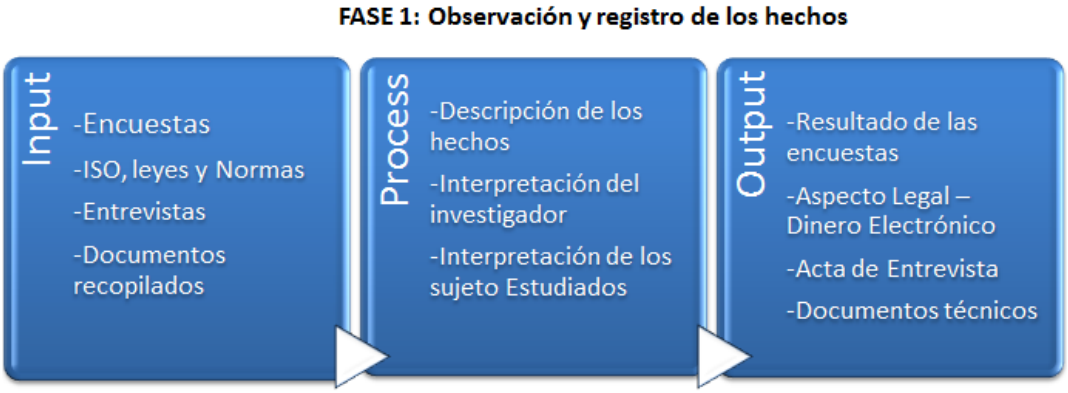


Figura 11: Proceso de observación y registro de los hechos
Fuente: Propia

a) Proceso: Descripción de los hechos

Aquí se describirá los acontecimientos más importantes cubriendo la realidad observada definiendo de forma más restrictiva el foco del análisis.

En este punto se enfocará a describir los elementos que serán materia de estudio como la arquitectura, información técnica asociada al BIM para lo cual

se realizará entrevistas a expertos, encuestas, identificación de las leyes y normas.

Toda la información obtenida por medio de fuentes digitales y físicas plasmado al comienzo de la tesis como antecedentes y bases teóricas de la billetera móvil, contribuirá en la descripción de los hechos.

Los documentos entregados por los expertos serán agregados como anexos al final de la tesis.

b) Proceso: Interpretación del investigador

Constará de dos partes, reflexiones teóricas y reacciones emotivas. La primera está directamente ligada al objetivo principal de la observación y representa un primer esfuerzo reflexivo dirigido a acumular material y puntos de arranque que serán luego unidos en el informe final. Pero tampoco hay que descuidar el segundo componente, el de la visión del investigador. La observación participante requiere una implicación del investigador que va más allá del puro compromiso intelectual: es más, algunos consideran que la participación emotiva es uno de los trámites para la comprensión. La explicitación y el registro, por tanto representa para el observador no sólo una forma de análisis útil para el desarrollo del trabajo, sino también una documentación aprovechable para futuras investigaciones que se puedan iniciar en base a este proyecto de investigación.

La información registrada en la descripción de los hechos permitirá conocer la arquitectura y así poder delimitar el foco de estudio de las vulnerabilidades respecto al BIM.

c) La interpretación de los sujetos estudiados

Aquí se obtendrá la información tal y como surgen de las frases escuchadas, de conversaciones informales con el observador y de entrevistas más formalizadas constituyen el tercer aspecto de esta documentación.

Se describirá el alcance de la tecnología BIM y se interpretara luego los documentos obtenidos como los son las encuestas, y diferentes documentos recopilados de los diferentes medios de comunicación y entidades asociadas al BIM como PDP y Asbanc.

2.2.1.2 Fase 2: Análisis de lo observado

A continuación se procederá al análisis de lo observado, donde se analizará la realidad como conjunto y luego se comparará con la situación de otros países.

Figura 12: Proceso de Análisis de lo observado
Fuente: Propia

2.2.1.3 Fase 3: Clasificación de la información obtenida.

En esta fase se clasificarán las vulnerabilidades existentes las cuales se observaron en el análisis de lo observado.

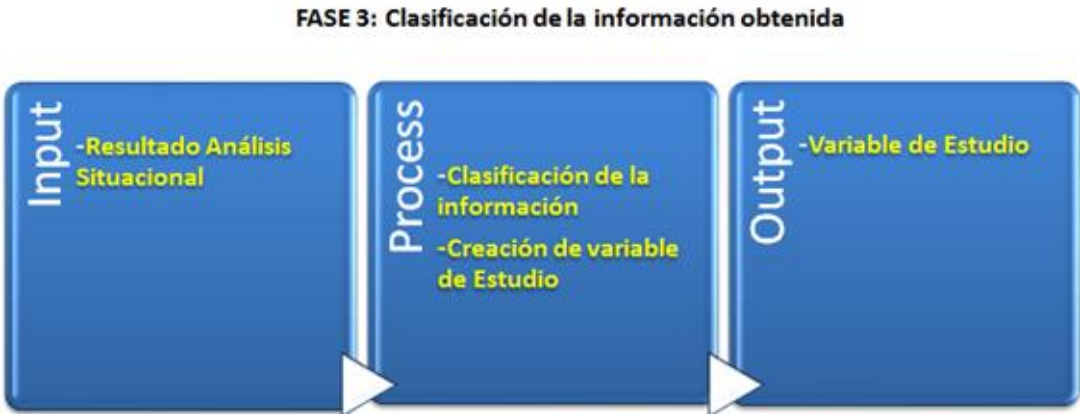


Figura 13: **Proceso de clasificación de la información obtenida**
Fuente: Propia

2.1.1.1 Fase 4: Formulación de los enunciados universales inferidos del proceso de investigación que se ha realizado

En esta última etapa la derivación inductiva que parte de los hechos y permite llegar a una generalización; esto supone que, tras una primera etapa de observación, análisis y clasificación de los hechos, se logra postular a una hipótesis que brinda una solución al problema.

Figura 14: Proceso de formulación de la hipótesis
Fuente: Propia

CAPÍTULO III
DESARROLLO DEL PROYECTO

3.1. Estudio de la percepción respecto al uso de la billetera móvil.

Para poder conocer la percepción que tienen las personas que viven en Lima Metropolitana se ha tomado una muestra de 50 personas para poder conocer si tienen conocimiento de la BIM, medidas de seguridad al realizar una operación así como de los riesgos a los cuales puede estar sometido.

3.1.1. Fase 1: Observación y registro de los hechos

En esta fase como documento input se encuentran las encuestas realizadas, la cual es necesaria para realizar los procesos: Descripción de los hechos, Interpretación del Investigador e Interpretación de los sujetos estudiados, obteniendo como output el resultado de las encuestas. En la siguiente figura se puede observar lo antes mencionado.

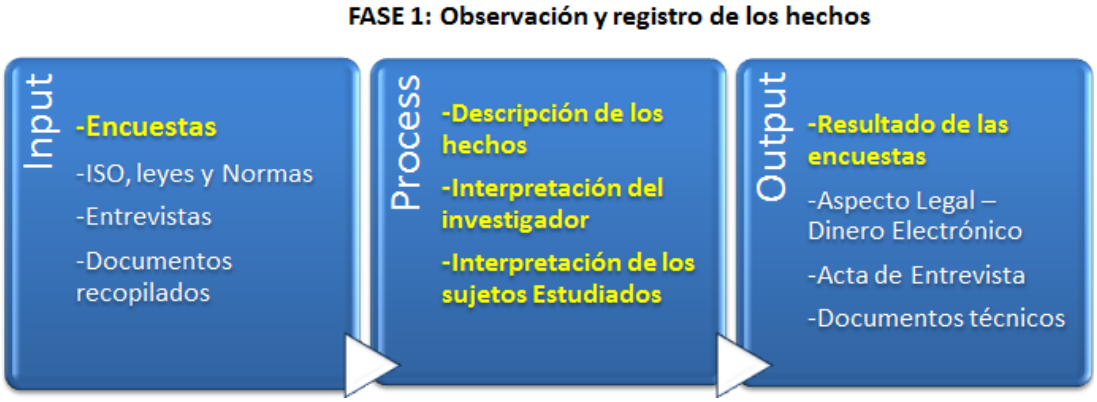


Figura 15: Primer entregable Fase I
Fuente: Propia

3.1.1.1 Proceso: Descripción de los hechos

Para poder conocer la percepción que tienen las personas que viven en Lima metropolitana se tomó una muestra de 50 personas para poder conocer si tienen conocimiento del BIM así como de los riesgos a los cuales puede estar sometido.

Antes de comenzar con el análisis de los datos que se lograron obtener a través de las encuestas realizadas en varios distritos de la ciudad es fundamental tener en cuenta que cualquiera sea el método que se utilice para analizar siempre será una interpretación de lo analizado pues al analizar se aísla porciones de discurso, se logra una selección particular de la información que posiblemente otro investigador no haría.

Obtener esta información no solo apoya a la experiencia de vida, el mundo sociocultural, sino también en la intuición y, fundamentalmente, en los objetivos e hipótesis por ello, al analizar, se agudiza los sentidos ya que, la mayoría de las veces, se toma un punto de vista del marco sociocultural que, por lo general, no es el de aquellos con quienes se realizó la investigación. Para realizar esta encuesta fue importante ver la posición social que ocupan las personas encuestadas, por ello se seleccionó 50 personas de diversos distritos de Lima, principalmente de los sector E.

Tabla 4: Clasificación sector económico del Perú

SECTOR	DETALLE	INGRESO BRUTO
A	Clase alta	S/.20 000 a mas
B	Clase media	S/. 8 000 a S/.19 000
C	Clase media baja	S/. 4 000 a S/.7 000
D	Clase pobre	S/.16 000 a S/.5 000
E	Clase en extrema pobreza	Menos de S/.1 500

Fuente: Propia

En la muestra aleatoria se tomó los siguientes distritos: Comas, Los Olivos, La Victoria, San Juan de Lurigancho, San Juan de Miraflores, El Agustino, Villa el Salvador y Villa María del triunfo.

Es necesario explicar cuál es el motivo fundamental de la encuesta que es poder tener información acerca del posicionamiento de la Billetera Móvil del Perú , cuanto conocen las personas acerca de esta herramienta, sus riesgos y la posibilidad de incluirse a este medio de pago electrónico que en futuro tendrá muchas más herramientas.

Muestra=50

Alcance= Lima metropolitana

N° de preguntas = 9

3.1.1.2 Proceso: Interpretación del investigador

Pregunta N°1

¿Sabe usted de la existencia de la Billetera Móvil en el Perú?

SÍ	54%
NO	46%

Se aprecia en los indicadores que si bien es cierta la mayoría de personas conoce de la existencia de esta herramienta de pago pero es preocupante el hecho de que hay un alto porcentaje de personas que desconocen su existencia por diversos factores que se percatan al momento de realizar la encuesta personalizada.

Pregunta N°2

¿Ha realizado alguna transacción con la billetera Móvil?

SÍ	2%
NO	98%

En esta pregunta se puede identificar que si bien es cierto que la mayoría de personas saben de la existencia de este medio de pago, la mayor parte de personas encuestadas (por no decir su totalidad) nunca ha hecho uso de este medio de pago, el objetivo en adelante será saber o identificar los motivos por el cual la muestra se resiste al uso de esta herramienta.

Pregunta N°3

¿Estaría dispuesto a utilizar la billetera móvil para realizar una transacción bancaria?

SÍ	**98%**
NO	2%

En esta pregunta la mayoría de entrevistados indican que sí están dispuestos a usar la herramienta si ésta asegura el hecho de no presentar problemas de seguridad en un futuro, garantizando una transacción satisfactoria, además que consideran una buena idea el no traer dinero en el bolsillo debido a la ola de delincuencia en la cual se encuentra en nuestra sociedad.

Pregunta N°4

¿Hasta qué importe estaría dispuesto realizar con una Billetera Móvil?

0	2%
Más de 10	22%
Más de 100	64%
Más de 500	12%

Se evidencia en los indicadores que la mayoría de personas estaría dispuesta a probar esta herramienta haciendo transacciones de más de 100 soles pues aseguran que si encuentran garantizable esta herramienta podrían hacer transacciones de más dinero en un futuro, evitando robos a futuro.

Pregunta N°5

¿Sabe usted sobre alguna medida de seguridad para este medio de pago?

SÍ	18%
NO	**82%**

En la presente pregunta se evidenció que la mayoría de la muestra no tenía conocimiento acerca de las medidas de seguridad con las que cuenta la billetera móvil, la mayoría de personas indicaban que estaban desinformadas acerca de este punto en particular y que quizás por este motivo no era popular el uso de la BIM.

Pregunta N°6

¿Conoce algún riesgo en usar la Billetera Móvil?

SÍ	**92%**

NO	8%

Al realizar esta pregunta a los encuestados se evidenció que la mayoría de personas encuestadas tiene cierto prejuicio con el uso de esta herramienta pues la considera insegura, en la mayoría de casos las personas se preguntan ¿Qué sucedería si me roban mi celular?, ¿Se van a apropiar de mi dinero?, existe conocimiento sobre medidas de seguridad en estos casos pero al parecer hay cierta desinformación en la población.

Pregunta N°7

¿El uso de la Billetera Móvil es un modo seguro?

SÍ	36%
NO	**64%**

Al realizar la presente pregunta a los encuestados se evidencio que la mayoría considera insegura esta herramienta de pago al desconocer todo lo que involucra a las medidas de seguridad, lo que genera cierto temor a utilizar este medio de pago.

Pregunta N°8

¿Utilizaría la Billetera Móvil de conocer las medidas de seguridad?

SÍ	**96%**
NO	4%

Se evidencia que las personas están dispuestas a utilizar este medio de pago si esta garantiza la completa seguridad de sus transacciones, la mayoría de personas aduce que esto los prevendría de robos a futuro y solucionaría muchos problemas.

Pregunta N°9

¿Suele utilizar tarjetas de créditos para realizar compras?

SÍ	**64%**
NO	36%

Se evidencia que la mayoría de los encuestados cuenta con una tarjeta de crédito pero a la vez desconoce acerca del uso de la herramienta por falta de información.

3.1.1.3 La interpretación de los sujetos estudiados

La interpretación de los objetos estudiados se ha plasmado en el documento Resultado de la Encuesta, *Ver Anexo 6.*

3.1.2. Fase 2: Análisis de lo observado

En esta fase se procede a realizar un análisis en base a la interpretación del investigador y el documento resultado de las encuestas.

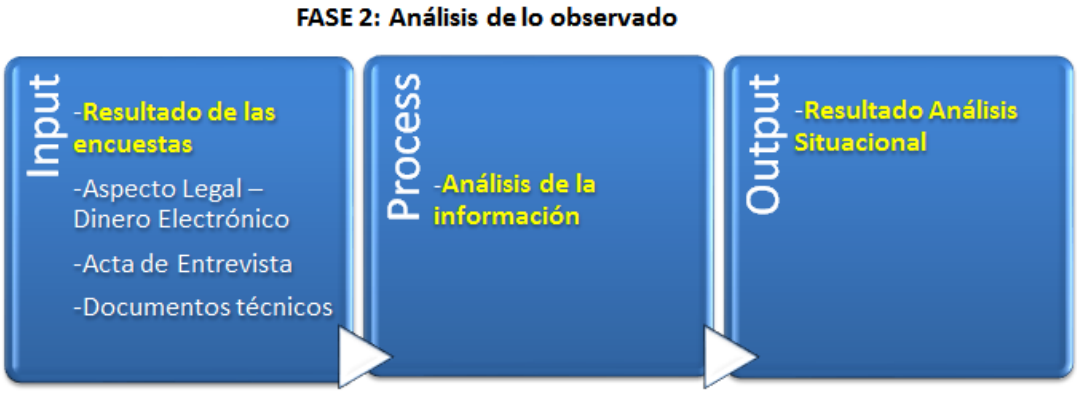


Figura 16: Entregable de la Fase 2 proveniente del Resultado de las encuestas
Fuente: Propia

3.2.1.1 Análisis de la Encuesta

En esta etapa se ingresaran los resultados de las preguntas realizadas en la encuesta.

Los resultados de la pregunta número 10 de la encuesta son recomendaciones brindadas por el usuario.

Qué recomendaciones daría Ud. para usar la Billetera Móvil?:

Estas recomendaciones se ingresaran a la herramienta Atlas.ti y así se logrará descubrir y analizar sistemáticamente los fenómenos complejos ocultos en los datos no estructurados, ya que este programa proporciona herramientas que permiten localizar las palabras como código y anotar los resultados en materia de datos principales para evaluar su importancia.

El análisis del resultado de la encuesta permitirá obtener las variables de estudio que posteriormente servirán para la formulación de hipótesis.

Análisis de la encuesta ver punto 3.3.2.2 b).

3.2. Normas de seguridad y tecnologías existentes en el Perú.

Las normas, leyes e ISO encontradas se registran en la fase de observación y registro de los hechos. Asimismo de los antecedentes registrados en esta tesis se puede observar que la tecnología usada en la BIM es el USSD información que se corrobora en la arquitectura del BIM que se puede observar más adelante en el punto 3.3.

3.2.1. Fase 1: Observación y registro de los hechos

En esta fase como documento input tenemos a las ISO, leyes y normas las cuales son necesarias para poder realizar los procesos: Descripción de los hechos, Interpretación del Investigador e Interpretación de los sujetos estudiados, obteniendo como output el aspecto legal del dinero electrónico. En la siguiente ilustración se puede observar lo antes mencionado.

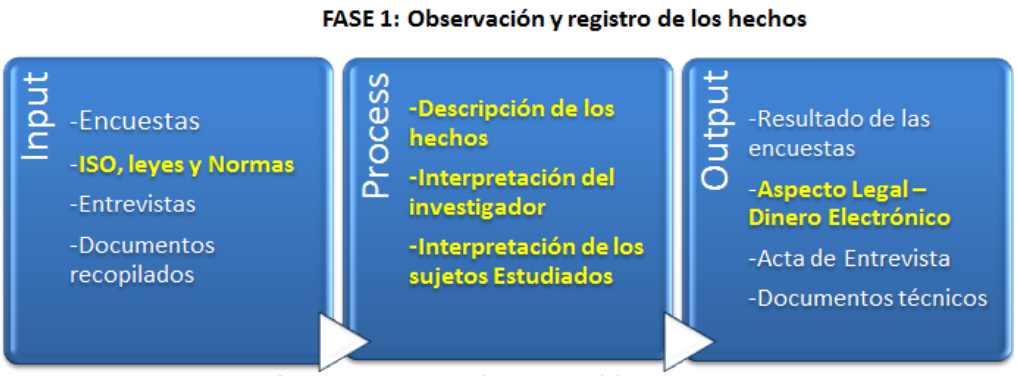


Figura 17: Segundo entregable Fase I
Fuente: Propia

3.2.1.1 Descripción de los hechos

Conocer las normas de seguridad que existen en el marco legal puede a ayudar a identificar cuan respaldado está el dinero de un cliente que este afiliado al servicio de dinero electrónico con el BIM. También el conocer que leyes relacionadas al dinero electrónico puede ayudar a reducir el impacto que tenga una vulnerabilidad si existen leyes que puedan aplicar alguna sanción a los involucrados en la causa que dio origen a dicha vulnerabilidad.

Las ISO que se necesitan para poder realizar el análisis sobre las medidas de seguridad relacionadas al BIM son:

- ISO 17799 (Capitulo 1, punto 1.3)
- ISO 27001 (Capitulo 1, punto 1.4)
- ISO 27002 (Capitulo 1, punto 1.5)

Los documentos que se necesitan para poder realizar el análisis sobre las normas legales que existen son:

- Ley N° 27799
- Normas emitidas por la SBS

3.2.1.2 Interpretación del Investigador

De acuerdo al punto anterior en el Perú actualmente existen normas que avalan el dinero electrónico, pero aún se analizará algunos puntos debido a que la presente tesis solo se concentra en el estudio de las normas que existen para el dinero electrónico, por lo cual se detallará en el marco legal las normas que se encontró y como estarían relacionadas con probables vulnerabilidades que pueden suceder. También se describirá como intervienen las ISO en el ámbito relacionado en la seguridad con el BIM.

a) Marco Legal del Dinero Electrónico en el Perú.

Las leyes, normas e ISO que se analizarán son las que están relacionadas con la primera fase del Modelo Perú, fase que se encuentra actualmente en funcionamiento. Como se puede ver en el siguiente gráfico.

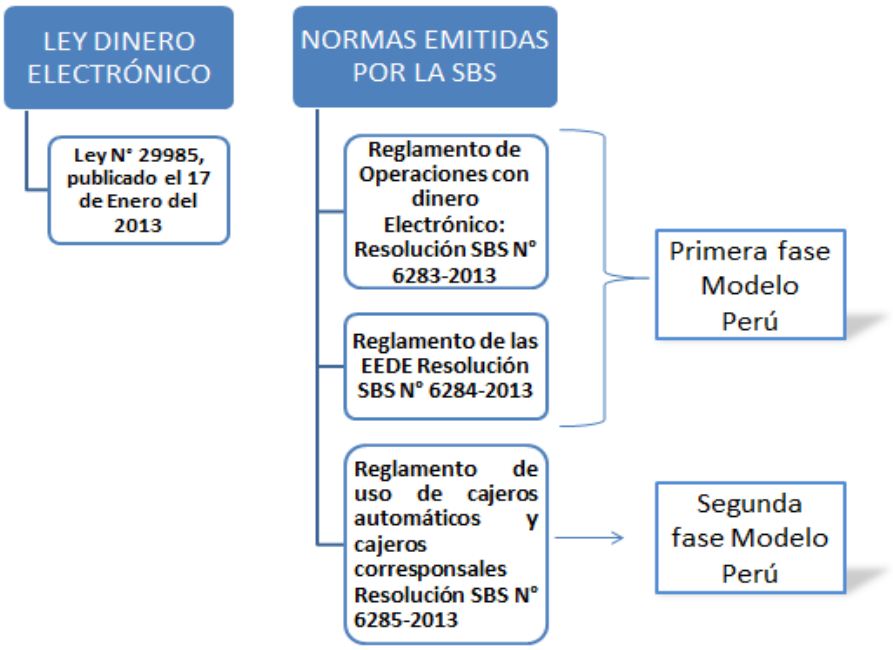


Figura 18: Reglamento de Dinero Electrónico
Fuente: Propia

b) ISO relacionadas con la seguridad en el BIM

De acuerdo a lo revisado en la ISO 17799 se presenta un cuadro de los puntos a considerar en el BIM para el análisis situacional.

Tabla 5: Trazabilidad ISO 17799

PUNTOS	ISO 17799
Confidencialidad. Asegurar que únicamente personal autorizado tenga acceso a la información.	-Políticas de Seguridad -Seguridad física y del Entorno.
Integridad. Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.	-Gestión de Comunicaciones y operaciones. -Clasificación y control de Activos

Disponibilidad. Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.	Aspectos organizativos para la seguridad -Control de accesos

Fuente: Propia

3.2.2. Fase 2: Análisis de lo observado

En esta fase se analizará la información de las leyes y normas encontradas en la fase anterior, el resultado será plasmado en el Resultado de Análisis Situacional.

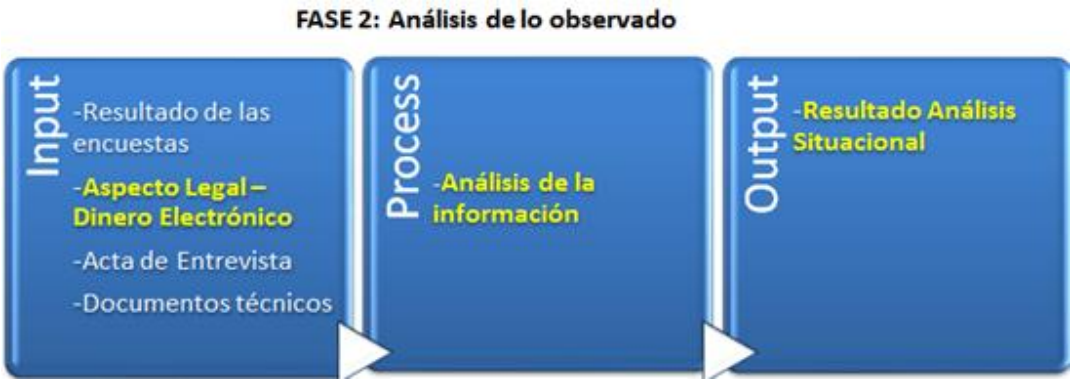


Figura 19: Entregable de la Fase 2 proveniente del Aspecto Legal
Fuente: Propia

A continuación se procede con el análisis de las normas legales identificadas.

3.2.2.1 Análisis Ley N° 29985 y Normas emitidas por la SBS.

En el Perú se cuenta con normas de seguridad tales como la Ley del dinero Electrónico: Ley N° 29985**,** publicado el 17 de Enero de 2013 en el diario El Peruano (El Peruano, 2013), el cual tiene como objetivo regular la emisión de dinero electrónico y determinar las empresas autorizadas a emitirlo. Esta ley ampara la protección de datos personales. En uno de los artículos se mencionada que se exonera el IGV a las Ventas por un período de 3 años, contado a partir de la vigencia de la presente ley. Es importante tener conocimiento de esto, debido a que puede pasar que un día se observe que se aplicó el IGV por alguna transacción realizada.

Un punto importante que debe tener claro el cliente afiliado al BIM es que si transcurren diez 10 años sin que una cuenta de dinero electrónico tenga movimientos y sin que nadie reclame, entonces estos fondos pasarían a la Dirección General de Endeudamiento y Tesoro Público del Ministerio de Economía y Finanzas.

Uno de los reglamentos donde se define el tipo de cuenta que usa la billetera móvil es el Reglamento de Operaciones con dinero Electrónico: Resolución SBS N° 6283-2013 (El Peruano, 2013), en este reglamento se menciona que las cuentas de dinero electrónico simplificadas (sujetas a límite por transacción) solo pueden ser abiertas por personas naturales nacionales y extranjeras, en moneda nacional en el territorio nacional. Esto podría brindar un apoyo en el marco legal para una prevención de lavado de activos o posibles robos masivos de dinero electrónico.

Si bien es cierto que existen normas como las antes mencionadas cabe indicar que aún no existe un reglamento preciso sobre cómo sería el procedimiento con personas que tengan una cuenta de dinero electrónico y que presentan problemas con la SUNAT. Por ejemplo, en una entrevista que realizó el periodista Aldo Mariátegui a Miguel Arce, Gerente Comercial de la Plataforma de ASBANC, sobre el BIM (Radio Capital, 2016), Arce indicó que el tipo de cuenta que maneja el cliente cuando se afilia al BIM es una cuenta de dinero electrónico (Sustituir el dinero físico en dinero virtual) que es considerado como una cuenta no bancarizada por lo tanto si un cliente presenta problemas con la SUNAT, lo que genera que no pueda tener ningún tipo de cuenta Bancaria porque la SUNAT absorbería todos sus ahorros o depósitos, esto no aplicaría para el BIM debido a que el BIM es normado por el concepto del Cuenta no bancarizada. Otro punto importante que se puede encontrar en la resolución son los reglamentos sobre las operaciones que pueden realizarse con dinero electrónico (conversión y reconversión, pagos, transferencias, etc.

Las empresas emisoras de dinero electrónico (EEDE) también están sometidas a reglamentos expuestos en el Reglamento de las EEDE Resolución SBS N° 6284-2013 (El Peruano, 2013), donde contempla como

una de las medidas prudenciales el que las EEDE deban contar con un patrimonio efectivo no menor al dos por ciento (2%) del total del dinero electrónico en circulación. Esto permite en cierto punto tener un respaldo legal de que el dinero electrónico se encuentra en circulación.

3.2.2.2 Análisis ISO

Se puede observar que existen ISO como la 17799 (El Peruano, 2007), ISO27001 (El Peruano, 2014) e ISO 27002 (El Peruano, 2007) relacionados con la seguridad en la información de los datos, así como la gestión de incidencias.

Respecto a la gestión de incidencias la BIM maneja un número telefónico - 0 -800-10838 - al cuál se puede llamar para registrar una incidencia o también se puede enviar un reclamo por la web - http://mibim.pe/reclamos/- llenando previamente un formulario con la información necesaria para analizar la incidencia reportada.

En torno a la seguridad de datos en el BIM el ingresar una clave para confirmar una operación se expone a que algunos programas intrusos puedan tomar la clave para fines de robo informático y dinero electrónico.

3.3. Vulnerabilidades a la cual puede estar expuesto el uso de la billetera móvil en el Perú.

A continuación para conocer las vulnerabilidades es necesario comenzar con la observación y registro de los hechos:

3.3.1. Fase 1: Observación y registro de los hechos

Se realizó una entrevista telefónica con la empresa de Pagos Digitales Peruanos para poder obtener información sobre el BIM. Se obtuvo información digital del documento “Modelo Perú” (Pagos Digitales Peruanos S.A., 2016), lo cual servirá para poder entender el funcionamiento. La información es de carácter confidencial y por lo tanto no se adjuntará como anexo. La información obtenida se puede ver a detalle en el documento Acta de entrevista. V*er Anexo 7*.

Para poder obtener un análisis objetivo también fue necesario apoyarse en otras fuentes tales como internet, tesis, noticias y otras entrevistas realizados por terceros. Toda esta información recopilada se puede ver en las bases teóricas.

Figura 20: Tercer entregable Fase 1
Fuente: Propia

3.3.1.1 Proceso: Descripción de los hechos

El modelo Perú (2016) tiene tres fases que fueron descritas en las bases teóricas en el capítulo I. En la presente tesis se limitará a analizar el entorno de la primera fase de este modelo, debido a que es la que actualmente está en funcionamiento en el Perú. Esta primera fase involucra todas las operaciones disponibles como recarga de celular, envío de dinero, retiro de dinero (sacar plata) y poner plata en el BIM, así como el pago a la institución de TEPSUP, este punto no será considerado en la tesis debido a que su análisis involucraría analizar las operaciones de pago que complementan a la segunda fase del proyecto Modelo Perú.

Entrevistas

Tabla 6: Resumen de entrevista

Empresa	Supuesto epistemológico del Objeto	Supuesto epistemológico del Investigador	Supuesto metodológico

PDP	Reconocer el Proyecto Modelo Perú	Colaborador	Observación y registros de los hechos

Fuente: Propia

La tesis se ha apoyado en el documento “Modelo Perú” que contiene información de la arquitectura y los componentes del BIM, para poder estudiar los elementos que intervienen en la arquitectura.

a) Elementos que intervienen en la Arquitectura del BIM

El BIM está basado en la solución de EWP (Ericsson Wallet Platform) de la compañía Ericsson.

La siguiente arquitectura ha sido tomada de una parte de la arquitectura del BIM que se encuentra en el documento “Modelo Perú”, así como la definición de sus elementos, esto con el fin de poder enfocarnos en la primera fase que se encuentra en funcionamiento (Pagos Digitales Peruanos S.A., 2016).

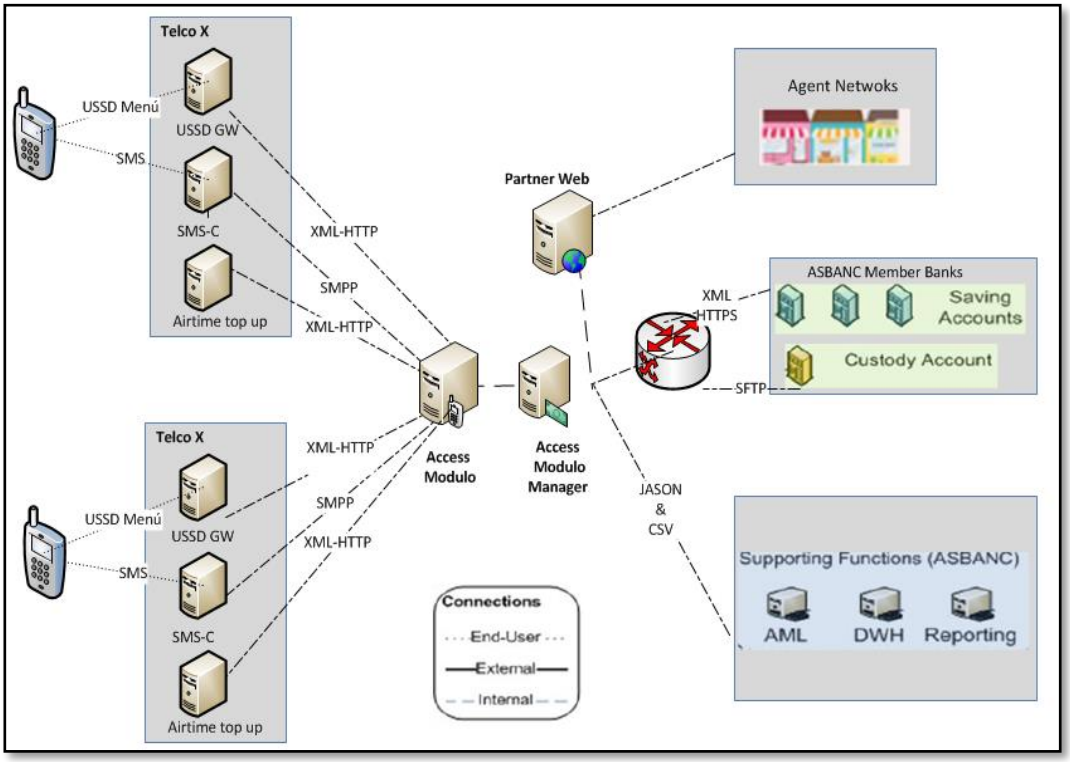


Figura 21: Arquitectura BIM modelo Perú
Fuente: Propia

Continuación se procede a describir los elementos que intervienen en la arquitectura del BIM con el fin de poder utilizarlos en el análisis.

- **TelCos:**

  Las TelCos son los operadores con los que trabaja el BIM, en esta primera etapa los operadores afiliados son Claro, Movistar y Entel quienes tienen la opción de integrarse a la plataforma por una conexión directa VPN o a través de la red Bancared. Cada tema será tratado en forma específica de acuerdo a la topología a definir.

- **Menú USSD**

Es la interfaz a la cual accede el usuario para afiliarse y realizar alguna operación. Para acceder a esta interfaz no es necesario descargar alguna aplicación.

El acceso USSD se activará con el comando *838#. Durante cada sesión USSD, el usuario puede recibir mensajes informativos y de acción, los cuales

no quedarán registrados en su celular al salir del sistema. El menú siempre mostrará el saldo de la billetera al ingresar. Al finalizar cada sesión, el usuario recibirá un mensaje SMS con la información de la transacción realizada.

- **USSD:**

Los mensajes USSD son los que transportan la clave al momento de confirmar una operación.

Las telcos serán responsables de manejar la lógica del menú y toda la validación de datos, tales como la solicitud de códigos PIN repetidas y la verificación del algoritmo del DNI antes de enviar las solicitudes a EWP.

Es un equipo de enlace USSD externo, administrado por una Telco, es responsable de proveer a los usuarios un canal de entrada basado en USSD integrándose con la EWP a través de protocolos basados en XML/IP. Ericsson Wallet Platform tiene capacidades para conectarse a múltiples USSD Gateways.

- **SMS:**

En el BIM los SMS se usan para la emisión de mensajes informativos como los de bienvenida, la cantidad de saldo que actualmente tienes, confirmación de una recarga.

- **SMS-C**

El SMSC es un equipo administrado por una Telco, estando a cargo de las notificaciones al usuario y se integra a EWP.

- **Ericsson XML sobre API de HTTP(s)**

La API de XML sobre HTTP es usada como el punto de integración para los sistemas internos de EWP.

- **Protocolos SSL**

El protocolo SSL permite que las aplicaciones se comuniquen en la red de una manera segura evitando la intercepción y alteración fraudulenta de información.

b) Uso del USSD y SMS en las operaciones:

A continuación se describe el tipo de tecnología usado en las operaciones. El acceso USSD se activará con el comando *838#. Durante cada sesión USSD, el usuario puede recibir mensajes informativos y de acción, según lo que informa PDP los mensajes no quedarán registrados en el celular al salir del sistema.

Para fines didácticos en los siguientes gráficos se mostraran los recuadros con color negro para el uso del USSD en los mensajes y los recuadros rojos para mensajes enviados vía SMS.

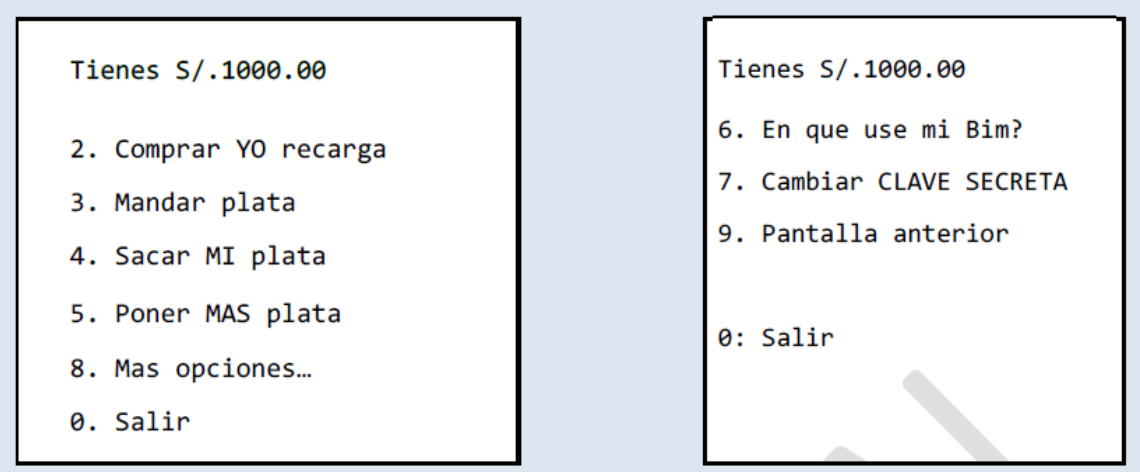


Figura 22: Menú USSD usuario registrado
Fuente: Propia

c) Ingreso al BIM

En el proceso de activación el cliente genera su clave secreta. La clave secreta es una clave numérica de cuatro dígitos con las siguientes restricciones: no puede tener más de 2 números repetidos o más de 2 números consecutivos, ni tampoco los cuatro primeros o últimos dígitos del DNI o del usuario. Tampoco ser iguales a las cuatro últimas claves secretas utilizadas anteriormente. A continuación se describen los pasos:

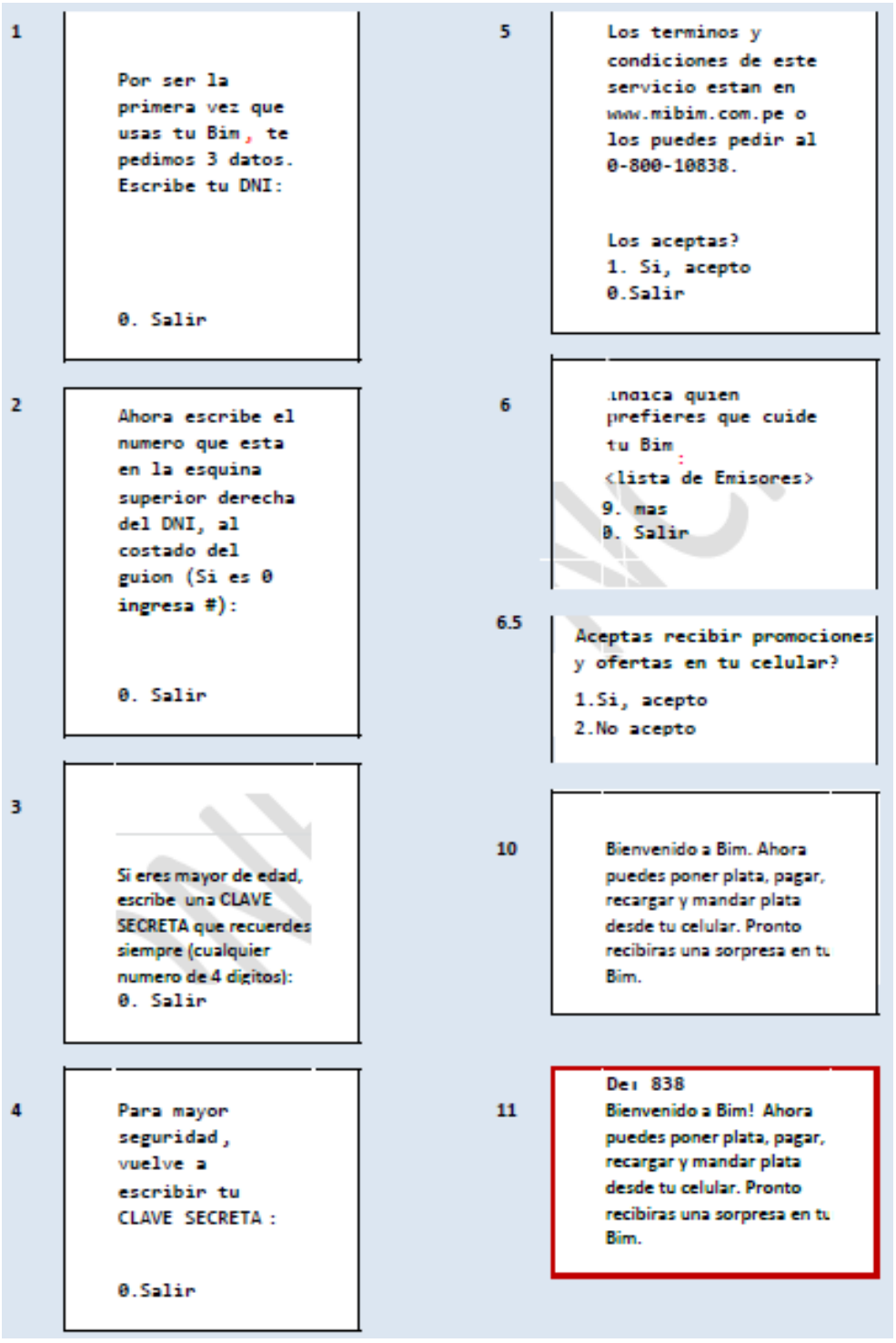


Figura 23: Menú actívate
Fuente: Propia

d) Comprar y/o Recarga

La billetera electrónica permite realizar la recarga de cualquier celular, sea propio o de terceros. Quien recarga, recibe un mensaje de confirmación de la

plataforma y un SMS. El celular recargado recibe un mensaje de su operador informándole de la recarga exitosa.

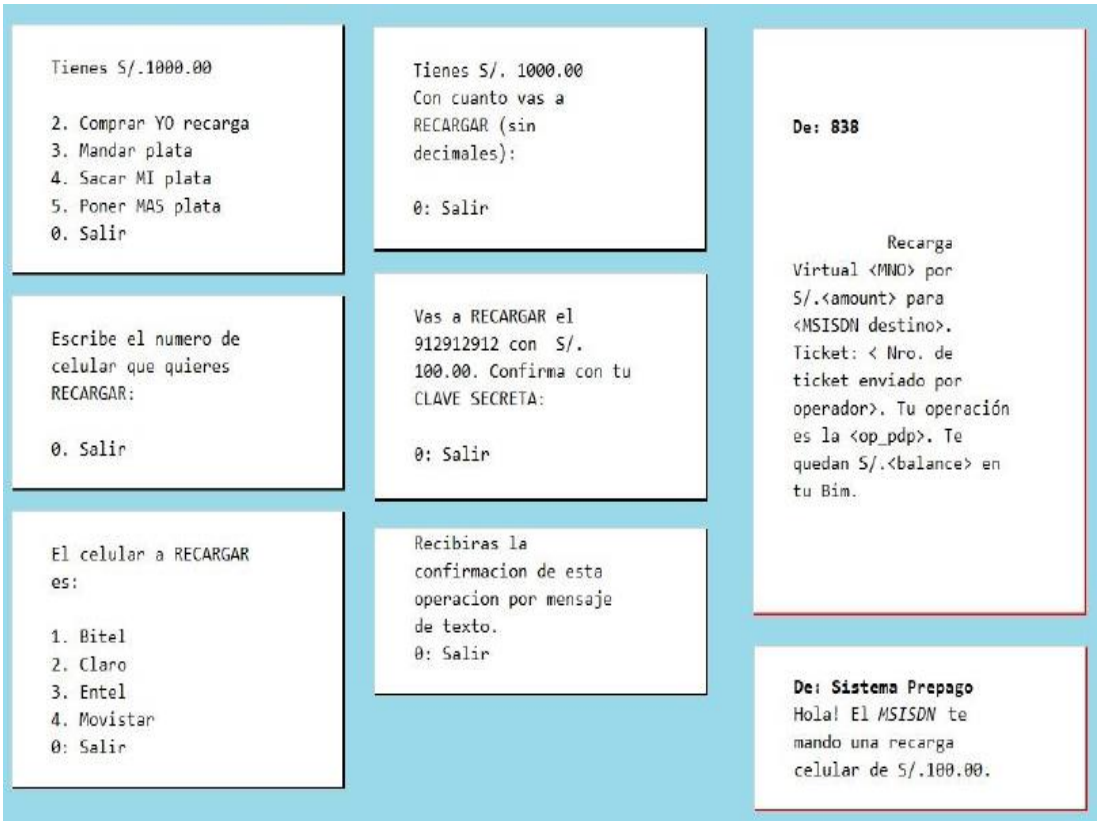


Figura 24: Menú mandar plata
Fuente: Propia

e) Mandar plata

Se puede mandar plata entre usuarios registrados en el sistema de billeteras electrónicas y también a celulares aún no registrados en la plataforma; este tipo de envío se llama “invitations”.

La plataforma revisará si el destinatario es un usuario registrado o no. De acuerdo a ello, se determinará la forma en la que se enviarán los fondos al destinatario.

Si el destinatario está registrado, el usuario especificará el monto, el celular del destinatario, y confirmará con su clave secreta.

Si el destinatario no está registrado aún, se notificará de la situación al remitente y, se le pedirá que confirme si quiere realizar el envío igualmente,

escriba su clave secreta. EWP le enviará al destinatario un SMS con un mensaje de invitación para que ingrese al *838# y se registre para recibir el dinero.

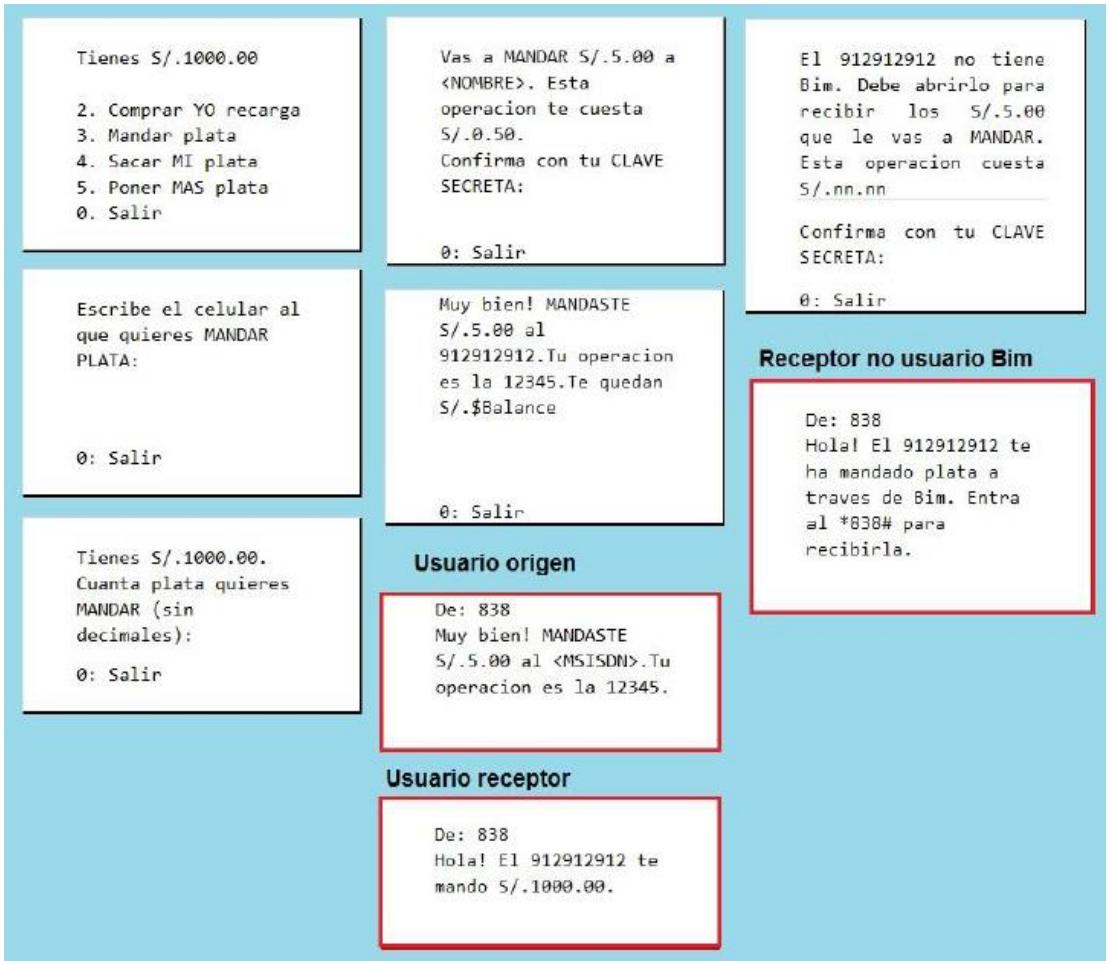


Figura 25: Menú comprar y/o recargar
Fuente: Propia

f) Sacar plata

Esta transacción es iniciada vía USSD o Partner web por el agente, previa indicación del usuario. El agente indicará el número asociado a la cuenta de dinero electrónico y el monto que el cliente desea retirar. Al concluir esta operación, el cliente recibirá un mensaje SMS para que ingrese al *838# y dé la confirmación del retiro con su clave secreta.

El usuario solo podrá tener una solicitud de sacar plata activa por vez. No podrá iniciar una nueva solicitud de sacar plata hasta después de confirmar la anterior o esperar que esta expire, válida por 10 minutos.

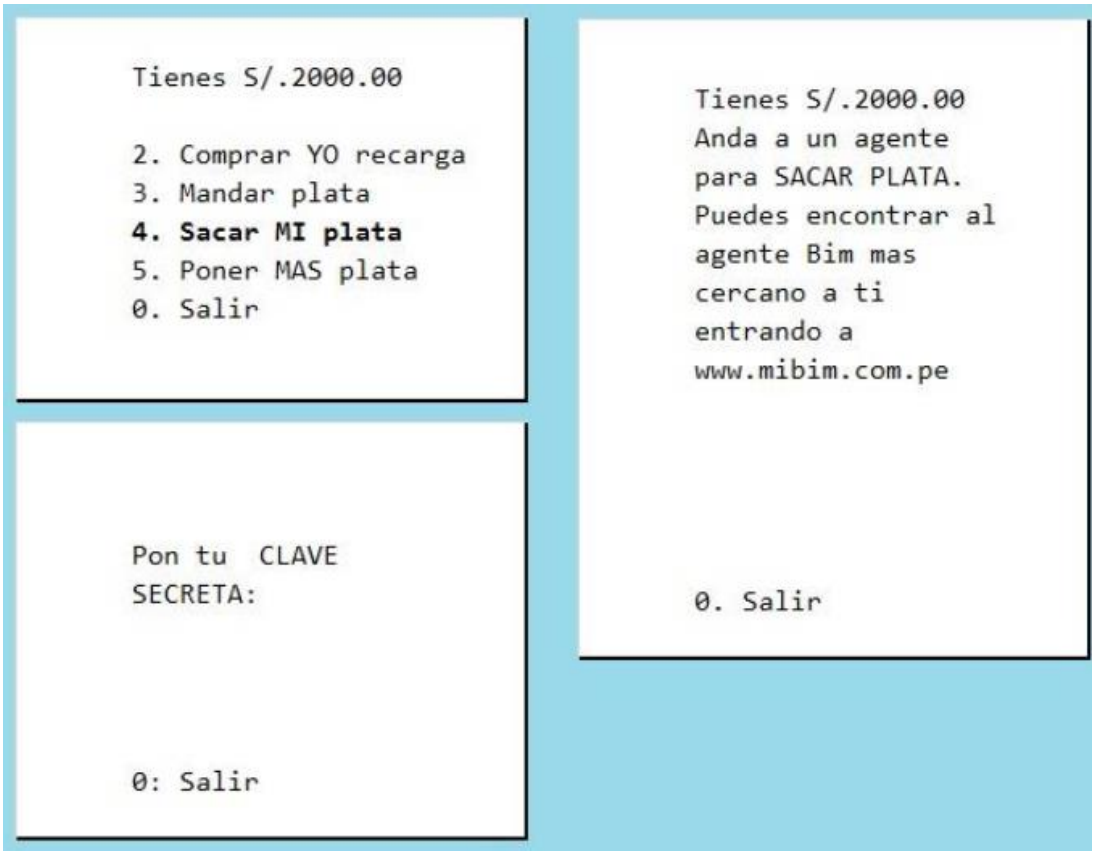


Figura 26: Menú sacar mi plata (Cuando el usuario no tiene registros pendientes)
Fuente: Propia

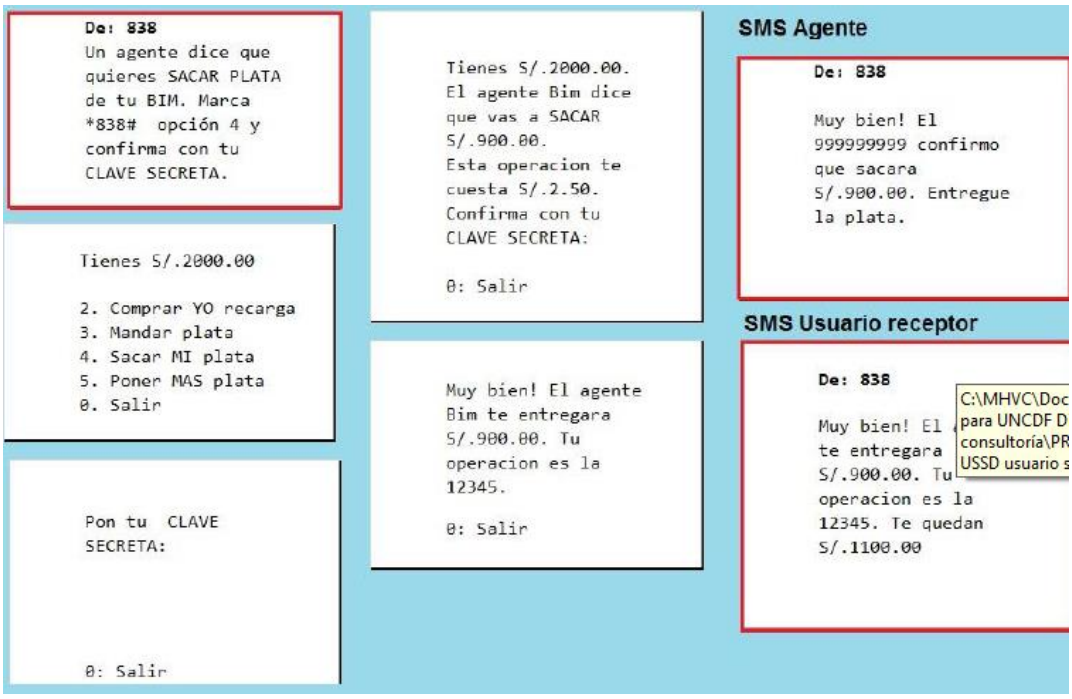


Figura 27: Menú sacar mi plata (Cuando el usuario si tiene registros pendientes)
Fuente: Propia

g) Poner más plata

Esta transacción se realiza en un agente autorizado (Agentes con letrero "BIM", de dinero electrónico y permite al usuario convertir su dinero físico en electrónico; es decir, cargar su billetera móvil.

Para esto, es requisito que el usuario esté registrado y activo, y que el agente esté registrado, activo y que cuente con fondos para poder realizar la transacción.

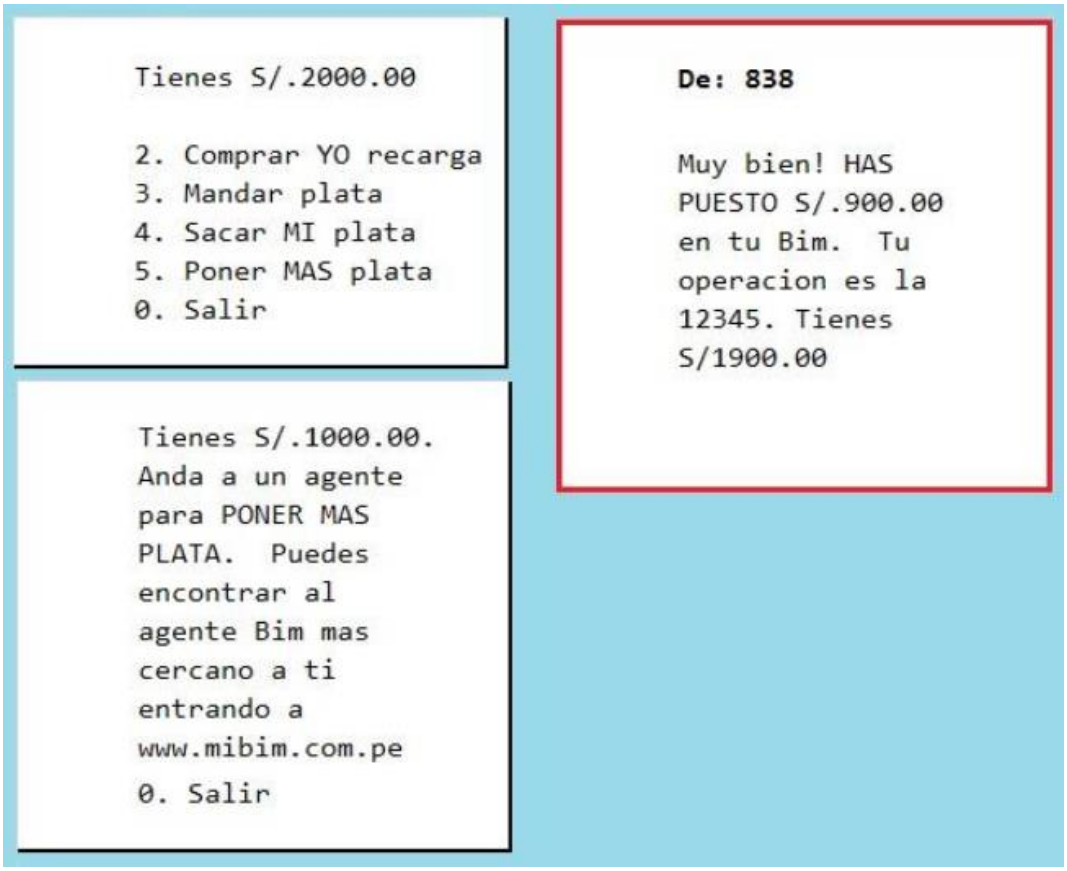


Figura 28: Menú poner más plata
Fuente: Propia

3.3.1.2 Proceso: Interpretación del investigador:

Para poder analizar las posibles vulnerabilidades a las que estaría expuesta la Billetera móvil (BIM) se enfocará en el tipo de comunicación que se usa para transportar el mensaje en la billetera móvil, debido a que según la arquitectura utilizada en el BIM son los tipos de comunicación los que se encargan de transmitir la información, ya sea la clave que se digita o el envío /recepción del mensaje, al momento de realizar una transacción por medio del celular. Se evidencia de los tipos de mensaje que usa el BIM son dos: El SMS que son para el envío de información y el USSD para realizar una acción en las operaciones.

3.3.1.3 Proceso: Interpretación de los objetos estudiados:

En el punto Elementos que intervienen en la Arquitectura del BIM se observaron varios elementos del BIM que pueden ser analizados de forma independiente para ver el nivel de amenazas a las que pueden estar expuestos. Pero el objetivo de la tesis es analizar la tecnología que usa el BIM para ver las vulnerabilidades a las que puede estar expuesto, en ese sentido se analizará la tecnología USSD y SMS, los cuales forman parte de los elementos que utiliza el BIM para realizar una transacción o para enviar información respectivamente.

3.3.2. Fase 2: Análisis de lo observado

En esta fase las Actas de Entrevista y documentos técnicos son analizados para la obtención del output resultado de análisis situacional.

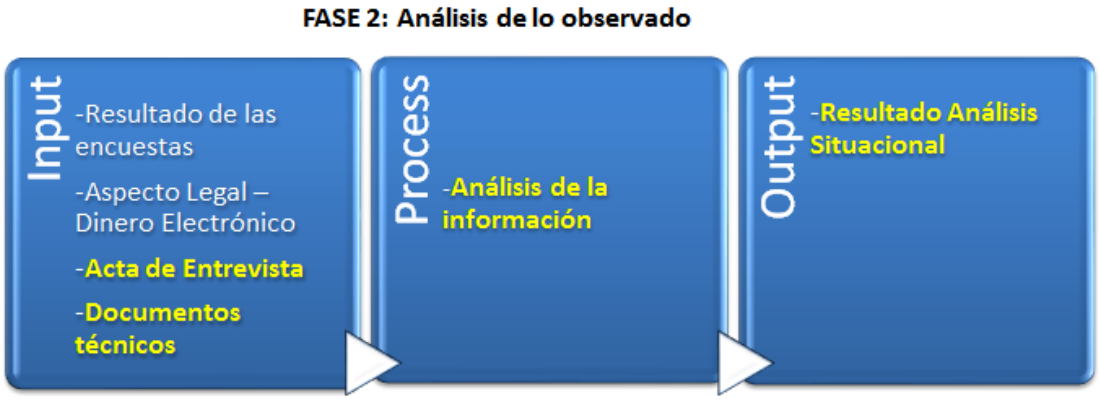


Figura 29: Entregable de la Fase 2 proveniente del acta de entrevista y documentos técnicos
Fuente: Propia

3.3.2.1 Análisis de las amenazas y vulnerabilidades

De acuerdo a la información registrada en las bases teóricas del capítulo I, se presenta un cuadro con las amenazas. Los cual resume los tipos de amenazas y riesgos a los que pueden estar expuestas las transacciones realizadas en la billetera BIM (Alliance for Financial Innclusion, 2013).

Tabla 7: Amenazas y riesgos en los servicios móviles

Tabla 1: Clasificación de amenazas tecnológicas de los SFM				
Amenazas	**Datos**	**Software**	**Hardware**	**Canal de Comunicaciones**
Modificación	Ocurre durante el almacenamiento, transmisión y cambio en el hardware físico	Sucede cuando se altera el software para realizar funciones o cómputos adicionales	–	Ocurre cuando los paquetes se enrutan hacia un destino diferente
Destrucción	Causada por fallas en el hardware y/o software	Destrucción debido a intenciones maliciosas, es decir, software malicioso *(malware)*	Ocasionada por desastres naturales, tales como inundaciones, incendios o por ataques terroristas	Causada por cortes en las líneas de fibra óptica o líneas arrendadas debido a eventos inesperados, es decir, inundaciones, robo o construcción de vías
Revelación	Ocurre cuando hay un acceso no autorizado a los datos/información de otra persona	–	–	–
Interceptación	Sucede cuando usuarios no autorizados reproducen la información confidencial	Ocurre cuando los programas de software se copian en forma ilegítima a partir de una fuente informática	Sucede cuando los usuarios no autorizados obtienen acceso físico al hardware	Ocurre cuando un tercero es capaz de interceptar (escuchar) puertos sin el conocimiento del usuario legítimo
Interrupción	–	Causada por el borrado de programas de software y/o funcionalidades específicas Puede ser el resultado de corrupción en el sistema operativo	Ocasionado por hardware dañado	Causado por ataques maliciosos, tales como saturación y denegación de servicio Puede ser el resultado de desastres naturales, interrupción del suministro eléctrico, problemas con las estaciones base o problemas en la red
Fabricación	Ocasionada por ataques de suplantación de identidad *(phishing)*	–	–	–

Fuente: (Alliance for Financial Innclusion, 2013)

La probabilidad de que una de las amenazas antes mencionadas pueda llegar a causar un daño en la BIM dependerá de cuan vulnerable sea la seguridad que controla la BIM frente a un ataque de software malintencionado. La tecnología USSD usada por la BIM, se da cuando el usuario marca *838#, también puede sufrir una amenaza cuando es ejecutado de forma automática como sucede en dispositivos Android.

a) Vulnerabilidad en los sistemas operativos Android

En la última Ekoparty (2012) realizada en Buenos Aires, se expuso una vulnerabilidad presente en casi todos los dispositivos con sistema operativo Android, el cual auto ejecuta todos los comandos USSD que recibe.

El atacante puede vulnerar el teléfono inteligente de la víctima con solo lograr que acceda a un sitio malicioso que explote este agujero de seguridad a través del envío de un código USSD específico. De este modo, cualquier usuario de un equipo móvil con sistemas operativos Android puede verse expuesto a perder su información a través de la ejecución de una línea de comando, puede realizar el borrado de todos los datos y volver a estado de fábrica el teléfono, de darse el ataque no le da oportunidad al usuario de cancelar o detener el ataque una vez que el mismo se inició.

Los canales de ataque o formas en que un atacante podría aprovechar esta vulnerabilidad son por ejemplo:

- SMS
- QR Codes
- Links recortados, los que suelen usarse en Twitter.
- Los Smartphones con tecnología NFC

b) Tecnologías USSD y tecnologías usadas en otras billeteras móviles

Como se puede observar hay tecnologías como el SMS, Sim Toolkit, WAP, etc.

Tabla 8: Tecnologías de comunicación utilizadas en billeteras móviles

TECNOLOGÍA	TERMINALES ACEPTADOS (COMPATIBILIDAD)	HABILIDADES REQUERIDAS AL USUARIO (USABILIDAD)	INTERACCIÓN DEL USUARIO CON EL SERVICIO (USABILIDAD)	TRAMO ENCRIPTADO DESDE EL TERMINAL AL SERVIDOR (SEGURIDAD)
IVR	• Todos	• Realizar llamadas y responder a indicaciones	• Responder a indicaciones vocales	• Sólo en tramo inalámbrico (según operador)
SMS	• Todos	• Escribir y leer SMS	• Enviar SMS para iniciar la transacción o responder con SMS para autorizar	• Sólo en tramo inalámbrico (según operador)
SIM Toolkit	• La mayoría de los GSM desde 2003	• Seleccionar menú, responder a indicaciones e introducir datos	• Seleccionar menú e interactuar utilizando menús textuales	• SIM al servidor del proveedor de SFM
USSD	• Todos los GSM (USSD1) • La mayoría de los GSM (USSD2)	• Escribir y leer USSD, responder a indicaciones e introducir datos	• Enviar USSD para iniciar la transacción, responder con USSD o seguir menú interactivo	• Sólo en tramo inalámbrico (según operador)
WAP	• Terminales de gama media y alta	• Seleccionar navegador, introducir dirección URL (o seleccionar marcador) y utilizar el navegador	• Seleccionar menú e interactuar en modo textual o con mini páginas para iniciar la transacción	• Navegador WAP al servidor del proveedor de SFM si está implementado SSL
HTTPS	• Terminales de gama alta y *smartphones*	• Seleccionar navegador, introducir dirección URL (o seleccionar marcador) y utilizar el navegador	• Seleccionar menú e interactuar en páginas web HTML para iniciar la transacción	• Navegador HTML al servidor del proveedor de SFM si está implementado SSL
JAVA (J2ME)	• Terminales GSM de gama media y alta	• Seleccionar microaplicativo y usar menús	• Seleccionar menú e interactuar en modo textual o con mini páginas para iniciar la transacción	• Microaplicativo al servidor del proveedor de SFM posible

Fuente: (Edgar Dunn & Company, 2008).

En el siguiente cuadro se puede observar un pequeño resumen de los casos de éxito donde en Filipinas, Sudafrica y Kenya, donde la tecnología más utilizada es el STK (SIM TOOLKIN) y en el aplicativo Wizzit de Sudáfrica es el USSD pero la diferencia con el BIM es de que Wizzit utiliza cuentas bancarizadas y el BIM no. El aplicativo de Asobancaria de la billetera móvil también usa tecnología USSD pero a diferencia del BIM, Asobancaria cuenta con la opción de usar huella digital o token para confirmar una transacción.

Tabla 9: Tecnologías usadas en algunas billeteras móviles con éxito

	SMART MONEY	GCASH	MTN BANKING	WIZZIT	M-PESA
País	Filipinas		Sudáfrica		Kenya
Año inicio	2003	2004	2005	2005	2007
Modelo	Transformacional				
Almacén de valor	Monedero móvil	Monedero móvil	Cuenta bancaria	Cuenta bancaria	Monedero móvil
Principales servicios	Tiempo-aire, pago de facturas, envíos de dinero, recepción de remesas	Tiempo-aire, pago de facturas, envíos de dinero, recepción de remesas	Tiempo-aire, compra en comercios, pago de facturas, envíos de dinero	Tiempo-aire, pago de facturas, envíos de dinero	Tiempo-aire, envíos de dinero
Impulsor	Smart (op.) y Banco de Oro	GXI (filial del op. Globe Telecom)	MTN (op.) y Standard Bank	Bank of Athens	Safaricom (op.)
Red móvil	Smart	Globe	MTN	Cualquiera	Safaricom
Tecnología	STK	STK	STK	USSD	STK
Distribución y apertura de cuentas	Apertura en tiendas Smart; ingresos en 12.000+ comercios asociados, ATMs u oficinas bancarias	Apertura, ingresos y retirada de efectivo en 4.900 agentes acreditados	Apertura online o en locales MTN y Standard Bank. Sin formulario KYC, funcionalidad restringida. Ingresos en comercios y EasyPay	Apertura con agentes (Wizz Kids) o en 400 tiendas Dunn; ingresos en PostBank, Absa o Bank of Athens; retirada en CNB.	Apertura, ingresos y retirada de efectivo en 850 agentes y centros de Safaricom
Supervisión	Bancaria	Supervisión ad-hoc del Banco Central	Bancaria	Bancaria	Supervisión no bancaria del Banco Central

Fuente: (Edgar Dunn & Company, 2008).

3.3.2.2 Resultado del análisis situacional

A continuación se realizará un análisis de todos los puntos relacionados a los objetivos específicos con el fin de poder determinar las variables de estudio en la siguiente fase.

a) Estudio de la percepción de la sociedad respecto al uso de la billetera móvil

Análisis del Resultado de la encuesta:

La mayoría de las personas encuestadas (54% de la muestra) conoce de la existencia de BIM, pero sólo el 2% ha realizado una transacción.

El 98% de los encuestados estarían dispuestos a realizar una transacción con BIM y el 32% estaría dispuesto a realizar transacciones por más de s/100 soles.

Respecto al conocimiento de medidas de seguridad la mayoría (82% de la muestra) respondió que no conocen las medidas de seguridad. Esto genera un entorno de temor acerca del uso de esta.

Según la muestra el 92% de personas encuestadas conoce de algún tipo de riesgo al usar el BIM. Asimismo el 96% estaría dispuesto a usar el BIM de conocer las medidas de seguridad.

Tabla 10: Cuadro resumen de análisis de encuestas

PREGUNTA		SÍ	NO	COMENTARIOS
1	¿Sabe usted de la existencia de la Billetera Móvil en el Perú?	54%	46%	**Conocimiento del BIM** Casi la mitad de la muestra encuestada conoce del BIM.
2	¿Ha realizado alguna transacción con la billetera Móvil?	2%	98%	**Transacciones realizadas** Existen poquísimas transacciones realizadas.
3	¿Estaría dispuesto a utilizar la billetera móvil para realizar una transacción bancaria?	98%	2%	**Aceptación del BIM** Las personas no presentan resistencia al BIM
4	¿Hasta qué importe estaría dispuesto realizar con una Billetera Móvil? Más de S/100	64%	Otros importes	**Importe a realizar en una transacción con la BIM** Las personas estarían dispuestas a realizar una transferencia el rango de S/100 y S/500.
5	¿Sabe usted sobre alguna medida de seguridad para este medio de pago?	18%	82%	**Desinformación de medidas de seguridad en el BIM**
6	¿Conoce algún riesgo en usar la Billetera Móvil?	92%	8%	**Conocimiento de Riesgos en las transacciones del BIM.** Las mayorías de las personas encuestadas conocen riesgos en el uso del BIM.
7	¿El uso de la Billetera Móvil es un modo seguro?	36%	64%	**Confianza en el BIM(disminuye)** Las mayorías de las personas encuestadas consideran el BIM como un modo no seguro en consecuencia esto disminuye la confianza en el BIM.
8		96%	4%	**Confianza de usar el BIM(aumenta)**

	¿Utilizaría la Billetera Móvil de conocer las medidas de seguridad?			La confianza aumentaría si se conocieran las medidas de seguridad al usar el BIM
9	¿Suele utilizar tarjetas de créditos para realizar compras.	64%	36%	**Uso de Tarjetas de Crédito** La mayoría de los encuestados cuenta con una tarjeta de crédito, se podría decir que no huyen de la tecnología.

Fuente: Propia

b) Analizar las normas de seguridad y tecnologías existentes en el Perú.

El análisis de las normas permitirá poder identificar las variables que se utilizaran en la formulación de la hipótesis.

Aspecto legal dinero electrónico:

Según lo revisado en la parte de análisis de las leyes que existen en el dinero electrónico se puede observar que no existen leyes específicas que regulen la tecnología USSD que utiliza el BIM, sino leyes de dinero electrónicas emitidas en el año 2013 que son tomadas por el BIM para ciertos puntos operacionales como se detalla en la fase de análisis del capítulo 3. Al no estar amparado bajo la ley el uso del USSD, los sistemas operativos de celulares como es el caso de Android puede ejecutar el USSD como parte de sus actualizaciones, tal ejecución puede ser captado por algún usuario intruso o software malicioso para enviar el dinero a otra cuenta BIM y retirarlo de un agente BIM con un celular que tenga acceso al BIM, recordar que la afiliación al BIM se podría realizar con un celular liberado y un número de DNI que fácilmente lo pueden afiliar teniendo el número.

Por otro lado, los operadores podrían aprovechar en incrementar el costo de uso del USSD a medida que el BIM sea más utilizado. Esta frecuencia creciente puede influir en que los operadores tengan problemas de congestión en la red por el uso del USSD y esto puede ser perjudicial para las redes que están alcanzando su capacidad máxima asimismo como consecuencia el usuario podría tener inestabilidad al realizar una transacción y su vez esto ser aprovecha por un software malicioso.

c) Vulnerabilidad a la cual puede estar expuesto el uso de la billetera móvil en el Perú

Gracias al documento de Acta de entrevistas y los documentos técnicos se pudo obtener información a la arquitectura del BIM, luego de la revisión se observó que el elemento que puede estar más vulnerable ante un ataque es el USSD. Se deduce que el proyecto Modelo Perú haya tomado en consideración el uso de USSD y no el SIM Toolkit, tecnología de entorno de programación integrado con la tarjeta SIM del usuario, también llamado STK, debido a que el propósito del BIM es la inclusión social, y el tomar en cuenta la innovación del Toolkit demandaba más costo, así como la modificación de la tarjeta SIM y falta de usabilidad. En la mayoría de proyectos de gran escala utilizan le tecnología USSD por el bajo costo.

La tecnología que utiliza el BIM según su arquitectura y análisis realizado son los SMS y USSD. Los SMS lo utiliza para enviar mensajes informativos como Cuánto dinero se tiene en el BIM, mensajes de error, mientras que el USSD lo utiliza para mostrar el menú donde el usuario accede para ver las operaciones disponibles y asimismo cuando va confirmar una operación se ejecuta el USSD.

En la parte de análisis de las amenazas a las cuales puede estar susceptible el USSD se realizó una clasificación donde se encuentran las vulnerabilidades de Modificación, Destrucción, Revelación, Intercepción, interrupción y Fabricación (Alliance for Financial Innclusion, 2013).

Los servicios financieros móviles son más vulnerables cuando se trata de un celular inteligente porque tiene acceso a internet, Bluetooth y más capacidad de almacenar información lo que deja un hueco ante cualquier ataque de software malicioso (Alliance for Financial Innclusion, 2013).

3.3.3. Fase 3: Clasificación de la información obtenida.

En este punto se realizará la creación de variables en base al punto *3.3.2.2. Resultado del análisis situacional*, lo cual permitirá formular la hipótesis sobre el análisis de las vulnerabilidades a las cuales está expuesta el BIM.

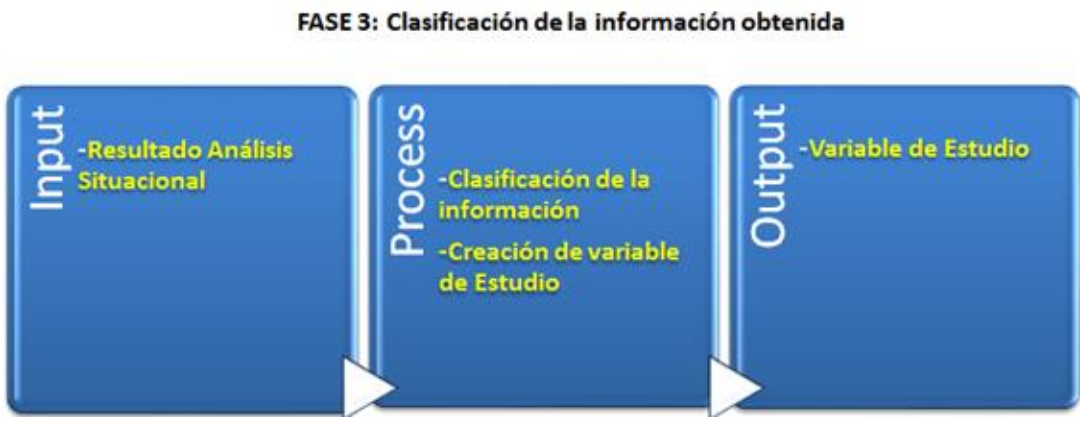


Figura 30: Proceso de clasificación de la información obtenida
Fuente: Propia

3.3.3.1 Creación de variables

A continuación se procederá con el registro de variables identificadas.

a) Estudio de la percepción de la sociedad respecto al uso de la billetera móvil.

CASO: Conocimiento de vulnerabilidades a las que puede estar expuesto el BIM.

Pregunta 1: ¿Hay confianza en los suscriptores al realizar transacciones con el BIM?

Variables Independientes:

- VI1: Desinformación de medidas de seguridad en el BIM.

Variables Dependientes:

- VD1: Transacciones realizadas con el BIM.
- VD2: Confianza en el BIM.

Pregunta 2: ¿Están conscientes los futuros suscriptores del BIM de las amenazas a las que puede estar expuesto el BIM?

Variables Independientes:

- VI1: Transacciones con el BIM

Variables Dependientes:

- VD1: Desconfianza.
- VD2: Riesgos en el BIM

Variable Interviniente:

- VINT1: Vulnerabilidades en las transacciones.

b) Normas de seguridad y tecnologías existentes en el Perú para aumentar la credibilidad en el uso de la billetera móvil

CASO: AMBITO LEGAL ASOCIADAS A LA TECNOLOGÍA USSD QUE USA EL BIM.

Pregunta: ¿El uso del USSD (tecnología usada por el BIM) está amparado por alguna Ley en el Perú?

Variables Independientes:

- VI1: No existe ley sobre el uso USSD en el Perú

Variables Dependientes:

- VD1: Acceso al USSD libre de restricciones.
- VD2: Vulnerabilidad de Intercepción, interrupción y fabricación.

Variables Interviniente:

- VINT1: El sistema operativo Android ejecuta USSD automáticamente

c) Vulnerabilidad a la cual puede estar expuesto el uso de la billetera móvil en el Perú

CASO: Seguridad de la tecnología USSD del BIM en el Perú.

Pregunta 1: ¿El uso del BIM es seguro?

Variables Independientes:

- VI1: Se confirma una operación digitando una contraseña en el celular.
- VI2: Realizar transacciones con el BIM.

Variables Dependientes:

- VD1: Vulnerabilidad de divulgación, Revelación, Intercepción y Fabricación.

Pregunta 2: ¿Existen Amenazas en los servicio móviles financieros?

Variables Independientes:

- VI1: Acceso a internet.
- VI2: Celular inteligente.

Variables Dependientes:

- VD1: Vulnerabilidad de Modificación, Destrucción, Intercepción, interrupción y Fabricación.
- VD2: Susceptible a ataque de software malicioso.

3.4. Tecnologías que pueden reducir las vulnerabilidades en el uso de la billetera móvil

En esta sección se dará a conocer la formulación de la hipótesis en base a la observación y registro de los hechos, luego de haberlos analizado.

3.4.1. Fase 4: Formulación de los enunciados universales inferidos del proceso de investigación que se ha realizado

Figura 31: Primer entregable Fase 4
Fuente: Propia

3.4.1.1 Proceso: Formular Hipótesis

La formulación de los enunciados universales inferidos del proceso de investigación que se ha realizado se analizó en las fases que describe la metodología elegida, es así que como resultado se tienen las variables de estudio:

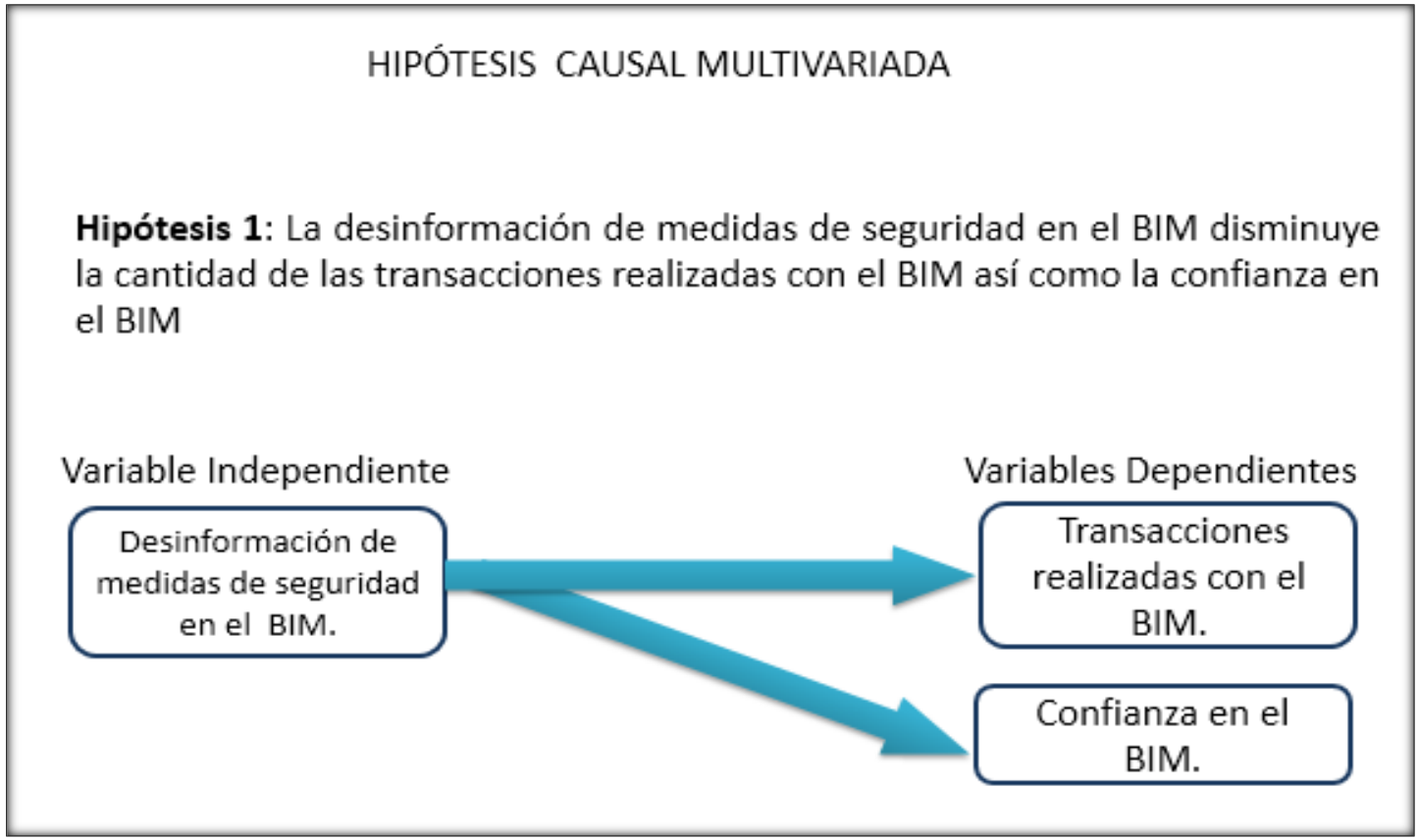


Figura 32: Hipótesis **1**
Fuente: Propia

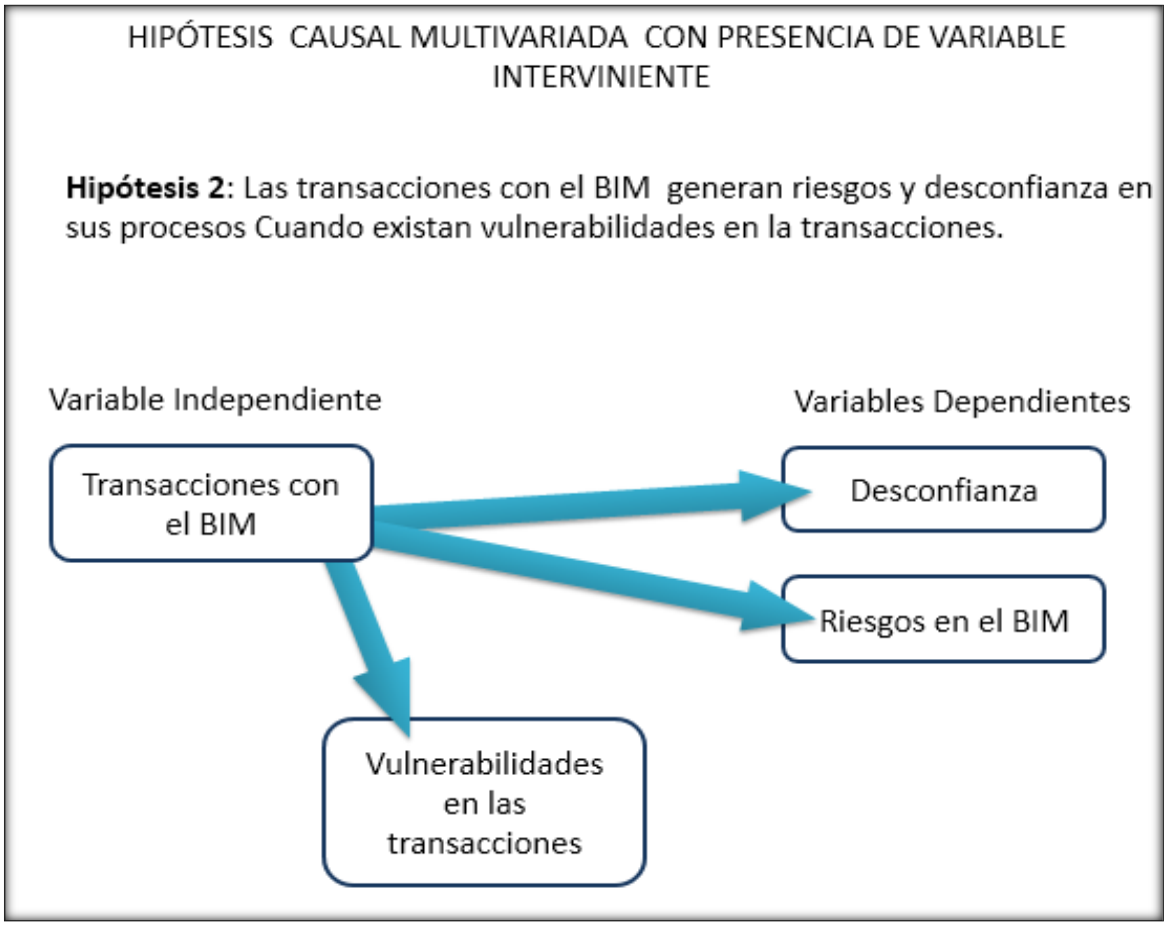


Figura 33: Hipótesis 2
Fuente: Propia

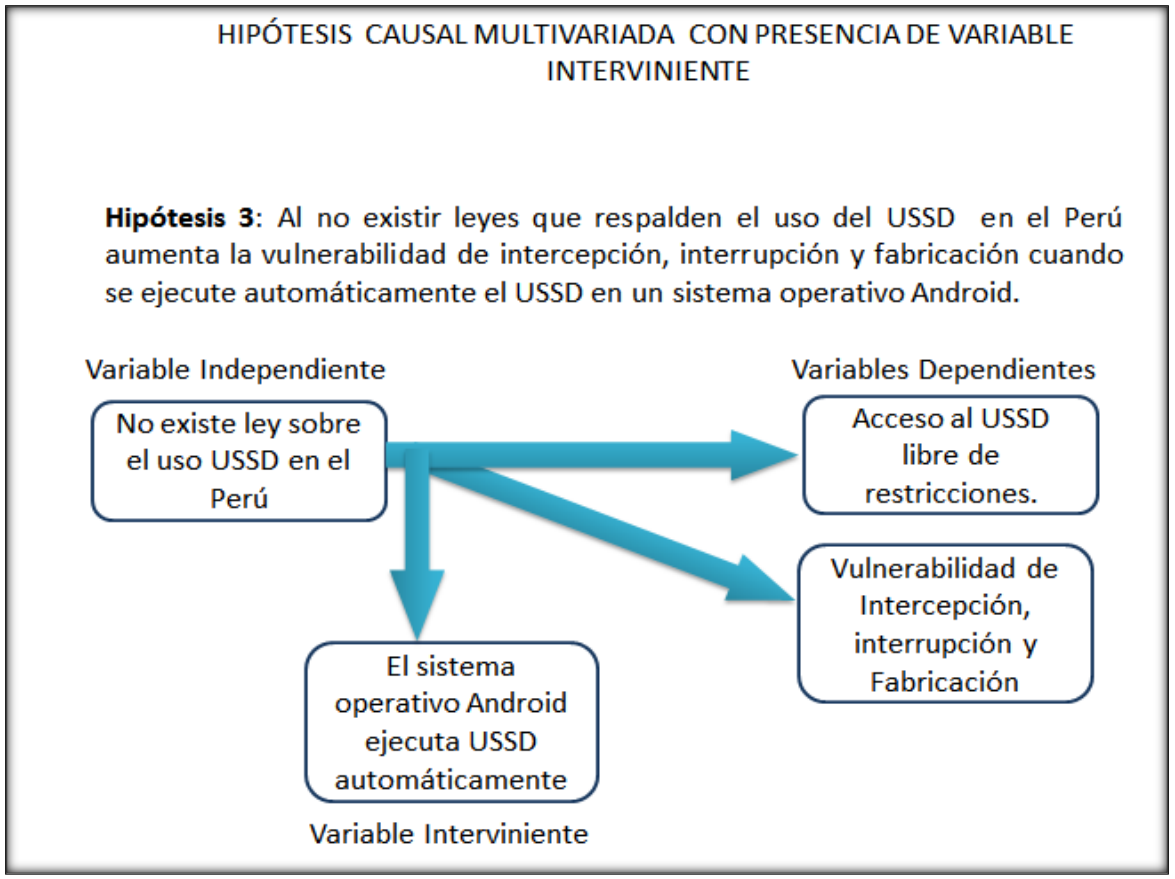


Figura 34: Hipótesis 3
Fuente: Propia

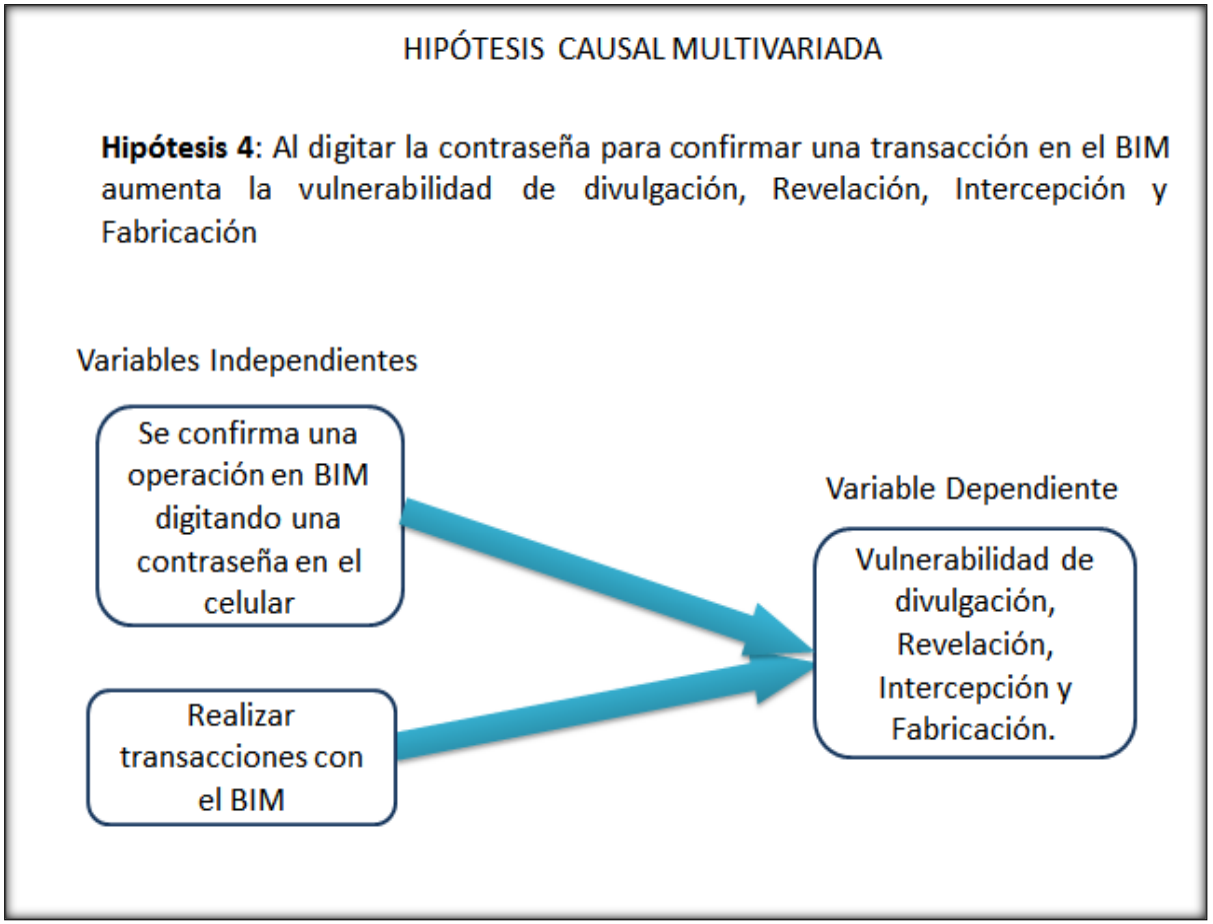


Figura 305: Hipótesis 4
Fuente: Propia

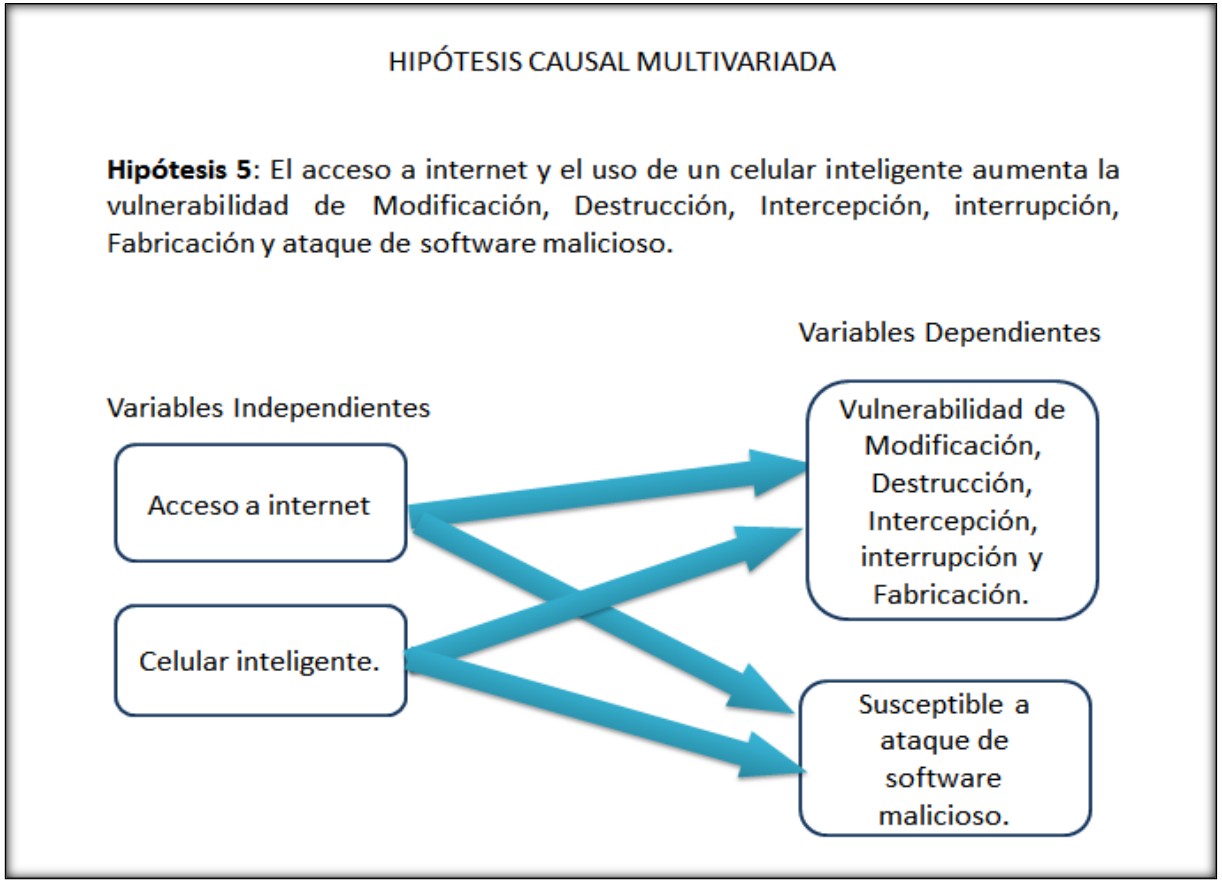


Figura 36: Hipótesis 5
Fuente: Propia

En base a las 5 hipótesis planteadas anteriormente se puede sacar una hipótesis en representación.

HIPÓTESIS:
El uso de la billetera móvil puede estar sujeto a vulnerabilidades que Pueden ser causadas por el registro de clave al usar el USSD como tecnología.

Tabla 11: Matriz de trazabilidad de Problema, Objetivos e Hipótesis

PROBLEMA	OBJETIVOS	VARIABLES	HIPÓTESIS
PROBLEMA GENERAL Limitada información de las vulnerabilidades asociadas a las tecnologías usadas en la billetera móvil en el Perú.	**OBJETIVO GENERAL** Identificar las vulnerabilidades asociadas a la tecnología y la seguridad utilizada en la billetera móvil	-	**HIPÓTESIS GENERAL** El uso de la billetera móvil puede estar sujeto a vulnerabilidades que Pueden ser causadas por el registro de clave al usar el USSD como tecnología.
PROBLEMAS ESPECÍFICOS:	**OBJETIVOS ESPECÍFICOS:**	**VARIABLES**	**HIPÓTESIS ESPECÍFICAS**
¿Hay confianza en los suscriptores en realizar transacciones con el BIM?	Realizar un estudio de percepción respecto al uso de la billetera móvil.	**Variable Independiente:** VI1: Desinformación de medidas de seguridad en el BIM. **Variables Dependientes:** VD1: Transacciones realizadas con el BIM. VD2: Confianza en el BIM.	La desinformación de medidas de seguridad en el BIM disminuye la cantidad de las transacciones realizadas con el BIM así como la confianza en el BIM.

¿Están conscientes los futuros suscriptores del BIM de las amenazas a las que puede estar expuesto el BIM?		**Variables Independientes:** VI1: Transacciones con el BIM **Variables Dependientes:** VD1: Desconfianza. VD2: Riesgos en el BIM **Variable Interviniente:** VINT1: Vulnerabilidades en las transacciones	Las transacciones con el BIM generan riesgos y desconfianza en sus procesos Cuando existan vulnerabilidades en la transacciones,
¿Existe el uso del USSD (tecnología usada por el BIM) está amparado por alguna Ley en el Perú?	Analizar las normas de seguridad y tecnologías existentes en el Perú.	**Variable Independiente:** VI1: No existe ley sobre el uso USSD en el Perú **Variables Dependientes:** VD1: Acceso al USSD libre de restricciones. VD2: Vulnerabilidad de Intercepción, interrupción y Fabricación. **Variable Interviniente:** VINT1: El sistema operativo Android ejecuta USSD automáticamente	Al no existir leyes que respalden el uso del USSD en el Perú aumenta la vulnerabilidad de intercepción, interrupción y fabricación cuando se ejecute automáticamente el USSD en un sistema operativo Android.
		Variables Independientes:	Al digitar la contraseña para confirmar una transacción en el BIM aumenta la

¿El uso del BIM es seguro? ¿Existen Amenazas en los servicio móviles financieros?	Evaluar la vulnerabilidad a la cual puede estar expuesto el uso de la billetera móvil en el Perú.	VI1: Se confirma una operación digitando una contraseña en el celular. VI2: Realizar transacciones con el BIM. **Variables Dependientes:** VD1: Vulnerabilidad de divulgación, Revelación, Intercepción y Fabricación. **Variables Independientes:** VI1: Acceso a internet. VI2: Celular inteligente. **Variables Dependientes:** VD1: Vulnerabilidad de Modificación, Destrucción, Intercepción, interrupción y Fabricación. VD2: Susceptible a ataque de software malicioso.	vulnerabilidad de divulgación, Revelación, Intercepción y Fabricación. El acceso a internet y el uso de un celular inteligente aumenta la vulnerabilidad de Modificación, Destrucción, Intercepción, interrupción, Fabricación y ataque de software malicioso.

Fuente: Propia

3.4.2. Propuesta de Medidas de seguridad y Tecnología

Según las hipótesis identificadas se proponen algunas medidas de seguridad y algunas tecnologías que pueden ser usadas adaptadas al BIM.

3.4.2.2 Medidas que podrían mejorar la seguridad del USSD

A continuación se describen algunas medidas de seguridad que podrían disminuir el efecto de una amenaza o al menos permitiría tener más control.

Figura 37: Segundo entregable Fase 4
Fuente: Propia

Uno de los principios rectores de la actividad regulatoria consiste en que esta debe ser lo menos restrictiva posible, en este caso, en lo que respecta a los operadores de telefonía móvil para conseguir el objetivo que se pretende ,aumento de la competencia y beneficio del consumidor, y debe además guardar la debida proporción con el riesgo que se enfrenta. La forma en que se aplique este principio en el contexto del acceso al USSD será específica de cada mercado. No obstante, vale la pena considerar la siguiente progresión de opciones para los entes reguladores:

Para cualquier mercado, la mejor solución que inicialmente cabe esperar es la concertación de convenios comerciales entre los operadores de redes de telefonía móvil y terceras partes para el suministro del USSD. Con ello se promovería la competencia y el desarrollo del mercado de servicios financieros móviles sin imponer restricciones a dichos operadores. Para

promover esa solución, los entes reguladores pueden probar un enfoque "blando" de persuasión moral, manifestando que prefieren que los operadores de telefonía móvil suministren acceso al USSD y exponiendo los fundamentos correspondientes. Diversos bancos centrales, entre ellos los de Kenia y Sudáfrica, han comunicado preferencias similares acerca de otras cuestiones relativas a la competencia, como la interoperabilidad en los pagos minoristas.

a) Otorgar acceso al USSD sólo a proveedores de bancos asociados:

Para Michel Hanouch y Gregory Chen (2015):

> El hecho de que los operadores de redes de telefonía móvil compitan por la prestación de servicios financieros móviles y controlen el USSD plantea interrogantes sobre cuándo puede ser necesaria la intervención reguladora, qué ente regulador es el más apropiado para intervenir y de qué opciones se dispone en el momento de la intervención (p.2).

> En los mercados en los que no llegan a concertarse convenios comerciales, se puede recurrir a un mecanismo coordinado para la resolución de disputas, conforme al cual el ente regulador financiero y el de las telecomunicaciones y posiblemente el de la competencia, podrían intervenir de manera conjunta para resolver cuestiones relacionadas con el acceso, la tarifación y/o la calidad del servicio. Este enfoque permitiría a los entes reguladores comprender la posición de cada una de las partes interesadas. Así, los operadores de redes de telefonía móvil tendrían la oportunidad de explicar sus argumentos para la restricción del acceso, como por ejemplo el posible impacto que tendría el suministro de USSD a gran escala sobre su actividad principal de telecomunicaciones. También proporcionaría a todas las partes la oportunidad de comunicar y detallar sus respectivas posturas acerca de la calidad, la tarifación y el costo del USSD. Los organismos reguladores de Bangladesh han adoptado un planteamiento de este tipo al constituir un comité consultivo sobre el USSD, integrado por

representantes del Banco Central de Bangladesh, el ente regulador de las telecomunicaciones, la asociación de telecomunicaciones y varios bancos. La pretensión de este comité es conocer mejor la situación y actuar como canal para el diálogo sobre el acceso al USSD. El resultado ideal de la aplicación de un mecanismo para la resolución de disputas, que contase además con la participación del sector privado, sería un convenio de mediación mutuamente aceptable. Todo mecanismo para la resolución de disputas debe tener cierta vigencia en el tiempo para que las nuevas diferencias que pudieran surgir se resuelvan diligentemente (p.3).

b) Leyes que puedan reglamentar el uso del USSD

La intervención regulatoria según Michel Hanouch y Gregory Chen (2015) está justificada cuando el mecanismo para la resolución de disputas no da lugar a una solución mutuamente aceptable y se considera que la negación del suministro de USSD dificulta la competencia. En tales casos, la forma de intervención más adecuada consiste en exigir a los operadores de redes de telefonía móvil que suministren acceso al USSD, pero sin regulación tarifaria. Por ejemplo, esta intervención puede ser la más idónea cuando un operador de telefonía móvil tiene un peso significativo en el mercado de voz y compite en el mercado de servicios financieros móviles. Cuando se plantean controversias sobre la calidad del acceso al USSD que no pudieron resolverse con los acuerdos sobre nivel de servicio suscriptos entre los operadores de telefonía celular y otros proveedores de servicios financieros móviles, el ente regulador puede considerar la introducción de estándares mínimos de calidad. Estos podrían adoptar la forma de un porcentaje máximo de sesiones que pueden interrumpirse por causas atribuibles al operador de redes de telefonía móvil, a partir de las cuales se pueden imponer multas u otras sanciones.

CGAP (2015):

Regulador de Servicios de Rwanda llamado Rwanda Utilities Regulatory Agency, ha aprobado normas de este tipo para el servicio de voz, que establecen en un 2 % trimestral la tasa máxima de llamadas interrumpidas.

Una de las dificultades que entraña esa regulación es identificar con precisión la causa por la que se interrumpe cada sesión del USSD. Las deficiencias de calidad podrían obedecer a una inversión insuficiente o una degradación selectiva de la calidad por parte del operador de telefonía móvil, aunque también podría deberse a motivos ajenos al operador. Cuando se usan las tarifas del USSD para obstaculizar la competencia, especialmente en el caso de operadores dominantes de redes de telefonía móvil, pueden ser necesarias medidas adicionales. La regulación de tarifas basada en la consideración detallada de los costos puede ser compleja, su control puede requerir mucho tiempo y puede resultar una tarea sumamente difícil de realizar de forma correcta. Por consiguiente, conviene evitarla en la medida de lo posible. Sin embargo, quizá resulte adecuado aplicar una norma sencilla, por ejemplo, exigir que las tarifas del USSD se apliquen de forma no discriminatoria, especialmente al proveedor de servicios financieros móviles del propio operador de telefonía celular o a su entidad bancaria asociada. Los organismos reguladores del Perú han adoptado este planteamiento y exigen que los operadores de telefonía celular establezcan una entidad separada para prestar servicios de pagos por móvil, lo que permite detectar con facilidad las tarificaciones discriminatorias del USSD (p.4).

Las alternativas enumeradas anteriormente brindan a los entes reguladores una posible secuencia de opciones a considerar; no obstante, en última instancia, las condiciones específicas del mercado determinarán cuál es la función óptima del organismo regulador. Por ejemplo, la Comisión de Regulación de Comunicaciones de Colombia exigió recientemente que se facilitara el acceso al USSD tras el fracaso de prolongadas negociaciones entre los bancos y los operadores de redes de telefonía móvil sobre ese particular. La Comisión consideró adecuado aplicar esta medida, sin recurrir a un mecanismo para la resolución de disputas, debido en parte a las prácticas previas de los operadores de telefonía móvil, que cobraban tarifas muy elevadas por servicios de mensajes de texto relacionados con servicios financieros móviles. Resulta prematuro extraer conclusiones sobre buenas

prácticas, dado que estas y otras intervenciones se han producido muy recientemente.

3.4.2.2 Tecnologías que utilizan sensores de reconocimiento para confirmar una operación en lugar de digitar la clave.

a) Uso de Huella Digital

El beneficio de poder realizar la confirmación de la operación con un sensor de huella digital permitirá que al momento de confirmar la operación la clave no se vea expuesta a ser manipulada. Además el usuario ya no tendrá que estar recordando la clave. Algunos celulares ya vienen con esta funcionalidad sólo faltaría que el menú USSD pueda ser adaptado para poder trabajar con las huellas digitales.

Figura 38: Huella Digital en teléfono móvil
Fuente: Propia

b) Reconocimiento Facial

En este caso el reconocimiento facial es una tecnología que actualmente se viene usando en algunos países por ejemplo lo utilizan algunas instituciones policiales por ejemplo en Perú lo utilizan para reconocer a la gente en una cámara. También lo usan los profesionales de seguridad y el gobierno.

Lo antes mencionado puede brindar una seguridad de que no se podría clonar el reconocimiento facial. Por lo cual podría ser utilizado como confirmación de alguna operación en vez de digitar la clave.

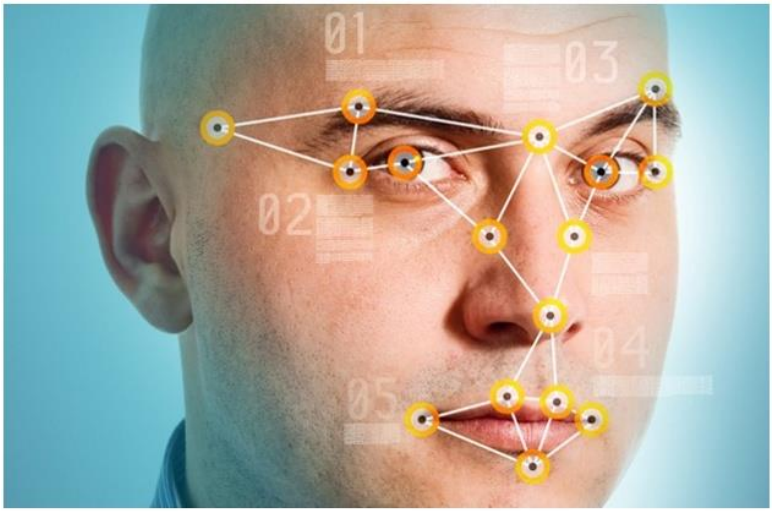


Figura 39: Reconocimiento facial
Fuente: (Welivesecurity, 2015)

c) Uso de Token

El uso de Token es muy utilizado para confirmar la ejecución de una operaciones como transferencias, pagos se servicios e instituciones, etc., realizados con tarjetas de crédito o débito. Por lo cual es un medio que a través del tiempo se viene usando por brindar menor riesgo. Por lo cual también sería una opción de poder utilizar el Token generando así un código dinámico que pueda confirmar la operación a realizar con la billetera móvil BIM. Un ejemplo de la billetera móvil que utiliza esta tecnología es la billetera móvil Asobancaria de Colombia que utiliza un sistema de autenticación de Token para confirmar la transacción.

Figura 40: Token
Fuente: Propia

CONCLUSIONES

Primera: Se puede concluir que la falta de información de la seguridad que existe al realizar una transacción con el BIM influye en los usuarios. En la muestra encuestada se pudo percibir que de los usuarios afiliados al BIM casi no han realizado operaciones con el BIM por temor de correr algún riesgo.

Segunda: Se logró identificar que no existen leyes que reglamenten de manera específica el uso del USSD en el Perú, en la actualidad solo existen tres reglamentos que se enfocan al entorno financiero y no técnico.

Tercera: Se logró identificar algunas de las vulnerabilidades a las cuales puede estar expuesto el BIM al hacer el uso de la tecnología USSD en los sistemas operativos Android.

Cuarta: El digitar la contraseña para confirmar una transacción en el BIM aumenta la vulnerabilidad de revelación, Interceptación y Fabricación.

Quinta Se logró identificar algunas tecnologías que podrían ser usadas para disminuir los riesgos al momento de confirmar una operación

RECOMENDACIONES

Primera: Realizar más estudios de percepción a nivel nacional para poder conocer el por qué algunas variables como son: Desinformación de medidas de seguridad en el BIM y desconfianza para realizar las transacciones disminuyen la cantidad de transacciones realizadas en el BIM.

Segunda: Reforzar la ley 29985 incluyendo regulaciones y restricciones en el uso de la tecnología USSD, como por ejemplo otorgar sólo el acceso al USSD al Banco que el usuario eligió para respaldar su BIM.

Tercera: Se debe informar al usuario las medidas de seguridad que debe tomar en cuenta cuando realiza una operación con el BIM. Informar periódicamente los sistemas operativos en los móviles que están siendo susceptibles algunos daños.

Cuarta: Para aumentar la seguridad en el BIM se recomienda adaptar sensores como por ejemplo el reconocimiento de huella digital o Token al menú USSD al momento de realizar la confirmación de las operaciones lo cual reemplazaría la digitación de la contraseña.

Quinta Las tecnologías recomendadas podrían ser evaluadas para brindar al usuario la opción de elegir si quiere usar una contraseña para confirmar una operación o utilizar un sensor de huella digitar o Token que podría tener costo adicional.

FUENTES DE INFORMACIÓN

Aguirre, H. (2014). *Dinero electrónico favorecerá inclusión financiera de 5 millones de peruanos*. Recuperado el 18 de agosto del 2014 de http://www.andina.com.pe/agencia/noticia-dinero-electronico-favorecera-inclusion-financiera-5-millones-peruanos-519386.aspx

AFI. (2013). *Alliance for Financial Inclusion*. Recuperado el 12 de septiembre del 2013 de http://www.afi-global.org/gpf-2013-malaysia

ASBANC. (2016). *Cómo la billetera móvil se volverá una estrategia de márketing*. Recuperado el 02 de abril del 2016 de http://www.asbanc.com.pe/Paginas/Noticias/DetalleNoticia.aspx?ItemID=215

Auditool. (2016). *Riesgo tecnológico. Su medición como prioridad para el aseguramiento del negocio*. Recuperado el 4 de junio del 2016 de http://www.auditool.org/blog/auditoria-de-ti/827-riesgo-tecnologico-su-medicion-como-prioridad-para-el-aseguramiento-del-negocio

Business School. (2015). *Dinero electrónico, pasos para abrir tu billetera móvil y aplicarlo en tu empresa – Lima Well Busines School*. Recuperado el 2 de abril del 2016 de http://www.limawell.edu.pe/dinero-electronico-billetera-movil-empresa/

Cuji Dután, D. (2014). *Análisis de la factibilidad para la implementación de la billetera móvil en la ciudad de cuenca*. Cuenca, Ecuador: Universidad politécnica salesiana. Tesis pregrado. Recuperado el 26 de Julio del 2014 de http://dspace.ups.edu.ec/bitstream/123456789/6798/1/UPS-CT003529.pdf

Diemo. (2014). *Dinero en movimiento, El ecosistema del pago móvil permite la bancarización.* Recuperado el 10 de Junio del 2014 de https://dineroenmovimiento.wordpress.com/2014/06/10/el-ecosistema-del-pago-movil-permite-la-bancarizacion/

El comercio. *Billetera móvil: 5 claves para hacer transferencias de dinero.*| Economía. Perú. Recuperado el 17 de febrero del 2016 de http://elcomercio.pe/economia/peru/banca-movil-cinco-claves-hacer-transferencias-dinero-noticia-1879292?ref=visor

Espinosa Peñaherrera, F; Soto Sarango, A. (2010). *Pago Electrónico a Través de Teléfonos Móviles*. Guayaquil, Ecuador: Escuela superior politécnica del Litoral. Tesis de grado. Recuperado el 17 de febrero del 2016 de https://www.dspace.espol.edu.ec/bitstream/123456789/9042/1/D-39870.pdf

Gobierno de Chile. (2013). *Inclusión Financiera*. Recuperado abril del 2013 de http://www.economia.gob.cl/wp-content/uploads/2014/04/Informe-Inclusi%C3%B3n-Financiera-y-Medios-de-Pago-Electr%C3%B3nicos.pdf

IATAI Enterprise. (2015). *IATAI at Billetera*. Recuperado el 26 de marzo del 2016, de http://www.iatai.com/blog/iatai-at-billetera.html

La República. (2013). *La billetera móvil: el medio de pago más rápido y seguro | Noticias del Perú*. Perú. Recuperado 2 de marzo del 2013 de http://larepublica.pe/02-03-2013/la-billetera-movil-el-medio-de-pago-mas-rapido-y-seguro

La Republica. (2016). *Con billetera móvil ya se puede enviar y recibir dinero a través del celular*. Perú. Recuperado el 1 de abril de 2016 de http://larepublica.pe/impresa/economia/741948-con-billetera-movil-ya-se-puede-enviar-y-recibir-dinero-traves-del-celular

La Republica. (2016). *Osiptel no tiene competencia si hay fallas en las transacciones de billetera móvil*. Perú. Recuperado el 1 de abril del 2016, de http://larepublica.pe/impresa/economia/748554-osiptel-no-tiene-competencia-si-hay-fallas-en-las-transacciones-de-billetera-movil

Mobey Forum. (2011). *Mobile wallet - definition and vision*

Neil Daly. (2010). *Mobile Money Transfer*

RPP noticias. (2016). *Diez entidades pueden brindar servicio de billetera móvil*. Recuperado el 1 de abril del 2016 de http://rpp.pe/economia/economia/osiptel-diez-entidades-pueden-brindar-servicio-de-billetera-movil-noticia-940867

Semana Economica. (2015). *Asbanc puso en marcha «Modelo Perú» de inclusión financiera a través del dinero electrónico*. Perú. Recuperado el 4 de junio del 2016 de http://semanaeconomica.com/article/mercados-y-finanzas/banca-y-finanzas/142319-asbanc-puso-en-marcha-modelo-peru-de-inclusion-financiera-a-traves-del-dinero-electronico/

Takehara, J. (2016). *Cómo la billetera móvil se volverá una estrategia de márquetin*. Recuperado el 07 de marzo del 2013 de http://www.codigo.pe/marketing/como-la-billetera-movil-se-volvera-una-estrategia-de-marketing/

Trivelli, C.; Pinto, M. (2016). *Bim: La plataforma común de inclusión financiera en el Perú* | *Portal Microfinanzas*. Recuperado el 2 de abril del 2016 de http://www.microfinancegateway.org/es/library/bim-la-plataforma-com%C3%BAn-de-inclusi%C3%B3n-financiera-en-el-per%C3%BA

Universidad Nacional Autónoma de Mexico. (2005). *Enter@te*. Recuperado el 19 de abril del 2016 de http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm

Welivesecurity. (2015). *¿Cómo funciona la tecnología de reconocimiento facial?* Recuperado el 9 de junio del 2016 de http://www.welivesecurity.com/la-es/2015/08/27/tecnologia-de-reconocimiento-facial/

ANEXOS

ANEXO N° 1

ISO 27001

Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos

Importante – No es el propósito de esta publicación incluir todas las provisiones necesarias de un contrato. Los usuarios son responsables de su correcta aplicación. El cumplimiento de un Estándar Internacional no quiere decir que confiere inmunidad de las obligaciones legales.

1 Alcance

1.1 General

Este Estándar Internacional abarca todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). Este Estándar Internacional especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.

El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.

NOTA 1: Las referencias a 'comerciales' en este Estándar Internacional se deben implementar ampliamente para significar aquellas actividades que son básicas para los propósitos de la existencia de la organización.

NOTA 2: ISO/IEC 17799 proporciona un lineamiento de implementación que se puede utilizar cuando se diseñan controles.

1.2 Aplicación

Los requerimientos establecidos en este Estándar Internacional son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza. No es aceptable la exclusión de ninguno de los requerimientos especificados en las Cláusulas 4, 5, 6, y 8 cuando una organización asegura su conformidad con este Estándar Internacional.

8

Cualquier exclusión de los controles vista como necesaria para satisfacer el criterio de aceptación del riesgo tiene que ser justificada y se debe proporcionar evidencia de que los riesgos asociados han sido aceptados por las personas responsables. Cuando se realizan exclusiones, las aseveraciones de conformidad con este estándar no son aceptables a no ser que estas exclusiones no afecten la capacidad y/o responsabilidad de la organización, para proporcionar seguridad de la información que satisfaga los requerimientos de seguridad determinados por la evaluación de riesgo y los requerimientos reguladores aplicables.

NOTA: Si una organización ya cuenta con un sistema de gestión de procesos comerciales operativos (por ejemplo, en relación con ISO 9001 o ISO 14001), en la mayoría de los casos es preferible satisfacer los requerimientos de este Estándar Internacional dentro de este sistema de gestión existente.

2 Referencias normativas

Los siguientes documentos mencionados son indispensables para la aplicación de este documento. Para referencias fechadas, sólo se aplica la edición citada. Para referencias no fechadas, se aplica la última edición del documento citado.

ISO/IEC 17799:2005, Tecnología de la información – Técnicas de seguridad – Código de práctica para la gestión de la seguridad de la información

3 Términos y definiciones

Para propósitos de este documento, se aplican los siguientes términos y definiciones.

3.1
activo

cualquier cosa que tenga valor para la organización
(ISO/IEC 13335-1:2004)

3.2
disponibilidad

la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada
(ISO/IEC 13335-1:2004)

3.3

confidencialidad

la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados

(ISO/IEC 13335-1:2004)

3.4

seguridad de información

preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad

(ISO/IEC 17799:2005)

3.5

evento de seguridad de la información

una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

(ISO/IEC TR 18044:2004)

3.6

incidente de seguridad de la información

un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

(ISO/IEC TR 18044:2004)

3.7

sistema de gestión de seguridad de la información SGSI

esa parte del sistema gerencial general, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información

NOTA: El sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos

3.8

integridad

la propiedad de salvaguardar la exactitud e integridad de los activos.

(ISO/IEC 13335-1:2004)

3.9

riesgo residual

el riesgo remanente después del tratamiento del riesgo

(ISO/IEC Guía 73:2002)

3.10

aceptación de riesgo

decisión de aceptar el riesgo

(ISO/IEC Guía 73:2002)

3.11

análisis de riesgo

uso sistemático de la información para identificar fuentes y para estimar el riesgo

(ISO/IEC Guía 73:2002)

3.12

valuación del riesgo

proceso general de análisis del riesgo y evaluación del riesgo

(ISO/IEC Guía 73:2002)

3.13

evaluación del riesgo

proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo

(ISO/IEC Guía 73:2002)

3.14

gestión del riesgo

actividades coordinadas para dirigir y controlar una organización con relación al riesgo

(ISO/IEC Guía 73:2002)

3.15

tratamiento del riesgo

proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo

(ISO/IEC Guía 73:2002)

NOTA: En este Estándar Internacional el término 'control' se utiliza como sinónimo de 'medida'.

3.16

enunciado de aplicabilidad

enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.

NOTA: Los objetivos de control y controles se basan en los resultados y conclusiones de los procesos de tasación del riesgo y los procesos de tratamiento del riesgo, los requerimientos legales o reguladores, las obligaciones contractuales y los requerimientos comerciales de la organización para la seguridad de la información.

4 Sistema de gestión de seguridad de la información

4.1 Requerimientos generales

La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan. Para propósitos de este Estándar Internacional, los procesos utilizados se basan en el modelo PDCA que se muestra en la Figura 1.

4.2 Establecer y manejar el SGSI

4.2.1 Establecer el SGSI

La organización debe hacer lo siguiente:

a) Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance (ver 1.2).

b) Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología que:

   1) incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información;
   2) tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual;
   3) esté alineada con el contexto de la gestión riesgo estratégico de la organización en el cual se dará el establecimiento y mantenimiento del SGSI;
   4) establezca el criterio con el que se evaluará el riesgo (ver 4.2.1c);
   5) haya sido aprobada por la gerencia.

NOTA: Para propósitos de este Estándar Internacional, la política SGSI es considerada como un super-conjunto de la política de seguridad de la información. Estas políticas se pueden describir en un documento.

c) Definir el enfoque de valuación del riesgo de la organización

1) Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.

2) Desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables (ver 5.1f).

La metodología de estimación del riesgo seleccionada debe asegurar que los cálculos del riesgo produzcan resultados comparables y reproducibles.

NOTA: Existen diferentes metodologías para el cálculo del riesgo. Los ejemplos de las metodologías de cálculo del riesgo se discuten en ISO/IEC TR 13335-3, Tecnología de información – Lineamiento para la gestión de la Seguridad TI – Técnicas para la gestión de la Seguridad TI

d) Identificar los riesgos

1) Identificar los activos dentro del alcance del SGSI y los propietarios[2] de estos activos.

2) Identificar las amenazas para aquellos activos.

3) Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.

4) Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

e) Analizar y evaluar el riesgo

1) Calcular el impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.

2) Calcular la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos, y los controles implementados actualmente.

3) Calcular los niveles de riesgo.

---

[2] El término 'propietario' identifica a la persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término 'propietario' no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

4) Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido en 4.2.1 (c) (2).

f) Identificar y evaluar las opciones para el tratamiento de los riesgos

Las acciones posibles incluyen:

1) aplicar los controles apropiados;

2) aceptar los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo (ver 4.2.1 c)2)) de la organización;

3) evitar los riesgos; y

4) transferir los riesgos comerciales asociados a otras entidades; por ejemplo, aseguradoras, proveedores.

g) Seleccionar objetivos de control y controles para el tratamiento de riesgos

Se deben seleccionar e implementar los objetivos de control y controles para cumplir con los requerimientos identificados por el proceso de tasación del riesgo y tratamiento del riesgo. Esta selección debe tomar en cuenta el criterio para aceptar los riesgos (ver 4.2.1(c), así como los requerimientos legales, reguladores y contractuales.

Se deben seleccionar los objetivos de control y los controles del Anexo A como parte de este proceso conforme sea apropiado para cubrir estos requerimientos.

Los objetivos de control y controles listados en el Anexo A no son exhaustivos y también se pueden seleccionar objetivos de control y controles adicionales.

NOTA: El Anexo A contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones. Se dirige a los usuarios de este Estándar Internacional como un punto de inicio para la selección de controles para asegurar que no se pase por alto ninguna opción de control importante.

h) Obtener la aprobación de la gerencia para los riesgos residuales propuestos.

i) Obtener la autorización de la gerencia para implementar y operar el SGSI.

j) Preparar un Enunciado de Aplicabilidad

Se debe preparar un Enunciado de Aplicabilidad que incluya lo siguiente:

1) los objetivos de control y los controles seleccionados en 4.2.1 (g) y las razones para su selección

2) los objetivos de control y controles implementados actualmente (ver 4.2.1 (e) 2); y

3) la exclusión de cualquier objetivo de control y control en el Anexo A y la justificación para su exclusión.

NOTA: El Enunciado de Aplicabilidad proporciona un resumen de las decisiones concernientes con el tratamiento del riesgo. El justificar las exclusiones proporciona un chequeo para asegurar que ningún control haya sido omitido inadvertidamente.

4.2.2 Implementar y operar el SGSI

La organización debe hacer lo siguiente:

a) Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información (ver 5).

b) Implementar el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.

c) Implementar los controles seleccionados en 4.2.1(g) para satisfacer los objetivos de control.

d) Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo se van a utilizar estas mediciones para evaluar la efectividad del control para producir resultados comparables y reproducibles (ver 4.2.3 c)).
NOTA: La medición de la efectividad de los controles permite a los gerentes y personal determinar lo bien que los controles logran los objetivos de control planeados.

e) Implementar los programas de capacitación y conocimiento (ver 5.2.2).

f) Manejar las operaciones del SGSI.

g) Manejar recursos para el SGSI (ver 5.2).

h) Implementar los procedimientos y otros controles capaces de permitir una pronta detección de y respuesta a incidentes de seguridad.

4.2.3 Monitorear y revisar el SGSI

La organización debe hacer lo siguiente:

a) Ejecutar procedimientos de monitoreo y revisión, y otros controles para:
   1) detectar prontamente los errores en los resultados de procesamiento;
   2) identificar prontamente los incidentes y violaciones de seguridad fallidos y exitosos;
   3) permitir a la gerencia determinar si las actividades de seguridad delegadas a las personas o implementadas mediante la tecnología de información se están realizando como se esperaba;
   4) ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores; y
   5) determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.

b) Realizar revisiones regulares de la efectividad del SGSI (incluyendo satisfacer la política y objetivos de seguridad del SGSI, y revisar los controles de seguridad) tomando en cuenta los resultados de auditorias de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas.

c) Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.

d) Revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:
   1) la organización;
   2) tecnología;
   3) objetivos y procesos comerciales;
   4) amenazas identificadas;
   5) efectividad de los controles implementados; y
   6) eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.

e) Realizar auditorias SGSI internas a intervalos planeados (ver 6).

NOTA: Las auditorías internas, algunas veces llamadas auditorías de primera persona, son realizadas por, o en representación de, la organización misma para propósitos internos.

f) Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI (ver 7.1).

g) Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.

h) Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI (ver 4.3.3).

4.2.4 Mantener y mejorar el SGSI

La organización debe realizar regularmente lo siguiente:

a) Implementar las mejoras identificadas en el SGSI.

b) Tomar las acciones correctivas y preventivas apropiadas en concordancia con 8.2 y 8.3. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma.

c) Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar cómo proceder.

d) Asegurar que las mejoras logren sus objetivos señalados.

4.3 Requerimientos de documentación

4.3.1 General

La documentación debe incluir los registros de las decisiones gerenciales, asegurar que las acciones puedan ser monitoreadas a las decisiones y políticas gerenciales, y los resultados registrados deben ser reproducibles.

Es importante ser capaces de demostrar la relación desde los controles seleccionados y de regreso a los resultados del proceso de evaluación del riesgo y tratamiento del riesgo, y subsecuentemente, de regreso a la política y objetivos del SGSI.

La documentación SGSI debe incluir lo siguiente:

a) enunciados documentados de la política SGSI (ver 4.2.1b)) y los objetivos;
b) el alcance del SGSI (ver 4.2.1a));
c) procedimientos y controles de soporte del SGSI;
d) una descripción de la metodología de evaluación del riesgo (ver 4.2.1c));
e) reporte de evaluación del riesgo (ver 4.2.1c) a 4.2.1g));
f) plan de tratamiento del riesgo (ver 4.2.2b));
g) Los procedimientos documentados necesarios por la organización para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles (ver 4.2.3c));
h) registros requeridos por este Estándar Internacional (ver 4.3.3); y
i) Enunciado de Aplicabilidad

NOTA 1: Cuando aparece el término 'procedimiento documentado' dentro este Estándar Internacional, significa que el procedimiento se establece, documenta, implementa y mantiene.

NOTA 2: La extensión de la documentación SGSI puede diferir de una organización a otro debido a:

- el tamaño de la organización y el tipo de sus actividades; y
- el alcance y complejidad de los requerimientos de seguridad y el sistema que se está manejando.

NOTA 3: Los documentos y registros pueden estar en cualquier forma o medio.

4.3.2 Control de documentos

Los documentos requeridos por el SGSI deben ser protegidos y controlados. Se debe establecer un procedimiento documentado para definir las acciones gerenciales necesarias para:

a) aprobar la idoneidad de los documentos antes de su emisión;
b) revisar y actualizar los documentos conforme sea necesario y re-aprobar los documentos;
c) asegurar que se identifiquen los cambios y el status de la revisión actual de los documentos;

d) asegurar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso;
e) asegurar que los documentos se mantengan legibles y fácilmente identificables;
f) asegurar que los documentos estén disponibles para aquellos que los necesitan; y sean transferidos, almacenados y finalmente eliminados en concordancia con los procedimientos aplicables para su clasificación;
g) asegurar que se identifiquen los documentos de origen externo;
h) asegurar que se controle la distribución de documentos;
i) evitar el uso indebido de documentos obsoletos; y
j) aplicarles una identificación adecuada si se van a retener por algún propósito.

4.3.3 Control de registros

Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI. Deben ser protegidos y controlados. El SGSI debe tomar en cuenta cualquier requerimiento legal o regulador relevante. Los registros deben mantenerse legibles, fácilmente identificables y recuperables. Se deben documentar e implementar los controles necesarios para la identificación, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros.

Se deben mantener registros del desempeño del proceso tal como se delinea en 4.2 y de todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI.

EJEMPLO
Son ejemplos de registros los libros de visitantes, los registros de auditoria y las solicitudes de autorización de acceso.

5 Responsabilidad de la gerencia

5.1 Compromiso de la gerencia

La gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI al:

a) establecer una política SGSI;
b) asegurar que se establezcan objetivos y planes SGSI;
c) establecer roles y responsabilidades para la seguridad de información;
d) comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información, sus responsabilidades bajo la ley y la necesidad de un mejoramiento continuo;

e) proporcionar los recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI (ver 5.2.1);
f) decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptables;
g) asegurar que se realicen las auditorías internas SGSI (ver 6); y
h) realizar revisiones gerenciales del SGSI (ver 7).

5.2 Gestión de recursos

5.2.1 Provisión de recursos

La organización debe determinar y proporcionar los recursos necesarios para:

a) establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI;
b) asegurar que los procedimientos de seguridad de la información respalden los requerimientos comerciales;
c) identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales;
d) mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados;
e) llevar a cabo revisiones cuando sean necesarias, y reaccionar apropiadamente ante los resultados de estas revisiones;
f) donde se requiera, mejorar la efectividad del SGSI.

5.2.2 Capacitación, conocimiento y capacidad

La organización debe asegurar que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas para:

a) determinar las capacidades necesarias para el personal que realiza trabajo que afecta el SGSI;
b) proporcionar la capacitación o realizar otras acciones (por ejemplo; emplear el personal competente) para satisfacer estas necesidades;
c) evaluar la efectividad de las acciones tomadas;
d) mantener registros de educación, capacitación, capacidades, experiencia y calificaciones (ver 4.3.3).

La organización también debe asegurarse que todo el personal relevante esté consciente de la relevancia e importancia de sus actividades de seguridad de la información y cómo ellos pueden contribuir al logro de los objetivos SGSI.

6 Auditorías internas SGSI

La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI:

a) cumplen con los requerimientos de este Estándar Internacional y la legislación y regulaciones relevantes;
b) cumplen con los requerimientos de seguridad de la información identificados;
c) se implementan y mantienen de manera efectiva; y
d) se realizan conforme lo esperado.

Se debe planear un programa de auditoría tomando en consideración el status e importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías previas. Se debe definir el criterio, alcance, frecuencia y métodos de auditoría. La selección de los auditores y la realización de las auditorías deben asegurar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

Las responsabilidades y requerimientos para la planeación y realización de las auditorías, y para el reporte de resultados y mantenimiento de registros (ver 4.3.3) se deben definir en un procedimiento documentado.

La gerencia responsable para el área siendo auditada debe asegurar que se den sin demora las acciones para eliminar las no-conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de verificación (ver 8).

NOTA: ISO 19011:2002, Lineamiento para auditar sistemas de gestión de calidad y/o ambiental, puede proporcionar un lineamiento útil para llevar a cabo auditorías internas.

7 Revisión Gerencial del SGSI

7.1 General

La gerencia debe revisar el SGSI de la organización a intervalos planeados (por lo menos una vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad. Esta revisión debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información. Los resultados de las revisiones deben documentarse claramente y se deben mantener registros (ver 4.3.3).

7.2 Insumo de la revisión

El insumo para la revisión gerencial debe incluir:

a) resultados de auditorias y revisiones del SGSI;
b) retroalimentación de las partes interesadas;
c) técnicas, productos o procedimientos, que se podrían utilizar en la organización para mejorar el desempeño y efectividad del SGSI;
d) status de acciones preventivas y correctivas;
e) vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo previa;
f) resultados de mediciones de efectividad;
g) acciones de seguimiento de las revisiones gerenciales previas;
h) cualquier cambio que pudiera afectar el SGSI; y
i) recomendaciones para el mejoramiento.

7.3 Resultado de la revisión

El resultado de la revisión gerencial debe incluir cualquier decisión y acción relacionada con lo siguiente:

a) mejoramiento de la efectividad del SGSI;
b) actualización de la evaluación del riesgo y el plan de tratamiento del riesgo;
c) modificación de procedimientos y controles que afectan la seguridad de la información, si fuese necesario, para responder a eventos internos o externos que pudieran tener impacto sobre el SGSI, incluyendo cambios en:
    1) requerimientos comerciales;
    2) requerimientos de seguridad;
    3) procesos comerciales que afectan los requerimientos comerciales existentes;
    4) requerimientos reguladores o legales;
    5) obligaciones contractuales; y
    6) niveles de riesgo y/o criterio de aceptación del riesgo.
d) necesidades de recursos;
e) mejoramiento de cómo se mide la efectividad de los controles.

8 Mejoramiento del SGSI

8.1 Mejoramiento continuo

La organización debe mejorar continuamente la efectividad del SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información, resultados de auditoria, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial.

8.2 Acción correctiva

La organización debe realizar las acciones para eliminar la causa de las no-conformidades con los requerimientos del SGSI para poder evitar la recurrencia. El procedimiento documentado para la acción correctiva debe definir los requerimientos para:

a) identificar las no-conformidades;
b) determinar las causas de las no-conformidades;
c) evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir;
d) determinar e implementar la acción correctiva necesaria;
e) registrar los resultados de la acción tomada (ver 4.3.3); y
f) revisar la acción correctiva tomada.

8.3 Acción preventiva

La organización debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requerimientos SGSI para evitar su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requerimientos para:

a) identificar las no-conformidades potenciales y sus causas;
b) evaluar la necesidad para la acción para evitar la ocurrencia de no-conformidades;
c) determinar e implementar la acción preventiva necesaria;
d) registrar los resultados de la acción tomada (ver 4.3.3); y
e) revisar la acción preventiva tomada.

La organización debe identificar los riesgos cambiados e identificar los requerimientos de acción preventiva enfocando la atención sobre los riesgos cambiados significativamente.

La prioridad de las acciones preventivas se debe determinar en base a los resultados de la evaluación del riesgo.

NOTA La acción para evitar las no-conformidades con frecuencia es más una acción efectiva en costo que la acción correctiva.

Anexo A

(Normativo)

Objetivos de control y controles

Los objetivos de control y los controles enumerados en la Tabla A.1 se derivan directamente de, y se alinean con, aquellos enumerados en BS ISO/IEC 17799:2005 Cláusulas del 5 al 15. Las listas en estas tablas no son exhaustivas y una organización podría considerar que son necesarios objetivos de control y controles adicionales. Los objetivos de control y los controles de estas tablas deben seleccionarse como parte del proceso SGSI especificado en 4.2.1.

El BS ISO/IEC 17799:2005 Cláusulas del 5 al 15 proporciona consulta y lineamientos para la implementación de las mejores prácticas en soporte de los controles especificados en A.5 al A.15.

Tabla A.1 – Objetivos de control y controles

A.5 Política de seguridad
A.5.1 Política de seguridad de información Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad

de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes		
A.5.1.1	Documentar política de seguridad de información	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
A,6 Organización de la seguridad de la información		
A.6.1 Organización interna Objetivo: Manejar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de información	Control Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Control Se deben definir claramente las responsabilidades de la seguridad de la información.
A.6.1.4	Proceso de autorización para los medios de procesamiento de información	Control Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con autoridades	Control Se debe mantener los contactos apropiados con las autoridades relevantes.
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.
A.6.2 Entidades externas		

Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.
A.6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	Control Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.
A.7 Gestión de activos		
A.7.1 *Responsabilidad por los activos*		
Objetivo*:* Lograr y mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	Inventarios de activos	Control Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad'[3] de una parte designada de a organización.
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
A.7.2 Clasificación de la información		
Objetivo: Asegurar que a información reciba un nivel de protección apropiado.		
A.7.2.1	Lineamientos de clasificación	Control La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.

[3] Explicación: El término 'propietario' identifica a una persona o entidad que tiene la responsabilidad gerencial aprobada para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término 'propietario' no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

A.8 Seguridad de los recursos humanos		
A.8.1 Antes del empleo[4] Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.		
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
A.8.1.2	Selección	Control Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.
A.8.2 *Durante el empleo* Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.		
A.8.2.1	Gestión de responsabilidades	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
A.8.2.2	Capacitación y educación en seguridad de la información	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
A.8.3 Terminación o cambio del empleo Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.		
A.8.3.1	Responsabilidades de terminación	Control Se deben definir y asignar claramente las

[4] Explicación: Aquí la palabra 'empleo' se utiliza para abarcar todas las siguientes situaciones diferentes: empleo de personas (temporal o larga duración), asignación de roles laborales, cambios de trabajo, asignación de contratos y la terminación de cualquiera de estos acuerdos.

		responsabilidades para realizar la terminación o cambio del empleo.
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.
A.8.3.3	Eliminación de derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.
A.9 Seguridad física y ambiental		
A.7.1 *Áreas seguras* Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.		
A.9.1.1	Perímetro de seguridad física	Control Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepción atendida) para proteger áreas que contienen información y medios de procesamiento de información.
A.9.1.2	Controles de entrada físicos	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
A.9.1.3	Seguridad de oficinas, habitaciones y medios	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
A.9.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
A.9.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
A.9.1.6	Áreas de acceso público, entrega y carga	Control Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.
A.9.2 *Seguridad del equipo* Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización		
A.9.2.1	Ubicación y protección del equipo	Control El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.2	Servicios públicos	Control El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.

A.9.2.3	Seguridad en el cableado	Control El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
A.9.2.4	Mantenimiento de equipo	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
A.9.2.5	Seguridad del equipo fuera-del-local	Control Se debe aplicar seguridad al equipo fuera-del-local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
A.9.2.6	Eliminación seguro o re-uso del equipo	Control Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.
A.9.2.7	Traslado de Propiedad	Control Equipos, información o software no deben ser sacados fuera de sus propiedad sin previa autorización.
A.10 Gestión de las comunicaciones y operaciones		
A.10.1 Procedimientos y responsabilidades operacionales Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información		
A.10.1.1	Procedimientos de operación documentados	Control Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de cambio	Control Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.
A.10.1.3	Segregación de deberes	Control Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización.
A.10.1.4	Separación de los medios de desarrollo y operacionales	Control Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.
A.10.2 Gestión de la entrega del servicio de terceros Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.		
A.10.2.1	Entrega del servicio	Control Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio de terceros.
A.10.2.2	Monitoreo y revisión de los servicios de terceros	Control Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.

A.10.2.3	Manejar los cambios en los servicios de terceros	Control Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la re-evaluación de los riesgos.
A.10.3 Planeación y aceptación del sistema Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Gestión de capacidad	Control Se deben monitorear, afinar y realizar proyecciones del uso de los recursos, para asegurar el desempeño del sistema requerido.
A.10.3.2	Aceptación del sistema	Control Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.
A.10.4 *Protección contra software malicioso y código móvil* Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra software malicioso	Control Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
A.10.4.2	Controles contra códigos móviles	Control Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado
A.10.5 Respaldo (back-up) Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.		
A.10.5.1	*Back-up y respaldo de la información*	Control Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
A.10.6 *Gestión de seguridad de redes* Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de red	Control Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de red	Control Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
A.10.7 Gestión de medios		

Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no-autorizada de los activos; y la interrupción de las actividades comerciales.		
A.10.7.1	Gestión de los medios removibles	Control Deben existir procedimientos para la gestión de medios removibles.
A.10.7.2	Eliminación de medios	Control Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.
A.10.7.3	Procedimientos de manejo de la información	Control Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.
A.10.7.4	Seguridad de documentación del sistema	Control Se debe proteger la documentación de un acceso no autorizado.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.		
A.10.8.1	Procedimientos y políticas de información y software	Control Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.
A.10.8.2	Acuerdos de intercambio	Control Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	Medios físicos en tránsito	Control Los medios que contienen información deben ser protegidos contra un acceso no-autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensajes electrónicos	Control Se debe proteger adecuadamente los mensajes electrónicos.
A.10.8.5	Sistemas de información comercial	Control Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
A.10.9 Servicios de comercio electrónico Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro		
A.10.9.1	Comercio electrónico	Control Se debe proteger la información involucrada en el comercio electrónico que se trasmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada.
A.10.9.2	Transacciones en-línea	Control Se debe proteger la información involucrada en las transacciones en-línea para evitar la transmisión incompleta, rutas equivocadas, alteración no-autorizada del mensaje, divulgación no-autorizada, y duplicación o re-envío no-autorizado del mensaje.
A.10.9.3	Información	Control

	disponible públicamente	Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.
A.10.10 Monitoreo Objetivo: Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1	*Registro de auditoria*	Control Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
A.10.10.2	*Uso del sistema de monitoreo*	Control Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.
A.10.10.3	Protección de la información del registro	Control Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.
A.10.10.4	Registros del administrador y operador	Control Se deben registrar las actividades del administrador y operador del sistema.
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.
A.10.10.6	Sincronización de relojes	Control Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.
A.11 Control de acceso		
A.11.1 Requerimiento comercial para el control del acceso Objetivo: Controlar acceso a la información		
A.11.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.
A.11.2 Gestión del acceso del usuario Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no-autorizado a los sistemas de información.		
A.11.2.1	Inscripción del usuario	Control Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Control Se debe restringir y controlar la asignación y uso de los privilegios.
A.11.2.3	Gestión de la clave del usuario	Control La asignación de claves se debe controlar a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso del usuario	Control La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
A.11.3 Responsabilidades del usuario Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.		

A.11.3.1	Uso de clave	Control Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.3.2	Equipo de usuario desatendido	Control Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido
A.11.3.3	Política de pantalla y escritorio limpio	Control Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
A.11.4 Control de acceso a redes Objetivo: Evitar el acceso no-autorizado a los servicios en red.		
A.11.4.1	Política sobre el uso de servicios en red	Control Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
A.11.4.2	Autenticación del usuario para conexiones externas	Control Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación del equipo en red	Control Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
A.11.4.4	Protección del puerto de diagnóstico remoto	Control Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
A.11.4.5	Segregación en redes	Control Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
A.11.4.6	Control conexión de redes	Control Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales (ver 11.1).
A.11.4.7	Control de 'routing' de redes	Control Se deben implementar controles 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.
A.11.5 Control de acceso al sistema de operación Objetivo: Evitar acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de registro en el terminal	Control Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.
A.11.5.2	Identificación y autenticación del usuario	Control Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la

		identidad del usuario.
A.11.5.3	Sistema de gestión de claves	Control Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.
A.11.5.4	Uso de utilidades del sistema	Control Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.
A.11.5.5	Sesión inactiva	Control Las sesiones inactivas deben cerrarse después de un período de inactividad definido.
A.11.5.6	Limitación de tiempo de conexión	Control Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.
A.11.6 Control de acceso a la aplicación e información Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.		
A.11.6.1	Restricción al acceso a la información	Control Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.
A.11.6.2	Aislamiento del sistema sensible	Control Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).
A.11.7 Computación móvil y tele-trabajo Objetivo: Asegurar la seguridad de la información cuando se utilice medios computación móvil y tele-trabajo.		
A.11.7.1	Computación móvil y comunicaciones	Control Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.
A.11.7.2	Tele-trabajo	Control Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.12.1 Requerimientos de seguridad de los sistemas Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificación de los requerimientos de seguridad	Control Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
A.12.2 Procesamiento correcto en las aplicaciones Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.		
A.12.2.1	Validación de data de Insumo	Control El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
A.12.2.2	Control de procesamiento interno	Control Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de

		procesamiento o actos deliberados.
A.12.2.3	Integridad del mensaje	Control Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
A.12.2.4	Validación de data de output	Control Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos.		
A.12.3.1	Política sobre el uso de controles criptográficos	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.12.3.2	Gestión clave	Control Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía en la organización.
A.12.4 Seguridad de los archivos del sistema Objetivo: Garantizar la seguridad de los archivos del sistema		
A.12.4.1	Control de software operacional	Control Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.4.2	Protección de la data de prueba del sistema	Control Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba
A.12.4.3	Control de acceso al código fuente del programa	Control Se debe restringir el acceso al código fuente del programa.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: Mantener la seguridad del software e información del sistema de aplicación		
A.12.5.1	Procedimientos de control de cambio	Control La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	Control Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
A.12.5.3	Restricciones sobre los cambios en los paquetes de software	Control No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
A.12.5.4	Filtración de información	Control Se deben evitar las oportunidades de filtraciones en la información.
A.12.5.5	Desarrollo de outsourced software	Control El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la

		organización.
A.12.6 Gestión de vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.
A. 13 Gestión de incidentes en la seguridad de la información		
A.13.1 Reporte de eventos y debilidades en la seguridad de la información Objetivo: Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.		
A.13.1.1	Reporte de eventos en la seguridad de la información	Control Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
A.13.1.2	Reporte de debilidades en la seguridad	Control Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	Control Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
A.13.2.3	Recolección de evidencia	Control Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.
A.14 Gestión de la continuidad comercial		
A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	Incluir seguridad de la información en el proceso de gestión de	Control Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los

	continuidad comercial	requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
A.14.1.2	Continuidad comercial y evaluación del riesgo	Control Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
A.14.1.4	Marco referencial para la planeación de la continuidad comercial	Control Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.
A.14.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales	Control Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.
A.15 Cumplimiento		
A.15.1 Cumplimiento con requerimientos legales Objetivo: Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad		
A.15.1.1	Identificación de legislación aplicable	Control Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.
A.15.1.2	Derechos de propiedad intelectual (IPR)	Control Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
A.15.1.3	Protección los registros organizacionales	Control Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
A.15.1.4	Protección de data y privacidad de información personal	Control Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.

A.15.1.5	Prevención de mal uso de medios de procesamiento de información	Control Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.
A.15.1.6	Regulación de controles criptográficos	Control Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.
A.15.2 Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.		
A.15.2.1	*Cumplimiento con las políticas y estándares de seguridad*	Control Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
A.15.2.2	*Chequeo de cumplimiento técnico*	Control Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.
A.15.3 Consideraciones de auditoria de los sistema de información Objetivo: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoria de los sistema de información.		
A.15.3.1	Controles de auditoria de sistemas de información	Control Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.
A.15.3.2	Protección de las herramientas de auditoria de los sistemas información	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

Anexo B

(Informativo)

Principios OECD y este Estándar Internacional

Los principios dados en los Lineamientos OECD para la Seguridad de los Sistemas y Redes de Información [1] se aplican a toda las políticas y niveles operacionales que gobiernan la seguridad de los sistemas y redes de información. Este Estándar Británico proporciona un marco referencial del sistema de gestión de la seguridad de la información para implementar algunos de los principios OECD utilizando el modelo PDCA y los procesos descritos en las Cláusulas 4, 5, 6 y 8 como se indica en la Tabla B.1.

Tabla B.1 – Principios OECD y el modelo PDCA

Principio OECD	Proceso SGSI correspondiente y fase PDCA
Conciencia	Esta actividad es parta de la fase **Hacer**

Los participantes deben estar al tanto de la necesidad de seguridad de los sistemas y redes de información y lo que pueden hacer para aumentar la seguridad	(ver 4.2.2 y 5.2.2)
Responsabilidad Todos los participantes son responsables de la seguridad de los sistemas y redes de información.	Esta actividad es parte de la fase **Hacer** (ver 4.2.2 y 5.1)
Respuesta Los participantes deben actuar de manera oportuna y cooperativa para evitar, detectar y responder a los incidentes de seguridad.	Esta es en parte una actividad de monitoreo de la fase **Chequear** (ver 4.2.3 y 6 al 7.3) y una actividad de respuesta de la fase **Actuar** (ver 4.2.4 y 8.1 al 8.3). Esto también puede ser abarcado por algunos aspectos de las fases **Planear** y **Chequear.**
Evaluación del riesgo Los participantes deben realizar evaluaciones de riesgo.	Esta actividad es una parte de la fase **Planear** (ver 4.2.1) y la evaluación del riesgo es parte de la fase **Chequear** (ver 4.2.3 y 6 al 7.3).
Diseño e implementación de la seguridad Los participantes deben incorporar la seguridad como un elementos esencial de los sistemas y redes de información.	Una vez que se ha completado la evaluación del riesgo, se seleccionan los controles para el tratamiento de riesgos como una parte de la fase **Planear** (ver 4.2.1) y la fase **Hacer** (ver 4.2.2 y 5.2) entonces abarca la implementación y uso operacional de estos controles.
Gestión de la seguridad Los participantes deben adoptar un enfoque integral para la gestión de la seguridad.	La gestión del riesgo es un proceso que incluye la prevención, detección y respuesta a los incidentes, mantenimiento continuo, revisión y auditoria. Todos estos aspectos son parte de las fases **Planear, Hacer, Chequear y Actuar.**
Reevaluación Los participantes deben revisar y reevaluar la seguridad de los sistemas y redes de información, y realizar las modificaciones apropiadas en las políticas, prácticas, medidas y procedimientos.	La reevaluación de la seguridad de la información es una parte de la fase **Chequear** (ver 4.2.3 y 6 a 7.3) donde se deben realizar revisiones regulares para chequear la efectividad del sistema de gestión de seguridad de la información, y mejorar la seguridad es parte de la fase **Actuar** (ver 4.2.4 y 8.1 al 8.3).

ANEXO N° 2

Ley N° 29985

Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera

LEY Nº 29985

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República

Ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY QUE REGULA LAS CARACTERÍSTICAS BÁSICAS DEL DINERO ELECTRÓNICO COMO INSTRUMENTO DE INCLUSIÓN FINANCIERA

Artículo 1. Objeto de la Ley

1.1 El objeto de la presente Ley es regular la emisión de dinero electrónico, determinar las empresas autorizadas a emitirlo y establecer el marco regulatorio y de supervisión de las Empresas Emisoras de Dinero Electrónico.

1.2 La emisión de dinero electrónico comprende las operaciones de emisión propiamente dicha de dinero electrónico, reconversión a efectivo, transferencias, pagos y cualquier movimiento u operación relacionada con el valor monetario del que disponga el titular y necesaria para las mismas.

Artículo 2. Dinero electrónico

El dinero electrónico es un valor monetario representado por un crédito exigible a su emisor, el cual tiene las siguientes características:

a) Es almacenado en un soporte electrónico.

b) Es aceptado como medio de pago por entidades o personas distintas del emisor y tiene efecto cancelatorio.

c) Es emitido por un valor igual a los fondos recibidos.

d) Es convertible a dinero en efectivo según el valor monetario del que disponga el titular, al valor nominal.

e) No constituye depósito y no genera intereses.

Artículo 3. Reserva de actividad

Solo pueden emitir dinero electrónico las empresas que operan bajo el ámbito de supervisión de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, listadas en el inciso A del artículo 16 y el numeral 6 del artículo 17 de la Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.

Artículo 4. Características y obligaciones de las Empresas Emisoras de Dinero Electrónico

4.1 Las Empresas Emisoras de Dinero Electrónico tienen como objeto principal la emisión de dinero electrónico, no conceden crédito con cargo a los fondos recibidos y solo pueden realizar otras operaciones relacionadas a su objeto principal.

4.2 Las Empresas Emisoras de Dinero Electrónico son sujetos obligados a proporcionar la información a que se refiere el artículo 3 de la Ley 27693, Ley que crea la Unidad de Inteligencia Financiera - Perú, y sus modificatorias, conforme a lo dispuesto en el literal a) del numeral 3.1 del artículo 3 de la Ley 29038, Ley que incorpora la Unidad de Inteligencia Financiera del Perú (UIF-PERÚ) a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, y sus normas reglamentarias. En tal sentido, se encuentran obligadas a cumplir con las disposiciones reglamentarias emitidas sobre prevención del lavado de activos y financiamiento del terrorismo que emita la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, siendo responsables de aplicar las normas del presente numeral a sus clientes o usuarios que adquieran el dinero electrónico que emitan.

Artículo 5. Emisores de dinero electrónico

Los emisores de dinero electrónico:

a) No pueden establecer un límite a la vigencia de los fondos de dinero electrónico, distinto al reglamentado. Cuando transcurran diez (10) años sin que una cuenta de dinero electrónico tenga movimientos y sin que medie reclamación durante ese lapso, dichos fondos son remitidos a la Dirección General de Endeudamiento y Tesoro Público del Ministerio de Economía y Finanzas para ser destinados a programas de inclusión financiera.

b) Están sujetos a los límites de emisión de dinero electrónico de una Unidad Impositiva Tributaria (UIT) por transacción, de acuerdo a las condiciones que se establezca en la reglamentación de la presente Ley.

c) Se sujetan a las disposiciones de encaje y a las que por la Ley 29440, Ley de los Sistemas de Pagos y de Liquidación de Valores, formule el Banco Central de Reserva del Perú.

Artículo 6. Protección al usuario

6.1 **Garantía de recursos.** Los emisores de dinero electrónico deben constituir fideicomisos por el valor del dinero electrónico emitido conforme a las disposiciones que dicta la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones. Dicho Organismo de Control puede regular otras modalidades alternativas de garantía para los fondos de dinero electrónico emitidos.

6.2 **Protección de datos.** La emisión de dinero electrónico constituye un servicio financiero, y la información del usuario de dinero electrónico y de las operaciones que realice están sujetas a la Ley 29733, Ley de Protección de Datos Personales, y a la protección del artículo 2, inciso 5, de la Constitución Política del Perú.

6.3 **Contratos.** La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones establece las modalidades de contratación aplicables al dinero electrónico, las que pueden ser escritas, electrónicas u otras, de acuerdo a la naturaleza de los productos, sus características y las circunstancias en que estos se ofrecen, en concordancia con lo dispuesto en la Ley 29571, Código de Protección y Defensa del Consumidor; la Ley 28587, Ley Complementaria a la Ley de Protección al Consumidor en Materia de Servicios Financieros, y las normas reglamentarias emitidas para garantizar su cumplimiento.

Artículo 7. Exoneración del Impuesto General a las Ventas

Exonerase del Impuesto General a las Ventas por un período de tres (3) años, contado a partir de la vigencia de la presente Ley, la emisión de dinero electrónico efectuada por las Empresas Emisoras de Dinero Electrónico.

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Empresas Emisoras de Dinero Electrónico

Incorpórase el numeral 6 al artículo 17 de la Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, de acuerdo al texto siguiente:

"**Artículo 17.- CAPITAL MÍNIMO DE EMPRESAS DE SERVICIOS COMPLEMENTARIOS Y CONEXOS.**

(...)

6. Empresas Emisoras de Dinero Electrónico: S/. 2 268 519,00. El citado capital corresponde al trimestre octubre - diciembre 2012 y posteriormente se sujeta a la actualización trimestral según el procedimiento señalado en el artículo 18 de la Ley 26702."

SEGUNDA. Procedimiento de autorización de organización y funcionamiento

Modifícanse el segundo párrafo del artículo 19 y el tercer párrafo del artículo 21 de la Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, conforme al siguiente texto:

"**Artículo 19.- ORGANIZADORES DE EMPRESAS.**

(...)

La Superintendencia está facultada para autorizar la organización y el funcionamiento de las empresas comprendidas en los artículos 16 y 17 de la presente Ley. En el caso de las empresas comprendidas en los incisos A, B y C del artículo 16 así como del numeral 6 del artículo 17 debe contar con la opinión previa del Banco Central.

Artículo 21.- SOLICITUD DE ORGANIZACIÓN.

(...)

Una vez recibida la documentación completa, la Superintendencia la pondrá en conocimiento del Banco Central cuando se trate de empresas precisadas en los incisos A, B y C del artículo 16, así como en el numeral 6 del artículo 17. El Banco Central debe emitir su opinión dentro de los treinta (30) días de recibido el oficio respectivo."

TERCERA. Autorización de la operación de emisión de dinero electrónico a empresas del sistema financiero

Incorpóranse como numeral 42 al artículo 221 y el literal h) a la trigésima primera disposición final y complementaria de la Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, según los textos siguientes:

"**221.- OPERACIONES Y SERVICIOS**

(...)

42. Emitir dinero electrónico.

(...)

TRIGÉSIMA PRIMERA:

(...)

h. Numeral 42 del artículo 221: Emitir dinero electrónico."

CUARTA. Sistemas de pagos y de liquidación de valores

Incorpórase el inciso n) al artículo 10 de la Ley 29440, Ley de los Sistemas de Pagos y de Liquidación de Valores, con el siguiente texto:

"10.- Órgano rector de los Sistemas de Pagos

(...)

n) Dictar, cuando estime necesario, normas, reglamentos, principios y estándares, así como supervisar su cumplimiento, a los Acuerdos de Pago y Proveedores de Servicios de Pagos, para propender a su funcionamiento seguro y eficiente.

(...)"

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Normas reglamentarias

El Ministerio de Economía y Finanzas, en coordinación con la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, como supervisor de las empresas bajo su control que emitan dinero electrónico, reglamenta la presente Ley en un plazo no mayor de cuarenta y cinco (45) días calendario posterior a su entrada en vigencia. Asimismo, la Superintendencia emite, en un plazo no mayor de noventa (90) días calendario posterior a la entrada en vigencia de esta Ley, las normas que sean necesarias sobre ingreso y salida al mercado, operaciones, límites, garantías o respaldo del dinero electrónico en circulación, régimen de inversiones, uso de fideicomisos, sanciones y demás aspectos necesarios para el adecuado y seguro funcionamiento de las Empresas Emisoras de Dinero Electrónico, así como para su supervisión.

SEGUNDA. Utilización de los servicios de telecomunicaciones y disposiciones regulatorias para el cumplimiento de la Ley

Los servicios de telecomunicaciones sujetos al Texto Único Ordenado de la Ley de Telecomunicaciones, aprobado por Decreto Supremo 013-93-TCC; y al Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado por Decreto Supremo 020-2007-MTC, que se utilicen para la prestación de servicios financieros, deben ser brindados en igualdad de condiciones a todas las empresas que provean estos servicios financieros.

El Organismo Supervisor de Inversión Privada en Telecomunicaciones (Osiptel) es competente para dictar las disposiciones que garanticen el acceso a los servicios de telecomunicaciones por parte de las empresas que provean servicios financieros, en igualdad de condiciones. En el marco de esta facultad y a falta de acuerdo entre las empresas que brindan servicios de telecomunicaciones y las que provean servicios financieros, dicta mandatos estableciendo las condiciones que fueran necesarias para garantizar dicho acceso.

TERCERA. Condiciones y oportunidades para la interoperabilidad

La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y el Banco Central de Reserva del Perú, en el ámbito de sus competencias, establecen a las entidades sujetas a su supervisión condiciones y oportunidades para la interoperabilidad.

Entiéndase por interoperabilidad aquella situación en la que un cliente pueda realizar transacciones con cualquier contraparte, independientemente del proveedor de servicios financieros.

CUARTA. Implementación de transacciones con DNI electrónico

En el marco del proceso de implementación del Documento Nacional de Identidad electrónico (DNIe), el Registro Nacional de Identificación y Estado Civil (Reniec), en coordinación con los sectores pertinentes, habilita las aplicaciones correspondientes para que en dicho documento se almacene información para usos financieros, bancarios y no bancarios, con autorización del usuario, conforme a la Ley 29733, Ley de Protección de Datos Personales; y al artículo 2, inciso 5, de la Constitución Política del Perú.

QUINTA. Incorporación de empresas con actividades similares

La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones puede incorporar en los alcances de la presente Ley a las empresas que realicen actividades similares a la emisión de dinero electrónico.

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los veintiún días del mes de diciembre de dos mil doce.

VÍCTOR ISLA ROJAS

Presidente del Congreso de la República

JOSÉ LEÓN LUNA GÁLVEZ

Tercer Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los dieciséis días del mes de enero del año dos mil trece.

OLLANTA HUMALA TASSO

Presidente Constitucional de la República

JUAN F. JIMÉNEZ MAYOR

Presidente del Consejo de Ministros

ANEXO N° 3

Resolución SBS Nº 6283-2013

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Lima, 18 de octubre de 2013

Resolución S.B.S.
Nº 6283-2013

El Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que, mediante Ley Nº 29985 se aprobó la Ley que regula las Características Básicas del Dinero Electrónico como Instrumento de Inclusión Financiera, en adelante la Ley;

Que, mediante Decreto Supremo N° 090-2013-EF se aprobó el Reglamento de la Ley Nº 29985 que Regula las Características Básicas del Dinero Electrónico;

Que, ambos dispositivos legales facultan a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, a emitir normas reglamentarias y complementarias sobre diversas materias relacionadas a las operaciones con dinero electrónico;

Que, en ese sentido resulta necesario establecer el marco normativo bajo el cual se regirá la realización de operaciones con dinero electrónico;

Que, mediante Resolución SBS N° 895-98 y sus normas modificatorias y complementarias se aprobó el Manual de Contabilidad para las Empresas del Sistema Financiero, en adelante Manual de Contabilidad;

Que, a efectos de recoger las opiniones del público en general, se dispuso la prepublicación del proyecto de resolución en el portal electrónico de la Superintendencia, al amparo de lo dispuesto en el Decreto Supremo Nº 001-2009-JUS;

Contando con el visto bueno de las Superintendencias Adjuntas de Banca y Microfinanzas, Riesgos, Estudios Económicos y Asesoría Jurídica, así como de la Gerencia de Productos y Servicios al Usuario; y,

En uso de las atribuciones conferidas en los numerales 7, 9, 13 y 19 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros – Ley N°26702 y sus normas modificatorias, en

adelante Ley General, así como las facultades otorgadas en la Ley Nº 29985 y su reglamento aprobado por Decreto Supremo N° 090-2013-EF;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento de Operaciones con Dinero Electrónico, según se indica a continuación:

"REGLAMENTO DE OPERACIONES CON DINERO ELECTRONICO

TÍTULO I
DE LAS DISPOSICIONES GENERALES

Artículo 1.- Alcance
Las disposiciones de la presente norma son aplicables a las empresas de operaciones múltiples comprendidas en el literal A del artículo 16° de la Ley General autorizadas a emitir dinero electrónico, a las empresas emisoras de dinero electrónico a que se refiere el numeral 6 del artículo 17° de la Ley General, al Banco de la Nación, al Banco Agropecuario, así como a las empresas que se consideren dentro del ámbito de la Ley, a criterio de esta Superintendencia, en aplicación de la Quinta Disposición Complementaria Final de la Ley, en adelante emisores de dinero electrónico.

Artículo 2.- Definiciones
Para efectos de lo dispuesto en la presente norma, considérense las siguientes definiciones:
a. Dinero electrónico: aquel definido de acuerdo con lo establecido en el artículo 1° del Reglamento de la Ley.
b. Emisión: comprende las operaciones de conversión a dinero electrónico, reconversión, transferencias, pagos y cualquier movimiento u operación relacionada con el valor monetario del que disponga el titular y necesaria para dichas operaciones.
c. Ley: Ley que Regula las Características Básicas del Dinero Electrónico, Ley Nº 29985.
d. Normas Complementarias para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo: Normas Complementarias para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo, aprobadas por la Resolución SBS N° 838-2008 y sus normas modificatorias.
e. Persona: se refiere a la persona natural o a la persona natural con negocio.
f. Reglamento de la Ley: Reglamento de la Ley Nº 29985 que Regula las Características Básicas del Dinero Electrónico, Decreto Supremo N° 090-2013-EF.
g. Reglamento de Transparencia de Información y Contratación con Usuarios del Sistema Financiero: Reglamento de Transparencia de Información y Contratación con Usuarios del Sistema Financiero aprobado por la Resolución SBS N° 8181-2012 y sus normas modificatorias.
h. Superintendencia: Superintendencia de Banca, Seguros y AFP.
i. Tarjeta prepago de dinero electrónico: es un soporte para el uso del dinero electrónico, en el cual se almacena valor monetario en una tarjeta, física o virtual, recargable o no, y cuyo uso se encuentra limitado al saldo existente en esta en cada momento.
j. Titular: persona que contrata con el emisor de dinero electrónico la prestación del servicio de emisión de dinero electrónico. También se considera titular a los menores de edad que tengan más de dieciséis (16) años, que cuenten con autorización de su tutor o apoderado legal o que cuenten con capacidad de ejercicio de acuerdo con la normativa vigente.

k. Transacción: Es la ejecución individual de las operaciones de conversión, reconversión, transferencias, pagos y cualquier movimiento u operación relacionada con el valor monetario del que disponga el titular y necesaria para dichas operaciones.

TÍTULO II
DEL DINERO ELECTRÓNICO

Artículo 3.- Operaciones con dinero electrónico
Las operaciones que pueden realizarse con dinero electrónico, según el tipo de cuenta de dinero electrónico, son:

a) Conversión.
b) Reconversión.
c) Pagos.
d) Transferencias.
e) Otras operaciones a los que el emisor de dinero electrónico haya sido autorizado por esta Superintendencia.

Artículo 4.- Soportes para uso de dinero electrónico
Los soportes mediante los cuales se puede hacer uso del dinero electrónico pueden ser los siguientes:
a) Teléfonos móviles
b) Tarjetas prepago.
c) Cualquier otro equipo o dispositivo electrónico, que cumpla los fines establecidos en la Ley.

Todos los soportes antes señalados deben 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.

La Superintendencia podrá autorizar plataformas tecnológicas que sigan otro esquema de transacciones, si considera que los controles a ser aplicados permiten administrar adecuadamente los riesgos asociados. En estos casos, el emisor de dinero electrónico proveerá información detallada acerca de la modalidad propuesta y adjuntará los informes preparados por la Unidad de Riesgo Operacional o equivalente.

Un mismo soporte puede ser utilizado y/o asociado para realizar transacciones con más de una cuenta de dinero electrónico.

Artículo 5.- Cuentas de dinero electrónico simplificadas
Se consideran "cuentas de dinero electrónico simplificadas" 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) Cada transacción se encuentra sujeta al límite de mil nuevos soles (S/. 1,000).
c) El saldo consolidado de cuentas de dinero electrónico de un mismo titular, bajo cualquier modalidad, en un mismo emisor de dinero electrónico, no puede ser superior a dos mil nuevos soles (S/. 2,000) en todo momento.
d) Las conversiones a dinero electrónico acumuladas de un mismo titular, bajo cualquier modalidad, en un mismo emisor en un mes, no pueden ser mayores a dos mil nuevos soles (S/. 2,000).

e) Las transacciones acumuladas (conversiones, transferencias, pagos, reconversiones, etc.) de un mismo titular, bajo cualquier modalidad, en un mismo emisor en un mes, no pueden exceder de cuatro mil nuevos soles (S/. 4,000).
f) Las cuentas de dinero electrónico simplificadas solo pueden ser abiertas y utilizadas en moneda nacional en el territorio nacional.

Los emisores de dinero electrónico deben definir procedimientos y medidas con el objetivo de monitorear el cumplimiento de los límites y condiciones antes señaladas.

Cuando los usuarios del dinero electrónico intenten efectuar transacciones que excedan los límites y condiciones antes establecidos, los emisores, a través del dispositivo utilizado, deberán informar a los usuarios que la transacción no puede ser llevada a cabo debido al incumplimiento de los límites.

Artículo 6.- Cuentas de dinero electrónico generales

Las cuentas de dinero electrónico que no cumplan las características para ser consideradas cuentas de dinero electrónico simplificadas, serán consideradas como cuentas de dinero electrónico generales y no estarán sujetas a los límites establecidos en el artículo anterior, pero sí al límite señalado en el literal b) del artículo 5° de la Ley.

Artículo 7.- Régimen Simplificado de conocimiento del cliente y debida diligencia de Lavado de activos y financiamiento del terrorismo

Las cuentas de dinero electrónico simplificadas se encuentran incluidas en el Régimen Simplificado de conocimiento del cliente y debida diligencia a que alude el artículo 9° de las Normas Complementarias para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo.

Para la apertura de las cuentas de dinero electrónico simplificadas se requerirá, como mínimo, la información correspondiente al nombre completo del titular, así como al número del Documento Nacional de Identidad (DNI) o al número del Carnet de Extranjería, según corresponda. La empresa deberá verificar la información antes señalada con la base de datos del Registro Nacional de Identificación y Estado Civil (RENIEC) o el Registro Central de Extranjería de la Dirección General de Migraciones y Naturalización, según corresponda, lo que podrá realizarse posteriormente a la apertura de la cuenta de dinero electrónico.

Para la apertura de cuentas de dinero electrónico simplificadas que tengan como soporte electrónico teléfonos móviles, se requerirá también el número de servicio de telefonía móvil asociado a dicho soporte electrónico.

Las empresas deberán desarrollar procedimientos de monitoreo, evaluación de riesgo y control a fin de prevenir el abuso de las cuentas de dinero electrónico simplificadas, garantizar su operatividad dentro de las condiciones establecidas y tomar las medidas adicionales que sean apropiadas para mantener el servicio dentro de los niveles propios de una cuenta de bajo riesgo en materia de lavado de activos y de financiamiento del terrorismo.

Las empresas podrán solicitar a la Superintendencia que otros servicios de dinero electrónico de bajo riesgo de lavado de activos y financiamiento del terrorismo sean considerados bajo el Régimen Simplificado de prevención de lavado de activos y financiamiento del terrorismo, para lo cual tendrán en cuenta lo establecido en el numeral 9.1 del artículo 9° de las Normas Complementarias para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo.

Artículo 8.- Régimen General de conocimiento del cliente y debida diligencia de lavado de activos y financiamiento del terrorismo
Los requisitos de identificación y verificación mínimos aplicables a los titulares para la apertura de las cuentas de dinero electrónico que no cumplan las características para ser consideradas cuentas de dinero electrónico simplificadas, se regirán por lo establecido en el artículo 8° de las Normas Complementarias para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo, con excepción de aquellos titulares que se encuentren sujetos al régimen de procedimiento reforzado de conocimiento del cliente, que establece el numeral 9.2 del artículo 9° de las citadas normas.

Para la apertura de cuentas de dinero electrónico antes señaladas que tengan como soporte electrónico teléfonos móviles, se requerirá también el número de servicio de telefonía móvil asociado a dicho soporte electrónico.

En el caso de extranjeros la contratación podrá efectuarse únicamente de manera presencial y escrita con la presentación de su Carnet de Extranjería o Pasaporte a satisfacción del emisor de dinero electrónico. La empresa deberá verificar esta información con la base de datos del Registro Central de Extranjería de la Dirección General de Migraciones y Naturalización, lo que podrá realizarse posteriormente a la apertura de la cuenta de dinero electrónico.

Artículo 9.- Transacciones realizadas a través de cajeros corresponsales
Los emisores de dinero electrónico deberán establecer mecanismos que aseguren que las transacciones con dinero electrónico realizadas a través de cajeros corresponsales, cumplan con lo establecido en los párrafos segundo o tercero del artículo 4° de la presente norma, según corresponda; ello implica no solo el registro de las transacciones en las cuentas de dinero electrónico de los titulares, sino también el registro del ingreso o salida de los recursos en los sistemas del emisor.

Conforme lo señalado en el artículo 7° del Reglamento de la Ley, en los casos que los emisores de dinero electrónico utilicen cuentas operativas de dinero electrónico con sus cajeros corresponsales, estas no estarán sujetas al límite establecido en el literal b) del artículo 5° de la Ley, ni a los límites establecidos en el artículo 5° de la presente norma.

Artículo 10.- Información a presentar a la Superintendencia
Los emisores de dinero electrónico deberán presentar a la Superintendencia, vía SUCAVE, el Reporte N° 32-A "Reporte Diario de Dinero Electrónico". Este Reporte deberá ser presentado diariamente hasta las 15:00 horas del día hábil siguiente.

Asimismo, los emisores de dinero electrónico deberán presentar a la Superintendencia, vía SUCAVE, el Reporte N° 32-B "Reporte Mensual de Dinero Electrónico". Este Reporte deberá ser presentado mensualmente dentro de los quince (15) días calendario siguientes a la fecha de cierre de cada mes.

TÍTULO III[1]
ASPECTOS APLICABLES EN MATERIA DE TRANSPARENCIA DE INFORMACIÓN, CONTRATACIÓN Y SERVICIOS DE ATENCIÓN AL USUARIO

[1] Título sustituido por la Resolución SBS N° 4628 de 13/08/2015

Artículo 11.- Aspectos generales en materia de transparencia de información y atención al usuario

11.1 La contratación de cuentas de dinero electrónico, tanto simplificadas como generales, se rige por las disposiciones del presente título, el cual desarrolla el Régimen Simplificado de Transparencia establecido con arreglo a la Sexta Disposición Final y Complementaria del Reglamento de Transparencia de Información y Contratación con Usuarios del Sistema Financiero, que resulta aplicable en forma complementaria a las disposiciones contempladas en el presente título, según corresponda.

11. 2 Para la prestación del servicio de dinero electrónico, los emisores de dinero electrónico deben poner a disposición de los usuarios, por lo menos, los siguientes canales de presentación de reclamos, que deben ser gratuitos y de fácil acceso:

a) Red de oficinas de atención al público, en caso cuenten con estos canales.
b) Al menos uno de los siguientes: Vía telefónica al número designado para la recepción de reclamos, al correo electrónico o a la página web establecida por el emisor de dinero electrónico para tal efecto.

La red de oficinas de atención al público de los emisores de dinero electrónico debe recibir y canalizar la información de sustento que otorguen los usuarios, como consecuencia de la presentación de un reclamo, sin importar el canal empleado para su presentación.

11.3 La presentación de requerimientos, tales como consultas, solicitudes de información que el emisor posee sobre la relación que mantiene con los usuarios y otras solicitudes por parte de estos, puede ser realizada por los medios y canales que los emisores de dinero electrónico definan para tal efecto, siempre que sean gratuitos y de fácil acceso, considerando lo señalado en la Circular de Servicio de Atención al Usuario.

11.4 Los emisores de dinero electrónico deben proporcionar capacitación adecuada a las personas involucradas en el proceso de contratación y sistema de atención al usuario del servicio de dinero electrónico, de sus oficinas de atención al público y atención por vía telefónica, con la finalidad de asegurar que se encuentren en capacidad de explicar la información que debe brindarse y/o la que sea requerida por los usuarios, considerando lo señalado en el presente título.

Asimismo, los emisores de dinero electrónico deben proporcionar capacitación a las personas involucradas en la operación de los cajeros corresponsales sobre la prestación del servicio de dinero electrónico.

11.5 En caso de requerirse la subcontratación de servicios para dar cumplimiento a lo dispuesto en el presente título, resulta aplicable lo dispuesto en el Reglamento de la Gestión Integral de Riesgos; y no debe quedar duda respecto de la identidad y responsabilidad que corresponde al emisor de dinero electrónico. En el caso de subcontratación del servicio provisto a través de páginas web y/o vía telefónica, el emisor de dinero electrónico debe establecer una conexión directa en su propia página web y/o teléfono para que los usuarios puedan acceder a dichos servicios subcontratados.

11.6 Con excepción de las disposiciones contempladas en el presente artículo sobre la presentación de reclamos y requerimientos, al servicio de dinero electrónico le resultan aplicables las demás disposiciones contenidas en la Circular de Servicio de Atención al Usuario.

Artículo 12.- Información al usuario

Los emisores de dinero electrónico deben brindar y/o poner a disposición de los usuarios, según corresponda al canal empleado, de manera previa a la celebración del contrato, la siguiente información a través de las oficinas de atención al público, en caso cuenten con estas, y en la página web establecida por el emisor:

a) El tarifario, que debe hacer referencia a las comisiones y gastos aplicables.
b) El formulario contractual, que debe contener un resumen de condiciones. El resumen debe incorporar, como mínimo: i) las comisiones y gastos aplicables a las operaciones con dinero electrónico, ii) las características y las condiciones para realizar operaciones con dinero electrónico, los límites asociados a las operaciones y las restricciones aplicables a la cuenta dinero electrónico, iii) los supuestos de responsabilidad de las partes, iv) los canales disponibles para la atención de requerimientos y reclamos; y, v) los mecanismos de comunicación a disposición de los usuarios para realizar el bloqueo de las cuentas de dinero electrónico por, entre otros, el extravío, sustracción, robo, hurto o uso no autorizado del soporte entregado por el emisor para el uso de dinero electrónico o de la información que contiene.

Adicionalmente, en caso el emisor de dinero electrónico permita realizar la contratación del servicio de dinero electrónico a través de un número telefónico designado por este y/o de cajeros corresponsales, se debe difundir y poner a disposición de los usuarios, a través de dichos canales, como mínimo: i) la información a que hace referencia el resumen de condiciones, la que en el caso de contratación presencial por cajeros corresponsales, debe encontrarse en un lugar destacado y de fácil acceso; ii) la información sobre los canales establecidos para acceder a la información adicional señalada en el presente título, y iii) la información sobre los canales establecidos para la atención de reclamos y requerimientos.

Artículo 13.- Difusión de aspectos relevantes referidos a los beneficios, riesgos y condiciones del servicio

La información sobre aspectos relevantes relacionados principalmente a los beneficios, riesgos y condiciones del servicio se debe incluir en los formularios contractuales y en la página web establecida por el emisor de dinero electrónico.

En dicha página web se debe considerar –como mínimo- la información que se detalla a continuación:

a) Las condiciones para el uso, conservación y seguridad del soporte entregado por el emisor para el uso del dinero electrónico, tales como tarjetas u otros, en caso corresponda.
b) El procedimiento aplicable en el caso de fallecimiento del titular de la cuenta de dinero electrónico.
c) El procedimiento para la presentación y atención de las solicitudes de resolución del contrato, indicándole todos los canales puestos a su disposición para tal fin. Dicho procedimiento no puede ser más engorroso que aquel dispuesto para contratar, por lo que no pueden establecerse requisitos o exigencias adicionales que dificulten el ejercicio del derecho a resolver el contrato.
d) El procedimiento aplicable para realizar el bloqueo de la cuenta de dinero electrónico.
e) Otros que establezcan los emisores de dinero electrónico o la Superintendencia, mediante oficio múltiple.

Artículo 14.- Determinación de comisiones y gastos

Para efectos de lo dispuesto en el presente título, se entiende por comisión o gasto a la retribución por la prestación de un servicio efectivo, que incluye la prestación del servicio de dinero electrónico, previamente acordado con el usuario y que cuente con justificación técnica.

Las comisiones son retribuciones por servicios prestados por los emisores de dinero electrónico y los gastos retribuciones por servicios en que incurren los emisores con terceros por cuenta del usuario.

Las disposiciones generales contenidas en el Reglamento de Transparencia de Información y Contratación con Usuarios del Sistema Financiero respecto de comisiones y gastos resultan aplicables, en lo que corresponda, atendiendo a las particularidades del servicio de dinero electrónico.

Artículo 14 – A°.- Contenido mínimo del contrato

El contrato de dinero electrónico debe contener, como mínimo, la siguiente información:

a) Las características y las condiciones para realizar operaciones con dinero electrónico, los límites asociados a las operaciones, así como las restricciones aplicables a la cuenta de dinero electrónico.
b) Las condiciones de reconversión.
c) Las condiciones para el uso, conservación y seguridad del soporte entregado por el emisor para el uso del dinero electrónico, tales como tarjetas u otros en caso corresponda.
d) Los canales puestos a su disposición para la realización de las operaciones con dinero electrónico, indicando los requisitos para su utilización.
e) La posibilidad de que el cliente solicite el bloqueo temporal o definitivo de su cuenta de dinero electrónico por, entre otros, el extravío, sustracción, robo, hurto o uso no autorizado del soporte entregado por el emisor para el uso de dinero electrónico o de la información que contiene.
f) Procedimiento aplicable para la resolución del contrato.
g) Los supuestos de responsabilidad de las partes considerando lo indicado en el artículo 14-E.
h) Otros que establezcan los emisores de dinero electrónico o la Superintendencia, mediante oficio múltiple.

Las cláusulas generales de contratación de los contratos de dinero electrónico deben ser aprobadas, previamente por la Superintendencia, considerando para tal efecto lo dispuesto en el Reglamento de Transparencia de Información y Contratación con Usuarios del Sistema Financiero.

Artículo 14-B°.- Contratación de dinero electrónico

Los emisores de dinero electrónico pueden celebrar contratos por canales presenciales o no presenciales, excepto en el caso de extranjeros, que solo podrán hacerlo de manera presencial y por escrito según lo establecido en el tercer párrafo del artículo 8°, considerando para tal efecto lo siguiente:

a) La contratación presencial y escrita se realiza a través de la firma-o huella digital, en caso de no saber firmar o estar impedido de hacerlo- del contrato y resumen de condiciones por duplicado, quedando un ejemplar en poder de los emisores de dinero electrónico como constancia de su entrega al cliente.
b) La contratación no presencial o presencial a través de mecanismos distintos al escrito, debe cumplir las siguientes condiciones:
    i. La contratación se realiza por teléfono o a través de medios electrónicos.
    ii. El emisor de dinero electrónico debe contar con mecanismos adecuados para garantizar la seguridad de la contratación en todas sus etapas y pueda dejarse constancia de la aceptación por parte del titular de la cuenta de dinero electrónico, de las estipulaciones contractuales, las cuales deben estar a disposición previa de los usuarios considerando lo dispuesto en el artículo 12°. En estos casos no se requerirá la firma -o huella digital, en caso de no saber firmar o estar impedido de hacerlo- de los formularios contractuales.
    iii. Los emisores de dinero electrónico pueden determinar que el contrato y el resumen de condiciones se entreguen y/o pongan a disposición, según corresponda al canal empleado, a través de alguno de los siguientes medios, siempre que sea comunicado previamente a los titulares de las cuentas de dinero electrónico, a través de medios físicos y/o electrónicos:
        - Mediante la entrega del contrato en el domicilio establecido por el cliente.

- Mediante el envío del contrato por correo electrónico, siempre que: i) se permita su lectura, impresión, conservación y reproducción sin cambios y ii) se cumplan los criterios de seguridad para autenticidad, integridad y disponibilidad, según lo establecido en la Circular G-140-2009 o la que la sustituya.
- Mediante la entrega del contrato en las oficinas de atención al público del emisor de dinero electrónico.
- Mediante la entrega del contrato a través de los cajeros corresponsales con los que opera el emisor de dinero electrónico.
- Mediante una página web señalada por el emisor de dinero electrónico, que permita el acceso del usuario al contrato, siempre que: i) sea fácilmente identificable, ii) se permita su lectura, impresión, conservación y reproducción sin cambios y iii) se guarden las medidas de seguridad apropiadas de autenticidad, integridad y disponibilidad de la información publicada, según lo establecido en la Circular G-140-2009 o la que la sustituya.

c) La entrega y/o puesta a disposición del contrato debe realizarse en un plazo máximo de quince (15) días de celebrado.

El emisor de dinero electrónico debe conservar la constancia de la celebración del contrato y de su entrega o puesta a disposición por el plazo establecido en el artículo 183° de la Ley General.

Artículo 14° - C.- Modificaciones contractuales
Las modificaciones unilaterales referidas a: i) comisiones, ii) gastos; y, iii) otras estipulaciones contractuales, solo proceden en la medida que su posibilidad haya sido previamente reconocidas en los contratos y comunicadas con una anticipación no menor a cuarenta y cinco (45) días, indicando la fecha o el momento, a partir del cual la modificación entrará en vigencia.

Los emisores de dinero electrónico deben pactar con el cliente los medios de comunicación idóneos para cumplir con la disposición de comunicación previa, considerando para tal efecto lo siguiente:

a) Se debe comunicar a través de medios de comunicación directos, tales como comunicaciones escritas al domicilio del cliente, correos electrónicos, mensajes de texto o comunicaciones telefónicas al cliente, las modificaciones contractuales referidas a:
   i. Comisiones y gastos cuando dichas modificaciones generen un perjuicio a los usuarios.
   ii. La resolución del contrato por causal distinta al incumplimiento.
   iii. La limitación o exoneración de responsabilidad por parte de los emisores de dinero electrónico.

   En caso se use mensajes de texto comunicando las modificaciones referidas al inciso i. precedente, estos deben incluir la totalidad de la modificación realizada, conforme se detalla en el literal c) del presente artículo.

   En caso se use mensajes de texto comunicando las modificaciones referidas a los incisos ii. y iii. precedentes, estos deben mencionar expresamente que se refiere a los aspectos contemplados en los referidos incisos y remitir de manera precisa y puntual, como mínimo, a dos medios de comunicación complementarios que permitan al usuario acceder y conocer la información completa de las referidas modificaciones.

b) Para comunicaciones sobre modificaciones contractuales de aspectos distintos a los previamente indicados, debe emplearse medios de comunicación que permitan al cliente tomar

conocimiento adecuado y oportuno de las modificaciones a ser efectuadas, de acuerdo con lo que para tal efecto se pacte con estos.

c) En las comunicaciones previas sobre modificaciones contractuales debe indicarse de manera expresa:
   i. Que se trata de una modificación en las condiciones pactadas, destacando aquellos conceptos que serán materia de cambio y señalando expresamente en qué consisten, a fin de permitir a los usuarios tomar conocimiento de ellos.
   ii. Que el cliente puede dar por concluida la relación contractual conforme a los términos del contrato.

d) Debe dejarse constancia respecto de las comunicaciones realizadas a los clientes.

Lo expuesto en el presente artículo no resulta aplicable cuando se trate de modificaciones contractuales que impliquen condiciones más favorables para el cliente las que se aplicarán de manera inmediata, no siendo exigible el envío de una comunicación previa. Sin perjuicio de lo indicado, el emisor de dinero electrónico debe informar de las nuevas condiciones a través de los mecanismos que para tal efecto pacte con los clientes.

Artículo 14° - D.- Mecanismo de comunicación a disposición de los usuarios para el bloqueo de cuentas de dinero electrónico

Los emisores de dinero electrónico deben contar con infraestructura y sistemas de atención, propios o de terceros, que permitan a los usuarios realizar el bloqueo de sus cuentas de dinero electrónico por, entre otros, el extravío, sustracción, robo, hurto o uso no autorizado del soporte entregado por el emisor para el uso de dinero electrónico, o de la información que contiene. Dicha infraestructura debe encontrarse disponible las veinticuatro (24) horas del día, todos los días del año.

Se deben registrar las comunicaciones de los usuarios, de tal forma que sea posible acreditar de manera fehaciente su fecha, hora y contenido. Por cada comunicación, se debe generar un código de registro a ser informado al usuario como constancia de la recepción de dicha comunicación. Asimismo, en caso el cliente lo solicite, se le debe enviar (a través de medios físicos o electrónicos) y/o poner a disposición, información sobre el registro de la comunicación efectuada, que por lo menos considere la fecha, hora, código de registro y motivo de la comunicación.

La información referida a los sistemas de atención establecidos por los emisores de dinero electrónico para dar cumplimiento a lo dispuesto en los párrafos precedentes, debe encontrarse publicada en la parte inicial de su página web, aun cuando se brinde el servicio de bloqueo a través de un enlace directo a otra página web establecida por el emisor, y en cualquier otro medio a criterio del emisor.

Lo expuesto en el presente artículo resulta aplicable, sin perjuicio de las demás exigencias establecidas por el marco normativo vigente en materia de atención de reclamos.

Artículo 14° - E.- Traslado de costos por la contratación de seguros y/o creación de mecanismos de protección o contingencia

El usuario no es responsable de ninguna pérdida en casos de operaciones no reconocidas que sean consecuencia de: i) clonación del soporte entregado por el emisor para el uso del dinero electrónico, ii) cuando las operaciones hayan sido realizadas luego de que el emisor fuera notificado del bloqueo de la cuenta de dinero electrónico, iii) suplantación del usuario en las oficinas de los emisores de dinero electrónico, o iv) funcionamiento defectuoso de los canales o sistemas puestos a su disposición por el emisor para efectuar operaciones; salvo que el emisor demuestre la responsabilidad del usuario.

Los emisores de dinero electrónico no pueden trasladar un gasto o comisión dirigido a cubrir el costo asociado a la contratación de pólizas de seguro y/o mecanismos de protección o contingencia, que tengan por objeto cubrir las pérdidas generadas como consecuencia de la realización de operaciones no reconocidas, de conformidad con lo señalado en el párrafo precedente.

TÍTULO IV
DE LAS GARANTIAS

Artículo 15.- Constitución de los fideicomisos
Los emisores de dinero electrónico, en calidad de fideicomitentes, deben constituir en empresas autorizadas para actuar como fiduciarios según la legislación vigente sobre la materia, diferentes del emisor de dinero electrónico, fideicomisos por el cien por ciento (100%) del dinero electrónico en circulación emitido bajo su responsabilidad, constituyendo patrimonios fideicometidos cuya finalidad exclusiva sea respaldar a los tenedores de cuentas de dinero electrónico.

Asimismo, en el acto constitutivo de los fideicomisos, se deberá designar a un fiduciario sustituto y el procedimiento de sustitución en caso de quiebra o cuando opere otra causal de remoción de este.

Artículo 16.- Valor de los patrimonios fideicometidos
Los emisores de dinero electrónico son responsables de establecer con los fiduciarios, los mecanismos que resulten necesarios para que el valor del patrimonio fideicometido sea superior o equivalente, en todo momento o por lo menos al final de cada día, al valor del dinero electrónico en circulación emitido bajo su responsabilidad.

Artículo 17.- Fondos de los patrimonios fideicometidos
Los fondos de los patrimonios fideicometidos constituidos por los emisores de dinero electrónico, solo podrán ser invertidos por el fiduciario, de la siguiente forma:

a) Depósitos de disposición inmediata que generen intereses, en empresas de operaciones múltiples clasificadas en categoría "A+", de acuerdo con lo establecido en el Reglamento para la Clasificación de Empresas del Sistema Financiero y de Empresas del Sistema de Seguros, aprobado por la Resolución SBS N° 18400-2010. La Superintendencia podrá requerir la diversificación de los referidos depósitos en más de una empresa.
b) Hasta un máximo del treinta (30%) de los recursos recibidos en bonos del Tesoro o instrumentos emitidos por el Banco Central de Reserva del Perú.
c) Otros activos líquidos que autorice la Superintendencia.

En caso el valor del patrimonio fideicometido sea menor al valor del dinero electrónico en circulación, dicha diferencia deberá ser cubierta con activos líquidos de propiedad del emisor de dinero electrónico. Los rendimientos del patrimonio fideicometido no serán de libre disponibilidad para el fideicomitente, pasando a formar parte de dicho patrimonio fideicometido.

Las inversiones a que se refieren los literales b) y c) deberán valorizarse al valor razonable de acuerdo con las normas emitidas por la Superintendencia.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

DISPOSICIONES FINALES Y COMPLEMENTARIAS

Primera.- Esta Superintendencia podrá considerar como dinero electrónico a aquellos servicios brindados por empresas supervisadas por ella, que presenten características similares a las establecidas en el artículo 2° de la Ley.

Segunda.- Las empresas de operaciones múltiples autorizadas a emitir dinero electrónico, no deberán considerar los activos ni los pasivos correspondientes al dinero electrónico en circulación, para la elaboración de los Anexos N° 15-A "Reporte de tesorería y posición diaria de liquidez", N° 15-B "Ratio de cobertura de liquidez" y N° 15-C "Posición mensual de liquidez" del Manual de Contabilidad contemplados en el Reglamento para la Gestión del Riesgo de Liquidez aprobado por la Resolución SBS N° 9075-2012 y sus normas modificatorias.

Asimismo, solo deberán considerar para la elaboración de los Anexos N° 16-A "Cuadro de Liquidez por Plazos de Vencimiento" y N° 16-B "Simulación de Escenarios de Estrés y Plan de Contingencia", los pasivos netos correspondientes al dinero electrónico en circulación.

Tercera.- Para la elaboración de los Anexos 7-A "Medición del Riesgo de Tasa de Interés – Ganancias en Riesgo" y 7-B "Medición del Riesgo de Tasa de Interés – Valor Patrimonial en Riesgo", las empresas de operaciones múltiples autorizadas a emitir dinero electrónico no deberán considerar los activos ni los pasivos correspondientes al dinero electrónico en circulación.

Cuarta[2].- Las cuentas operativas de dinero electrónico que mantienen los agregadores de operadores de cajeros corresponsales y/o los operadores de cajeros corresponsales con los emisores de dinero electrónico no se encuentran sujetas a las disposiciones contempladas en el Título III, "Aspectos aplicables en materia de transparencia de información, contratación y servicios de atención al usuario". A dichas cuentas les resulta aplicable la tercera disposición final y complementaria del Reglamento de Transparencia, en lo que corresponda.

DISPOSICIÓN TRANSITORIA

Las empresas supervisadas que al momento de la entrada en vigencia de la presente norma, brinden servicios que se consideren dinero electrónico, los deberán identificar y ponerlos en conocimiento de esta Superintendencia, dentro de los quince 15 días calendario de la entrada en vigencia de la presente norma, para los fines pertinentes."

Artículo Segundo.- Los servicios financieros a los que se refieren la Segunda Disposición Complementaria Final de la Ley N° 29985 y el artículo 12° del Reglamento de la Ley Nº 29985 que Regula las Características Básicas del Dinero Electrónico, aprobado por Decreto Supremo N° 090-2013-EF, consideran a los productos y servicios brindados a los usuarios que impliquen el uso de servicios de telecomunicaciones, en especial a los servicios que usan el teléfono móvil como soporte.

Artículo Tercero.- Modificar el Manual de Contabilidad para las Empresas del Sistema Financiero, conforme al Anexo adjunto a la presente resolución, el cual se publica en el Portal Institucional (www.sbs.gob.pe), según lo dispuesto en el Decreto Supremo N° 001-2009-JUS.

[2] Disposición incorporada por la Resolución SBS N°4628 de 13/08/2015

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Artículo Cuarto.- La presente Resolución entra en vigencia al día siguiente de su publicación en el diario oficial El Peruano, salvo lo dispuesto en el artículo tercero que entrará en vigencia para la información correspondiente al mes de enero de 2014.

Las empresas que al momento de la entrada en vigencia del Reglamento de las Operaciones con Dinero Electrónico brinden servicios que se consideren dinero electrónico, tendrán sesenta (60) días calendario para adecuarse a lo establecido en el Reglamento antes mencionado.

Regístrese, comuníquese y publíquese.

JAVIER POGGI CAMPODÓNICO
Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones (a.i.)

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

ANEXO

MODIFICACIONES AL MANUAL DE CONTABILIDAD PARA LAS EMPRESAS DEL SISTEMA FINANCIERO

I. Modifíquese el Capítulo V "Información Complementaria" del Manual de Contabilidad para las Empresas del Sistema Financiero, en los siguientes términos:

1. Incorpórense los Reportes N° 32-A "Reporte Diario de Dinero Electrónico" y N° 32-B "Reporte Mensual de Dinero Electrónico", de acuerdo con los formatos que se adjuntan a continuación:

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Reporte N° 32-A

REPORTE DIARIO DE DINERO ELECTRÓNICO

Fecha: Día / Mes / Año

TOTAL DINERO ELECTRÓNICO EN CIRCULACIÓN Y VALOR DEL PATRIMONIO FIDEICOMETIDO[1/]

	Total dinero electrónico en circulación (en S/.)	Valor del Patrimonio Fideicometido (en S/.)
Fin del día		

NOTA DEL REPORTE N° 32-A:
1/ Para efectos de la reexpresión de moneda extranjera a moneda nacional se utilizará el tipo de cambio contable del día a que corresponde el reporte.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Reporte N° 32-B

REPORTE MENSUAL DE DINERO ELECTRÓNICO

En el mes de .....de .....

I. OPERACIONES CON DINERO ELECTRÓNICO

Operaciones / Tipo de cuenta	Conversiones		Transferencias y Pagos		Reconversiones		Otras	
	Monto	Número de operaciones	Monto	Número de operaciones	Monto	Número de operaciones	Monto	Número de operaciones
Moneda Nacional (en S/.)								
Cuentas simplificadas								
Cuentas generales								
Total MN								
Moneda Extranjera (en $)								
Cuentas generales								
Total (en S/.)[1/]								
Cuentas simplificadas								
Cuentas generales								
Total								

II. DINERO ELECTRÓNICO EN CIRCULACIÓN

	Moneda nacional (en S/.)	Moneda extranjera (en $)	Total (en S/.)[1/]
Dinero electrónico en circulación correspondiente a cuentas simplificadas al inicio del mes[2/]			
Dinero electrónico en circulación correspondiente a cuentas generales al inicio del mes[2/]			
Dinero electrónico en circulación correspondiente a cuentas simplificadas a fin de mes[3/]			
Dinero electrónico en circulación correspondiente a cuentas generales a fin de mes[3/]			

Los Laureles Nº 214 - Lima 27 - Perú Telf. : (511)6309000 Fax: (511) 6309239

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

III. NUMERO DE CUENTAS Y TITULARES DE CUENTAS DE DINERO ELECTRONICO

	Cuentas Simplificadas		Cuentas Generales	
	Número de Cuentas	Número de titulares[3/]	Número de Cuentas	Número de titulares[3/]
Cuentas Vigentes al inicio de mes[2/]				
Cuentas Abiertas durante el mes				
Cuentas Cerradas durante el mes				
Cuentas Vigentes a fin de mes[2/]				

IV. TOTAL DINERO ELECTRÓNICO EN CIRCULACIÓN Y VALOR DEL PATRIMONIO FIDEICOMETIDO[1/]

	Total dinero electrónico en circulación (en S/.)	Valor del Patrimonio Fideicometido (en S/.)
Inicio del mes[2/]		
Fin de mes[2/]		

NOTAS DEL REPORTE N°32-B:
1/ Para efectos de la reexpresión de moneda extranjera a moneda nacional se utilizará el tipo de cambio contable del último día hábil del mes de reporte.
2/ Considerar el primer o último día hábil del mes, según corresponda.
3/ En caso un mismo titular tenga más de una cuenta de dinero electrónico en la entidad, considerarlo una sola vez.

ANEXO N° 4

Resolución SBS Nº 6284-2013

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Lima, 18 de octubre de 2013

Resolución S.B.S.
N° 6284-2013

El Superintendente de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que, el artículo 345° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley N° 26702 y sus normas modificatorias, en adelante Ley General, establece que la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, en adelante la Superintendencia, ejerce en el ámbito de sus atribuciones, el control y la supervisión de las empresas conformantes del Sistema Financiero y del Sistema de Seguros y de las demás personas naturales o jurídicas incorporadas por esta ley o por leyes especiales, de manera exclusiva en los aspectos que le corresponda;

Que, mediante la Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera, Ley N° 29985, se incorporó como empresas reguladas y supervisadas por esta Superintendencia a las Empresas Emisoras de Dinero Electrónico (EEDE), incluyéndolas en el numeral 6 del artículo 17° de la Ley General;

Que, la Primera Disposición Complementaria Final de la Ley que Regula las Características Básicas del Dinero Electrónico como Instrumento de Inclusión Financiera establece que la Superintendencia emitirá las normas que sean necesarias sobre ingreso y salida al mercado, operaciones, límites, garantías o respaldo del dinero electrónico en circulación, régimen de inversiones, uso de fideicomisos, sanciones y demás aspectos necesarios para el adecuado y seguro funcionamiento de las EEDE, así como para su supervisión;

Que, mediante Decreto Supremo N° 090-2013-EF, se aprobó el Reglamento de la Ley N° 29985, Ley que Regula las Características Básicas del Dinero Electrónico como Instrumento de Inclusión Financiera, estableciéndose disposiciones adicionales referidas a la emisión de dinero electrónico;

Que, es necesario emitir la normativa correspondiente con el fin de reglamentar los principales aspectos de las EEDE, tales como objeto social, autorización de organización y funcionamiento, operaciones permitidas, medidas prudenciales aplicables, entre otros;

Que, mediante Resoluciones SBS N° 11699-2008 y N° 17026-2010 y sus normas modificatorias, se aprobaron el Reglamento de Auditoría Interna y el Reglamento de Auditoría Externa, respectivamente, aplicable a las empresas señaladas en los artículos 16° y 17° de la Ley General y administradoras privadas de fondos de pensiones;

Los Laureles Nº 214 - Lima 27 - Perú Telf.: (511) 6309000 Fax: (511) 6309239

Que, mediante la Resolución SBS Nº 895-98 y sus normas modificatorias y complementarias, se aprobó el Manual de Contabilidad para las Empresas del Sistema Financiero, el cual contiene disposiciones referentes a la información complementaria que deberá remitirse a esta Superintendencia;

Que, corresponde a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, conforme a la autonomía funcional que le confiere el artículo 346° de la Ley General y al artículo 38° de la Ley Nº 27444, aprobar las modificaciones del Texto Único de Procedimientos Administrativos – TUPA institucional;

Que, a efectos de recoger las opiniones del público en general respecto a la propuesta de normativa, se dispuso la prepublicación del proyecto de resolución sobre la materia en el portal electrónico de la Superintendencia, al amparo de lo dispuesto en el Decreto Supremo Nº 001-2009-JUS;

Contando con el visto bueno de las Superintendencias Adjuntas de Banca y Microfinanzas, Riesgos, Estudios Económicos y Asesoría Jurídica, así como de la Gerencia de Productos y Servicios al Usuario; y,

En uso de las atribuciones conferidas por los numerales 7, 9 y 13 del artículo 349º de la Ley General, así como las facultades otorgadas en la Ley Nº 29985 y su reglamento aprobado por Decreto Supremo N° 090-2013-EF;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento de las Empresas Emisoras de Dinero Electrónico, en los siguientes términos:

"REGLAMENTO DE LAS EMPRESAS EMISORAS DE DINERO ELECTRÓNICO

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1.- Alcance
Las disposiciones del presente Reglamento son aplicables a las Empresas Emisoras de Dinero Electrónico (EEDE) a que hace referencia el numeral 6 del artículo 17° de la Ley General, así como a las empresas que se consideren dentro del ámbito de la Ley N° 29985, a criterio de la Superintendencia, en aplicación de la Quinta Disposición Complementaria Final de dicha Ley.

Artículo 2.- Definiciones
Para la aplicación del presente Reglamento deberán considerarse las siguientes definiciones:

a) Cajero corresponsal: de acuerdo con lo definido en el Reglamento de Apertura, Conversión, Traslado o Cierre de Oficinas, Uso de Locales Compartidos, Cajeros Automáticos y Cajeros Corresponsales, aprobado por la Resolución SBS N° 6285-2013.

b) Dinero electrónico: es un valor monetario representado por un crédito exigible a su emisor, el cual cumple con las características establecidas en la Ley y en el Reglamento de la Ley.
c) Emisión de dinero electrónico: comprende las operaciones de conversión a dinero electrónico, reconversión, transferencias, pagos y cualquier movimiento u operación relacionada con el valor monetario del que disponga el titular y necesaria para dichas operaciones.
d) Ley: Ley que Regula las Características Básicas del Dinero Electrónico como Instrumento de Inclusión Financiera, Ley N° 29985.
e) Ley General: Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley N° 26702 y sus normas modificatorias.
f) Manual de Contabilidad: Manual de Contabilidad para las Empresas del Sistema Financiero aprobado por la Resolución SBS N° 895-98 y sus normas modificatorias y complementarias.
g) Reglamento de la Ley: Reglamento de la Ley Nº 29985 que Regula las Características Básicas del Dinero Electrónico como Instrumento de Inclusión Financiera, aprobado por Decreto Supremo N° 090-2013-EF.
h) Reglamento de Operaciones con Dinero Electrónico: Reglamento de Operaciones con Dinero Electrónico, aprobado por la Resolución SBS N° 6283-2013.
i) Superintendencia: Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

CAPÍTULO II
DE LAS EMPRESAS EMISORAS DE DINERO ELECTRÓNICO

Artículo 3.- Objeto social
Las EEDE son empresas de servicios complementarios y conexos del sistema financiero constituidas como sociedades anónimas en concordancia con lo establecido en el artículo 12° de la Ley General. Los accionistas de las EEDE podrán ser personas naturales o jurídicas.

Las EEDE tienen como objeto principal la emisión de dinero electrónico, no conceden crédito con cargo a los fondos recibidos y solo pueden realizar otras operaciones relacionadas a su objeto principal, de acuerdo con lo establecido en el artículo 5° de este Reglamento.

Artículo 4.- Constitución, funcionamiento y capital mínimo
Para su constitución y funcionamiento, las EEDE deberán cumplir, en lo aplicable conforme a su naturaleza y objeto social, con lo dispuesto en el Reglamento para la Constitución, Reorganización y Establecimiento de Empresas y Representantes de los Sistemas Financiero y de Seguros, aprobado por la Resolución SBS N° 10440-2008. Además, deberán cumplir con lo señalado en los artículos 17° y 18° de la Ley General respecto al capital mínimo con el que deben contar.

Artículo 5.- Operaciones permitidas
Las EEDE podrán realizar, con sus propios recursos, las operaciones establecidas en los numerales 11, 17, 18, 19, 20, 21, 22, 23, 28, 29 y 42 del artículo 221° de la Ley General.

Además, las EEDE podrán realizar otras operaciones relacionadas con su objeto principal señaladas en el artículo 221° de la Ley General, para lo cual deberán contar con autorización previa de la Superintendencia. Para tal efecto, será de aplicación lo establecido en el Reglamento para la Ampliación de Operaciones, aprobado por la Resolución SBS N° 11698-2008.

Para efectos de realizar operaciones de emisión de dinero electrónico, las EEDE deberán cumplir los lineamientos y disposiciones establecidos en la Ley, el Reglamento de la Ley y el Reglamento de Operaciones con Dinero Electrónico.

Artículo 6.- Órganos de gobierno
Las EEDE deberán cumplir con las normas vigentes emitidas por la Superintendencia que resulten aplicables a la junta general de accionistas, al directorio, a los gerentes y a los principales funcionarios.

Artículo 7.- Clasificación de riesgo
Las EEDE no se encuentran obligadas a contar con una clasificación de riesgo; sin perjuicio de ello, pueden someterse a la clasificación de una empresa clasificadora de riesgo en caso lo consideren conveniente. Cuando ello ocurra, deben cumplir con lo dispuesto en las normas emitidas por la Superintendencia sobre clasificación de riesgo.

CAPÍTULO III
DE LAS MEDIDAS PRUDENCIALES

Artículo 8.- Límites a las operaciones de emisión de dinero electrónico
Las EEDE se encuentran sujetas a los límites de emisión de dinero electrónico por transacción y otros, a que se refieren la Ley, el Reglamento de la Ley y el Reglamento de Operaciones con Dinero Electrónico.

Artículo 9.- Patrimonio efectivo y requerimiento de patrimonio efectivo
Son aplicables a las EEDE, en lo que corresponda a las operaciones que se encuentran autorizadas a realizar, las disposiciones emitidas por la Superintendencia sobre cómputo del patrimonio efectivo.

Las EEDE deberán contar en todo momento, con un patrimonio efectivo no menor al dos por ciento (2%) del total del dinero electrónico en circulación.

Si el monto del patrimonio efectivo fuese menor al dos por ciento (2%) del total del dinero electrónico en circulación, el Gerente General, bajo responsabilidad, comunicará dicha situación al Directorio, órgano que convocará a la Junta General de Accionistas, a fin de que se adopten las medidas correctivas pertinentes. Este hecho deberá ser informado a la Superintendencia dentro de los dos (2) días útiles posteriores a la fecha en que ocurra. Asimismo, en un plazo no mayor de quince (15) días calendario posteriores a la fecha de ocurrencia deberá presentar a la Superintendencia un plan de adecuación aprobado por el Directorio.

En tanto subsista la deficiencia de patrimonio efectivo antes señalada, la EEDE quedará impedida de repartir dividendos o efectuar alguna otra forma de distribución de utilidades.

Artículo 10.- Tratamiento de las inversiones
Las EEDE deben sujetarse, según corresponda, a lo dispuesto en el Reglamento de Clasificación y Valorización de las Inversiones de las Empresas del Sistema Financiero aprobado por la Resolución SBS N° 7033-2012, en las Normas para la Inversión en Instrumentos Negociados a Través de Mecanismos No Centralizados de Negociación aprobadas mediante la Resolución SBS N° 964-2002 y sus normas modificatorias, y en el Reglamento de las Operaciones de Reporte y los Pactos de Recompra aprobado mediante la Resolución SBS N° 1067-2005.

Estas inversiones son las que se efectúan con los recursos propios de las EEDE, las cuales son diferentes de las que se efectúan con los recursos destinados a la constitución de las garantías a que se refiere el numeral 6.1 del artículo 6° de la Ley.

Artículo 11.- Tratamiento de los fideicomisos
Son aplicables a las EEDE, en su calidad de fideicomitentes, las normas sobre fideicomiso emitidas por la Superintendencia, así como lo dispuesto en el Reglamento de Operaciones con Dinero Electrónico.

Artículo 12.- Gestión de riesgos
Las EEDE deberán implementar una oportuna gestión de los riesgos que afrontan en la realización de sus operaciones, para ello deberán sujetarse a los lineamientos establecidos en el Reglamento de la Gestión Integral de Riesgos aprobado por la Resolución SBS N° 37-2008 y sus normas modificatorias, en el Reglamento para la Gestión del Riesgo Operacional aprobado por la Resolución SBS N° 2116-2009, y otras normas que resulten aplicables, en función a las operaciones que las EEDE se encuentran autorizadas a realizar.

CAPÍTULO IV
DE LA INFORMACIÓN A PRESENTAR A LA SUPERINTENDENCIA

Artículo 13.- Registro contable
Las EEDE deben registrar sus operaciones y elaborar su información financiera de acuerdo con lo dispuesto en el Manual de Contabilidad y otras normas contables emitidas por la Superintendencia.

Artículo 14.- Presentación de información
Las EEDE deben presentar a la Superintendencia la siguiente información contemplada en el Manual de Contabilidad, en lo que corresponda a las operaciones que se encuentran autorizadas a realizar, de acuerdo con la periodicidad y plazos consignados en la Circular N° B-2108-2002, F-0447-2002, CM-0294-2002, EAF-0206-2002, CR-0163-2002, EDPYME-0092-2002, FOGAPI-0011-2002, ESF-001-2002 y sus actualizaciones:

Forma A - Estado de Situación Financiera.
Forma B-1 - Estado de Resultados.
Forma B-2 – Estado de Resultados y Otro Resultado Integral.
Forma C – Estado de Flujos de Efectivo.
Forma D – Estado de Cambios en el Patrimonio.
Forma F – Balance de Comprobación de Saldos.
Reporte 1 - Transferencias de Acciones
Reporte 3 – Patrimonio Efectivo.

Reporte 32-B - Reporte Mensual de Dinero Electrónico.

Las Formas, los Anexos y los Reportes antes señalados deben ser remitidos a la Superintendencia vía SUCAVE y/o vía impresa, en los casos que así lo señale la Circular N° B-2108-2002, F-0447-2002, CM-0294-2002, EAF-0206-2002, CR-0163-2002, EDPYME-0092-2002, FOGAPI-0011-2002, ESF-001-2002 y sus actualizaciones, y teniendo en cuenta lo dispuesto la Resolución SBS N° 1270-2007.

La Superintendencia podrá requerir, mediante Oficio, información adicional a la anteriormente señalada, en caso lo considere conveniente para efectos de su labor de supervisión y control.

DISPOSICIONES FINALES Y COMPLEMENTARIAS

Primera.- Otra normativa aplicable
Las disposiciones contenidas en la Ley General referidas a las empresas del sistema financiero son de aplicación a las EEDE, en lo que resulte pertinente teniendo en cuenta las operaciones que se encuentran autorizadas a realizar.

Las EEDE se encuentran sujetas, en lo que resulte pertinente teniendo en cuenta las operaciones que se encuentran autorizadas a realizar, a toda norma o disposición emitida por la Superintendencia que haga referencia en su alcance o que resulte aplicable, de manera conjunta, a las empresas del sistema financiero:

- Reglamento de operaciones con dinero electrónico, aprobado por la Resolución SBS N° 6283-2013,
- Reglamento de Transparencia de Información y Contratación con Usuarios del Sistema Financiero aprobado por la Resolución SBS N° 8181-2012 y sus normas modificatorias,
- Reglamento de Sanciones aprobado por la Resolución SBS N° 816-2005 y sus normas modificatorias,
- Normas Complementarias para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo aprobadas por la Resolución SBS N° 838-2008 y sus normas modificatorias,
- Normas Especiales sobre Vinculación y Grupo Económico aprobadas por la Resolución SBS N° 445-2000 y sus normas modificatorias,
- Reglamento de Apertura, Conversión, Traslado o Cierre de Oficinas, Uso de Locales Compartidos, Cajeros Automáticos y Cajeros Corresponsales aprobado por la Resolución SBS N° 6285-2013,
- Reglamento de Auditoría Interna aprobado por la Resolución SBS N° 11699-2008 y sus normas modificatorias,
- Reglamento de Auditoría Externa aprobado por la Resolución SBS N° 17026-2010,
- Reglamento de los Regímenes Especiales y de la Liquidación de las Empresas del Sistema Financiero y del Sistema de Seguros aprobado por la Resolución SBS N° 455-99 y sus normas modificatorias,
- Disposiciones relativas al servicio de atención a los usuarios por parte de las entidades supervisadas - Circular SBS N° G-146-2009,
- Gestión de la Continuidad del Negocio – Circular SBS N° G-139-2009,
- Gestión de la Seguridad de la Información – Circular SBS N° G-140-2009.

- La Circular N° B-2197-2011, F-537-2011, CM-385-2011, CR-253-2011, EF-6-2011, EAH-12-2011, EAF-247-2011, EDPYME-140-2011 sobre aplicación de normas prudenciales conforme el artículo 85° del Código de Protección y Defensa del Consumidor.[2]

La Superintendencia podrá determinar la aplicación a las EEDE de otras normas y disposiciones emitidas por ella.

Segunda.- Procedimiento de Adecuación
Las empresas que al momento de entrada en vigencia del presente Reglamento se encuentren incursas en la definición de EEDE establecida en esta norma, deberán presentar una solicitud de autorización de adecuación para poder continuar operando, dentro de los sesenta (60) días calendarios posteriores a la entrada en la vigencia del presente reglamento, adjuntando la información que se señala en el siguiente procedimiento de adecuación:

1) Presentación de Documentos
   a) Acreditar el capital mínimo conforme a lo establecido en los artículos 17º y 18º de la Ley General.
   b) Estados Financieros de los últimos dos (2) años y del trimestre anterior al de la fecha de solicitud de adecuación.
   c) Informe en el que describa su modelo y estrategia de negocios, así como su modelo operativo.
   d) Modificaciones que se consideren necesarias en el estatuto de la empresa, para adecuarlo a las disposiciones aplicables de la Ley General, la Ley, el Reglamento de la Ley, el Reglamento de Operaciones con Dinero Electrónico y el presente Reglamento.
   e) Últimas modificaciones a la escritura pública de constitución social.
   f) Señalar quiénes son los accionistas y su participación en la propiedad de la empresa. En el caso que el accionista sea una persona jurídica deberá presentarse, además, la escritura pública de constitución social de la persona jurídica accionista, así como señalar a sus beneficiarios finales. En el caso que el accionista sea un ente jurídico, indicar sus beneficiarios finales, así como adjuntar información financiera relevante.
   g) Declaración jurada de los accionistas de no estar incursos en los impedimentos señalados en los artículos 52º y 54° de la Ley General.
   h) Declaración jurada de no tener antecedentes penales ni policiales en el país para los accionistas residentes, y en el país de domicilio para los accionistas no residentes.
   i) Currículum Vitae y Declaración Jurada de los Directores y principales funcionarios de no encontrarse incursos en los impedimentos señalados en el artículo 81º de la Ley General.
   j) Relación de personas naturales, jurídicas o entes jurídicos con las que los accionistas se encuentran vinculados, y con las que conforma un grupo económico de acuerdo con la reglamentación de la Superintendencia vigente sobre la materia. Dicha relación deberá incluir la estructura de propiedad y de gestión del grupo económico.
   k) Declaración jurada de no registrar protestos en los últimos cinco (5) años, tanto de los accionistas como de la empresa en adecuación, en ninguna Cámara de Comercio del país, o en la entidad del extranjero que corresponda.
   l) Estructura orgánica actualizada de la empresa, con detalle del personal y oficinas en funcionamiento al momento de la solicitud de adecuación.

[2] Incorporado por la Resolución SBS N° 4628-2015 del 13 de agosto de 2015.

m) Relación de empresas con las cuales haya suscrito contratos relacionados con sus operaciones con dinero electrónico, y según corresponda, de las autorizaciones de los organismos competentes.
n) Manuales de Organización y Funciones y de Procedimientos, especialmente los referidos a las operaciones con dinero electrónico, los cuales deberán estar aprobados por el Directorio.
o) Demostrar la existencia de la infraestructura adecuada para realizar las operaciones con dinero electrónico, en especial manuales, procedimientos, formatos, entre otros, así como para el cumplimiento con la regulación vigente relativa a la prevención del lavado de activos y financiamiento del terrorismo, que les es aplicable conforme lo señalado en el numeral 4.2 del artículo 4° de la Ley.
p) Informe que contenga el plan de adecuación a la normativa señalada en la Primera Disposición Final y Complementaria de este Reglamento.
q) Señalar las políticas y procedimientos implementados de seguridad de la información y de continuidad de negocios para los procesos, productos y servicios críticos, de acuerdo con la normativa vigente.
r) Informar si se han implementado los sistemas informáticos y/o medios de comunicación necesarios para el proceso de consolidación y validación de la información financiera consolidada, tanto contable como no contable, requerida por esta Superintendencia.
s) Describir las medidas de seguridad física y ambiental implementadas en sus oficinas.
t) Describir las características principales de su plataforma tecnológica y la arquitectura de los sistemas informáticos empleados.

En esta etapa del procedimiento, la Superintendencia podrá solicitar las rectificaciones y/o subsanaciones de aquellos documentos e informaciones que considere incompletos o inadecuados, así como requerir información adicional cuando lo estime pertinente.

2) Publicación

La Superintendencia, después de verificar la presentación completa y adecuada de la información requerida en el numeral anterior, mediante las comprobaciones que resulten pertinentes, dispone que la empresa en adecuación publique por dos (2) veces alternadas, la primera en el Diario Oficial y la segunda en uno de extensa circulación nacional, un aviso haciendo saber al público sobre el proceso de adecuación, así como los nombres de los accionistas, citando a toda persona interesada para que, en el término de quince (15) días, contado a partir de la fecha del último aviso, formule cualquier objeción fundamentada a la adecuación de la empresa o a los accionistas que la conforman.

3) Autorización de Adecuación

Vencidos los plazos de las publicaciones referidas en el numeral anterior, sin que se produzcan objeciones fundamentadas y válidas, la Superintendencia expide la correspondiente resolución autoritativa de adecuación, la que debe exhibirse permanentemente en las diferentes oficinas de la EEDE, en lugar visible al público. La referida resolución autoritativa de adecuación es de vigencia indefinida y puede ser cancelada por la Superintendencia como sanción a una falta muy grave en que incurra la EEDE.

Las empresas a que se refiere la presente disposición final y complementaria, que no soliciten o no culminen satisfactoriamente el proceso de adecuación antes señalado, en los términos, condiciones y plazos señalados en el presente Reglamento, no podrán continuar ofreciendo al público los servicios de dinero electrónico.

El incumplimiento de lo señalado en el párrafo anterior, originará que la Superintendencia imponga las sanciones y/o realice las acciones que a su juicio correspondan, así como difunda al público respecto a la no presentación o culminación satisfactoria de la solicitud de adecuación.

Las empresas que hubieran iniciado el trámite de autorización de adecuación ante esta Superintendencia, deberán cumplir con las normas que se establecen en la Ley, el Reglamento de la Ley y el Reglamento de Operaciones con Dinero Electrónico, para cuyos efectos, la Superintendencia podrá otorgar plazos adicionales conforme el estado del procedimiento de autorización en curso."

Artículo Segundo.- Incorporar en el apartado III Informes aplicables a las empresas de servicios complementarios y conexos" del Anexo I "Informes complementarios a cargo de las sociedades de auditoría externa" del Reglamento de Auditoría Externa, aprobado por la Resolución SBS N° 17026-2010 y sus normas modificatorias, lo siguiente:

"Empresas Emisoras de Dinero Electrónico

1. *Revisión de temas específicos del giro del negocio, el informe deberá contener como mínimo lo siguiente:*
   - *-Las políticas y procedimientos para la realización de operaciones con dinero electrónico.*
   - *-Los grupos económicos, personas naturales, personas jurídicas y entes jurídicos vinculados según los criterios establecidos por la Superintendencia.*
   - *-Los procedimientos de registro, supervisión y centralización de las operaciones de los cajeros corresponsales.*
   - *-Cumplimiento de los límites establecidos en la normativa.*
   - *-Cumplimiento de las disposiciones respecto de los fondos recibidos: constitución de fideicomisos, funcionamiento, saldos y efectiva cobertura del fideicomiso, etc.*
   - *-Revisión de la gestión de riesgos.*
2. *Revisión de los controles existentes en la empresa, de la seguridad y de la confiabilidad de los sistemas informáticos que producen la información financiera, en el ámbito de la auditoría externa."*

Artículo Tercero.- Incorporar como numeral 8) del apartado III "Empresas de servicios complementarios y conexos" del Anexo "Actividades Programadas" del Reglamento de Auditoría Interna aprobado por la Resolución SBS N° 11699-2008 y sus normas modificatorias, lo siguiente:

"8) Adicionalmente, las Empresas Emisoras de Dinero Electrónico (EEDE) deberán incluir en el Plan de Trabajo las siguientes actividades:

- *Evaluación del cumplimiento de los límites y condiciones operativas establecidos por la Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera, Ley N° 29985; el Reglamento de la Ley Nº 29985 que regula las características básicas del dinero electrónico como instrumento de inclusión financiera, aprobado por el Decreto Supremo N° 090-2013-EF; y el Reglamento de Operaciones con Dinero Electrónico, aprobado por la Resolución SBS N° 6283-2013.*
- *Evaluación de las comisiones cobradas por operaciones, así como su registro contable.*
- *Evaluación del cumplimiento de los compromisos asumidos con los clientes, así como de la adecuada información y publicidad brindada a estos.*
- *Evaluación del cumplimiento de Acuerdos del Directorio.*
- *Evaluación del cumplimiento de las disposiciones respecto a los fondos recibidos: constitución de fideicomiso, funcionamiento, saldos y efectiva cobertura del fideicomiso, etc.*

- *Evaluación de la adecuada supervisión y centralización de operaciones de los cajeros corresponsales, en caso de contar con ellos."*

Artículo Cuarto.- Modificar el numeral 1 del literal B "Alcances" del Capítulo I "Disposiciones Generales" del Manual de Contabilidad, en los siguientes términos:

"1. Las entidades que deben aplicar el presente Manual son las empresas señaladas en los literales A y B del artículo 16° de la Ley General, el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo - COFIDE, el Fondo MIVIVIENDA S.A., las Empresas Emisoras de Dinero Electrónico, y en el caso de otras empresas cuando su aplicación sea requerida por la Superintendencia.

Asimismo, el Manual es aplicable a cada una de las sucursales del exterior de las empresas señaladas anteriormente."

Artículo Quinto.- Modificar la denominación del procedimiento número 01 del TUPA de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, aprobado mediante Resolución SBS N° 3082-2011 de fecha 11 de marzo de 2011, por la siguiente denominación: "Autorización para la Constitución de empresas referidas en el artículo 16º de la Ley Nº 26702: Empresas de Operaciones Múltiples, Empresas de Seguros, Bancos de Inversión, Empresas Especializadas, así como de Empresas Emisoras de Dinero Electrónico, en lo pertinente."

Artículo Sexto.- La presente Resolución entra en vigencia al día siguiente de su publicación en el diario oficial El Peruano.

Regístrese, comuníquese y publíquese,

JAVIER POGGI CAMPODÓNICO
Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones (a.i.)

ANEXO N° 5

Resolución SBS Nº 6285-2013

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

PREPUBLICACION

Lima,

Resolución S.B.S.
N° -2015

El Superintendente de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones:

CONSIDERANDO:

Que, mediante Resolución SBS N° 6285-2013 se aprobó el Reglamento de Apertura, conversión, traslado o cierre de oficinas, uso de locales compartidos, cajeros automáticos y cajeros corresponsales;

Que, esta Superintendencia ha considerado pertinente ampliar los tipos de canales complementarios de atención al público para lograr una mayor inclusión financiera, así como realizar otras precisiones en la norma antes señalada;

Que, a efectos de recoger las opiniones del público en general respecto de las propuestas de modificación a la normativa del sistema financiero, se dispuso la prepublicación del proyecto de resolución en el portal electrónico de la Superintendencia, al amparo de lo dispuesto en el Decreto Supremo Nº 001-2009-JUS;

Contando con el visto bueno de las Superintendencias Adjuntas de Banca y Microfinanzas, Seguros, de Riesgos, de Estudios Económicos y de Asesoría Jurídica, y;

En uso de las atribuciones conferidas por los numerales 7 y 9 del artículo 349° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros – Ley N° 26702 y sus normas modificatorias;

RESUELVE:

Artículo Primero.- Aprobar el nuevo Reglamento de Apertura, conversión, traslado o cierre de oficinas, uso de locales compartidos, cajeros automáticos, establecimientos de operaciones básicas y cajeros corresponsales, según se indica a continuación:

"REGLAMENTO DE APERTURA, CONVERSIÓN, TRASLADO O CIERRE DE OFICINAS, USO DE LOCALES COMPARTIDOS, CAJEROS AUTOMÁTICOS, ESTABLECIMIENTOS DE OPERACIONES BÁSICAS Y CAJEROS CORRESPONSALES

1. **Alcance**

La presente norma es de aplicación a las empresas de operaciones múltiples, empresas especializadas y empresas de seguros, señaladas en los literales A, B y D del artículo 16° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus normas modificatorias, en adelante Ley General, al Banco de la Nación, al Banco Agropecuario, a la Corporación Financiera de Desarrollo (COFIDE), al Fondo Mivivienda S.A., y a las Empresas Emisoras de Dinero Electrónico (EEDE), en adelante empresas, según corresponda.

CAPITULO I
OFICINAS

2. **Oficinas**

Son establecimientos físicos a través de los cuales la empresa atiende al público para realizar operaciones y servicios. Existen diversos tipos de oficinas:

2.1. Oficina principal

Es la oficina constituida como domicilio legal de la empresa, que puede realizar cualquiera de las operaciones y servicios permitidos a la empresa y donde generalmente se encuentra la alta dirección que organiza, administra y dirige las actividades y negocios que son propios del objeto social de la institución.

2.2. Agencia

Es la oficina que depende de la oficina principal, puede efectuar todas las operaciones y servicios permitidos a la empresa y puede llevar contabilidad propia. Asimismo, puede supervisar a otras agencias y oficinas especiales, caso en el que están autorizadas a centralizar la contabilidad de las oficinas a su cargo.

2.3. Sucursal

Es la oficina ubicada en el exterior, depende de la oficina principal y puede realizar todas las operaciones y servicios permitidos a la empresa. La sucursal lleva contabilidad propia.

2.4. Oficina especial

Es la oficina distinta a las oficinas descritas en los numerales precedentes, que depende de la oficina principal o de alguna agencia y que solo puede realizar algunas de las operaciones y servicios permitidos a la empresa. Pueden realizar operaciones adicionales a las permitidas a los establecimientos de operaciones básicas (EOB).

La oficina especial puede ser:

i) Fija o móvil.

ii) Permanente o Temporal. La oficina temporal no puede estar vigente por un período mayor a seis meses y usualmente está asociada a un evento específico.

2.5. Local Compartido

Es la modalidad de oficina en la que una Agencia u Oficina especial comparte espacio físico con otras empresas, para la prestación de las operaciones y servicios a que están facultadas. Esta modalidad de oficina incluye acuerdos que permiten compartir diferentes ventanillas de atención al público, así como de arrendamiento de espacios, entre otras formas. El proceso de autorización respectivo se detalla en el numeral 3.2 del presente reglamento.

3. Autorización para apertura, conversión, traslado o cierre de oficinas

3.1. Oficina principal, agencias y oficinas especiales

3.1.1. Las empresas deberán solicitar, según corresponda, autorización previa para la apertura, conversión, traslado o cierre de sus oficinas, indicando su ubicación y dirección exacta y adjuntando copia del acuerdo del órgano social competente. En el caso de oficina especial móvil, en lugar de dirección exacta, se deberá señalar el ámbito geográfico en que desarrollará sus operaciones.

3.1.2. En los casos de apertura y conversión, la empresa deberá mantener a disposición de esta Superintendencia, el correspondiente estudio de factibilidad con el contenido mínimo señalado en el Anexo A del presente reglamento, para las acciones de supervisión que correspondan.

3.1.3. En los casos de traslado o cierre, el requisito para la autorización respectiva es solo lo indicado en el numeral 3.1.1 del presente reglamento.

3.2. Autorización para compartir locales

3.2.1. La empresa que acuerde la apertura de una agencia u oficina especial bajo la modalidad de local compartido, deberá presentar una solicitud de autorización previa a esta Superintendencia, indicando su ubicación y dirección exacta y adjuntando copia de los acuerdos de los órganos sociales de las empresas que deciden compartir locales.

3.2.2. La empresa deberá mantener a disposición de esta Superintendencia el estudio de factibilidad indicado en el numeral 3.1.2 del presente reglamento y el contrato suscrito por ambas partes indicando el período de vigencia, las operaciones y servicios que cada una de ellas brindará en el local a compartir; entre otros aspectos.

3.2.3. Para el caso de traslados o cierres, los correspondientes trámites de autorización deben ser realizados en forma independiente por cada empresa que comparte local.

3.2.4. Durante el uso de locales compartidos, las empresas deben cumplir las siguientes medidas: a) Indicar en la parte exterior del inmueble, los nombres completos, incluyendo los símbolos de las empresas que comparten el inmueble; y b) Identificar de manera adecuada la respectiva ubicación de los lugares asignados.

3.3. Sucursales

3.3.1. Las empresas del sistema financiero y de seguros deberán solicitar la autorización previa de esta Superintendencia para la apertura, traslado y cierre de sucursales, indicando su ubicación y dirección exacta y adjuntando copia del acuerdo del órgano social competente. Para el caso de apertura deberán adjuntar adicionalmente el estudio de factibilidad con el contenido mínimo señalado en el Anexo A, así como una declaración de cumplimiento de los requisitos establecidos para tal fin en la legislación del país anfitrión.

3.3.2. La Superintendencia recabará la opinión del Banco Central de Reserva antes de expedir su pronunciamiento sobre la apertura de una sucursal de una empresa del sistema financiero. El traslado o cierre de toda sucursal del sistema financiero será puesto en conocimiento del referido Banco Central.

CAPITULO II
CANALES COMPLEMENTARIOS

4. Cajeros Corresponsales

Son puntos de atención que funcionan en establecimientos fijos o móviles, pertenecientes a un operador.

Se considera operador de cajeros corresponsales a la persona natural o jurídica, diferente de las empresas que integran el sistema financiero y diferente de las EEDE, que opera los cajeros corresponsales.

Se considera agregador de operadores de cajeros corresponsales a la persona jurídica que realiza la afiliación y administración de operadores de cajeros corresponsales.

Las empresas del sistema financiero y las EEDE podrán suscribir contratos con los operadores o con los agregadores de operadores de cajeros corresponsales para prestar, en su representación y bajo su responsabilidad, las operaciones y servicios autorizados por la presente norma.

Las empresas del sistema financiero y las EEDE, son responsables del cumplimiento de los requisitos y condiciones aplicables a los operadores y a los agregadores de operadores de cajeros corresponsales, con quienes contratan, señalados en la presente norma.

Los operadores y agregadores de operadores de cajeros corresponsales podrán operar con varias empresas del sistema financiero y/o empresas emisoras de dinero electrónico.

Los operadores de cajeros corresponsales deberán mantener en los locales de los cajeros corresponsales paneles que de forma visible al público, muestren de forma clara su condición de operador de cajero corresponsal de las empresas del sistema financiero y/o empresas emisoras de dinero electrónico a las cuales representa, pudiendo diseñar paneles ad-hoc al servicio que ofrecen.

Operaciones de cajeros corresponsales

Mediante cajeros corresponsales la empresa del sistema financiero o la EEDE podrá realizar las siguientes operaciones, según corresponda a las operaciones que se encuentran autorizadas a realizar:

a) Cobranza de créditos.
b) Permitir el retiro de dinero.
c) Transferencias de fondos.
d) Depósitos en efectivo en cuentas del cliente o de terceros.
e) Apertura y cierre de cuentas básicas.
f) Pago de servicios y cobranzas en general.
g) Pago a entidades del Estado por orden de los usuarios.
h) Pago de remesas remitidas desde el exterior.
i) Apertura y cierre de cuentas de dinero electrónico simplificadas, con excepción de las correspondientes a menores de edad.
j) Operaciones con dinero electrónico, descritas en el Reglamento de Operaciones con Dinero Electrónico.
k) Venta de micro seguros.
l) Otros servicios, previa conformidad de esta Superintendencia, para lo cual deberán describir las características del servicio a brindar, y adjuntar el informe de evaluación de riesgos elaborado por la Unidad de Riesgos de la empresa del sistema financiero o EEDE.

Asimismo, en el marco del régimen general de debida diligencia en el conocimiento del cliente, y bajo responsabilidad de las empresas del sistema financiero, mediante cajeros corresponsales se podrán recibir solicitudes de personas naturales respecto a la apertura de cuentas de depósitos a la vista, a plazo y de ahorros, así como solicitudes de créditos personales, las cuales serán remitidas por el cajero corresponsal a la empresa del sistema financiero, conforme a los procedimientos acordados entre ambas partes.

Las empresas del sistema financiero podrán realizar publicidad y entregar información que facilite la apertura de otras cuentas de depósitos y/o concesión de créditos en forma posterior en las oficinas de la empresa. En el caso de las EEDE, podrán realizar publicidad y entregar información que facilite la apertura de cuentas de dinero electrónico generales en forma posterior en las oficinas de la EEDE.

Las operaciones que se realicen mediante cajeros corresponsales deberán ser aquellas que impliquen abonos y/o cargos automáticos en cuentas y/o líneas de crédito, según corresponda, sin que requieran conciliaciones o verificaciones distintas a aquellas que se realicen en terminales

electrónicos que estén interconectados con la empresa del sistema financiero o EEDE. En el caso de apertura de cuentas básicas o cuentas de dinero electrónico simplificadas, las empresas del sistema financiero o EEDE, según corresponda, podrán establecer mecanismos complementarios según sea requerido.

La Superintendencia podrá autorizar operaciones que sigan otro esquema operativo o utilicen otras modalidades de prestación de servicios, si considera que los controles a ser aplicados permiten administrar adecuadamente los riesgos asociados; caso en el que se proveerá información detallada acerca de la modalidad propuesta, y se adjuntará los informes preparados por la Unidad de Riesgos.

La empresa del sistema financiero y EEDE deberá establecer límites para la prestación de los servicios que se acuerden a través de los cajeros corresponsales, los que deberán ser prudentes y estar en relación con el movimiento de efectivo propio del operador. Dichos límites deberán ser establecidos por persona y por tipo de transacción, de ser el caso.

Las empresas del sistema financiero y EEDEs deberán mantener un registro actualizado de los operadores y agregadores de operadores de cajeros corresponsales, así como de los cajeros corresponsales con los que operan, incluyendo: datos de identificación del operador y del agregador (en caso corresponda), ubicación de los cajeros corresponsales, ámbito geográfico donde operan cuando sean móviles, operaciones permitidas, entre otros. Asimismo, deberán publicar en su página web, aquella información del citado registro, que permita a los usuarios, la identificación de los cajeros corresponsales autorizados para operar en su representación

5. Establecimientos de operaciones básicas (EOB)

Los establecimientos de operaciones básicas son puntos de atención que funcionan en establecimientos fijos o móviles, operados por la propia empresa del sistema financiero o EEDE, y solo pueden realizar las operaciones permitidas a los cajeros corresponsales.

Asimismo, en el marco del régimen general de debida diligencia en el conocimiento del cliente, mediante establecimientos de operaciones básicas se podrán recibir solicitudes de personas naturales respecto a la apertura de cuentas de depósitos a la vista, a plazo y de ahorros, así como solicitudes de créditos personales, las cuales serán remitidas a las oficinas de la empresa del sistema financiero.

Las empresas del sistema financiero podrán realizar en los EOB publicidad y entregar información que facilite la apertura de otras cuentas de depósitos y/o concesión de créditos en forma posterior en sus oficinas. En el caso de las EEDE, podrán realizar publicidad y entregar información que facilite la apertura de cuentas de dinero electrónico generales en forma posterior en las oficinas de la EEDE.

Las operaciones que se realicen mediante establecimientos de operaciones básicas deberán ser aquellas que impliquen abonos y/o cargos automáticos en cuentas y/o líneas de crédito, según corresponda, sin que requieran conciliaciones o verificaciones distintas a aquellas que se realicen en terminales electrónicos que estén interconectados con la empresa del sistema financiero o

EEDE. En el caso de apertura de cuentas básicas o cuentas de dinero electrónico simplificadas, las empresas podrán establecer mecanismos complementarios según sea requerido.

La Superintendencia podrá autorizar operaciones que sigan otro esquema operativo o utilicen otras modalidades de prestación de servicios, si considera que los controles a ser aplicados permiten administrar adecuadamente los riesgos asociados; caso en el que se proveerá información detallada acerca de la modalidad propuesta, y se adjuntará los informes preparados por la Unidad de Riesgos.

La empresa del sistema financiero y EEDE deberá establecer límites para la prestación de los servicios a través de los establecimientos de operaciones básicas, los que deberán ser prudentes y estar en relación con el movimiento de efectivo propio del tamaño de estos establecimientos. Dichos límites deberán ser establecidos por persona y por tipo de transacción, de ser el caso.

La empresa del sistema financiero y EEDE deberá contar con información del número y monto de transacciones realizadas, por tipo de servicio prestado a través de cada establecimiento de operaciones básicas, así como monitorear el efectivo cumplimiento de límites y otras medidas prudenciales establecidas según el caso.

La empresa del sistema financiero y EEDE deberá publicar en su página web, la relación de sus establecimientos de operaciones básicas, ubicación, ámbito geográfico donde operan cuando sean móviles y operaciones permitidas, con sus correspondientes límites.

6. Autorización de cajeros corresponsales y establecimientos de operaciones básicas.

6.1. Autorización para operar con Cajeros Corresponsales

6.1.1. Las empresas del sistema financiero y/o empresas emisoras de dinero electrónico podrán operar a través de los cajeros corresponsales a que se refiere el numeral 4 del presente reglamento, previa autorización expresa de la Superintendencia, siempre que se cumpla con las condiciones y requisitos que se indican en el Anexo D de este reglamento.

6.1.2. Las empresas del sistema financiero y EEDEs que deseen obtener autorización para operar con cajeros corresponsales, deben presentar una solicitud a esta Superintendencia, y adjuntar la información señalada en el Anexo C del presente reglamento. La autorización para operar con cajeros corresponsales se otorga una sola vez.

6.2. Autorización para operar con establecimientos de operaciones básicas.

6.2.1. Las empresas del sistema financiero y empresas emisoras de dinero electrónico podrán operar a través de establecimientos de operaciones básicas a que se refiere el numeral 5 del presente reglamento, previa autorización expresa de la Superintendencia.

6.2.2. Las empresas del sistema financiero y EEDEs que deseen obtener autorización para operar con establecimientos de operaciones básicas, deben presentar una solicitud a esta Superintendencia, y adjuntar la información señalada en el Anexo G del presente reglamento. La autorización para operar con establecimientos de operaciones básicas se otorga una sola vez.

7. Cajeros automáticos

Los cajeros automáticos son dispositivos electrónicos que están interconectados con la empresa del sistema financiero y que le permiten brindar diversas operaciones y servicios a los usuarios mediante la utilización de tarjetas de crédito, de débito u otros mecanismos de identificación que requieran el empleo de firmas electrónicas o similares, según el procedimiento establecido por la empresa del sistema financiero, debidamente comunicado al cliente y aceptado por este.

CAPITULO III
OTRAS DISPOSICIONES

8. Remisión de información

8.1. Las empresas deberán remitir a esta Superintendencia, a más tardar el 31 de marzo de cada año, la programación anual de apertura, conversión, traslado y cierre de oficinas y locales compartidos, con el contenido y formato que se establece en el Anexo E del presente reglamento.

La remisión física de la citada programación y su actualización podrá ser sustituida por su remisión y/o ingreso por aplicativos informáticos que establezca esta Superintendencia. Dicha programación y sus respectivas modificaciones deberán estar aprobadas por el órgano social correspondiente.

8.2. Dentro de los siete (7) días calendario de formalizada la apertura, traslado, conversión o cierre de las oficinas o utilización de locales compartidos, las empresas deberán reportar a esta Superintendencia el Anexo B "Movimiento de Oficinas" conforme los aplicativos informáticos que establezca esta Superintendencia.

8.3. Las empresas del sistema financiero y/o empresas emisoras de dinero electrónico, comunicarán periódicamente a esta Superintendencia el número de cajeros automáticos, cajeros corresponsales y establecimientos de operaciones básicas que mantienen, según corresponda, conforme los formatos electrónicos que para tal efecto se establezca.

8.4. Las empresas deberán remitir dentro de los primeros treinta (30) días calendario del mes de enero un inventario de las oficinas en funcionamiento con corte al cierre del ejercicio anterior de acuerdo con el formato del Anexo F del presente reglamento, según el formato electrónico o aplicativo establecido por esta Superintendencia.

En los casos de fusión por absorción o constitución de nueva entidad, la nueva sociedad o la absorbente deberá remitir dentro de los quince (15) días calendario de producida la

correspondiente autorización de la Superintendencia, la relación de oficinas que se mantienen en vigencia después de la fusión, debiendo remitirse en el mismo plazo, las solicitudes de autorización que se consideren necesarias.

9. Disposiciones Finales

9.1. El órgano social competente podrá delegar en la Gerencia General, o en un Comité de Gerencia, la capacidad de aprobar y solicitar autorización a esta Superintendencia para la apertura, traslado y cierre de oficinas especiales, en cuyo caso, la copia del acuerdo del órgano social competente indicado en el numeral 3.1.1 podrá ser reemplazada por la indicación en la solicitud a esta Superintendencia, de la fecha y órgano que tomó la decisión.

9.2. El traslado de las oficinas a que aluden los numerales 3.1 y 3.2 del presente reglamento, solo puede referirse al área de influencia geográfica y económica indicada en el Anexo A "Perfil de Factibilidad Económica" elaborado por la empresa para la apertura o conversión de la oficina a trasladar. Cuando el traslado de oficina deba realizarse fuera del área de influencia antes señalada, se considerará como cierre y apertura de oficina respectivamente.

9.3. No está sujeta a autorización previa ni constituye un tipo de oficina aquellas instalaciones que tienen la función exclusiva de prestar servicios de promoción e información sobre operaciones para las cuales se encuentra facultada la empresa y/o recabar documentación relacionada a estas, siendo la empresa responsable por la documentación recibida. En estas instalaciones no se puede realizar ningún tipo de operación. La Superintendencia podrá solicitar la relación, ubicación y características de estas instalaciones, mediante los formatos electrónicos que para el efecto se establezcan.

9.4. Para el caso de las autorizaciones a que se refieren los numerales 3.1. y 3.2 del presente reglamento, relativas a oficinas comprendidas en la programación anual y sus respectivas actualizaciones, las empresas clasificadas en la categoría de riesgo "A", y que hubieran tenido dicha clasificación durante los dos semestres anteriores, solo deberán comunicar previamente la ubicación y dirección exacta de las oficinas objeto de autorización, así como el área de influencia geográfica y económica de la oficina en los casos de apertura, traslado y conversión, debiendo mantener a disposición de esta Superintendencia, toda la documentación señalada en los referidos numerales. Las correspondientes resoluciones autoritativas serán emitidas en un plazo no mayor de cinco (5) días útiles de recibida la referida comunicación.

9.5. Para el caso de empresas del sistema financiero o EEDEs autorizadas para abrir establecimientos de operaciones básicas y cajeros corresponsales, en el caso que se produzca un incremento significativo en los límites de prestación de servicios informados a esta Superintendencia, este debe ser considerado un cambio importante en el ambiente operativo y, en consecuencia, debe realizarse una evaluación de riesgos conforme lo establecido en la Circular Nº G-165-2012, relativa al "Informe de riesgos por nuevos productos o cambios importantes en el ambiente de negocios, operativo o informático" y ser

informado a esta Superintendencia. Se considera "incremento importante" todo incremento mayor al 100% del límite informado a la SBS.

9.6. Cuando transcurra más de un (1) año calendario, contado a partir de la fecha de la correspondiente resolución autoritativa, sin que se implemente la autorización y se remita el correspondiente Anexo B "Movimiento de Oficinas", dicha autorización quedará sin efecto.

9.7. Lo dispuesto en el numeral 6.1 de este Reglamento no resulta aplicable para aquellas empresas del sistema financiero o EEDE que a la fecha de entrada en vigencia de la presente norma cuenten con autorización para operar con cajeros corresponsales"

Artículo Segundo.- Incorporar en el artículo 14° del "Reglamento de las Empresas Emisoras de Dinero Electrónico", aprobado mediante Resolución SBS N° 6284-2013, como información que deben remitir las EEDE, al Reporte N° 30 "Cajeros Automáticos y Cajeros Corresponsales" del Capítulo V "Información Complementaria" del Manual de Contabilidad para las Empresas del Sistema Financiero".

Artículo Tercero.- Los Anexos A al G del Reglamento de Apertura, Conversión, Traslado o Cierre de Oficinas, Uso de Locales Compartidos, Cajeros Automáticos, Establecimientos de Operaciones Básicas y Cajeros Corresponsales se publican en el Portal Institucional (www.sbs.gob.pe), según lo dispuesto en el Decreto Supremo N° 001-2009-JUS.

Artículo Cuarto.- La presente resolución entrará en vigencia a partir del día siguiente de su publicación en el Diario Oficial "El Peruano", fecha a partir de la cual quedará sin efecto la Resolución SBS N° 6285-2013.

Regístrese, comuníquese y publíquese.

ANEXO A

PERFIL DE FACTIBILIDAD ECONÓMICA

Deberá contener como mínimo la siguiente información:

1. Área de influencia geográfica y económica de la oficina propuesta. Se indicará además la ubicación donde funcionará la oficina.

2. Población total y población económicamente activa de la zona de operación.[1]

3. Análisis del mercado relevante, en los últimos dos (02) años, así como una estimación de la participación de la oficina propuesta en dicho mercado. Para el caso de empresas de seguros, estudio del desarrollo del mercado de seguros en la zona a ubicarse, con una retrospectiva de dos (2) años. [1]

4. Operaciones y servicios que se pretende realizar.

5. Organigrama funcional y cuadro de necesidades de personal, indicando la dependencia orgánica de la oficina en mención, así como las oficinas bajo su responsabilidad de ser el caso.

6. Proyección de estados financieros, cálculo de rentabilidad y punto de equilibrio. [1]

7. Medidas de seguridad adoptadas para la oficina, conforme el riesgo de las operaciones que realiza.

[1] Estos aspectos no serán exigibles para el caso de oficinas especiales temporales.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

PREPUBLICACION

ANEXO B

MOVIMIENTO DE OFICINAS

NOMBRE DE LA EMPRESA ..... **CÓDIGO DE LA EMPRESA**.....
CODIGO DE LA OFICINA.....

I. Tipo de movimiento autorizado
(marcar con aspa el recuadro correspondiente)

Tipo de Oficina	Movimiento			
	Apertura	Conversión	Traslado	Cierre
Oficina Principal				
Agencia				
Sucursal				
Oficina Especial				

II. Local compartido

Local compartido		Nombre de la empresa/s con la que se comparte el local	
		Tipo de oficina	

III. Autorización de la S.B.S.

Resolución S.B.S. Nº :	Fecha:
Fecha de notificación:	

IV. Datos de la oficina autorizada
Fecha de ejecución del movimiento de oficina:

UBICACIÓN	NUEVA OFICINA	ANTERIOR OFICINA (*)
País(**)		
Departamento		
Provincia		
Distrito		
Urbanización		
Dirección		
Teléfono		

(*) Solo en caso de traslados
(**)Solo en caso de sucursales

V.- Organización funcional de la oficina

Oficina supervisora o dependiente de la oficina	
Lleva o no su propia contabilidad	
Número de personal que labora en la oficina autorizada	
Número de cajeros automáticos que dependen de la oficina	
Número de cajeros corresponsales que dependen de la oficina	
Número de EOBs que dependen de la oficina	

GERENTE GENERAL

CONTADOR GENERAL
Reg. Nº .....

ANEXO C

DOCUMENTOS REQUERIDOS PARA OBTENER LA AUTORIZACIÓN PARA OPERAR A TRAVÉS DE CAJEROS CORRESPONSALES

a. Copia del acta del Directorio donde conste la decisión de suscribir contratos de cajeros corresponsales.
b. Plan de negocios para el desarrollo e implementación de cajeros corresponsales, en el cual debe señalarse la estrategia de implementación, los servicios a ser brindados, límites internos a ser aplicados de ser el caso, cobertura geográfica inicial y proyectada, criterios de selección de los cajeros, esquema tecnológico a ser utilizado, entre otros aspectos.
c. Las políticas y procedimientos aplicables a la prestación de servicios a través de cajeros corresponsales.
d. Copia del Informe de la Unidad de Riesgos o equivalente que contenga la evaluación de los riesgos asociados a las operaciones que se brindarán a través de cajeros corresponsales y determinación de las medidas que se tomarán para controlar los riesgos identificados, de acuerdo con la normativa vigente.
e. Las modificaciones estatutarias de la empresa del sistema financiero o EEDE, de ser pertinente.

ANEXO D

CONDICIONES Y REQUISITOS PARA OPERAR CON CAJEROS CORRESPONSALES

Las empresas del sistema financiero y/o empresas emisoras de dinero electrónico que operen con cajeros corresponsales deberán cumplir con las siguientes condiciones y requisitos:

1. Desarrollar e implementar políticas y procedimientos para seleccionar a los operadores y agregadores de operadores de cajeros corresponsales con los cuales suscribirán contratos para la provisión de dichos servicios. Para ello, deberán establecer criterios de evaluación que consideren, entre otros, los siguientes aspectos, siempre que sean aplicables:

   a) Situación financiera, lo que incluye como mínimo, no haber sido clasificado, en su condición de deudor, en las categorías de deficiente, dudoso o pérdida en el sistema financiero.
   b) Liquidez necesaria de los operadores para realizar operaciones con efectivo.
   c) Reputación.
   d) Infraestructura y seguridad de los establecimientos donde se brindarán los servicios.

   El cumplimiento de los requisitos definidos por la empresa del sistema financiero o EEDE para la selección de operadores y agregadores de operadores de cajeros corresponsales deberá ser monitoreado periódicamente.

2. La empresa del sistema financiero o EEDE deberá proporcionar manuales operativos a las personas naturales y/o jurídicas que operarán los cajeros corresponsales, y que sean necesarios para la adecuada prestación de servicios a los clientes y que deberán incluir los límites a los que alude el siguiente numeral.

3. La empresa del sistema financiero o EEDE deberá proporcionar debida capacitación a las personas involucradas en la operación de los cajeros corresponsales para desarrollar adecuadamente las operaciones y servicios acordados, que incluyan al menos los aspectos referidos a la adecuada identificación y atención de los clientes, confidencialidad de la información y secreto bancario.

4. Se deberá implementar medidas que controlen el riesgo operacional y el riesgo de lavado de activos; asimismo, se deberá establecer en el contrato las responsabilidades que serán asumidas por las personas naturales y/o jurídicas que operarán el cajero corresponsal.

5. La empresa del sistema financiero o EEDE mantiene la responsabilidad frente al cliente o usuario y ante la Superintendencia por la prestación de los servicios, la administración de riesgos y el cumplimiento normativo relacionado con las operaciones que se brindarán a través de los cajeros corresponsales. Asimismo, la empresa del sistema financiero o EEDE es responsable de adoptar las medidas necesarias para cumplir con lo establecido en el artículo

6° del Reglamento de la Ley que Regula las Características Básicas del Dinero Electrónico como Instrumento de Inclusión Financiera, aprobado por el Decreto Supremo N° 090-2013-EF.

6. La empresa del sistema financiero o EEDE deberá contar con mecanismos que permitan a su clientela o usuarios identificar adecuadamente al cajero corresponsal, así como informar sobre los servicios que prestan a través de ellos, y los mecanismos establecidos para la atención de consultas y reclamos.

ANEXO G

DOCUMENTOS REQUERIDOS PARA OBTENER LA AUTORIZACIÓN PARA OPERAR CON ESTABLECIMIENTOS DE OPERACIONES BÁSICAS

a. Copia del acta del Directorio donde conste la decisión de operar con establecimientos de operaciones básicas.
b. Plan de negocios para el desarrollo e implementación de establecimientos de operaciones básicas, en el cual debe señalarse la estrategia de implementación, características de diferenciación con las oficinas, los servicios a ser brindados, límites internos de prestación de servicios a ser aplicados de ser el caso, tamaño, personal e infraestructura de los puntos de atención, cobertura geográfica inicial y proyectada, esquema tecnológico a ser utilizado, entre otros aspectos.
c. Las políticas y procedimientos aplicables a la prestación de servicios a través de establecimientos de operaciones básicas.
d. Copia del Informe de la Unidad de Riesgos o equivalente que contenga la evaluación de los riesgos asociados a las operaciones que se brindarán a través de establecimientos de operaciones básicas y determinación de las medidas que se tomarán para controlar los riesgos identificados, de acuerdo con la normativa vigente.
e. Las modificaciones estatutarias de la empresa del sistema financiero o EEDE, de ser pertinente.

ANEXO N° 6

Resultado de la Encuesta

ENCUESTA BILLETERA MOVIL

La encuesta fue realizada en lima metropolitana , en diversos distritos de la ciudad : Comas , Los Olivos, La Victoria , San Juan de Lurigancho, San juan de Miraflores , El Agustino, Villa el Salvador y Villa María del triunfo.

Se realizaron 9 preguntas y se escogió una muestra de 50 personas pertenecientes al sector E, de nuestro mapa macroeconómico del Perú

Gráfico 1

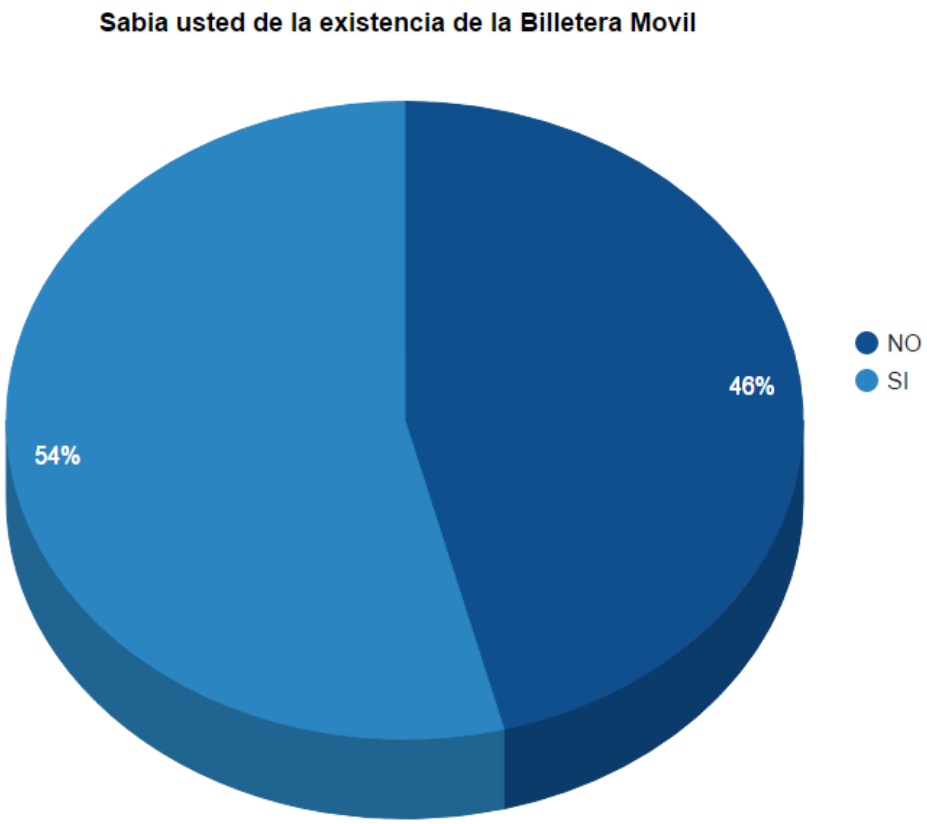


Gráfico 2

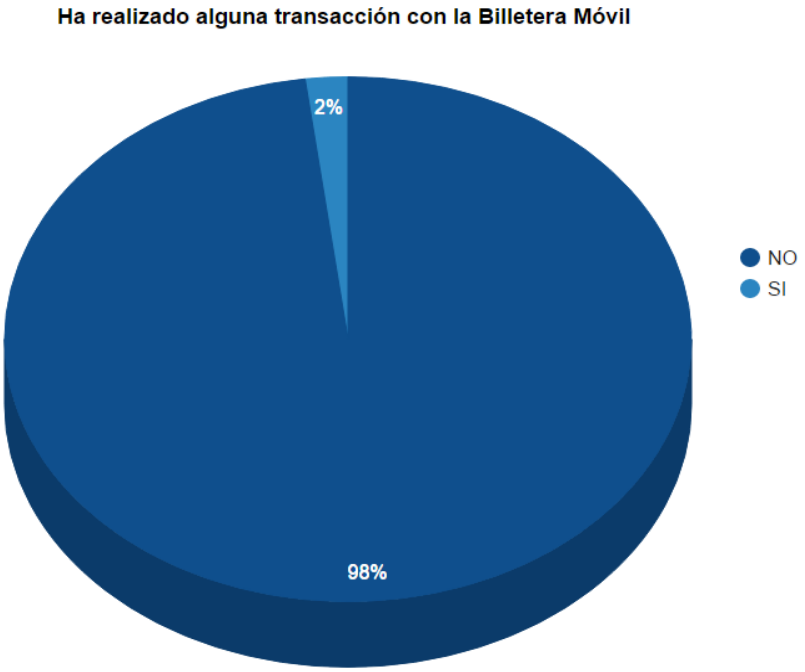


Gráfico 3

Gráfico 4

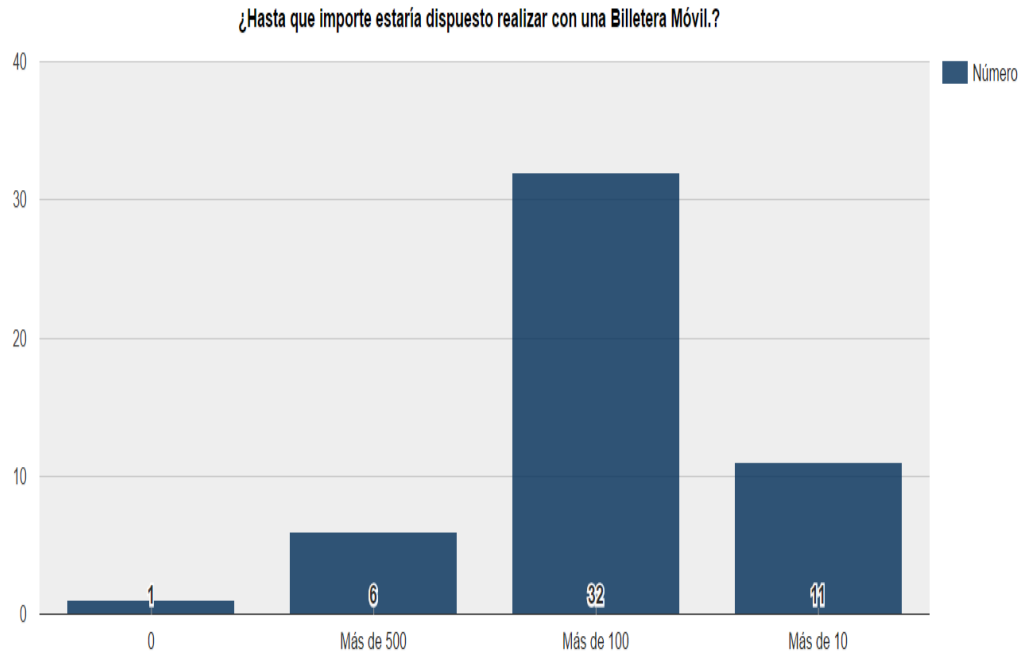


Gráfico 5

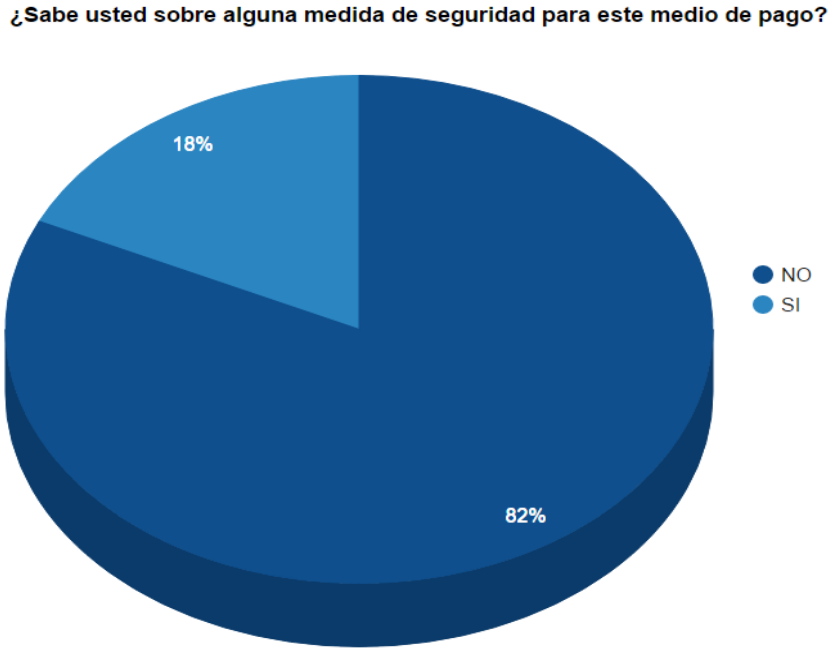


Gráfico 6

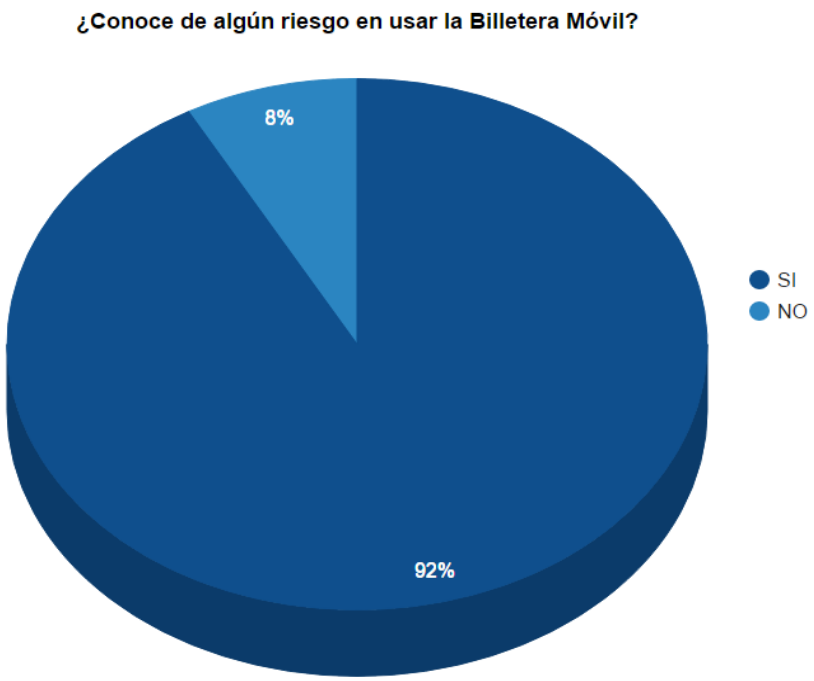


Gráfico 7

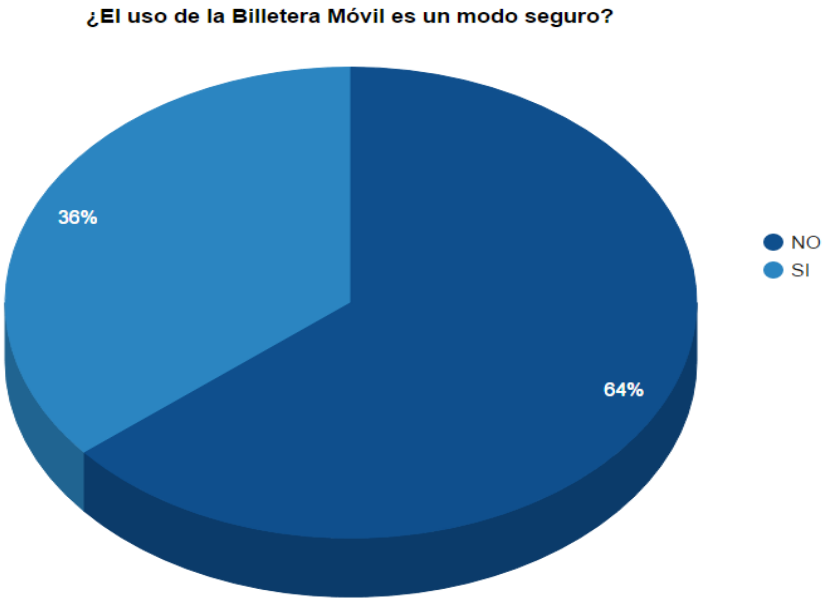


Gráfico 8

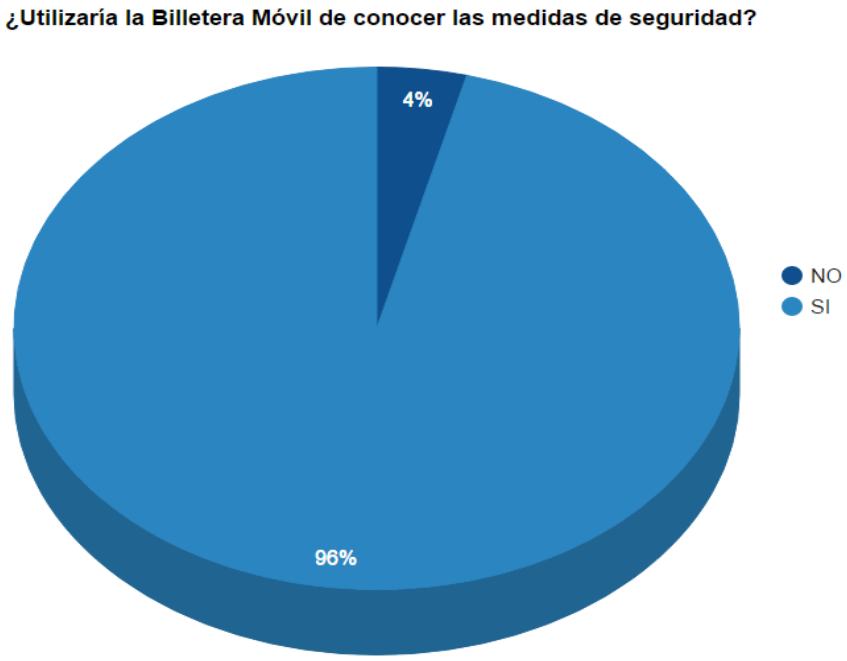
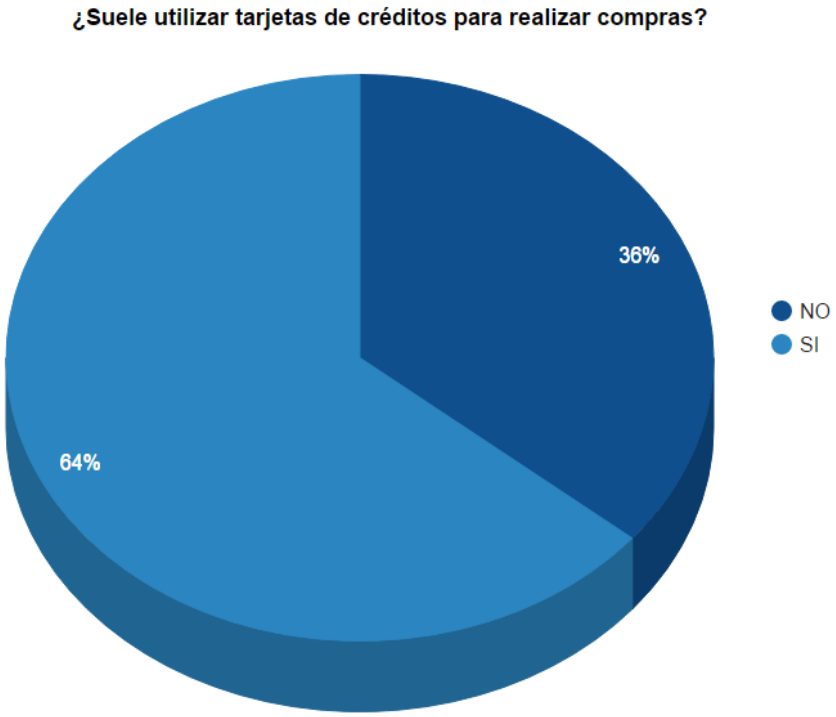


Gráfico 9



ANEXO N° 7

Acta de Entrevista

COMITÉ DE TESIS	
Reunión:	Comité de Tesis
Usuario Principal:	Asbanc
Lugar:	Calle 41 #975, Urb. Córpac - San Isidro
Convocado por:	Karol Gamboa – Stephanie Aguirre
Fecha:	26/04/2016
Hora:	5.30 p.m. – 5.30 pm.

ASISTENTES

NOMBRE DE LOS PARTICIPANTES	INICIALES	CARGO	DIVISIÓN / GERENCIA / JEFATURA	EMPRESA	ASISTENCIA
Oscar Rivera	OR	Gerente de Proyecto	Sistemas y Comunicaciones	Asbanc	✓
Karol Gamboa	KG	Solicitante	Comite de Tesis	USMP	✓
Stephanie Aguirre	SA	Solicitante	Comite de Tesis	USMP	✓

Asistió: (✓)
No Asistió: (*)

AGENDA DE LA REUNIÓN
Reunion de Comite de Tesis

TEMAS / COMPROMISOS

No	Descripción	Responsable	Fecha compromiso	Estado
1	Discutir la importancia de la billetera móvil en el Perú, cuanto tiempo estimo el Modelo Perú comprendiendo las diferencias con la implementación de la billetera móvil en otros países	OR,KG,SA	26/04/2016	Cerrado
2	Explicar en qué consiste la segunda fase del Proyecto, que iniciara a partir de Julio del presente año y abarcar los pagos de servicios como telefonía fija, móvil, pago de pensiones en universidades, servicios de luz y agua.	OR,KG,SA	26/04/2016	Cerrado
3	Explicar la tercera fase del proyecto Modelo Perú consistirá en el ámbito de Marketing en el Bim, donde las empresas se suscribirán y ofrecerán descuentos y más para las personas que utilicen este aplicativo	OR,KG,SA	26/04/2016	Cerrado
4	Explicar el proceso a nivel usuario del uso de este aplicativo y las de seguridad a nivel usuario del mismo.	OR,KG,SA	26/04/2016	Cerrado
5	Explicar la finalidad del proyecto, buscar la inclusión social financiera de personas que no dispongan de una tarjeta de crédito y que no cuenten con un celular de ultima tecnología	OR,KG,SA	26/04/2016	Cerrado

TEMAS / COMPROMISOS				
No	Descripción	Respon-sable	Fecha compromiso	Estado
1	Pactar una reunión con Erickson y PDP para comprender la parte técnica del Proyecto	KG,SA	28/04/2016	Pendiente

Acta elaborada por: Stephanie Aguirre- Karol Gamboa

De acuerdo a lo redactado en el presente documento, solicitamos se sirvan brindarnos sus opiniones, discrepancias y aprobaciones sobre el presente, contando con un plazo no mayor de 24 horas, siendo el mismo, el plazo máximo de opinión. En caso contrario se dara por aceptado el presente documento

COMITÉ DE TESIS	
Reunión:	Comité de Tesis
Usuario Principal:	PDP
Lugar:	Calle Uno Oeste 31- San Isidro Lima
Convocado por:	Karol Gamboa – Stephanie Aguirre
Fecha:	28/04/2016
Hora:	4.00 p.m. – 5.00 pm.

ASISTENTES

NOMBRE DE LOS PARTICIPANTES	INICIALES	CARGO	DIVISIÓN / GERENCIA / JEFATURA	EMPRESA	ASISTENCIA
Carolina Trivelli	CT	Gerente de Proyecto	Sistemas y Comunicaciones	PDP	✓
Karol Gamboa	KG	Solicitante	Comite de Tesis	USMP	✓
Stephanie Aguirre	SA	Solicitante	Comite de Tesis	USMP	✓

Asistió: (✓)
No Asistió: (*)

AGENDA DE LA REUNIÓN

Reunión de Comité de Tesis

TEMAS / COMPROMISOS

No	Descripción	Responsable	Fecha compromiso	Estado
1	Explicar la conformación de PDP y su involucración con la Bim, las alianzas con los operadores móviles del País , sus accionistas principales (Bancos, entidades financieras y cajas municipales)	CT	28/04/2016	Cerrado
2	Definir el alcance del Modelo Perú y Bim.	CT	28/04/2016	Cerrado
3	Explicar las vulnerabilidades a los que la billetera móvil podría estar expuesta.	CT,KG,SA	28/04/2016	Cerrado
4	Explicar la plataforma Bim	CT,KG,SA	28/04/2016	Cerrado
5	Entregar la Guía de Operaciones V1.5 del Modelo Perú	CT	28/04/2016	Cerrado

Acta elaborada por: Stephanie Aguirre- Karol Gamboa

De acuerdo a lo redactado en el presente documento, solicitamos se sirvan brindarnos sus opiniones, discrepancias y aprobaciones sobre el presente, contando con un plazo no mayor de 24 horas, siendo el mismo, el plazo máximo de opinión. En caso contrario se dará por aceptado el presente documento