PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

INFORME FINAL CASO DE ESTUDIO PARA UNIDAD DE TITULACIÓN ESPECIAL

TEMA:

"Análisis de comunicaciones y seguridades en la implementación del cobro de servicios de transporte público mediante tecnología NFC basada en la plataforma de dinero electrónico del Ecuador"

PORTILLA PEÑAFIEL JEFFERSON JAVIER

Quito – 2016

AUTORÍA

Yo, Jefferson Javier Portilla Peñafiel, portador de la cédula de ciudadanía No. 0401189147, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se ha respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

_____

Jefferson Javier Portilla Peñafiel

Contenido

Contenido de Ilustraciones

Contenido de Tablas

1. INTRODUCCIÓN

El presente trabajo se enfoca en un meticuloso análisis de comunicaciones y seguridades en la implementación del cobro de servicios de transporte público mediante tecnología NFC basada en la plataforma de dinero electrónico del Ecuador. La participación del Banco Central del Ecuador, en la vida de las personas y los sectores productivos, es totalmente palpable al facilitar que las actividades económicas puedan realizarse con normalidad.

La tecnología NFC es una tecnología muy reciente, pero que ofrece muchas posibilidades, debido a que cuenta con muchas ventajas: es muy fácil de utilizar y muy intuitiva, es bastante segura y eficiente, lo que la hace idónea para intercambios de información entre dos terminales.

Mediante dicha investigación se pretende conocer los fundamentos de la tecnología NFC y sus aplicaciones más importantes mediante la plataforma de dinero electrónico, ya que con el pasar del tiempo las conexiones físicas desaparecen para transmitir información, los equipos y plataformas que trabajan con NFC permiten, en segundos, conectar un dispositivo con múltiples aparatos móviles a través de la identificación de radiofrecuencia (RFID).

La tecnología NFC, es una herramienta inalámbrica de corto alcance que permite una interconexión entre dispositivos electrónicos de una manera intuitiva, sencilla y simple, mediante el uso del teléfono celular sin importar las características que posee el mismo, ya que

esta herramienta móvil permite trasmitir instrucciones e información acerca de la transacción a ejecutar.

El estudio está enfocado a comprobar mediante los resultados obtenidos el grado de seguridad que tenga la transacción financiera en el transporte público, haciendo uso de la tecnología NFC mediante la aplicación del sistema electrónico del Ecuador.

2. JUSTIFICACIÓN

En Ecuador actualmente han existido diferentes medios para realizar transacciones financieras, entre ellos están cheques, tarjetas de crédito / débito, la moneda física, con el pasar del tiempo se han dado avances tecnológicos, como es el caso de los mejoras en el área de telecomunicaciones que han permitido que el dinero electrónico tenga un constante crecimiento, convirtiéndose así en una herramienta de uso diario para que el usuario realice sus transacciones financieras.

Con lo antes mencionado y para dar proceso al caso de estudio, es importante plantear una serie de objetivos específicos, los mismos que darán paso al cumplimiento cronológico de las actividades a desarrollar durante todo el proceso de estudio.

El investigador debe fundamentar teóricamente sobre el objeto de estudio, en este caso sobre la tecnología NFC basada en la plataforma de dinero electrónico, ya que al desarrollar el tema de estudio, el investigador está sustentando teórica y conceptualmente la investigación, definiendo los eventos y exponiendo la teoría de la cual se va a partir el estudio, apoyándose en autores para respaldar cada uno de los planteamientos conceptuales.

Se debe diagnosticar la situación actual del manejo de las transacciones financieras basándose en la plataforma de dinero electrónico, de manera que le permita al usuario tener una visión más amplia del entorno real en el que se encuentra el caso de estudio, obteniendo una explicación previa del porque es importante la implementación de esta nueva investigación.

Con los resultados obtenidos se procede a determinar los elementos constitutivos de la tecnología NFC para el cobro de transporte público, basada en el sistema de dinero electrónico del Ecuador, ya que es un mecanismo que facilitan los flujos entre distintos agentes económicos

a través del uso de: dispositivos electrónicos, móviles, tarjetas inteligentes y otros dispositivos que se adopten a este sistema, según lo requiera el estudio.

Al establecer los elementos constitutivos de la tecnología NFC, es importante que el investigador realice un análisis comparativo de dicha tecnología que ha desarrollado con otras tecnologías usadas para la ejecución de transacciones financieras basadas en dinero electrónico, de manera que aporte sugerencias de mejoras para el desarrollo del caso de estudio

Con todo lo antes mencionado se aporta al cumplimiento del objetivo general propuesto para este caso de estudio.

3. ANTECEDENTES

Tecnología NFC (Near Field Communication) ha evolucionado rápidamente facilitando la forma en la que se convive con la tecnología, ya que es una plataforma abierta pensada desde el inicio para teléfonos y dispositivos móviles, su función consiste principalmente en el intercambio de información instantánea entre dispositivos cuando éstos se encuentran muy cerca, a diferencia del Wi-Fi o el Bluetooth, que permiten estar incluso en habitaciones distintas y transmitir grandes cantidades de datos, debido a que lo único que se debe hacer es activar la función NFC y juntar los dispositivos justo a la altura de donde están los chips NFC.

Con el pasar del tiempo y el constante avance de la tecnología las monedas y billetes de curso legal van desapareciendo, debido a la utilización del pago móvil y el uso de la tecnología NFC para realizar transacciones financieras, según lo requiera el usuario, ya que esta tecnología trae consigo ventajas como: permite una transacción rápida y segura entre el emisor y el receptor, en este caso se hace referencia al pago de transportes públicos, donde el tiempo de conexión entre dos dispositivos con NFC es tan solo de 0,1 segundos, tan rápido que todo se hace automáticamente, es por ello que la comodidad y la rapidez son sus mayores ventajas.

La tecnología NFC, es una herramienta de comunicación inalámbrica de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos. Además presenta una característica particular y es su compatibilidad con las demás tecnologías inalámbricas ya existentes como el Bluetooth y RFID, por lo que hace más interesante su uso. Todo lo expresado anteriormente denota un gran futuro para la aplicación de la tecnología NFC

mediante la plataforma de dinero electrónico, debido a sus características, principios de funcionamiento, estándares y análisis comparativo con otras tecnologías.

4. OBJETIVOS

Objetivo General

Estudiar las comunicaciones y seguridades en el cobro de servicios de transporte público mediante tecnología NFC que contribuya al manejo seguro de las transacciones financieras, basada en la plataforma de dinero electrónico del Ecuador.

Objetivos Específicos:

1. Fundamentar teóricamente sobre las comunicaciones y seguridades en el cobro de servicios de transporte público mediante tecnología NFC basada en la plataforma de dinero electrónico del Ecuador.
2. Diagnosticar la situación actual del manejo de las transacciones financieras mediante el sistema de dinero electrónico en los usuarios.
3. Determinar los elementos constitutivos de la tecnología NFC para el cobro de transporte público, basada en la plataforma de dinero electrónico del Ecuador.
4. Comparar la tecnología NFC con otras tecnologías usadas para la ejecución de transacciones financieras basadas en dinero electrónico.

5. DESARROLLO CASO DE ESTUDIO

5.1. Sistema de transporte urbano de pasajeros

Los diferentes métodos de transporte que utilizan los residentes de una ciudad se reconoce como sistema de transporte urbano de pasajeros, suele estar categorizado en dos grupos: transporte público y transporte privado.

5.1.1. Transporte público

Este sistema de se encuentra disponible para todo público, se rige a rutas y horarios previamente establecidos, cubriendo la necesidad de movilizarse a los diferentes lugares de la ciudad, los costos se encentran regulados por las municipalidades de cada una de las ciudades, así también se encargan del control y supervisión de los medios de trasporte público. Dentro de este tipo de transporte se encuentra varios servicios como: autobuses, taxis, camionetas, camiones.

5.1.1.1. Transporte público masivo

El transporte público masivo se caracteriza por transportar una gran cantidad de pasajeros, es decir, se trata de vehículos de gran capacidad con corredores exclusivos y paradas establecidas; En Ecuador no todas las ciudades cuentan con este tipo de transporte, ya que depende del número de habitantes y dimensión de la ciudad.

5.1.1.2. Transporte público colectivo

El transporte público colectivo utiliza buses en vías normales, es decir, no tienen corredor exclusivo, se ven afectados por el tráfico de la ciudad; dentro de las implicaciones de

este tipo de trasporte se tiene mayor congestión en las vías, aumento en el tiempo de espera del usuario, mayor contaminación ambiental y mayor número de paradas.

Las unidades de transporte público se encuentran implementando mejoras tecnológicas; algunas de ellas brindan el servicio de Wifi para disponibilidad de los usuarios, servicio de cámaras integradas para una mayor seguridad, contador automatizado para llevar un control eficiente de ingresos y uso de la unidad.

Para la integración entre el sistema de transporte público y la plataforma de dinero electrónico del Ecuador es necesario implementar en cada una de las unidades de transporte público colectivo y en cada una de las paradas del transporte público masivo lectores NFC con módem GSM para la comunicación de voz y datos hacia la plataforma.

5.1.2. GSM

5.1.2.1. Generalidades

GSM (Sistema Global de comunicaciones móviles) es considerado por su velocidad de transmisión y otras características un sistema digital multioperador, debido a que presta servicios de voz de alta calidad, permitiendo de tal manera que varios operadores pudieran compartir el espectro, garantizando la efectividad en los mismos, resultando ser de mayor capacidad al sistema analógico en cuanto se refiere a los costes y centrales de conmutación.

5.1.3. Near Field Communication NFC

5.1.3.1.Conceptos asociados

NFC (Near Field Communication) tecnología de comunicación inalámbrica que se caracteriza por su corto alcance y su alta frecuencia facilitando el intercambio de datos entre dispositivos, actualmente dicha tecnología se usa para realizar una serie de transacciones financieras debido a su seguridad y el tiempo en las transacciones, esto se lleva a cabo activando la función NFC y juntando los dispositivos que se desea compartir la información de marera rápida y sencilla para que pueda acceder el usuario.

5.1.4. Modos de operación NFC

NFC define dos modos de operación entre los dispositivos que desean establecer una comunicación: modo Pasivo y modo Activo.

- **Modo Pasivo**

En este modo de operación pasivo intervienen dos elementos: uno de ellos es el dispositivo activo el cual está conformado por una fuente de alimentación propia generando una señal electromagnética, y el otro elemento que lo conforma es un dispositivo pasivo el mismo que no cuenta con fuente autónoma de energía, por lo cual se requiere la energía del campo magnético provocando un efecto de acoplamiento inductivo para poder alimentar al circuito.

- **Modo Activo**

Para este tipo de modo lo conforman dos dispositivos activos, que como se mencionó anteriormente dichos elementos poseen alimentación propia, generando así sus propios campos electromagnéticos facilitando el intercambio de información o datos.

5.1.5. Arquitectura NFC

5.1.5.1.. Modo peer-to-peer

El modo peer-to-peer tiene la capacidad de comunicar dos elementos NFC permitiendo el intercambio de información de forma fácil debido a su corto alcance, lo que permite que dicha información sea envía por un canal de comunicaciones bidireccional half-duplex, es decir, cuando un dispositivo transmite, el otro debe escuchar, y únicamente se puede iniciar una transmisión sólo cuando el primero ha terminado, la velocidad máxima de transmisión de datos es 424 kbps, a continuación se esquematiza la arquitectura del modo peer-to-peer:

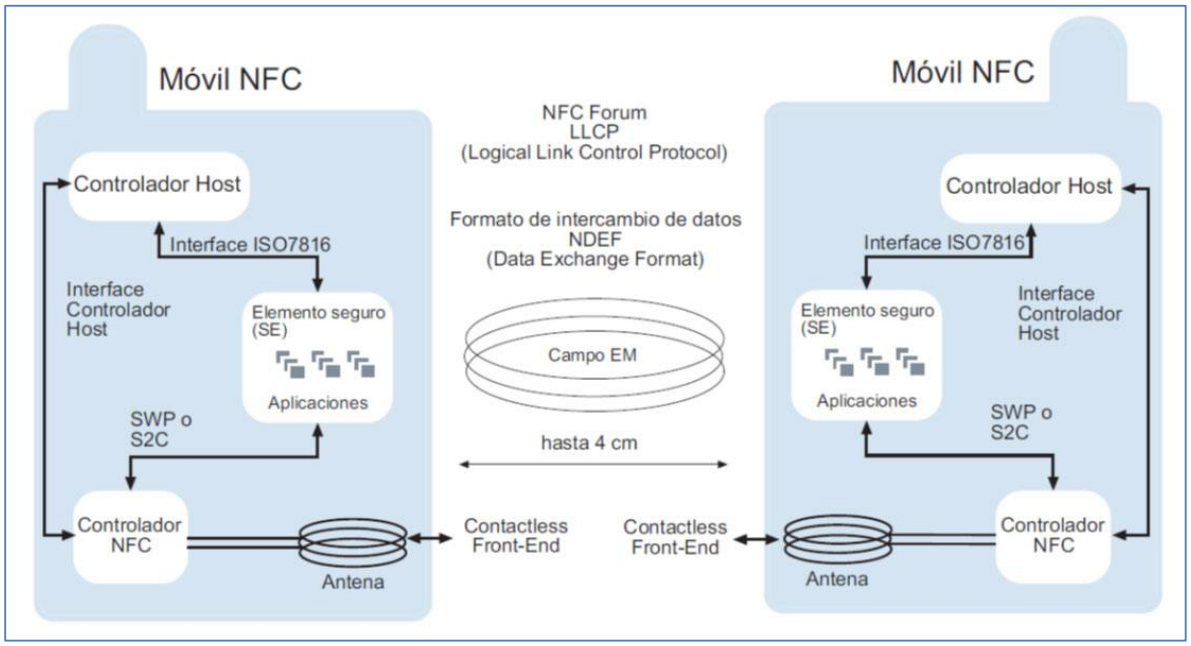


Ilustración 1: Esquema de arquitectura del Modo peer-to-peer

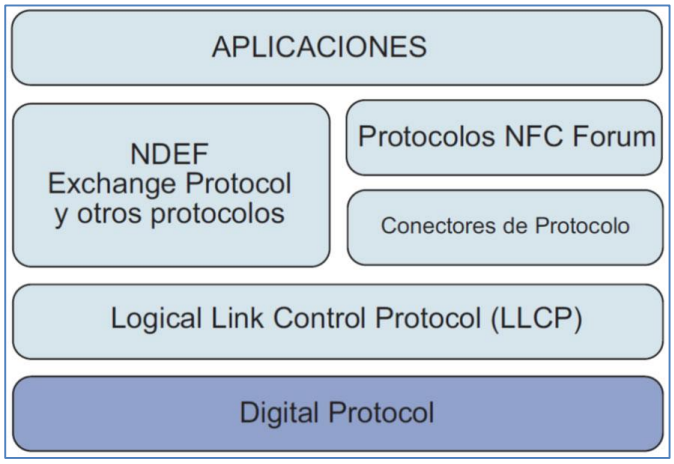


Ilustración 2: Esquema *NFCIP-1 (ISO/IEC 18092)*

El NFCIP-1 (Near Fiel Communication Interface and Protocol-1) es un esquema que describe modulaciones, codificaciones, velocidades de transferencia y frame formats del interface RF, este esquema tiene la capacidad de definir el protocolo de transporte, incluyendo métodos para la activación de protocolo e intercambio de datos, definiendo la comunicación de cualquier forma para los actores que intervienen en la misma.

Finalmente al hablar de LLCP (Logical Link Control Protocol) se hace referencia a un protocolo que está diseñado para resistir pequeñas aplicaciones, lo que incluye requerimientos limitados al momento de realizar la transmisión de datos.

5.1.5.2. Modo emulación tarjeta

Este modo de Emulación tarjeta se puede comportar como una tarjeta inteligente aunque también puede utilizarse como un tag la misma que se define como un transponder que

tienen un cierto tipo de memoria y que contiene datos formateados según NDEF, el modo emulación tarjeta es considerado como un teléfono con las características de la tecnología NFC por su corto alcance y alta frecuencia, permitiendo de tal manera que el usuario pueda efectuar una serie de transacciones financieras de forma ágil y segura, manteniendo su funcionalidad aun cuando el dispositivo se encuentre apagado.

En cuanto se refiere al proceso de emulación cabe recalcar que la emulación no es efectuada por el procesador NFC en el interior del dispositivo, si no por un componente hardware denominado Elemento Seguro (SE-Secure Element) que es un elemento físicamente protegido, el mismo que puede ser integrado en el interior del controlador NFC, o bien es posible utilizar una tarjeta SIM especial (UICC) que soporte el protocolo SWP (Single Wire Protocol),resultando ser un modelo diseñado para la comunicación entre el controlador NFC y el UICC (tarjeta SIM),a continuación se detalla el proceso de funcionalidad de este modo en el siguiente esquema:

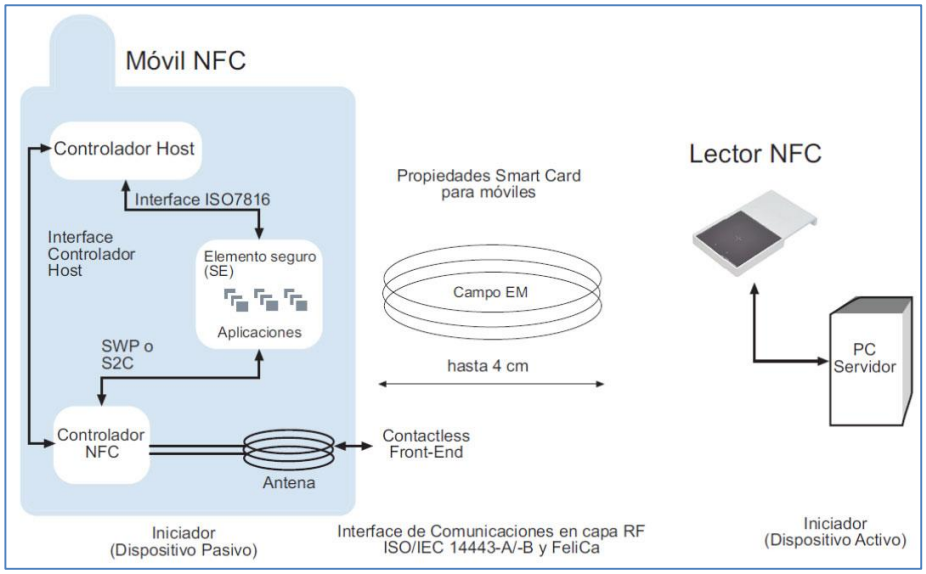


Ilustración 3: Esquema del modo emulación tarjeta

5.1.6. Arquitectura de un móvil NFC

Un smartphone con tecnología NFC está compuesto de varios circuitos integrados, es decir, uno o más elementos seguros (SE) y un interfaz NFC, los elementos que forman parte de dicha arquitectura se encuentran:

- NFC Contactless Front-End (NFC CLF)
- Una antena RFID
- Controlador NFC para las transacciones NFC

Típicamente un Smartphone para ser considerado como un dispositivo con tecnología NFC, al menos debe estar compuesto por un Elemento Seguro, en este caso la tarjeta SIM, de manera que permita realizar las transacciones financieras que requiera el usuario mediante un dispositivo NFC, el beneficio de un elemento seguro es que permite la memorización segura de datos privados y de valor en los servicios facultados por la tecnología NFC, el elemento seguro puede ser controlado y accedido internamente desde el controlador host o bien desde el campo RF externo, siendo trascendental tener conocimiento que el controlador host es el corazón de cualquier Smartphone, ya que fija la modalidad operativa, procesa los datos enviados y recibidos y establece la conexión entre el controlador NFC y el elemento seguro, a continuación se muestra una esquematización de la arquitectura móvil NFC:

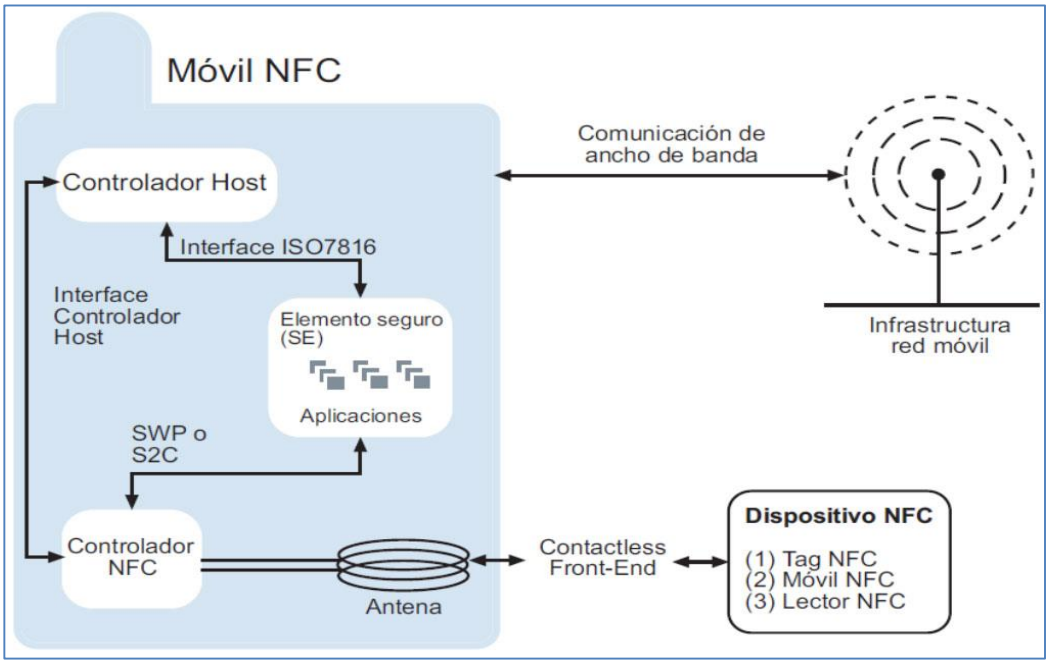


Ilustración 4: Esquema de arquitectura de un móvil NFC

5.1.7. Seguridad en terminales

Para poder implementar esta función de forma segura, lo cual es indispensable para su uso en transacciones bancarias, el dispositivo compatible estará equipado con un hardware seguro llamado Secure Elemet o Elemento Seguro que será accesible por chip NFC aun estando en modo pasivo.

Este elemento seguro puede ser un hardware adicional en el interior del teléfono, estar integrado en la tarjeta SIM o en otros dispositivos externos, por ejemplo una tarjeta SD insertada en el teléfono, aun no hay un acuerdo sobre el estándar de implementación del SE, aunque parece que las soluciones más populares son las dos primeras.

El SE integra un entorno seguro y una solución de cifrado para las aplicaciones de pago y los datos bancarios del usuario, del envío y almacenamiento de estos datos en el teléfono se hace cargo una entidad conocida genéricamente como Trusted Service Mananger, que es quien posee las claves públicas para los Elementos Seguros y actúa como tercero de confianza.

Actualmente existe una gran número de proyectos piloto basados en tecnología NFC, cada uno de ellos es desarrollado por un número pequeño de actores diferentes: un banco conjuntamente con un operador móvil y alguna cadena comercial, y utiliza diferentes formatos y protocolos e mensajes, esta situación no se puede considerar y utiliza diferentes formatos y protocolos de mensajes, es por eso que o se puede considerar como ideal para desarrollar la tecnología, ya que en un futuro podría ralentizar y obstaculizar su progreso debido a incompatibilidad de formato o desacuerdos entre actores.

Para solucionar esta situación surge la figura de los Trusted Service Manager (TSM), que actúan como enlace entre los diferentes actores, facilitando el intercambio de datos entre ellos. Además, es la figura que se encarga de proporcionar seguridad en las conexiones entre los diversos actores y sobre los datos del consumidor.

Tanto los TSM como otros actores forman parte de lo que la SmartCard Alliance llama “modelo colaborativo”, que viene a explicar el flujo de información entre las entidades que forman parte del ecosistema del modelo de pago mediante NFC. Un ejemplo de primera provisión de un teléfono seguirá el siguiente flujo:

- Las entidades financieras genera los datos bancarios que van a almacenarse en el Elemento Seguro del teléfono.

- Estos datos son enviados a las TSM a través de interfaces diseñadas para la comunicación entre ambos y se almacenan en una base de datos segura.
- Cuando el usuario pide la provisión del teléfono se hace una petición al TSM a través de las redes móviles, que responderá con los datos de pago de usuario.
- Una vez en el teléfono, estos datos se almacenarán cifrados en el Elemento Seguro.

Evidentemente, es necesario que estos datos se envíen cifrados y no en texto en claro. Cada uno de los actores es responsable del cifrado de su parte del proceso. Así, las entidades financieras son responsables del cifrado de los datos, el TSM de las interfaces con las entidades financieras y los operadores de red móvil, además de la securización de sus bases de datos. Estos últimos, por su parte, deben garantizar que los datos no puedan ser capturados. Todas estas comunicaciones se aseguran usando tecnologías probadas y fiables, como conexiones TL/SSL y cifrado PKI, además de cifrado aplicado por GSM o CDMA. En total, en la transmisión de estos datos se aplicarán hasta tres capas de cifrado, lo que la comunicación se considere confiable.

En cambio a la red de pago, las entidades financieras (tanto bancarias como entidades de pago) deben habilitar el pago a través de NFC, suponer un obstáculo, ya que el pago móvil utiliza las mismas condiciones que las tarjetas de crédito y tarjetas inteligentes.

El otro gran grupo de agentes implicados está formado por los operadores de telefonía móvil. Estos están encargados de las comunicaciones entre los demás actores y debe garantizar la seguridad en las comunicaciones de datos, además de ser en última instancia los propietarios de la tarjeta UICC o SIM (en caso de que el Elemento Seguro esté implementado en ella)

Otros actores importantes son los fabricantes de dispositivos móviles y electrónica en general, que son los últimos responsables de la introducción de la tecnología NFC en los dispositivos y en la sociedad, incluyendo la tecnología en sus productos.

5.1.7.1. Seguridad en pagos financieros con NFC

5.1.7.1.1. Seguridad en transacciones

Para el proceso de la seguridad en las transacciones a través de la tecnología NFC los datos se almacenan y administran de forma segura ya que se recopilan en una unidad bancaria y son enviados al elemento seguro (Secure Element SE), por lo que son totalmente protegidos debido a que el proceso de operación en dicha tecnología consta de los siguientes pasos: descubrimiento de dispositivos NFC, autenticación, negociación, transferencia de información y confirmación, es importante destacar que a bajo nivel, se incluye un procedimiento para la autenticación segura y mecanismos anti-colisión para evitar la escucha del canal de comunicación, con todo lo mencionado resulta ser la estructura de este sistema compleja que cualquier intento de hackearla o interceptarla resulta un proceso con mucha dificultad.

5.1.8. Análisis de seguridad en la plataforma de dinero electrónico

5.1.8.1. Seguridades que posee la plataforma de Dinero Electrónico

5.1.8.1.1. Seguridad en NFC

NFC es un nuevo medio de pago electrónico, que facilita el acceso a diversas operaciones transaccionales, y los usuarios tendrán la información esencial sobre el manejo de sus cuentas, quedando protegidos así sus beneficios, donde los intercambios se realizan por medio de dispositivos móviles mediante servicio de mensajería e integración electrónica y

servirán para canalizar el desarrollo productivo y potenciar el dinamismo económico en el Ecuador.

El Banco Central del Ecuador tiene una relación directa con la estructura de la plataforma de dinero electrónico, comprende la programación, organización, dirección, ejecución, coordinación y control del desarrollo de un sistema de integración vía WebServices, el mismo que está basado en el monitor transaccional, plataforma desarrollada por SIPECOM y que se encuentra funcionando en varias instituciones del Ecuador, permitiendo de esta manera asegurar y garantizar la información que se envíe y se reciba de forma online, considerándose en su conjunto un instrumento práctico, ágil e idóneo.

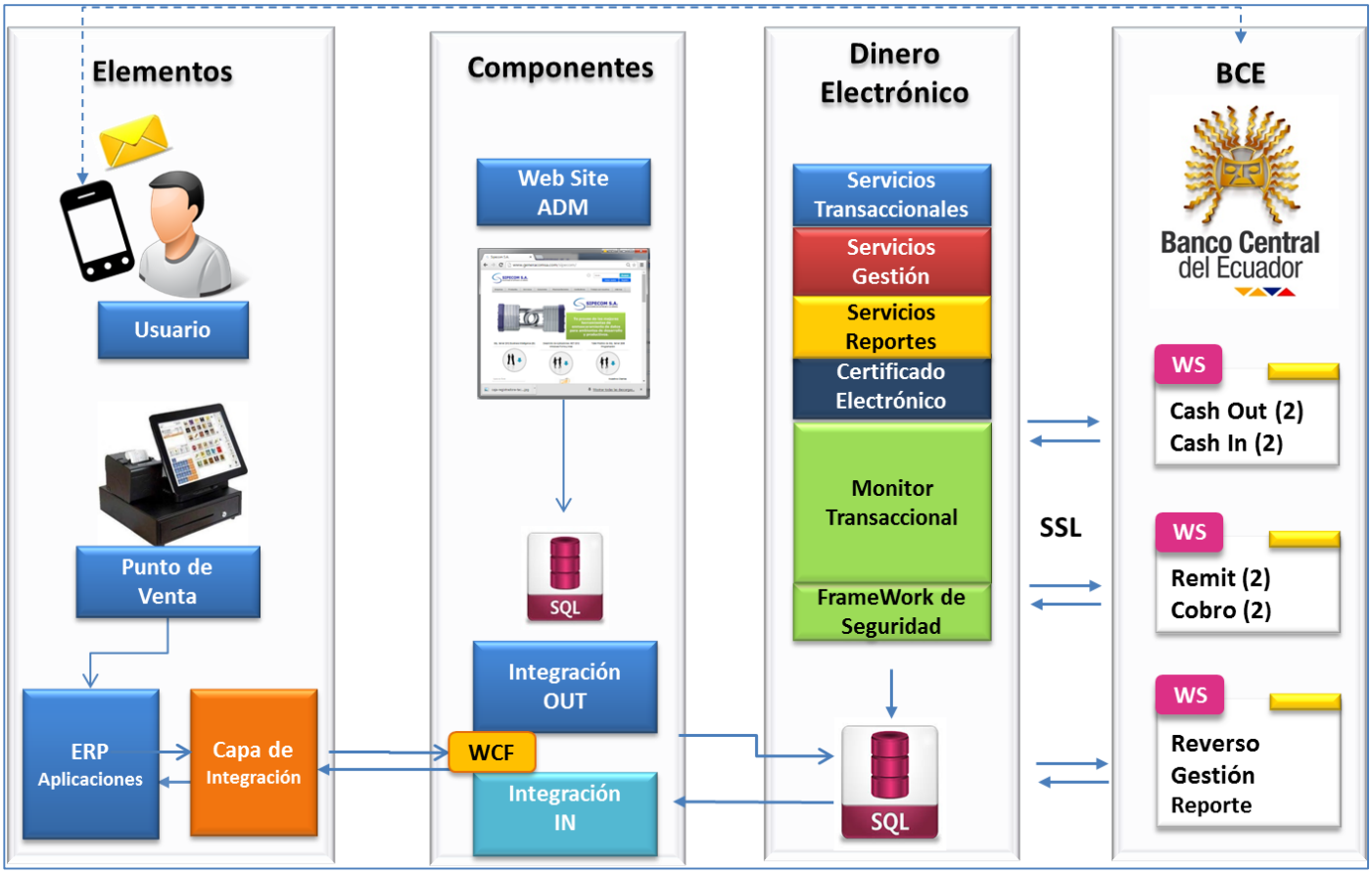


Ilustración 5: Seguridad en NFC de dinero electrónico

Fuente: Banco Central del Ecuador

5.1.8.2. Seguridad infraestructura del Banco Central

5.1.8.2.1. Seguridades Implementadas en la Interfaz USSD Sobre la Red GSM de las Operadoras Telefónicas.

Por lado del Banco Central del Ecuador.

Dentro de las operaciones transaccionales que están a disposición por la interface USSD, actualmente se encuentran implementadas las seguridades emitidas por el Banco Central del Ecuador y entre ellas se destacan las siguientes:

- Políticas para recopilar datos de identificación del Usuario.
- Solicitud de un PIN de seguridad.
- Bloqueo de cuenta por un número limitado de intentos fallidos de PIN para confirmación de transacción.

5.1.8.3. Seguridades Implementadas en Transacciones USSD

- **Auto registro**

El sistema está programado para reconocer mediante una serie de interrogantes la identidad de usuario, comprobando así su validación de acuerdo a las exigencias del sistema y si las respuestas son correctas el sistema envía un PIN temporal vía mensaje.

- **Pagos**

Se puede efectuar los pagos entre usuarios con tan solo ingresar el número celular del beneficiario, el sistema controla si es una cuenta válida, donde el usuario ingresa el monto a pagar, el sistema controla los montos permitidos y si es necesario también verifica el monto para poder realizar la transacción, una vez constatado dichos datos se procede a confirmar la transacción con el PIN de seguridad, en caso de que el PIN ingresado sea incorrecto la plataforma permite tres reintentos después se bloquea la cuenta de forma automática.

- **Auto descarga**

El usuario puede efectuar el proceso de Auto Descarga, es decir, la obtención de dinero físico, el sistema está coordinado para fijar un monto de descarga, dicho monto se lo realiza mediante la confirmación del PIN de seguridad, el sistema entrega un OTP (one time

password) el mismo que tiene un tiempo de validez de 4 horas, en donde el PIN se encuentra vinculado al monto solicitado y a la cuenta de dinero electrónico del usuario.

- **Recargas a celulares**

Los suscriptores pueden realizar recargas mediante el ingreso de número celular beneficiario y el monto de la transacción mediante su PIN de confirmación, el mismo que si es inválido por tres reintentos, el estado de la cuenta pasa a ser bloqueado automáticamente

- **Consulta de saldo Consulta Últimas Transacciones Cambio de Clave.**

Mediante el PIN de seguridad, se puede confirmar su validez, dando así respuesta a dichas consultas y de igual manera el sistema bloquea la cuenta en el caso de que el PIN sobrepase tres reingresos fallidos.

Por lado de las Operadoras Tecnológicas.

La tecnología GSM posee un elevado grado de seguridad en la interfaz radio UM, la misma que evita abusos y accesos prohibidos garantizando así confidencialidad al usuario, dentro de las medidas de seguridad se destacan las siguientes:

Autenticación de usuarios – Acceso seguro

- Confidencialidad al operador, ya que garantiza la conexión a la red únicamente a los usuarios que superen el proceso de validación.
- Autenticación de las estaciones móviles (MS).
- Seguridad en los terminales utilizados: Lista Blanca, Lista gris y lista negra.
- Protección al abonado, de manera que no permite el acceso a terceros.

- Cada estación móvil debe utilizar el mecanismo de autenticación de usuarios y la verificación de equipos antes de cada registro de red, cada tentativa de llamada y al solicitar la obtención de los servicios suplementarios (USSD).
- Protección mediante cifrado toda la información transmitida (cifrado y descifrado)
- El sistema de conmutación (SSS) decide la versión del algoritmo A5 y la clave de cifrado kc que se utiliza cada vez

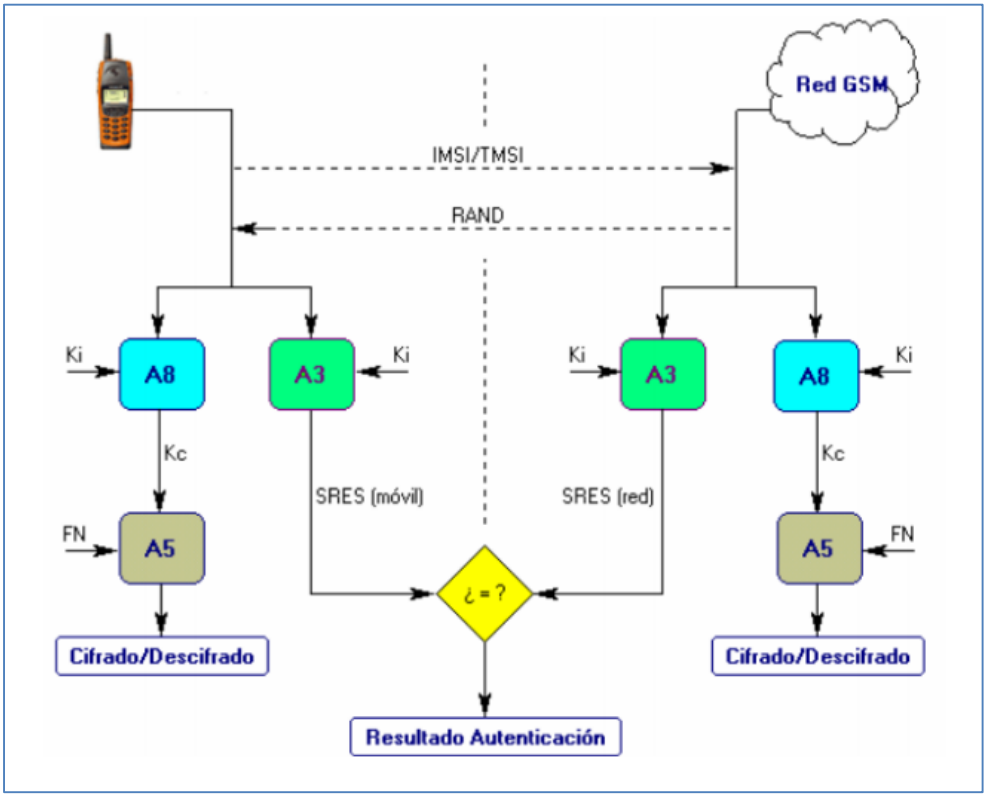


Ilustración 6 : Confidencialidad de datos del usuario y de la información

Autenticación de suscriptores

El AUC tiene como función proporcionar los datos necesarios al MSC/VLR para realizar la autenticación del suscriptor y a su vez establecer el proceso que se va a generar en este caso, aportando con la siguiente tripleta que se menciona y se esquematiza en a continuación:

- RAND – Número aleatorio no predecible
- SRES – Señal de respuesta
- Kc – Clave de cifrado

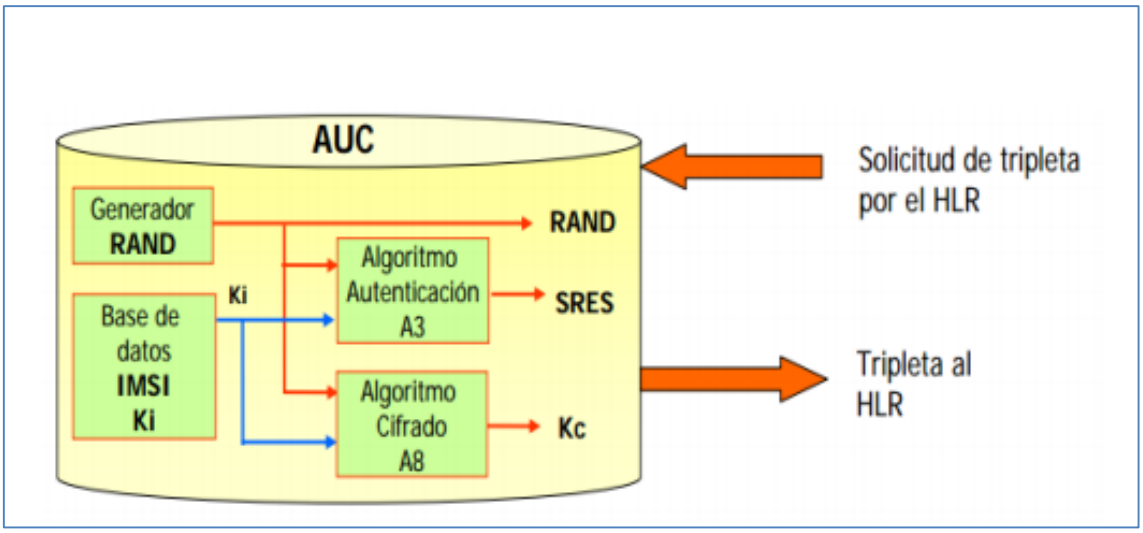


Ilustración 7: Generación de tripleta

La tripleta se ejecuta para establecer a cada usuario una clave de autenticación junto con al IMSI (Identificador internacional del suscriptor), las cuales son almacenadas de forma automática en el AUC y en el SIM, el proceso para el almacenamiento es el siguiente:

- El MSC/VLR transmite el RAND al MS

- El MS calcula a firma SRES usando el RAND, Ki y el Algoritmo A3.
- La firma SRES es enviada al MSC/VLR, que procede a la autenticación, comparando el SRES enviado por el móvil con el generado internamente, si estos son iguales se habilita el acceso.

Este proceso se realiza cada vez que se vaya a ejecutar el registro de u suscriptor ya sea que se den en los siguientes casos:

- Cando se transmita un llamada
- Actualización de localización
- Activar y desactivar servicios suplementarios.

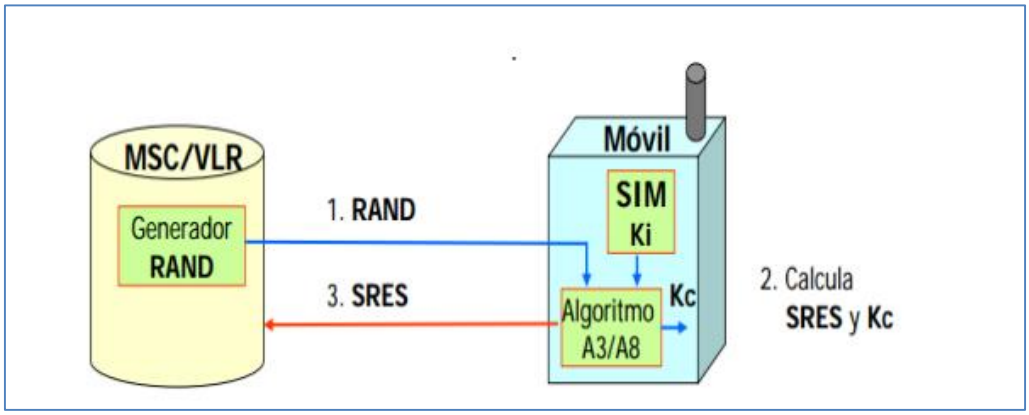


Ilustración 8 : Proceso autenticación de usuario

Cifrado de Datos

El proceso para elaborar el cifrado e datos se la menciona a continuación:

- La clave Kc se calcula a partir de la clave ki y el número aleatorio RAND mediante el algoritmo A8, toda esta información es almacenada en la SIM en su memoria no volátil.
- La secuencia del cifrado se produce por el uso del Kc y el número de trama TDMA, como entradas al Algoritmo A5, donde el número de trama es igual a 22 bits (0 – 2715.647) y el Kc es igual a 64 bits.
- Para poder acceder al cifrado de datos se envía una muestra de información mediante el comando de modo cifrado (M), donde la salida del algoritmo A5 es utilizada para cifrar los datos de la información (M) mediante una operación OR_EXCLUSIVE.

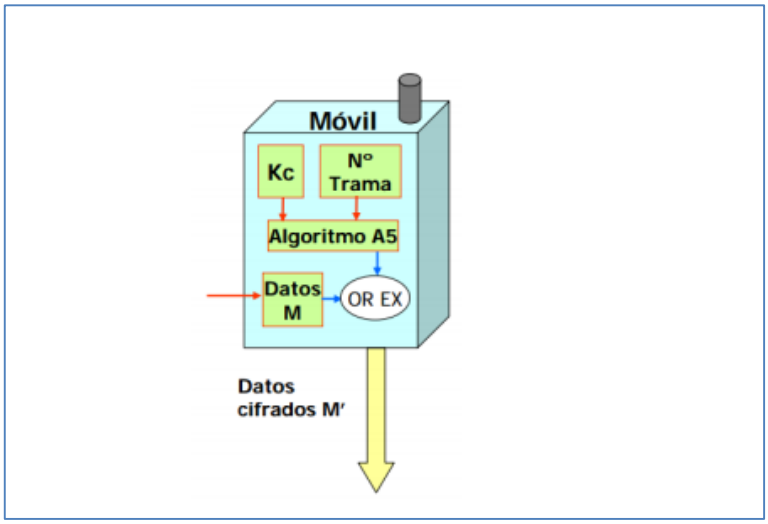


Ilustración 9: Cifrado de Datos

A continuación se enumera el proceso para obtener el cifrado:

- M y Kc son enviados desde el MSC/VLR a la BTS.
- M es reenviado a por la BTS al MS.
- M es cifrado usando Kc y el número de trama TDMA mediante el algoritmo A5.
- El mensaje cifrado M’ es enviado a la BTS.

- El mensaje es descifrado en la BTS usando el Kc, el número de trama y el algoritmo A5.
- Si el descifrado fue correcto, se comunica al MSC, toda la información en el interfaz aire es ahora cifrado por el mismo procedimiento.

5.1.8.4. Seguridades implementadas en la interfaz Web

La Plataforma de Dinero Electrónico es un servicio que permite a los suscriptores la Web Pública de Usuarios y la Web de Agentes, las seguridades que implica este interfaz se expresan a continuación:

- Autenticación Básica, mediante un usuario y contraseña, la misma que permitirá el ingreso al portal tanto de usuarios como de agentes.
- El agente y suscriptor al momento d realizar una operación transaccional debe confirmar con la clave privada asignada para cada uno de ellos.
- En cambio en el caso de Macro Agentes que se integran por la interfaz de servicios web se establece una conexión VPN entre el Banco Central del Ecuador y la entidad.
- Servicio de monitoreo de Anti-Phishing, en el caso de un hackeo se procede a dar de baja las páginas que fueron atacadas por un tercero.
- Autenticación y cifrado de la información mediante certificado SSL.

5.1.8.4.1. Transacciones por la interfaz WEB

Web Pública de Usuarios

Al suscriptor se le otorga a parte de la interfaz USSD, la opción de un portal Web la misma que brinda los siguientes servicios:

- Pago

- Cambio de contraseña
- Obtención de Balance
- Consulta de movimientos
- Asociación de Entidad Financiera
- Modificación de datos personales
- Web para Macro Agentes, los mismos que podrán acceder al portal web realizar las siguientes operaciones:
    - Cargas
    - Descargas
    - Pagos
    - Cobro
    - Fondeo Local
    - Reportes
    - Auto Gestión de Agentes
    - Pago Masivo

5.2. Aplicaciones y servicios con NFC

Para conocer de mejor manera la funcionalidad de la tecnología NFC, se destacan una serie de aplicaciones prácticas en donde actualmente ya se está involucrando la tecnología en diferentes países y con referencia a lo resultante se está estudiando factibilidad de la ejecución o desarrollo de la misma en otros ámbitos, entre ellas se mencionan las siguientes aplicaciones:

- **Transacciones.**

Para ejemplificar las transacciones que se puede efectuar con la tecnología NFC se acentúan las siguientes: el pago del pasaje del metro (medio de transporte), ya es usual realizar este tipo de transacciones, de esta forma se está aplicando en diferentes países, dichos servicios se los puede efectuar de diversas maneras, entre ellas:

- Realizar el pago de un ticket del metro, mediante la utilización de una tarjeta, simplemente acercándola al dispositivo de validación se puede ejecutar la transacción.
- Descontar el saldo que ha costado el viaje y abrir la barrera para que el usuario pueda acceder al metro.
- Realizar un pedido en un restaurante, simplemente con la utilización de alguna aplicación para este tipo de servicio.
- Ejecutar una transferencia de dinero de una persona a otra, únicamente con acercar el teléfono al de un amigo y validar la transacción.

La finalidad y utilización de este mecanismo invita a integrar y coordinar la utilización del dinero electrónico, logrando ser una herramienta eficiente.

- **Folletos digitales**

Muchas de las personas suelen entregar folletos para promocionar una eventualidad de cualquier índole, para evitar este tipo de servicio en la actualidad se puede hacer uso de la aplicación de esta nueva tecnología, la misma que permite transmitir el contenido de cada una de las publicidades vigentes de forma digital, de tal manera que cada persona pueda recopilar el contenido de la información del folleto con su dispositivo móvil o puede leer todo el periódico desde su Smartphone, optimizando así el uso de papel y sus costos.

- **Control de pacientes en un hospital**

Para el control de pacientes en un hospital es indispensable que el Doctor requiera el acceso a toda la información que sea posible de su paciente, es por eso que con la aplicación de la tecnología NFC es posible que el médico tenga la facilidad de adquirir la información mediante un dispositivo, de manera que pueda conocer la situación del paciente y sus datos de manera rápida y sencilla.

- **Identificación**

Actualmente la tecnología NFC está siendo utilizada por los usuarios como un sistema de identificación en oficinas, en donde los empleados acceden a su lugar de trabajo de forma directa desde su Smartphone, con el avance de la tecnología se asume que en los próximos años también se inicie con la ejecución de pasaportes o permisos de conducir integrados con los teléfonos móviles de forma que se aproveche todo el potencial de la aplicación de NFC.

- **Redes y tarjetas de visita**

En la sociedad actual cada vez se va implementando el servicio de redes de profesionales que aportan conocimientos sobre un mismo interés entre un grupo de colaboradores, socios o inversor, en dichos encuentros los participantes reciben ciertas cantidades de tarjetas de visitas y a muchas de ellas no se les da utilidad. Con la aplicación NFC permite evitar esto y concentrar toda la información de los contactos de dicha redes de profesionales de forma más sencilla.

- **Compartir datos.**

Tradicionalmente para intercambiar información entre usuarios se lo ha realizado mediante la opción de bluetooth, pues con el avance de la tecnología, en este caso de la aplicación NFC existe la posibilidad de utilizar dicha herramienta para compartir datos sin limitaciones, con el requerimiento único de juntar los teléfonos entre dos usuarios que soliciten el intercambio de información.

- **Analizar el sueño**

Uno de los problemas con más frecuencia que se ha identificado en las personas es el trastorno del sueño, es por eso que a través de dicha tecnología, se pretende poder ayudar a las personas con dicha dificultad, el proceso consiste en que un dispositivo se conecten de forma directa el brazo del usuario durante toda la noche para poder hacer un seguimiento del mismo, grabando la actividad durante el sueño, al día siguiente se transmite la información a través de la tecnología NFC y mediante una aplicación se analiza los datos resultantes del proceso efectuado, proporcionando una serie de consejos para de alguna manera optimizar el sueño del usuario.

- **Control ambiental**

Gracias a la aplicación de esta novedosa tecnología ha despertado una variedad de funcionalidades que se pueden efectuar con NFC, en este caso es posible por ejemplo, manejar una casa domótica, en donde se puede controlar la luz, la temperatura, el encendido o apagado de un ordenador, brindando de tal manera un uso importante para el control del ambiente en cualquier entorno en el que se encuentre.

- **Utilización en vehículos**

Otro de los usos de la tecnología NFC, se puede aplicar al mando de un vehículo, ya que es posible abrir y cerrar un vehículo, pudiendo con el tiempo adaptar al vehículo a la persona que conduce, es decir, una persona entra al vehículo y a través de su Smartphone transmite al vehículo una posición del sillón, de los espejos retrovisores y también la posición del volante, haciendo que los teléfonos móviles sean los que estén programados para ejecutar la orden al vehículo para que se adapte al usuario.

- **Ayudar a los discapacitados visuales**

Mediante la tecnología NFC se pretende brindar una ayuda a las personas que tienen discapacidad visual, facilitando una de las actividades que se ejecutan en el diario vivir, por ejemplo a la hora de adquirir productos en un supermercado, lo que se trata es que con el teléfono del usuario se pase por cada producto y que éste lea las características del mismo, facilitando así al usuario la selección del producto que va adquirir.

- **Fotografía y etiquetado**

Con la tecnología NFC se puede ejecutar una serie de fotos de una persona, mediante una simple etiqueta NFC las cámaras enfocan a cada persona que aparece en la foto, es decir, que cada usuario tendrá una copia de forma rápida y automática de todas las fotos generadas.

- **Datos de localización**

Dentro de la localización de un sitio específico, la tecnología NFC juega un papel significativo, ya que habitualmente para llegar a un sitio se lo hace utilizando mapas de Internet o con la activación de un GPS, actualmente gracias a la tecnología NFC se puede mejorar

algunos aspectos, para ejemplificar se los hace en un museo de arte, con el teléfono móvil o Smartphone se podría ir apreciando cada uno de los cuadros, su historia, su explicación de forma práctica y personalizada.

- **Pago en parqueaderos**

El pago por el uso de un parqueadero, resulta ser un aspecto tedioso, y gracias a la tecnología NFC el pago con móvil es posible, ya que con esta tecnología alerta al usuario los minutos restantes para desocupar un parqueadero y se cancela de forma automática el uso del mismo.

- **Automatización de puertas**

Para la automatización de puertas suele ser necesario y por comodidad personal el contar con un sistema NFC ya que facilita el acceso a un lugar con el hecho de acercar el teléfono móvil poder abrir la puerta, evitando las incomodas llaves que habitualmente se usan para acceder a un sitio.

5.2.1. C**omercio móvil – Dinero Electrónico**

5.2.2. Transacciones financieras con NFC

Mediante la aplicación de la tecnología NFC el usuario puede efectuar distintas transacciones financieras que usualmente las realiza de forma cotidiana y que por efectividad resultan ser ágiles y seguras, entre ellas se destacan:

- Disminución en los costos al efectuar una transacción financiera.
- No existe limitaciones para poder acceder al sistema financiero.

- Con el avance de la tecnología, NFC es una herramienta que tiende a crecer debido a la efectividad en cuanto a su aplicación se refiere.
- Esta herramienta NFC es de mucha utilidad tanto para pequeños y grandes emprendimientos.
- NFC resulta ser una tecnología de mejoramiento en el comercio ya que es un sistema de pago sencillo, de fácil acceso y barato.
- Debido a la complejidad en el proceso operativo de esta tecnología garantiza al usuario la confidencialidad y seguridad al momento de efectuar una transacción financiera.
- De acuerdo a los beneficios que brinda la tecnología NFC resulta ser atractiva la familiarización con dicho sistema, de manera que los usuarios puedan acceder a diferentes transacciones financieras.

5.2.3. Pagos con NFC

La tecnología NFC debido a su efectividad está intentando implantar como un nuevo canal de pago, debido a que resulta ser para el usuario una herramienta de fácil uso por su rapidez y seguridad para ejecutar cualquier transacción financiera con tan solo el uso de una telefonía móvil mediante diversas modalidades, entre ellas se destacan las siguientes:

- Al momento de recargar una tarjeta bancaria en el teléfono móvil.
- Contar con un monedero en la tarjeta, el mismo que este tramitado por una sociedad de gestión de dinero.
- Cargar las operaciones de forma directa en la cuenta del MNO.

5.3. Dinero Electrónico en el Ecuador

5.3.1. Generalidades

El dinero electrónico es un medio transaccional, implementado por el Banco Central del Ecuador, cuyo respaldo es el dinero físico, brindando la facilidad a los ciudadanos Ecuatorianos poder acceder a este sistema con tan solo abrir una cuenta de dinero electrónico, a través de un teléfono móvil, solicitando la autorización a una de las instituciones financieras legalizadas por el Banco Central, portando su cédula y el dinero físico que desea acreditar a su cuenta de dinero electrónico.

El proceso a seguir para la activación de la cuenta de dinero electrónico en el Ecuador es el siguiente:

- Se activa marcando al *153# desde un teléfono celular.
- La operadora realiza una serie de preguntas, como: ¿Desea activar una cuenta de dinero electrónico? ¿Conoce y acepta las condiciones de uso de la cuenta de dinero electrónico?
- Se ingresa el número de cédula del usuario, confirmando a su vez nombres y apellidos
- Se continúa respondiendo las preguntas de validación para que el sistema registre sus datos y le envíe la clave de seguridad a través de un mensaje de texto.

El usuario debe conocer que el dinero físico que acreditó a la cuenta de dinero electrónico, lo puede retirar en una de las instituciones financieras autorizados por el Banco Central del Ecuador, con tan solo presentar la cédula de identidad.

El mecanismo de aplicación del dinero electrónico en el Ecuador facilita los flujos, almacenamiento y transferencias entre distintos agentes económicos, mediante el uso de:

dispositivos electrónicos, electromecánicos, móviles, tarjetas inteligentes, y otros que se incorporen al avance tecnológico.

No cabe duda que el dinero electrónico no significa la emisión de una nueva moneda, ni tampoco es el sustituto del dólar, ya que toda transacción se la puede realizar mediante cualquier telefonía celular que no requiere ser un teléfono inteligente, ni siquiera debe tener Internet, cada dólar electrónico está respaldado por un dólar físico, es por ello que el usuario puede acercarse a cualquier punto de pago autorizado para hacer efectivo de forma física su dinero, en caso de requerirlo necesario.

5.3.2. Casos de uso

El dinero electrónico se usa en los siguientes casos:

- Realizar cualquier tipo de depósito o retiro de dinero.
- Transferencias entre usuarios.
- Transferencias entre gobierno y personas.
- Transferencias locales comerciales y personas.

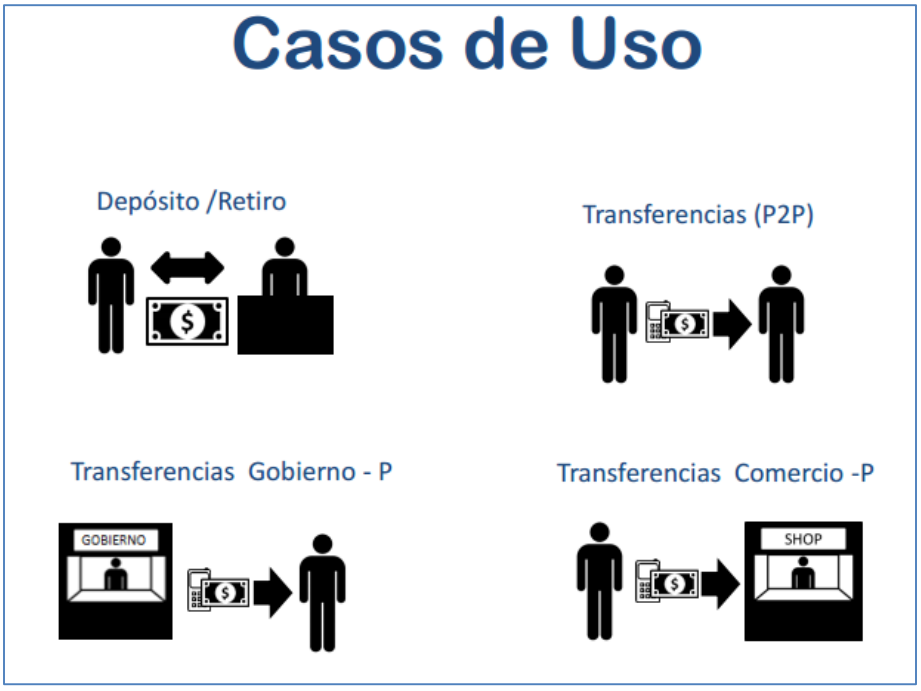


Ilustración 10: Casos de uso del dinero electrónico en el Ecuador**.**

Fuente: Banco Central del Ecuador

5.3.2. Sector Plataforma de Dinero Electrónico del Banco Central del Ecuador

5.3.2.1. Sistema Dinero Electrónico

El Sistema de Dinero Electrónico es una plataforma que permite realizar transacciones de dinero electrónico desde un teléfono móvil mediante la tecnología NFC y en tiempo real. El Sistema de Dinero Electrónico permite a sus usuarios efectuar una serie de servicios transaccionales de forma ágil y con la optimización del tiempo. Con la utilización del dinero electrónico se puede realizar los siguientes servicios, pago de cuentas, compra de saldo de comunicación telefónica, retirar el efectivo o enviarlo a otro usuario. Siendo así que el dinero electrónico es un proyecto impulsado por el Banco Central del Ecuador para que sea un medio de

pago como son las monedas fraccionarias, las tarjetas de débito, cheques y transferencias electrónicas.

5.3.2.2. Arquitectura de la Plataforma de Dinero Electrónico.

La plataforma de Dinero Electrónico cuenta con dos módulos principales:

- Módulo de aplicaciones
- Módulo de base de Datos

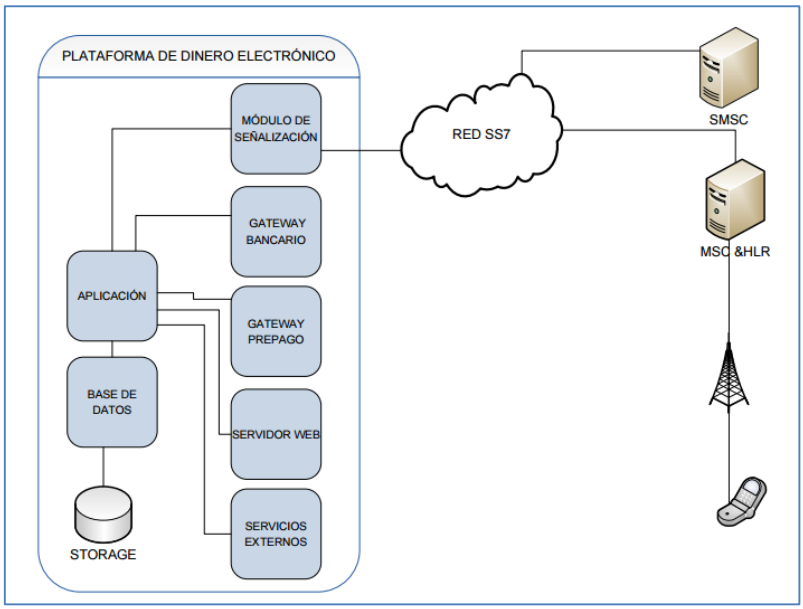


Ilustración 11: Arquitectura del Dinero Electrón

El módulo de aplicación absorbe la lógica del sistema. Es el encargado de las siguientes tareas:

- Solicitudes a la base de datos, sistemas prepagos o de facturación.
- Ejecución del retiro/depósito de efectivo, recepción de las solicitudes de recarga o de información del agente.

- Envío de confirmaciones o de mensajes de error.
- Generación de tickets administrativos/transaccionales.

5.3.2.3. Infraestructura Tecnológica de Dinero Electrónico (HARDWARE)

La configuración de hardware básica de la plataforma SDE para el BCE se compone de 18 servidores, en donde 5 de ellos se encuentran en 2 sitios geográficamente diferentes y los 18 servidores están encargados de la lógica de la aplicación Sistema de Dinero Electrónico del Banco Central del Ecuador, de la interfaz con la red de señalización SIGTRAN, de las interfaces externas y del manejo de las bases de datos del sistema. Incluye 1 kit de Storage NetApp para el almacenamiento de datos (datos en tiempo real y datos históricos). Los dos sitios geográficos que se mencionan son los siguientes:

Quito (UIO)

- Servidores de señalización
- Servidor de WEB / Servicios Web
- Servidores de aplicación
- Servidores de base de datos OLTP
- Servidor de base de datos histórica
- Servidores de ambiente de desarrollo o pruebas

Guayaquil (GYE)

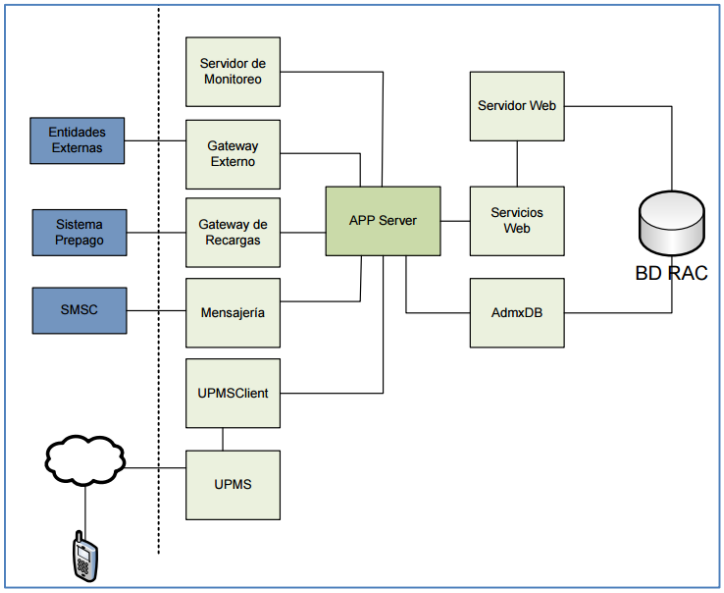
- Servidores de señalización
- Servidor de WEB / Servicios Web
- Servidores de aplicación

- Servidores de base de datos OLTP

5.3.2.4. Módulos de conectividad de la Plataforma de Dinero Electrónico (SOFTWARE)

La plataforma de Dinero Electrónico que promueve el Banco Central del Ecuador está perfilado por distintos módulos de software, en donde cada módulo desempeña una función delimitada, se puede estacar que una de las ventajas de este tipo de arquitectura es que puede modificarse o añadirse un determinado módulo sin el riesgo de que cualquier transformación afecte al sistema, a continuación se esquematiza la arquitectura modular de la plataforma de dinero electrónico (software):

Ilustración 12: Modulación de la plataforma de dinero electrónico.



Entre los módulos de software se destacan los siguientes:

- **Módulo UPMS**

Este módulo permite la señalización de red (SIGTRAN) para la recepción y envío de datos por parte del sistema de dinero electrónico, también este módulo está conectado a la red

de señalización SS7 a través de SIGTRAN, mediante este módulo es factible recibir y enviar mensajes efectuados por el usuario.

- **Módulo Mensajería**

Permite el envío de mensaje al SMSC de las operadoras móviles, de tal manera que los mensajes son entregados al SMSC y enviados al usuario final mediante SMSC del operador.

- **Módulo Gateway de Recargas**

Permite la conexión con servidores de prepago para poder realizar una recarga de saldo vía Sistema de Dinero Electrónico.

- **Módulo APP Server**

Conjunto de librerías de procesamiento de transacciones del Sistema de Dinero Electrónico, componiendo el CORE de la aplicación ejecutada.

- **Módulo SB APP Server**

Conjunto de librerías encargadas de resolver las invocaciones hacia el CORE de MTS desde las distintas interfaces (USSD, WEB y WEB Service).

- **Módulo SB AuxNode**

Nodo Erlang auxiliar que sirve al módulo SB APP Server como proveedor de una estructura de almacenamiento de datos de los servicios de la plataforma.

- **Módulo UPMSClient**

Módulo encargado de recibir información de señalización por parte del módulo UPMS con destino al SDE, la información es comunicada en lenguaje Erlang con los distintos módulos Erlang de la plataforma.

- **WEB Administrativa**

Interfaz WEB de acceso privado al Banco Central del Ecuador con todas las funcionalidades administrativas del Sistema de Dinero Electrónico.

- **Módulo AdmDB**

Permite ejecutar las conexiones a la base de datos para los módulos SB APP Server y MTS APP Server.

- **Módulo Ticket**

Permite generar tickets y operaciones transaccionales que brinda la plataforma Sistema de Dinero Electrónico.

- **Base de datos Histórica**

Base de datos de replicación histórica del RAC.

- **Storage**

Es un módulo que permite la recopilación de datos de la base de datos online e histórica del sistema.

Ilustración 13: Esquema Operacional del Dinero Electrónico en el Ecuador.

Fuente: Banco Central del Ecuador

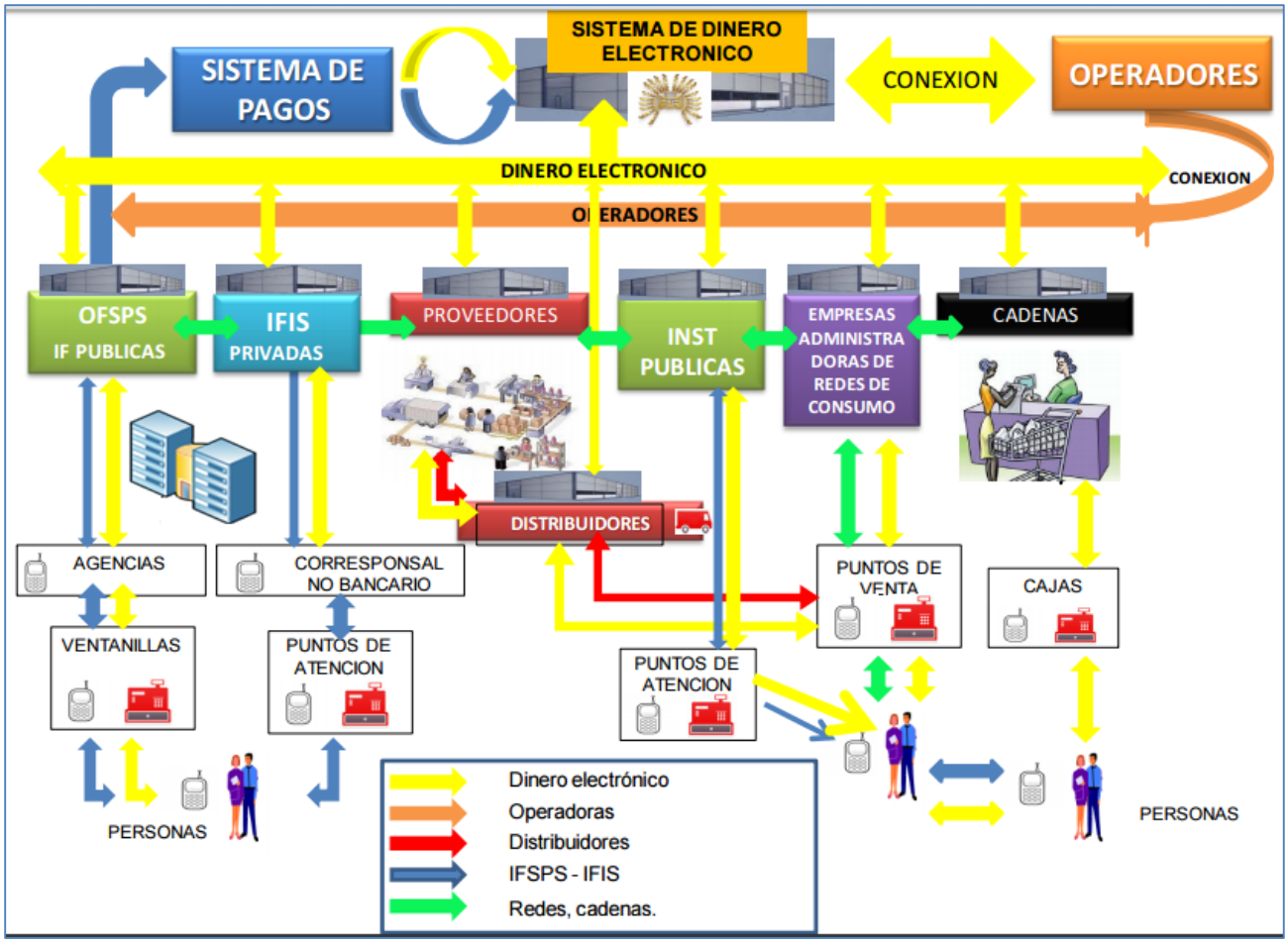


Ilustración 14: Arquitectura del Dinero Electrónico en el Ecuador

Fuente: Banco Central del Ecuador

5.3.3. Entidades o participantes

En la plataforma de dinero electrónico del Ecuador se encuentra integrado por las siguientes entidades mencionadas a continuación:

- Emisor y administrador (Banco Central del Ecuador)
- Entidades reguladoras
- Canales tecnológicos

- Macro agentes (empresas, organizaciones e institución públicas y privadas, instituciones financieras y del sistema popular y solidario)
- Centros transaccionales (oficinas de atención de los macro agentes directas o corresponsales.)
- Personas.

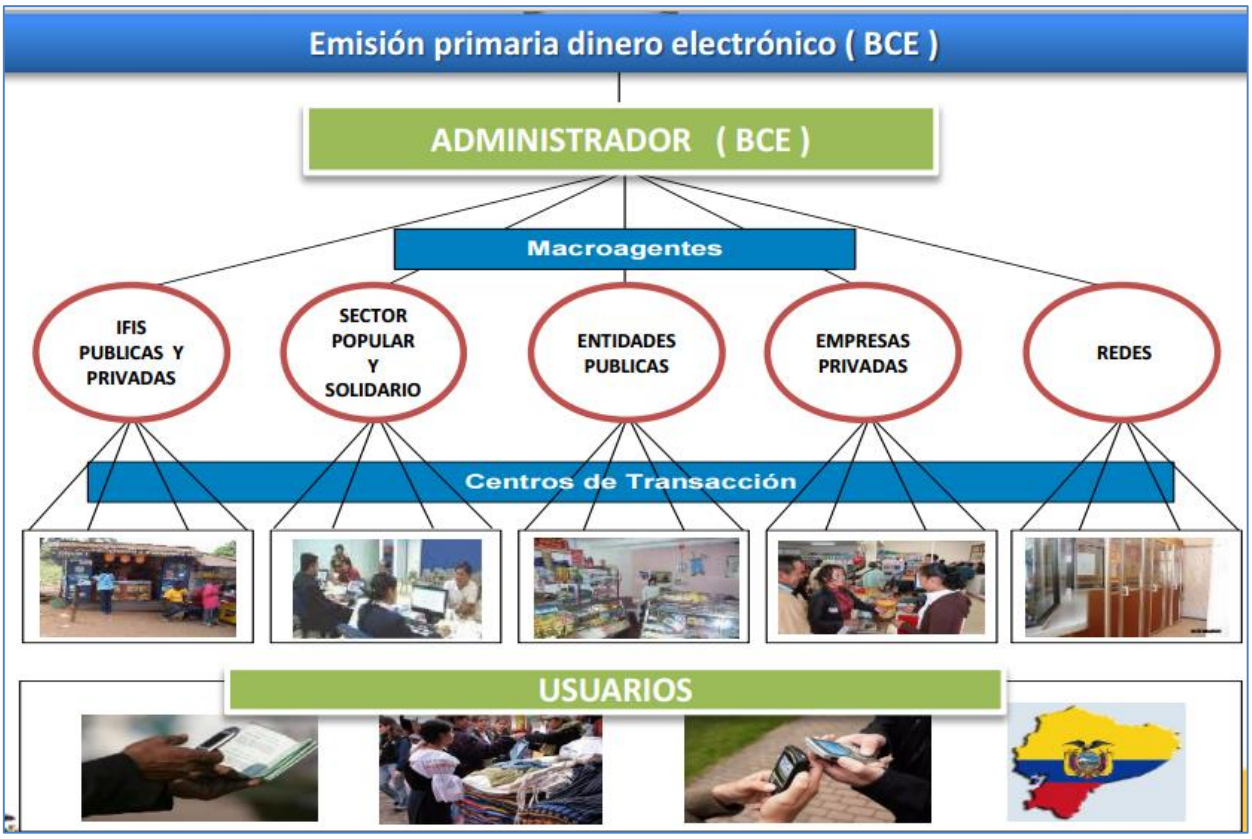


Ilustración 15: Emisión primaria del Dinero Electrónico

Fuente: Banco Central del Ecuador

5.4. Comparativa de Tecnologías semejantes a NFC

5.4.1. Servicio NFC en el Ecuador para Dinero Electrónico

5.4.1.1. Estado Actual

En la actualidad el Sistema de Dinero Electrónico en el país, constituye una herramienta de inclusión y agilización de las transacciones entre personas, instituciones y el gobierno para un manejo más eficiente y seguro en las transacciones, gracias a la confidencialidad en los datos recopilados de los usuarios.

Near Field Communication (NFC) es una tecnología atractiva, por su efectividad en las transacciones financieras facilitando el pago con el móvil sin necesidad de tener que llevar dinero físico, simplemente al juntar los dispositivos activando la funcionalidad NFC para proceder a transmitir la información entre dispositivo.

Hoy en día, Ecuador va camino a convertirse en uno de los países que promueve la moneda electrónica que será emitida y distribuida por el organismo regulador (Banco Central) que será fácil su utilización mediante la red de celulares; reemplazando el sistema tradicional de pagos basado en especies físicas (billetes o monedas), aprovechando la infraestructura existente y reduciendo los costos de transacción, este será un dinero que fluya a través de la red celular. Debiendo socializar de esta nueva implementación e incentivar a más entidades a unirse a este sistema para que las transacciones sean cada vez más sencillas y ágiles.

5.4.1.2. Factores importantes

La innovación del Sistema de Dinero Electrónico en el Ecuador, es una de las propuestas económicas que tiene en mente el gobierno, ya que con la aplicación de la tecnología NFC, permite efectuar transacciones financieras de forma segura y con optimización del tiempo,

generando así un crecimiento social, económico y financiero en la población ecuatoriana, conforme se lo ha analizado en el desarrollo del tema, materia de investigación, brindando a los usuarios un alto índice de seguridad, promulgando el ahorro familiar, optimización de tiempo y facilidad en el pago de las transacciones financieras, mejorando de esta manera la economía del país, haciendo que el sistema sea más dinámico en la circulación.

5.4.1.3. Banca Móvil

Con la implementación de este servicio, permite al usuario tener acceso a diferentes servicios financieros propuestos por instituciones financieras, ya sean éstas bancos o cooperativas, también es considerado como el canal que ofrece al usuario un servicio en el cual pueda realizar transferencias, como por ejemplo: compras de minutos de telefonía celular, pago de tarjetas de crédito, cancelaciones de servicios básicos, consultas de manera fácil, rápida, segura y oportuna en cualquier momento y desde cualquier lugar del país. Es importante destacar que al realizar un pago con el Smartphone, contribuye con una funcionalidad mucho más rápida y sencilla gracias a la ejecución de la tecnología NFC ya que permite efectuar la operación y proceder al pago inmediato de una transacción

5.4.1.4. Cuadro comparativo entre tecnologías similares a NFC

Tabla 1 : Cuadro comparativo entre tecnologías similares a NFC

	NFC	**RFID**	**WiFi**	**Bluetooth**	**ZigBee**	**IrDA**
Estándar	ISO/IEC 18092	ISO/IEC 14443	IEEE 802.11	IEEE 802.15.1	IEEE 802.15.4	IrDA
Tasa de transferencia	106- 424 Kbps	106- 424 Kbps	11-200 Mbps	1- 480 Mbps	20- 250 Kbps	1 Kbps- 100 Mbps
Frecuencia de funcionamiento	13,56 MHz	13,56 MHz	2.4, 5.25, 5.6, 5.8 GHz	2.4 GHz	868/915 MHz 2.4 GHz	
Cantidad máxima de dispositivos que se puedan interactuar	2	2	Indefinida	8	Indefinida	2

Tiempo de inicialización	<0,1ms	<0,1ms	<0,1ms	6s	<0,1ms	0,5 ms
Alcance	<20 cm	<3 m	<100 m	<30 m	<500 m	<5 m
Seguridad	Dada por la cercanía entre dispositivos	Dada por la cercanía entre dispositivos	Determinada por los mecanismos de encriptación que se usen	Determinada por los mecanismos de encriptación que se usen	Determinada por los mecanismos de encriptación que se usen	Dada por el requerimiento de ambos dispositivos que estén en la línea de vista
Consumo de energía	Mínimo o Inexistente	Mínimo o inexistente	Alto para dispositivos alimentados con baterías	Alto para dispositivos alimentados con baterías	Muy Bajo	Bajo

Objetivo	Simplificar la interacción entre dispositivos electrónicos	Realizar seguimiento de objetivos y control de acceso	Reemplazar cables en redes extensas, fundamentalmente en tipo LANs	Reemplazar cables para conectar dispositivos electrónicos cercanos	Control y monitoreo inalámbrico	Reemplazar cables para conectar dispositivos electrónicos
Ejemplo de aplicación	Intercambio de tarjetas personales electrónicas acercando dos teléfonos celulares	Control de inventarios en supermercados	Conexión entre dispositivos de una oficina (PCs, notebooks, impresoras, etc.) dentro de un mismo edificio o entre edificios	Conexión de periféricos (Teclado, mouse, etc.) notebook en la misma habitación	Manejo de sistema y de riesgo de fertilización en sembrados usando sensores de acuerdo a los	Trasferencias de archivos entre teléfono celular y una notebook

			cercanos		valores de ciertas variables accionan los mecanismos correspondientes	

5.4.1.5. Análisis de costo

El costo es considerado como desembolso o salida de dinero, esenciales para determinar la calidad y cantidad de recursos o componentes necesarios asociados a un determinado proyecto, se procede a realizar el análisis de costo con la finalidad de considerar el costo que tiene la implementación del pago de transporte público mediante tecnología NFC, de manera que permita apreciar su rentabilidad, que para este caso se estima en base a la tarifa que cobra el BCE por efecto transacción de cobro a los macro agentes (operadoras de transporte público), con la elaboración de dicho análisis facilita una adecuada y oportuna toma de decisiones para emprender y dar continuidad al proyecto.

Para realizar el análisis de costo se toma en cuenta los estudios de movilidad realizados en el Distrito Metropolitano de Quito en el cual entre los datos más relevantes se tiene la cantidad de buses convencionales urbanos que es alrededor de 1542 y los viajes realizados por día en una cantidad aproximada de 1700000; además se cuenta a la fecha del análisis la cantidad de 230000 usuarios en la plataforma de dinero electrónico por tal motivo se asume que los usuarios deben contar con tarjetas NFC y los buses con lectores NFC.

Tabla 2 Análisis de costos

Elaborado por: Portilla Jefferson

Análisis de Costo											
Artículo Tecnología NFC											
Fecha	Detalle	Materia prima directa (MPD)			Mano de obra directa (MOD)			Costos indirectos de implementación			
		Cant	Costo Unit	Total	Cant	Costo Unit	Total	Detalle	Cant	Costo Unit	Total
05/11/2016	Tarjetas NFC	230000	3	690000	0	0	0		0	0	0
	Lector NFC con módem GSM	1542	20	30840	0	0	0		0	0	0
		SUMAN		720840	SUMAN		0	SUMAN			0

RESUMEN	VALOR	RESUMEN
Materia prima directa (MPD)	720840	Para calcular el costo de implementación se realiza el siguiente cálculo:
Mano de obra directa MOD	0	Costo de implementación = Costo primo + Costo indirecto de implementación
Costo primo directo	720840	CI = 720840 + 0
Costos indirectos de implementación	0	CI = 720840
Costo de implementación	720840	
Precio de costo	3.113241772	Para obtener el precio de costo se realiza mediante el siguiente cálculo:
		Precio de costo = Costo de implementación / # de unidades
		PC = 720840 / 231542
		PC = 3,11
		En este caso de estudio se considera utilidad a los siguientes costos:
		Utilidad = Tarifa cobrada por el BCE por tansacción (cobro) - Pago realizado por el BCE a operadoras telefónicas
		Tarifa cobrada por el BCE por transacción = 0,02
		Comisión pagada por el BCE a operadoras telefónicas = 0,0075
		Utilidad por transacción = 0,02 - 0,0075
		Utilidad por transacción = 0,0125
		Valor que representa un ingreso al BCE

6. CONCUSIONES Y RECOMENDACIONES.

6.1. CONCLUSIONES

- El sistema de dinero electrónico en el Ecuador fue idealizado como una herramienta de inclusión financiera y agilización de transacciones monetarias entre los diferentes actores como personas e instituciones, por tal motivo el pago de transporte público se convierte en un pilar importante para el desarrollo de la tecnología.
- El pago de transporte público y otras transacciones monetarias que utilicen tecnología NFC deben tomar en cuenta el elemento seguro, para de esta forma evitar fraudes en las transacciones.
- Las tarifas que actualmente cobra el BCE deben ser analizadas y previo un estudio eliminar para el caso de cobro en el transporte público con el fin de masificar el servicio sin afectar a los diferentes actores es decir usuarios y operadoras de transporte público.
- El hardware y el software de la plataforma de dinero electrónico permite garantizar la disponibilidad del servicio, debido a su arquitectura redundante; la seguridad a nivel tecnológico tiene grandes ventajas ya que intervienen tres actores: en primer lugar el operador telefónico que brida la red GSM y garantiza la seguridad de transacciones mediante autenticación de usuario y cifrado de información; como segundo componente el Banco Central del Ecuador que en el registro de suscriptores se comunica con otras instituciones públicas para validar la información y evitar fraudes en las aperturas de cuenta, además de proporcionar un PIN para la realización de transacciones; y como último actor es el usuario, cuya responsabilidad radica en mantener su PIN de forma personal, confidencial e intransferible.

6.2. RECOMENDACIONES

- Se recomienda al Banco Central del Ecuador como el ente principal del sistema de dinero electrónico, socializar e incentivar el uso de la plataforma, de tal manera que el usuario pueda conocer y comprender las ventajas del uso del dinero electrónico.
- Se recomienda hacer uso de medios electrónicos de pago para agilizar la economía de la sociedad y evitar el uso de billetes físicos ya que el Ecuador al poseer una moneda extranjera le cuesta la importación y canje de billetes.
- Se recomienda implementar constantemente nuevas funcionalidades en la plataforma de dinero electrónico, de manera que permita realizar mejoras en cuanto a su arquitectura y al avance de la tecnología.

BIBLIOGRAFÍA.

Balarezo, V. (02 de 11 de 2014). *SISTEMA DE DINERO ELECTRÓNICO EN EL ECUADOR.* Recuperado el 16 de 06 de 2016, de http://comunidad.todocomercioexterior.com.ec/profiles/blogs/sistema-de-dinero-electr-nico-en-el-ecuador-1

Bueno M.V., P. P. (11 de 04 de 2011). *Artículo Científico La tecnología NFC y sus aplicaciones en un entorno.* Recuperado el 08 de 06 de 2016, de http://repositorio.upct.es/bitstream/handle/10317/2494/2.1.pdf%202011;jsessionid=E85CAAE5191FE110F9F2FA045B592B46?sequence=1

Ecuador, B. C. (2014). *Sistema de Dinero Eletrónico*. Recuperado el 28 de 06 de 2016, de http://www.scpm.gob.ec/wp-content/uploads/2014/01/2.6-Fausto-Valencia-BCE-Sistema-de-dinero-electr%C3%B3nico.pdf

Ecuador, M. (23 de 05 de 2016). ¿Qué es el dinero electrónico y cómo se usa en Ecuador ? pág. 1.

J, N. (13 de 02 de 2015). *MPACTO ECONÓMICO DE LA IMPLEMENTACIÓN DE SISTEMA DE DINERO ELECTRÓNICO EN EL ECUADOR.* Recuperado el 23 de 06 de 2016, de http://www.eumed.net/cursecon/ecolat/ec/2015/dinero-electronico.html

López M., E. J. (09 de 02 de 2012). *NFC el avance imparable del pago por móvil*. Recuperado el 10 de 06 de 2016, de file:///C:/Users/Lisita/Downloads/Art%C3%ADculo%20NFC%20SIC.pdf

Marcombo, S. (1998). *Telecomunicaciones Móviles.* Barcelona: Segunda Edición.

Plus, P. H. (2012). *Modulo formativo Universitario de creación de empresas de base tecnológica.* Quito: Fundación Universidades Castilla y León.

Transermobile. (2011). *Aplicacione NFC.* Recuperado el 10 de 06 de 2016, de http://transermobile.com/nfc

Zaragoza, A. (08 de 02 de 2016). *Tecnología NFC aplicada a la banca móvil.* Recuperado el 24 de 06 de 2016, de http://www.aratecnia.es/seguridad-tecnologia-nfc-banca-movil/