ANÁLISIS TEÓRICO DE LOS REQUISITOS DE SEGURIDAD Y USO DEL DINERO ELECTRÓNICO EN EL ECUADOR

THEORETICAL ANALYSIS OF THE REQUIREMENTS OF SAFETY AND USE OF ELECTRONIC MONEY IN ECUADOR

(Entregado 19- 08-2016 –Revisado 10 – 10 - 2016)

EDUARDO PATRICIO CANDO SALAS
Ingeniero en Informática, Universidad Católica del Ecuador. Maestrante en Auditoria de Tecnologías de la Información, Universidad de Especialidades Espíritu Santo – Ecuador.

MARCO ANTONIO YANDUN VELASTEGUÍ
Magíster en Sistemas Informáticos Educativos, Universidad Israel – Ecuador. Master Degree in Distance Education, Caribbean International University – Curazao. Licenciado en Sistemas Computacionales, Universidad Autónoma de los Andes - Ecuador. Maestrante en Auditoria de Tecnologías de la Información, Universidad de Especialidades Espíritu Santo - Ecuador

Cooperativa de Ahorro y Crédito "Tulcán"
Universidad Politécnica Estatal del Carchi (UPEC - ECUADOR)

patricio.cando@live.com
yandunmarco@gmail.com

Resumen

En este artículo se realiza un análisis teórico de los aspectos relevantes de la seguridad que utiliza el Sistema de Dinero Electrónico en base a los requisitos legales y técnicos;señalando los roles del Banco Central del Ecuador, Macro Agentes, Centros de Transacción y finalmente los usuarios, como actores principales del Sistema de Dinero Electrónico, los posibles riesgos y amenazas tecnológicas a los cuales están expuestos, como medida de prevención en el uso de los servicios de esta nueva forma de pago; otorgando así al usuario los conocimientos básicos de protección de la información, así como también sensibilizar a los macro agentes, centros de transacciones y operadoras móviles a implementar software y talento humano apropiados, generando una cultura organizacional que involucre estándares internacionales de seguridad; provocando que cada cual en su ámbito de acción incentiven al uso del dinero electrónico con el conocimiento y los controles de seguridad de la información adecuados.

Palabras clave: *Seguridad, Riesgos, Estándares, Controles, Inclusión Financiera*

Abstract

This paper presents the theoretical analysis of the relevant aspects of security that uses the electronic cash system based on the legal and technical requirements are carried out; indicating roles of the Banco Central Ecuador, Macro Agents, trading centers and ultimately users, as main actors of system of electronic money, potential risks and technology to which threats are exposed, as a preventive measure in use services of this new form of payment; thus giving the user the basic knowledge of data protection, as well as macro sensitizing agents, transaction centers and mobile operators to deploy software and appropriate human talent, creating an organizational culture that involves international security standards; causing each within its own sphere of action encourage the use of electronic money with the knowledge and security controls adequate information.

Keywords: Security, Risks, Standards, Controls, Financial Inclusion
.

1. Introducción

El Ecuador dentro del desarrollo tecnológico ha incursionado en una nueva forma de pago llamada Dinero Electrónico; cabe indicar que nuestros ancestros utilizaban intercambio a base de pepas de cacao, monedas, billetes, cheques, tarjetas de débito/crédito, transferencias electrónicas (BCE, s.f.). Por consiguiente el Gobierno Nacional con la implementación de esta nueva forma de pago impulsa la inclusión financiera, atendiendo a los sectores excluidos y aprovechando la tecnología (de Olloqui, Andrade, & Herrera, 2015). Ahora el 40% de la población económicamente activa (PEA) no está incluida financieramente; es decir, no forma parte activa del sistema financiero nacional, se estima una población de 2'800.000 ciudadanos que serán incluidos al sistema financiero ecuatoriano.(BCE, s.f.).

Ante aquello es importante citar que existen 16,9 millones de líneas de telefonía móvil; 13,8 millones son prepago y 3,1 millones son post pago (Zauzich, 2015), con estos antecedentes se avizora el uso masivo del Dinero Electrónico; en consecuencia el Banco Central del Ecuador (BCE) asume la implementación del Sistema de Dinero Electrónico(SDE) según Resolución No.005-2014-M de la Junta de Política y Regulación Monetaria y Financiera(Junta de Política y Regulación Monetaria y Financiera, 2014).

Con la finalidad de viabilizar los objetivos de inclusión financiera, el Ecuador luego de una licitación con varias empresas internacionales adquiere el software llamado In Switch Solution, una aplicación informática que gestionará las transacciones electrónicas, esta plataforma ya opera en Paraguay y cubrirá a toda la población del territorio ecuatoriano. (Perea, 2014).

El presente estudio se encamina a realizar un análisis de la seguridad y uso que utiliza el Sistema de Dinero Electrónico (SDE), basado en el estándar GSM y el protocolo de comunicación USSD, Servicios web, protocolos SSL, redes privadas virtuales y acuerdos legales, respecto a los actores que interactúan mediante la digitación del comando *153#, desde el teléfono celular y la incorporación de Software de aplicación, que permita integrar al SDE con los llamados Macro Agentes, los cuales iniciarán sus operaciones de carga y descarga de dinero físico a electrónico y viceversa, en coordinación con sus centros de transacciones, generando así que el SDE se fortalezca

y empiece a masificarse(BCE, s.f.). En beneficio de los miles de usuarios que utilizarán este sistema y su nueva forma de pago.

Se realiza un análisis básico respecto a las posibles amenazas de pudieren afectar a los servicios del sistema de dinero electrónico a razón de experiencia de otras realidades y poner énfasis en disponer de los controles adecuado para cubrir ciertas vulnerabilidades.

2. Marco Teórico

2.1. Dinero Electrónico

(Villalva, s.f.) "explica que el dinero electrónico es un medio de pago electrónico que permite hacer transacciones con un menor costo y en un menor tiempo".

2.2. Sistema de Dinero Electrónico (SDE)

Es el conjunto de operaciones, mecanismos y normativas que facilitan los flujos, almacenamiento y transferencias en tiempo real, entre los distintos Agentes Económicos, a través del uso de: dispositivos electrónicos, electromecánicos, móviles, fijos, tarjetas inteligentes, computadoras y otros que se incorporen como producto del avance tecnológico (Junta de Política y Regulación Monetaria y Financiera, 2014)

La Plataforma de software Multi-Service-Center, garantizará la operación del dinero electrónico integrado con protocolos USSD, el estándar de conectividad GSM y la SIMCARD (SIM), con las debidas seguridades, controles anti fraude, consumos de servicios web que integran a los diferentes macro agentes, operadoras móviles y así proveer del servicio sin fines de lucro (IN Switch Solutions).

2.3. Seguridad de las transacciones realizadas mediante celular.

Para que un usuario que disponga de un celular acceda a los servicios del SDE, se analiza la arquitectura tecnológica y la seguridad con cada actor tecnológico así:

2.3.1. Tarjeta SIM (Módulo de Identificación de Usuario), es una tarjeta inteligente que almacena datos personales, número de línea celular y puede ser utilizado en otro celular mediante la red GSM (Movistar, s.f.). Sin embargo, al disponer de información sensible en este dispositivo, es indispensable protegerla ante posibles riesgos en caso de extraviarse; de manera que al adquirir una línea telefónica consecuentemente se debe activar el código PIN de la tarjeta SIM diferente a 1234 que es la del fabricante, así nadie podrá utilizar el teléfono o la tarjeta SIM en otro dispositivo móvil (Savitsky, 2014).

2.3.2. Servicio Suplementario de Datos no estructurados (USSD), es un servicio orientado a activar una sesión donde su uso es continuo, es decir la conexión finaliza por el tiempo de inactividad o cierre del usuario (Kasera & Narang, 2004).Respecto a la seguridad, Los datos tecleados en la sesión establecida no se guardan en el teléfono celular, cuando existe sesión abierta la señal no es interceptada por otros dispositivos móviles, ya que se establece una conexión exclusiva entre la tarjeta SIM y el operador móvil sin necesidad del servicio de internet.

En efecto la operación del servicio y acceso al SDE corresponde en digitar la siguiente sintaxis el símbolo * luego el número del servicio en este caso el 153 y finalmente el símbolo #, luego de ello si no se encuentra matriculado el usuario el sistema le solicita activar una cuenta de dinero electrónico, al aceptar el servicio le solicita sus datos personales, el sistema le asigna una clave temporal, para en su primer ingreso registrar una clave definitiva que solo el usuario debe conocer; si se encuentra ya matriculado en el sistema, le aparecerá un menú para realizar sus transacciones, otorgando así más criterios de seguridad lo que se sabe "la clave", lo que se tiene "número de celular", y lo que se es "cédula atada al celular" (BCE, s.f.).

En Ecuador existen tres operadoras móviles: Movistar, Claro y CNT, ésta última como empresa de telefonía pública; las cuales cubren todo el territorio nacional, de manera abierta y digital, soportado los servicios de USSD, SMS, para que las operadoras sean parte del SDE, éstas deben suscribir el Acuerdo de Conexión (ACO) en donde se detallan todas las condiciones Legales. (Junta de Política y Regulación Monetaria y Financiera, 2014), a través del Sistema Global de Comunicaciones (GSM), que es un estándar internacional de comunicaciones móviles el cual permite integrar a millones de usuarios en forma local y roaming mundial otorgando servicios de alta calidad en trasmisión de datos, voz, video (Fernández Gómez, 2004).

Por esta razón en un sistema GSM las funcionalidades de seguridad básicas son: el cifrado de los enlaces de radio, la protección de la identidad y autenticación del usuario, con la finalidad de evitar accesos no autorizados, prevenir intrusiones y localización por medio de un actor externo (Marcombo S.A, 1998).

2.4. Seguridad de las transacciones realizadas entre el SDE y los Macro Agentes.

El BCE ha considerado cubrir el mercado mediante los denominados Macro Agentes y los centros de transacción; los cuales pueden operar si han cumplido con lo solicitado en el acuerdo de Macro Agente debidamente legalizado entre las partes, aquí se detallan los aspectos operativos, funcionales y tecnológicos para que los usuarios puedan realizar carga y descarga de dinero (Junta de Política y Regulación Monetaria y Financiera, 2014).

La carga corresponde entregar dinero físico en el Centro de transacción y a su vez colocar el mismo valor electrónico en el monedero; como medida de seguridad, para realizar esta transacción se la realiza presentando la cédula y número de celular que corresponde al monedero o registro virtual asociado a una única cuenta de dinero electrónico, que dispone de un valor máximo de transacción hasta 200 dólares. La carga corresponde a la manera inversa del proceso indicado; cabe indicar que se adiciona un número de control remitido vía SMS al celular del usuario, el cual debe entregar al centro de transacción para que pueda recibir dinero físico; así se genera un factor de seguridad y confirmación de la transacción (BCE, s.f.).

Sin embargo, para ejecutar estas transacciones, existen dos formas de operar:

Si el Macro Agente no tiene la capacidad de integrar su aplicación al SDE, el BCE proveerá de credenciales y accesos vía internet, para que pueda operar el centro de transacción; el cual deberá

cumplir con ciertos requisitos básicos como son: antivirus, conexión a internet 512 Kbps, celular con servicios de SMS y USSD e impresora opcional en caso de entrega de recibos.
Ahora para el caso de que el Macro Agente si disponga de la capacidad de integrarse al SDE; éste debe adquirir, desarrollar o definir su Aplicación de Gestión del Dinero Electrónico, que para nuestro caso de estudio lo definiremos (AGDE). Esta aplicación debe interconectarse mediante una Red Privada Virtual (VPN), disponer de una capa de protección segura SSL y así consumir los servicios web (BCE, s.f.). Los servicios web ofrecen un sinnúmero de aplicaciones y tecnologías que permiten lograr una interconexión entre sistemas heterogéneos a partir de la publicación y solicitud de consumo acordada, usando los protocolos http/https de comunicación web de manera estándar e interactiva, especificando la sintaxis y los mecanismos de intercambio de información (The Word Wide Web Consortium, s.f.).

De esta forma los servicios web del SDE, proveen de conexiones a varias aplicaciones heterogéneas; es decir, el AGDE consumirá estos servidos web de manera independiente, una vez que el Macro Agente firme el Acuerdo de Confidencialidad de la Información y el BCE provea de la normativa técnica de conectividad y consumo de servicios web (BCE, s.f.)Por otra parte debe considerarse la construcción de web services seguros, que permitan proteger la información que se intercambia entre entidades; a fin de cumplir con los principios de seguridad como son: autenticación, autorización, confidencialidad, integridad y disponibilidad, aplicando principios de auditoría y trazabilidad en las transacciones (Web Service Interporability Organization, 2010).

Otro de los requisitos de interconexión y consumo del SDE y la AGDE es la utilización de una VPN, con la finalidad de que se cree un túnel seguro, encriptado, autorizado y restringido con su respectivo registro de actividad (Colobran Huguet, Arqués Soldevila, & Galindo, 2008).

Para otorgar mayor seguridad, SSL es un protocolo de seguridad que puede utilizarse entre las dos entidades y es responsable de dotar de autenticación confidencialidad e integridad en la trasmisión de la información de los servicios web utilizados. En Ecuador el BCE, provee de los certificados SSL como entidad certificadora calificada; este certificado debe estar registrado en el servidor físico, donde se alojará en la AGDE con la finalidad de garantizar la fiabilidad de dicha conexión y protección de la misma (GlobalSign, s.f.).

Para el caso de este estudio, el dinero electrónico esta soportado por dinero físico; es decir, 1 dólar electrónico equivale a 1 dólar físico, de manera que la seguridad física también se refleja en seguridades electrónicas equivalentes al dinero físico. (BCE, s.f.), por consiguiente, la homologación física electrónica es posible en cualquier moneda, según el país que quiera adoptar seguridades.

Se considera de alta importancia dentro del proceso de aseguramiento del dinero electrónico el algoritmo criptográfico asimétrico, el cual se basa en Rivest-Shamir-Adleman(RSA), de gran aceptación respecto a las características que posee (Stallings, 2003). “La criptografía permite a las personas confiar en los sistemas para poder pasar del mundo físico al mundo electrónico, permitiéndoles así hacer negocios electrónicamente sin miedo al engaño y al fraude” (pág. 8) (García León, 2005).

2.5. Posibles Riesgos Tecnológicos en Dinero Electrónico

Es importante detallar algunos riesgos que pueden afectar al funcionamiento del sistema de dinero electrónico, en pos de que el usuario pueda prevenir algún ataque o denegación de servicio. Los ciber delincuentes se enfocan en obtener dinero e información confidencial de los usuarios en cuentas bancarias, contactos, SMS, a través de la instalación de spyware en dispositivos móviles. Un claro ejemplo de ataques sofisticados de denegación de servicios a la infraestructura es el caso de BITcoin (McAfee, 2013).

Por consiguiente, Bitcoin al ser una moneda electrónica y popular es la más afectada en Ciber ataques, pueden ejecutarse códigos maliciosos en su infraestructura con la finalidad de descubrir la generación y creación de monedas o el robo directo de las billeteras electrónicas (Guojon, 2013).

El uso de protocolos de comunicación USSD especialmente de los Smartphone conectados al internet están expuestos a recibir ataques por ejecución secuencias de comandos java entre páginas web y así robar información de claves, datos personales, obtener una sesión activa del usuario y conectarla a tecnología maliciosa.

3. Discusión, Análisis, Propuesta

Una vez conocidas las normas, requisitos, seguridades y operatividad del Dinero Electrónico, tomando como base la experiencia de otros países, el Gobierno ha invertido en un sistema que cuenta con estándares internacionales de seguridad de la información que de alguna manera genera confianza a los usuarios en la utilización de esa nueva forma de pago.

Los locales comerciales del país aún no están en la capacidad de operar y desconocen las seguridades que se debe implementar, y esta limitante se considera un retraso en la implementación, sin embargo, pueden operar con el SDE de manera directa con requisitos legales y técnicos mínimos de operación.

Las AGDE tienen un costo de desarrollo, implementación del sistema, cumplimiento de recursos humanos, tecnológicos, legales, operativos, los cuales deben acoplarse y monitorizarse en base a las políticas de la entidad de control, en este caso el BCE y los Macro Agentes, que a su vez deben implementar seguridades en sus sistemas internos, adoptar medidas de seguridad, ya que pueden ser puntos vulnerables de fuga de información. Por parte de los Macro Agentes deben asumir el riesgo de ciber ataques, asegurar transacciones con pólizas seguros, estar en constante actualización de herramientas de monitoreo y seguimiento de incidentes de seguridad en base a eventos presentados.

4. Conclusión

En este trabajo se ha presentado un análisis teórico de los requisitos de seguridad, para que los usuarios tengan los conocimientos de protección de la información en el uso del dinero electrónico.

Por otra parte, concienciar a los macro agentes, centros de transacciones y operadoras móviles en su ámbito de acción, para que incentiven al uso del dinero electrónico con los controles de seguridad de la información adecuados. Esto conlleva a que las áreas financieras y el manejo del

dinero puedan transaccionar de manera directa y segura minimizando algunos riesgos que pueden afectar al usuario final.

BIBLIOGRAFÍA Y LINKOGRAFÍA

- BCE. (s.f.). *Dinero Electrónico*. Recuperado el 10 de Ago de 2015, de Dinero Electronico: http://www.dineroelectronico.ec
- Colobran Huguet, M., Arqués Soldevila, J. M., & Galindo, E. M. (2008). *Administración de sistemas operativos en red.* UOC. Recuperado el 10 de Ago de 2015, de https://books.google.com.ec/books?id=w4utLelkYgkC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- de Olloqui, F., Andrade, G., & Herrera, D. (01 de Jun de 2015). *Inclusión financiera en América Latina y el Caribe: Coyuntura actual y desafíos para los próximos años*. Recuperado el 01 de Jun de 2015, de Banco Interamericano de Desarrollo: http://publications.iadb.org/handle/11319/6990
- Fernández Gómez, E. (2004). *Conocimientos y aplicaciones tecnológicas para la dirección comercial.* ESIC.
- García León, M. (2 de Dic de 2005). Generación de Billetes Digitales Anónimos. *Instituto Politécnico Nacional*. Mexico D.F.
- GlobalSign. (s.f.). *Centro de Información SSL*. Recuperado el 14 de Ago de 2015, de Global Sign GMO INTERNET GROUP: https://www.globalsign.es/centro-informacion-ssl/que-es-un-certificado-ssl.html
- Guojon, A. (22 de Jul de 2013). *Bitcoins, Litecoins, Namecoins y cómo roban dinero electrónico en Internet*. Recuperado el 15 de Ago de 2015, de welivesecurity: http://www.welivesecurity.com/la-es/2013/07/22/bitcoins-litecoins-namecoins-como-roban-dinero-electronico-internet/
- IN Switch Solutions. (s.f.). *Multi-Service Center.*Recuperado el 01 de Ago de 2015, de Demo Center: http://www.inswitch.us/index.php/demo-center/94-contenido-paginas/249-videomsc
- Junta de Política y Regulación Monetaria y Financiera. (06 de Nov de 2014). *Resoluciones Junta de Política y Regulación Monetaria y Financiera.* Recuperado el 14 de Ago de 2015, de Junta de Política y Regulación Monetaria y Financiera: http://www.juntamonetariafinanciera.gob.ec/resolucion_M.html?dl=0
- Kasera, S., & Narang, N. (12 de 09 de 2004). *3G Networks Architecture, Protocols and procedures.*Tata McGraw-Hill. Obtenido de Todo es Electrónico: https://books.google.com.ec/books?id=b5d0_au-z9MC&printsec=frontcover&hl=es#v=onepage&q&f=false
- Marcombo S.A. (1998). *Telecomunicaciones Móviles.* Barcelona: Marcombo.
- McAfee. (2013). *Informe de McAfee sobre Amenazas.* Madrid. Obtenido de http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q2-2013-summary.pdf

- Movistar. (s.f.). *Que es una SimCard de Movistar*. Recuperado el 01 de Ago de 2015, de Equipos: http://www.movistar.com.ve/particulares/ayuda/preguntas_frecuentes/equipos.asp#.VcwUafn1KJ8
- Perea, A. (17 de Jun de 2014). Si logramos un ecosistema con dinero electrónico va a ser un excelente negocio. (G. Losa, Entrevistador)
- Savitsky, A. (17 de Nov de 2014). *Por qué la Seguridad de las SIM-cards Importa*. Recuperado el 14 de Ago de 2015, de KASPERSKY Lab DAILY: https://blog.kaspersky.com.mx/por-que-la-seguridad-de-las-sim-cards-importa/4541/
- Stallings, W. (2003). *Fundamentos de seguridad en redes Aplicaciones y Standares 2da Edicion.* Pearson Educación. Recuperado el jul de 2015
- The Word Wide Web Consortium. (s.f.). *Guía Breve de Servicios Web*. Obtenido de W3C España: http://www.w3c.es/Divulgacion/GuiasBreves/ServiciosWeb
- Villalva, M. (s.f.). *Dinero Electrónico*. Obtenido de Dinero Electrónico.
- Web Service Interporability Organization. (09 de Nov de 2010). *Basic Profile Version 1.2*. Obtenido de Web Service Interporability Organization: http://ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html
- Zauzich, I. (07 de Jul de 2015). *El ABC del dinero electrónico*. Obtenido de Cobiscorp Blog | Innovación Financiera A Tu Alcance: http://blog.cobiscorp.com/abc-del-dinero-electronico