EASYSOLUTIONS

SUDEBAN 641-10, REGULACIÓN SOBRE LOS SERVICIOS ELECTRÓNICOS EN VENEZUELA

COMO CUMPLIR CON LA NORMA Y PROTEGER SU NEGOCIO DE FORMA FÁCIL Y EFECTIVA

Resumen

Con el auge de los servicios electrónicos, nuevos retos de seguridad han aparecido para las instituciones financieras latinoamericanas. Los gobiernos cada vez toman un rol más activo estableciendo normas y regulaciones para elevar los niveles de seguridad y proteger a los usuarios. La resolución 641-10 de Sudeban es un ejemplo de este tipo de normativas, que aunque de gran utilidad pueden resultar complejas para las instituciones financieras.

Easy Solutions, es experta en protección contra fraude electrónico, y ofrece sus productos, servicios y experiencia para ayudar a los bancos a cumplir con reglamentaciones como la de Sudeban, fortaleciendo la seguridad de la información y mejorando la relación banco – usuarios.

TABLA DE CONTENIDO

EL MARCO REGULATORIO ANTI-FRAUDE ELECTRÓNICO EN LATINOAMÉRICA

1

El auge de las nuevas tecnologías para la descentralización de los servicios bancarios ha traído mayor conveniencia a los usuarios, pero también han generado mayores riesgos de seguridad. Es así como la seguridad informática ha tomado gran importancia en el contexto financiero global y latinoamericano en los últimos años. Términos como phishing, pharming, detección de vulnerabilidades, autenticación de múltiples factores, firmas digitales, medidas biométricas, calificación de riesgo transaccional y detección de fraude son ahora términos comúnmente escuchados por las instituciones financieras que buscan cumplir con las reglamentaciones de seguridad y ofrecer a sus usuarios confiabilidad y efectividad en los medios electrónicos.

Los gobiernos latinoamericanos han impulsado la adopción de estándares internacionales que brindan mayor seguridad en las operaciones financieras, por medio de decretos y resoluciones que buscan regular los servicios de banca electrónica en la región. Algunos ejemplos de estos estándares son el PCI-DSS, marco de referencia para la protección de datos y prevención de fraudes con tarjetas débito y crédito, y el EMV, conjunto de especificaciones de tarjetas con chip para sistemas de pago desarrollado por Europay, Mastercard y Visa.

Otro estándar que está siendo adoptado por la industria en la región es el de Factores Adicionales de Autenticación, que incluye el uso de claves de un sólo uso u OTP (One Time Password), imágenes de seguridad, medidas biométricas, etc. El uso de este tipo de mecanismos permite a los usuarios de la banca ingresar de forma más segura a las plataformas electrónicas de sus instituciones financieras.

A pesar de estas iniciativas, aun hacen falta más pronunciamientos de las autoridades bancarias de los diferentes países, que sirvan tanto para regular los servicios bancarios vía electrónica, como para guiar a las instituciones financieras en la prevención y lucha contra las prácticas fraudulentas que atentan contra la seguridad de la información. Algunos países latinoamericanos ya han fijado estándares y regulaciones para la prestación segura de los servicios de banca electrónica. No obstante, gran parte de la región sigue atrasada en materia de legislación sobre seguridad, confidencialidad y protección de la información sensible.

Un ejemplo de esto es Argentina, donde la regulación de la banca electrónica aún se encuentra en desarrollo. La Ley 26.637 de 2010 [1] contempla las medidas mínimas a implementar en las sucursales y cajeros electrónico de los bancos. En cuanto a sanciones para las actividades fraudulentas en los medios electrónicos, el país cuenta con la Ley 26.388 [2], que se establece las penas para aquellos que accedan de manera ilegal a los sistemas de información públicos o privados, compartan o utilicen información con fines criminales.

México, uno de los países más avanzados de

EL MARCO REGULATORIO ANTI-FRAUDE ELECTRÓNICO EN LATINOAMÉRICA

1

Latinoamérica en banca electrónica, expidió la Circular Única de Bancos [3], donde se establecen procedimientos de identificación y autenticación de usuarios de servicios electrónicos y las responsabilidades de los bancos en cuanto a adopción de medidas de seguridad.

En Panamá, el Acuerdo No. 5 [4] y la más reciente Ley de Tarjetas de Crédito [5], definen las características de la banca electrónica, campos de acción, servicios y responsabilidades con los clientes, en cuanto al manejo, uso y protección de la información. Las Unidades de Riesgo de los bancos tienen el deber de identificar, evaluar y controlar los riesgos asociados al servicio de banca electrónica, adoptando métodos para la verificación de la identidad de los clientes y la preservación de la confidencialidad y seguridad de la información.

La Superintendencia Financiera de Colombia [6], se pronunció sobre varios temas de seguridad informática que incluyen: detección de vulnerabilidades, banca por internet, implementación EMV en puntos de pago (POS), sistemas de audio respuesta IVR, entre otros. La Superintendencia define los requerimientos mínimos que toda entidad financiera debe adoptar, entre ellos: hardware y software apropiados; gestión de la seguridad de la información (estándares ISO 17799 y 27001), medidas de protección contra software malicioso, identificación y autenticación en los dispositivos y sistemas de cómputo, implementación de tecnología contra amenazas como keyloggers y screenloggers y elaboración de perfiles de costumbres transaccionales.

En Ecuador aún no hay reglamentaciones específicas sobre servicios de banca, pero el uso de mensajes de datos, firma electrónica, servicios de certificación, prestación de servicios electrónicos, comercio electrónico y mecanismos de protección de los usuarios se encuentra regulado [7].

En marzo de 2010, la Superintendencia de Banca, Seguros y AFP del Perú presentó un panorama de la situación de la banca electrónica en ese país [8]. La Circular Nº G- 140 [9] establece que las transacciones en medios electrónicos deben contar con esquemas de autenticación de mínimo dos factores. Para transacciones en Internet, uno de dichos factores deberá ser de generación o asignación dinámica.

Por último, una de las reglamentaciones más completas y recientes de Latinoamérica es la de Venezuela. La Superintendencia de las Instituciones del Sector Bancario (Sudeban) emitió la resolución 641-10 del 31 de diciembre de 2010, que consigna las normas que regulan el uso de los servicios de la Banca Electrónica. En esta resolución se incluye, entre otras medidas de seguridad, la necesidad de adoptar factores de autenticación múltiples para la protección de datos durante cualquier transacción electrónica.

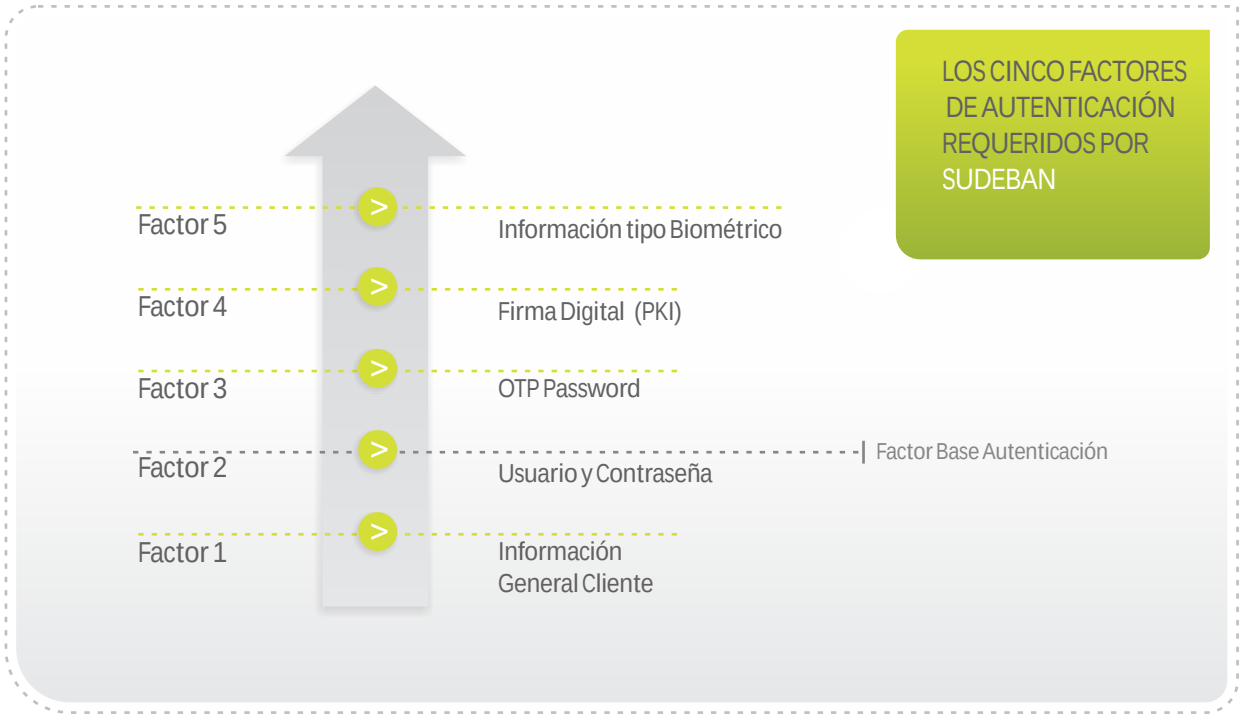
LA REGLAMENTACIÓN 641-10 DE SUDEBAN

2

El 23 de diciembre de 2010, la Superintendencia de Instituciones del Sector Bancario (Sudeban) emitió la resolución 641-10, que regula el uso de los servicios de la banca electrónica en Venezuela. Esta resolución contiene los mecanismos de autenticación requeridos para incrementar la seguridad de los clientes de la banca electrónica ante el creciente número de fraudes electrónicos.

Se han establecido cinco tipos de factores, que deben ser incorporados en las operaciones electrónicas, dependiendo del nivel de seguridad requerido:

- Factor 1: Información obtenida de la ficha del cliente.
- Factor 2: Usuario y contraseña conocida por el cliente.
- Factor 3: Claves dinámicas OTP (tokens).
- Factor 4: Firmas electrónicas certificadas y emitidas a nombre del cliente.
- Factor 5: Información de tipo biométrico.



LA REGLAMENTACIÓN 641-10 DE SUDEBAN

2

Antes de la resolución, la autenticación de usuarios empleaba el factor tipo 2 (usuario y contraseña), que era suficiente para realizar la mayoría de operaciones en línea. Con la emisión de esta resolución, el factor mínimo exigido por Sudeban para iniciar sesión en la banca electrónica continua siendo el tipo 2, pero para realizar cualquier tipo de transacción que involucre movimientos de dinero o modificación de información de la cuenta, se exige un factor de tipo 3, 4 o 5. (OTPs, firmas electrónicas o información biométrica).

La siguiente gráfica ilustra los factores de autenticación adicionales requeridos según el tipo de operación:

Tipo de Operaciones y Factores de Autenticación Requeridos	Factor Autenticación Requerido (antes circular 641-10)	Factor Autenticación Adicional Requerido (circular 641-10 por SUDEBAN)
Afiliación y desafiliación de productos y servicios	2	3,4,5
Mantenimiento de productos y servicios programados de pago	2	3,4,5
Pagos o transferencias electrónicas a terceros	2	3,4,5
Retiros o adelantos en efectivo	2	3,4,5
Aperturas de segundas cuentas o productos financieros	2	4
Actualización de datos de la ficha de cliente a través banca por internet	2	4
Mantenimiento de contraseñas, activación o desactivación de tarjetas	1,2	N/A
Consultas	2	N/A
Transacciones ofrecidas a traves de dispositivos de autoservicio	2	N/A
Pagos o transferencias electrónicas mismo titular y mismo banco.	2	N/A

* Muestra los factores actuales y los adicionales que son requeridos con la resolución 641-10

Factor de autenticación	
1	Información de la ficha del cliente
2	Clave y contraseña conocida por el cliente
3	Clave de un solo uso (Dispositivo OTP)
4	Firma Digital emitida a nombre del cliente (PKI)
5	Medida biométrica

LA REGLAMENTACIÓN 641-10 DE SUDEBAN

2

Los bancos y demás instituciones del sector bancario deben planear y cumplir con la implementación de los factores adicionales de autenticación requeridos para cada canal transaccional y servicio específico, de acuerdo con los plazos establecidos por la Superintendencia:

- Primera etapa: envío de un plan de trabajo a Sudeban, que incluye información detallada sobre la tecnología escogida y el plan de implementación (a entregar en un plazo máximo de cuatro meses después de la entrada en vigencia de la normativa).

- Segunda etapa: proceso de implementación (en un plazo de 18 meses adicionales, contados a partir de la entrega del informe mencionado en la primera etapa).

Según esta reglamentación, los bancos y demás instituciones del sector financiero también adelantar campañas educativas para asegurar que los usuarios estén al tanto de las medidas de seguridad implementadas y para que conozcan la forma como funcionan los diferentes canales electrónicos.

COMO EASY SOLUTIONS LE AYUDA A CUMPLIR CON LA REGLAMENTACIÓN

3

Easy Solutions, el único proveedor de seguridad enfocado exclusivamente en protección contra fraude electrónico, puede ayudar a los bancos a proteger su negocio y clientes y a la vez a cumplir con la normatividad 641-10 de Sudeban.

Detect ID de Easy Solutions es una solución de autenticación multi-factorial que extiende el proceso de autenticación hasta el dispositivo donde las transacciones son efectuadas, capturando información específica del dispositivo que después es utilizado como token válido de autenticación. Esta solución se integra de forma rápida y sencilla con factores adicionales de autenticación como tarjetas de coordenadas, OTPs, SMS-OTP y tokens (propietarios y de terceros), factores que son exigidos para la realización de diferentes transacciones electrónicas por la resolución 641-10.

Detect ID también cuenta con un sistema de autenticación de sitios web por medio de una imagen de seguridad. Esta funcionalidad permite al usuario seleccionar una imagen que sólo él conoce, garantizando que el usuario identifique su sitio trasnacional y no introduzca sus datos en sitios fraudulentos.

La plataforma de Detect ID se integra fácilmente por medio de servicios web, reduciendo la cantidad de código que debe ser añadida en la aplicación actual. También permite el registro de los dispositivos habituales que el usuario utiliza para realizar sus transacciones, mediante la generación de una serie de preguntas de desafío que sólo el usuario conoce. Si el usuario responde correctamente, el dispositivo es incluido en la lista de confianza.

Otra de las características de Detect ID es el reporte de dispositivos fraudulentos. Cuando se detecta un dispositivo realizando actividades ilegales, su huella es ingresada a una lista negra institucional, permitiendo anticipar toda actividad fraudulenta y bloquear el dispositivo. Easy Solutions posee una lista negra a nivel global de dispositivos sospechosos, que contiene información valiosa que beneficia a todos los usuarios de Detect ID.

COMO EASY SOLUTIONS LE AYUDA A CUMPLIR CON LA REGLAMENTACIÓN

3

SUDEBAN NORMATIVA 641-10	SOLUCION OFRECIDA POR EASY SOLUTIONS
CAPITULO I DE LA AFILIACION, IDENTIFICACION Y LA AUTENTICACION DEL CLIENTE, EN LOSSERVICIOS DE LA BANCA ELECTRONICA. Artículo 5 Los Bancos y demás Instituciones financieras deberán utilizar los factores de autenticación para verificar la identidad de sus clientes y la cualidad de estos para realizar operaciones mediante la banca electrónica. Dichos factores serán los siguientes: Factor de autenticación 1: se compone de la información obtenida de la ficha del Cliente. Factor de autenticación 2: se compone de la contraseña que solo el cliente conoce. Factor de autenticación 3: claves dinámicas de uso único OTP (One Time Password) Factor de autenticación 4:firmas electrónicas (PKI) Factor de autenticación 5: información derivada de características biométricas.	Detect ID Autenticación multi-factorial y multi-canal.

Easy Solutions también ofrece a las instituciones financieras otros productos y servicios complementarios a Detect ID que permiten cumplir con los parámetros establecidos por la resolución 641.10 de Sudeban y mejorar al mismo tiempo la relación banco-cliente, proteger la información sensible y prevenir prácticas fraudulentas y crímenes electrónicos como phishing, pharming, ataques de ingeniería social, man-in the-middle, etc.

PROTECCIÓN
MÁS ALLÁ DE LA RESOLUCIÓN

4

"El problema NO es la resolución, es el creciente fraude electrónico"

Mediante la publicación de resoluciones que regulan los estándares y medidas de protección de datos, Sudeban ha contribuido de forma significativa con la modernización y seguridad de la banca electrónica de Venezuela. La adopción del estándar EMV en los canales electrónicos, es un ejemplo claro del compromiso de incrementar la cobertura de la banca de forma eficiente y segura. La Circular N° SBIF-DSB-II-GGTI-GRT-01907 junto con la resolución 641-10 de 2010, forman parte de la estrategia para el crecimiento de la banca electrónica y la reducción de las amenazas de fraude en los canales transaccionales.

Aunque las iniciativas adoptadas por Sudeban han sido importantes para lograr una mayor seguridad en el contexto electrónico, el sistema bancario se encuentra todos los días ante grandes retos que deben ser enfrentados de forma proactiva. Uno de ellos se deriva de la reciente adopción de los estándares PCI-DSS, que tiene como fin combatir la copia y uso fraudulento de las tarjetas débito y crédito. El éxito obtenido en el cumplimiento de este objetivo ha sido tal, que cada vez es más difícil encontrar fraudes con este tipo de tarjetas. En consecuencia, otros medios transaccionales menos protegidos como los canales presenciales, IVRs, la banca por internet y la móvil son los nuevos objetivos de los criminales.

Easy Solutions tiene una visión holística y multi-canal del fraude electrónico que permite a las instituciones financieras protegerse integralmente y estar un paso delante de los criminales. En la siguiente tabla se mencionan los retos de la banca en Venezuela ante amenazas de seguridad emergentes y las soluciones que ofrece Easy Solutions para enfrentarlas.

NECESIDAD ANTI-FRAUDE ELECTRONICO	SOLUCION OFRECIDA POR EASY SOLUTIONS
Pruebas de vulnerabilidades a la plataforma tecnológica	Detect Vulnerability Scanning Service
Monitoreo trasnacional	Detect TA
Perfiles transaccionales (Institucionales / perfiles de usuarios)	Detect TA
Anti-phishing/Anti-pharming)	Detect Monitoring Service, Detect Safe Browsing

PROTECCIÓN
MÁS ALLÁ DE LA RESOLUCIÓN

4

CUMPLA CON LOS ESTANDARES EXIGIDOS POR SUDEBAN Y PROTEJA SU NEGOCIO Y SUS USUARIOS EN UN SOLO PASO, CON LA ESTRATEGIA DE PROTECCION TOTAL CONTRA FRAUDE ELECTRONICO® DE EASY SOLUTIONS

Para más información, contáctenos o visite el sitio web de Easy Solutions:

www. easysol.net

David López
Business Development Manager
para la Region Andina
dlopez@easysol.net,
Tel: +571 - 7425570 Ext. 108
+57 301 728 21 31

REFERENCIAS

[1] Senado y Cámara de Diputados de la Nación Argentina. Ley 26.637 - Entidades financieras. Septiembre de 2010.

[2] Ley 26.388, mediante la cual se agregan los delitos informáticos al Código Penal argentino. Junio de 2008.

[3] Comisión Nacional de Bancos y Valores de México (CNBV). Circular Única de Bancos. Diciembre de 2005.

[4] Superintendencia de Bancos de Panamá. Acuerdo No. 5-2003. Junio de 2003

[5] Ley 81 de Tarjetas de Crédito. Diciembre de 2009.

[6] Superintendencia Financiera de Colombia. Circular Externa 052. 2007.

[7] Ecuador. Ley No. 2002-67 de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. 2002.

[8] Sotomayor V., Narda (Superintendencia de Banca, Seguros y APF del Perú). Presentación "Regulación para la banca móvil en Perú: una historia de progreso". Marzo de 2010.

[9] Superintendencia de Banca, Seguros y APF del Perú. Circular Nº G- 140. 2009

ACERCA DE EASY SOLUTIONS

5

Establecida en el 2002, con oficina principal en Sunrise, Florida, Easy Solutions Inc. es el único proveedor de seguridad enfocado exclusivamente en prevención del fraude, ofreciendo productos y servicios anti-phishing, anti-pharming, autenticación multi-factor y detección de transacciones anómalas.

Easy Solutions posee un enfoque integral para manejar la prevención del fraude multi-canal y trabaja en alianza con líderes de la industria de otras áreas de seguridad soportando un amplio rango de plataformas heterogéneas. Easy Solutions es miembro del Anti-Phishing Working Group (APWG) y de ABA (American Bankers Association).

Nuestras tecnologías y metodologías propietarias, junto con los esfuerzos permanentes en investigación nos permiten reaccionar y adaptarnos fácilmente a la aparición de nuevas amenazas.

EASYSOLUTIONS

Headquarters:
1401 Sawgrass Corporate Parkway, Sunrise, FL 33323
– Tel. +1-866-5244782
Latin America:
Cra. 13A No. 98 – 21 Of. 401 Bogotá, Colombia
– Tel. +57 1- 7425570

www.easysol.net