SEGURIDAD DE DATOS DE TARJETAHABIENTE APLICANDO NORMAS, REGULACIÓN Y BUENAS PRÁCTICAS.

Prieto Téllez, Diana Alexandra
dalexandrapt@gmail.com
Universidad Piloto de Colombia

***Resumen*—**El uso de tarjeta débito o crédito en distintos canales, incluyendo internet y aplicaciones móviles, implica una serie de controles que detallan las normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) que afecta a los comercios, entidades financieras o proveedores que almacenen, procesen o transmitan el número de tarjeta y datos sensibles de autenticación. Todo esto con el fin de proteger los datos de tarjetahabientes, y evitar el fraude, así, es importante saber la necesidad de estar a la vanguardia en seguridad, uniendo esfuerzos teniendo en cuenta las buenas prácticas y la regulación local.

***Índice de Términos*—**COBIT, fraude, ISO27001, PCI DSS, seguridad, titular de tarjeta, tarjetahabiente.

***Abstract*—**The use of credit or debit card on different channels including internet and mobile applications, involves a series of controls that detail the Data Security Standards for Payment Card Industry (PCI DSS) including merchants, financial institutions or providers that store, process or transmit the PAN and sensitive authentication data, all this in order to protect cardholder data and prevent fraud, so it is important to know the need to be at the forefront of security, by join forces considering the best practices and the local regulation.

***Key Words*—**Cardholder, COBIT, fraud, ISO27001, PCI DSS, security.

I. INTRODUCCIÓN

CON el impulso y el incremento del uso de productos y servicios financieros, el acceso a una tarjeta débito y/o crédito se facilita aún más, entonces, tener este dinero "plástico" le permite a un cliente realizar distintas transacciones en una oficina de la entidad financiera, cajeros electrónicos, datáfonos en comercios, vía telefónica, portales en internet y aplicaciones para móviles, entre otros, generando el aumento de población a nivel mundial que usa el dinero plástico. Estos clientes se nombrarán en este documento como "tarjetahabientes" (titulares de tarjetas).

Este artículo busca presentar la situación del tarjetahabiente, el fraude, las normas que las franquicias exigen para protección de los datos de tarjeta, el camino para aplicar estos controles, además se presenta de forma general la relación con ISO27001, COBIT y la regulación en Colombia.

II. EL TARJETAHABIENTE, EL USO DE TARJETAS Y EL FRAUDE

Las ventajas que encuentra una persona al poder realizar transacciones como pagar sus servicios públicos desde internet en cualquier momento del día, comprar sus entradas a una obra de teatro, tomar un servicio de transporte desde el celular o poder aprovechar promociones "únicas" de un "cyberlunes" con descuentos en viajes, electrodomésticos, ropa y accesorios de grandes marcas, entre otras situaciones, se reflejan en comodidad, facilidades de compra, ahorro de tiempo, promociones que no se encuentran en los almacenes, entre otros, sin embargo para realizar la compra según el medio de pago seleccionado, la persona debe digitar sus nombres y apellidos, información de contacto, el número completo de su tarjeta de crédito, fecha de vencimiento y códigos de seguridad, ya sea desde un computador personal o por medio de aplicaciones para smartphones o tablets, datos que se solicitan para observar así no se decida finalmente realizar la compra.

Entonces, ¿qué pasa con esta información? ¿se almacena?, ¿cómo y por dónde viaja?, ¿es seguro ese camino?, son preguntas que no todos se hacen, pero aún así se espera que detrás de cada transacción existan unos controles que no permitan que se presente pérdida de confidencialidad, que existan robos de información que posteriormente es

usada para materializar un robo de dinero y fraudes en distintas modalidades. Un caso de fraude conocido a nivel mundial fue el de los supermercados Target en Estados Unidos "La cadena minorista informó que 'hackers' pudieron haber falsificado 40 millones de tarjetas; los ladrones obtuvieron nombres, números de pago, fechas de vencimiento y códigos de seguridad." [1], el cual implicó pérdidas monetarias para los clientes, impacto reputacional para la empresa, multas, entre otros.

En Colombia los casos de robos de información masivos o fraudes derivados de estos delitos, generalmente no son públicos, pocos salen a la luz y no existe una estadística con datos que lo soporten, como dice el gerente de la compañía IQ Information Quality que ofrece servicios de seguridad de la información: "Aquí falta regulación para que las empresas sean obligadas a reportar, en EE.UU. las empresas están obligadas a reportar la fuga e incluso a llamar al usuario final y advertir del fraude, en Latinoamérica no existe eso y por eso no hay datos de los casos que se han presentado." [2], aún así algunos eventos de este tipo se han conocido por amigos, algunas noticias parciales o de impacto internacional, por lo cual el país no es ajeno a esta problemática y la necesidad de proteger los datos para prevenir los robos y fraudes.

III. PANORAMA DE LAS NORMAS PARA LA PROTECCIÓN DE DATOS DE TARJETA

A. Razón de ser de PCI y sus requisitos

Entonces, entendemos que uno de los derechos y necesidades del tarjetahabiente es la seguridad de sus datos, así mismo es una de las responsabilidades de los comercios y entidades financieras, que procesan, almacenan o transmitan datos de tarjeta, de la mano de sus proveedores, con el fin de evitar el fraude y pérdidas monetarias, por lo cual en todos sus procesos y flujos de datos deben aplicar los controles necesarios para proteger y preservar la disponibilidad, integridad y confidencialidad de la información.

Este es el objetivo de las llamadas normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS), que se encuentran actualmente en su versión 3.1 de abril de 2015, y que "se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial.". Corrían los primeros años de la década de 2000 y los casos de fraude con tarjetas de pago (crédito y débito) iban en aumento en forma alarmante [3], esto motivó a que en el año 2006 se estableciera el PCI Security Standards Council (PCI SSC), conformado principalmente por distintas franquicias como VISA, Master Card, American Express, JCB International, entre otras, [4] y que fruto de su experiencia en el sector y del conocimiento en seguridad generaran las normas.

Se considera como dato clave en este contexto el denominado PAN: Primary Account Number, que corresponde al número de tarjeta, además de otros datos sensibles como el código de seguridad (CVV o CVC), la clave, información completa de la banda magnética y/o chip necesarios para la autorización de transacciones de pago [3].

Los siguientes son los 12 requisitos de alto nivel que contiene la norma [4]:

TABLA I
REQUISITOS PCI DSS

Requisitos	Requisitos de alto nivel PCI
Crear y mantener una red segura	1. Instalar y mantener una configuración de firewall para proteger los datos.
	2. No utilizar las contraseñas ni otros parámetros de seguridad predefinidos por el fabricante del sistema.
Proteger los datos de los titulares de tarjetas	3. Proteger los datos almacenados de los titulares de tarjetas.
	4. Cifrar la transmisión de los datos y la información confidencial de los titulares de tarjetas a través de redes públicas.
Mantener un programa de gestión de vulnerabilidades	5. Utilizar y actualizar con regularidad los programas antivirus.
	6. Desarrollar y mantener aplicaciones seguras.

Fuente: Industria de Tarjetas de Pago (PCI) Normas de Seguridad de Datos. Versión 3.1., 2015.

TABLA I (CONTINUACIÓN)

Implantar medidas sólidas de control de acceso	7. Restringir el acceso a los datos según las necesidades comerciales para que solamente puedan ser consultados por aquellas personas que de verdad lo necesiten.
	8. Asignar un número de ID único a cada persona con acceso a los equipos.
	9. Restringir el acceso físico a los datos de los titulares de tarjetas.
Supervisar y evaluar las redes con regularidad	10. Hacer un seguimiento y una supervisión de todos los accesos a los recursos de red y a los datos de los titulares de tarjetas.
	11. Comprobar regularmente la seguridad de los sistemas y procesos.
Mantener una política de seguridad de la información	12. Disponer de una política sobre seguridad de la información

Fuente: Industria de Tarjetas de Pago (PCI) Normas de Seguridad de Datos (DSS). Versión 3.1., 2015.

Los controles que implica cada punto, se resuelven con la documentación de políticas, procedimientos, aplicando mejores prácticas en seguridad de la información, cláusulas en contratos, con implementaciones de infraestructura y comunicaciones, desarrollo de nuevas aplicaciones o hasta cambios complejos de las existentes.

Entre implementaciones puntuales necesarias para dar cumplimiento se encuentran por ejemplo, inclusión de cláusulas en contratos de servicios especificando cumplimiento de PCI DSS, la configuración de la autenticación de dos o más factores para acceso remoto (método de autenticación de un usuario mediante la comprobación de dos o más factores. Los factores incluyen algo que el usuario posee, algo que sabe o algo que el usuario es o hace [5]), la instalación de un servidor de centralización de logs de auditoría con la configuración correspondiente para monitoreo, el enmascaramiento del número de tarjeta en las aplicaciones donde el número completo solo sea observado por los perfiles que por su función necesiten tener el dato y además se identifique y asuman el riesgo, los análisis de vulnerabilidades con una frecuencia exigida que sea realizada mínimo trimestralmente para el sistema operativo y las aplicaciones, entre otros, son implementaciones que pueden implicar la generación de nuevos proyectos, investigación, pruebas piloto, la asignación y aprobación de un alto presupuesto, de recursos disponibles para ejecutar y mantener todas las labores necesarias.

B. El camino a la certificación PCI DSS

Con el fin de ejecutar las actividades necesarias para el cumplimiento de cada requisito, y obtener la certificación en las normas PCI, un comercio, entidad financiera o proveedor debería emprender las siguientes actividades:

1) Conseguir el apoyo y compromiso de la alta gerencia, mostrando los beneficios de obtener el cumplimiento y la certificación en PCI DSS, como la importancia de incrementar la confianza del cliente y de mejorar la protección frente a pérdidas financieras y costos que pueden implicar las brechas de seguridad. Esta labor inicial es complicada generalmente por las implicaciones que tiene en personal y presupuesto, pero que justificada debidamente y generando conciencia de las amenazas a los que la información está expuesta, se puede soportar.

2) Validar toda la infraestructura, elementos de comunicaciones, aplicaciones donde se almacena, procesa o transmite datos de tarjeta, identificando el flujo de información a través de estos componentes.

3) Revisar cómo reducir el alcance identificado en el ítem anterior, que es una labor de análisis para identificar dónde se puede dejar de transmitir, procesar o almacenar el PAN sin afectar la operación, generando una estrategia para este fin.

4) Definir el alcance de PCI en la organización de acuerdo a la revisión.

5) Conocer el estado actual, es decir, saber qué tan lejana está la aplicación de los controles actuales a los exigidos por PCI DSS (lo que se denomina GAP: Guidelines for the Assesment Process). Este estado actual se puede identificar por medio de unos cuestionarios de autoevaluación (SAQ: Self Assessment Questionnaires) disponibles en la página oficial

de PCI DSS según el tipo de empresa, que puede ser apoyado por un QSA: Qualified Security Assessor, que es el evaluador de seguridad certificado, empresa autorizada por el PCI SSC para realizar evaluaciones in situ del cumplimiento de las normas PCI DSS [5], donde se levanta inicialmente información para saber el estado de cada uno de los requisitos con un resultado "implementado" o "no implementado", los que no aplican y cuáles tienen controles compensatorios.

6) Generar el plan de acción con actividades detalladas, responsables, fechas, para cumplimiento de los ítems que aplican.
7) Ejecutar el plan de acción programado.
8) Realizar la evaluación con un QSA para obtener la certificación final.
9) Mantener el cumplimiento, por lo cual si un nuevo componente ingresa a ser parte del alcance PCI, debe estar cumpliendo los requisitos.
10) Realizar cada año la evaluación de cumplimiento con un QSA de PCI DSS para mantener el certificado.

Dentro de la documentación que ofrece PCI DSS en su página oficial, presenta una guía de priorización [6] con una herramienta en excel asociada, cuya idea es que de acuerdo al factor de riesgo y las amenazas agrupados en 6 hitos, se asignan a cada uno de los requisitos de la norma, y permite organizar un plan de trabajo recomendado, más no obligatorio, dado que cada empresa es libre de generar sus planes de acción según su concepto. Los hitos consisten en: El primero en eliminar datos sensibles de autenticación y limitar la retención de datos, el segundo se refiere a proteger las redes y sistemas y estar preparados para responder a una brecha de seguridad, el tercero consiste en asegurar las aplicaciones, el cuarto en monitorear y controlar el acceso a los sistemas, el quinto en proteger los datos almacenados, y el sexto que consiste en completar los requerimientos faltantes con las políticas y procedimientos necesarios para proteger el ambiente de los datos de tarjetahabientes [6].

En el mercado existen amplios portafolios de productos y servicios, ya sea aplicaciones de pago (que ya cumplen con PA DSS: Payment Application Data Security Standard, es decir con los requisitos específicos de PCI para las aplicaciones de pago) o soluciones de soporte de requisitos puntuales de la norma (por ejemplo herramientas de análisis de vulnerabilidades, antivirus, entre otros), es importante evaluarlas de acuerdo a las necesidades, posibilidad de administración y mantenimiento, limitaciones presupuestales de cada empresa, uso por parte de los funcionarios, entre otros.

Es posible que por limitantes técnicas o administrativas no sea viable aplicar algún control de acuerdo con algún requerimiento de la norma, en estos casos las PCI DSS permiten documentar y aplicar unos "controles compensatorios", los cuales deben mitigar el riesgo asociado con el requisito de forma suficiente, [4] esta opción en varios casos es muy útil para las entidades desde que se cumplan las condiciones de la norma, entre las que se encuentra que no pueden ser requisitos de la norma para el caso en cuestión, estos deben ser revisados por el QSA para validar si son aceptados.

No se debe olvidar en todo este camino la importancia de la concientización de los colaboradores de las empresas, su conocimiento y compromiso con la seguridad de la información que manejan, que aunque es parte de la norma en el Requisito 12.6 [3] relacionado con un programa de sensibilización para que todo el personal sea consciente de la importancia de la seguridad de los datos de los tarjetahabientes, es importante que estos funcionarios tengan presente las implicaciones de alguna pérdida de confidencialidad, disponibilidad o integridad de los activos de información, que se adecuen a cambios, restricciones, nuevas formas de trabajo, procedimientos estrictos, siendo la cultura en seguridad la clave para alcanzar los objetivos.

C. Las PCI DSS, ISO 27001 y COBIT

Es importante tener en cuenta que si una organización ha realizado el establecimiento, implementación, operación, seguimiento, revisión,

mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en el estándar ISO 27001 (actualmente en la versión del 2013) [7] implica que tiene un avance importante de implementación de las normas PCI DSS, a través de políticas, procedimientos, formatos, controles documentados y aplicados. Se puede por ejemplo agregar dentro del alcance del SGSI todos los procesos y activos de información que estén involucrados en el almacenamiento, transmisión y procesamiento de datos de tarjetahabientes, así se aplicarían ajustes y se complementaría lo necesario para dar cumplimiento a los requisitos teniendo en cuenta que PCI es más detallado en el resultado esperado según el control que se aplique respecto a ISO27001.

En el caso de COBIT 5 (publicado en el año 2012), el cual proporciona un marco de referencia que apoya a las organizaciones a alcanzar sus objetivos de gobierno y gestión de Tecnologías de Información, al mismo tiempo, respalda la necesidad de cumplir los requerimientos de seguridad con procesos y actividades de gestión como indica el Ph. D. Stefan Beissel [8], quien también muestra que el cruce de los procesos de COBIT 5 con los requerimientos de seguridad de PCI DSS 3.0 (versión vigente cuando el autor la referenció) facilita la aplicación simultánea de COBIT 5 y PCI DSS 3.0, siendo un juicio de experto que permite indicar la relación existente entre éstos, y que las entidades que deban cumplir PCI DSS se pueden ver beneficiadas adoptando el marco de referencia.

Teniendo en cuenta el interés dado a la seguridad de la información, los autores de COBIT generaron dentro de los documentos en la última versión uno completamente enfocado a este tema, "(COBIT 5 for information security), que tiene como base el framework de mejores prácticas, con la característica de que agrega guías prácticas detalladas para la protección de la información para todos los niveles en las organizaciones." [9]

D. Las PCI DSS y la regulación en Colombia

"Las PCI DSS no sustituyen las leyes locales ni regionales, las regulaciones gubernamentales ni otros requisitos legales" [4], por ejemplo en Colombia las entidades que son vigiladas por la Superintendencia Financiera de Colombia, están obligadas a cumplir con las circulares que ésta emite, entre ellas la circular externa 042 de 2012 (nació de la circular externa 052 de 2009), en su capítulo décimo segundo se enfoca en los controles de seguridad y calidad en cada canal de servicio de dichas entidades [10], donde cada vez son más estrictos los controles y su exigencia, y como es de obligatorio cumplimiento en estas entidades ya están en marcha estos controles y su mantenimiento. También, en la circular externa 029 de 2014, en la parte I, título I, capítulo IV: sistema de control interno, en los ítems "4.4.1: Información" y "5.2.1.13: Seguridad de los sistemas", donde se solicitan procedimientos y recursos relacionados "con el objeto de salvaguardar la información contra usos no autorizados, divulgación, modificación, daño o pérdida" y "para que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento en los sistemas de información", entre otros [11].

Además, la Superintendencia de Industria y Comercio generó la ley de protección de datos personales, ley 1581 de octubre de 2012, para garantizar el derecho de las personas a acceder, rectificar, actualizar y cancelar sus datos personales, "de esta manera se obliga a todas las empresas a incorporar políticas de seguridad de protección de los datos y a ser bastante cuidadosos al momento de usar información suministrada por terceros" como dice el consultor en derecho informático Germán Realpe Delgado[12].

Entonces, un plan de acción como el que se hace referencia en la sección B de este artículo, implica que la documentación o implementación que se realice debe ser pensada para cumplir toda la normatividad al respecto, así que si maneja también datos de tarjetahabiente, se pueden unir esfuerzos para cumplir con lo que indica la ISO 27001, COBIT, la Superintendencia Financiera de

Colombia, la Superintendencia de Industria y Comercio y las PCI DSS.

Un ejemplo de esta sinergia es la gestión de incidentes, cada uno tiene un capítulo que hace referencia al tema, en las normas PCI se refiere a gestión de incidentes de seguridad en el "requisito 12.10: Implementar un plan de respuesta de incidentes" , en la ISO 27001 se plasma en el "anexo A.16: Gestión de incidentes de seguridad de la información", en COBIT 5 se refiere en los objetivos de control del "DSS05: Garantizar la seguridad de los sistemas", en cada uno se identifican controles, los aspectos a tener en cuenta para los procedimientos, reporte, evaluación y respuesta a incidentes, entre otros, siendo un solo plan de acción el que podría atender las 3 normas y prácticas en una organización.

Como requisito de seguridad y calidad en la circular externa 042 de 2012, se solicita: "3.1.15: Definir los procedimientos y medidas que se deberán ejecutar cuando se encuentre evidencia de la alteración de los dispositivos usados en los canales de distribución de servicios financieros." [10] y en la circular externa 029 de 2014, en la parte I, título I, capítulo IV, se requiere en el numeral: "5.2.1.13.3: Manejo de incidentes, información y seguimiento" [11], que al incluirlo en el plan de acción generado para el ejemplo. Como este caso hay muchos más que pueden ser identificados y aprovechados en pro de complementar los planes de acción necesarios.

E. El tarjetahabiente

Aunque se ha descrito sobre la responsabilidad y acciones que deben realizar las empresas para velar por la seguridad de los datos del tarjetahabiente, hay un actor en el flujo de información que no se debe olvidar, y es que si el mismo usuario no protege sus datos personales, sus credenciales de autenticación, información de su tarjeta para compras con tarjeta presente (tarjeta física) o no presente, así se blinden las máquinas, las conexiones y las aplicaciones, no habrá poder tecnológico que evite un robo de información que se materialice en un fraude, por lo cual es importante que el tarjetahabiente conozca y siga recomendaciones para los distintos canales como: "No pierda de vista la tarjeta al efectuar sus transacciones en caso de ser necesario solicite un datafono inalámbrico. Tape el teclado cuando digite la clave. Verifique que no haya ningún objeto extraño adherido al cajero. No se deje distraer, intimidar o apurar en hacer su transacción en el cajero automático. No arroje a la basura los comprobantes de pago en los cuales estén registrados sus datos (firma, teléfono, número de tarjeta, número de cédula). No utilice computadores públicos para efectuar operaciones en banca por internet. No anote sus claves, memorícelas." [13], estas recomendaciones pueden ser evidentes para muchos, nuevas para otros, pero es cierto que para varias personas el no haberlas aplicado costó un paseo millonario, la clonación de su tarjeta, pérdida de dinero cuando delincuentes desocuparon sus cuentas de ahorros o exigieron realizar avances con tarjetas de crédito, entre otros, por lo que las entidades financieras deben mantener y fortalecer las campañas para informar a sus clientes de este tipo de recomendaciones, y a su vez que los clientes se informen proactivamente para validar lo que consideren sospechoso y que sean conscientes que también tienen una alta responsabilidad en proteger su información.

IV. EMPRESAS A LA VANGUARDIA CON LAS PCI DSS

En Colombia, algunas de las entidades que transmiten, procesan o almacenan información ya están cumpliendo con la norma y están certificadas en PCI DSS, ganando mejoras en sus procesos y presentándose a sus clientes como una opción que ofrece altos estándares de seguridad, entre estas entidades se encuentra el banco BBVA que "se mantiene durante cuatro años consecutivos (desde 2011) como único banco del sistema financiero colombiano en obtener esta certificación" [14], redes de procesamiento de transacciones como Credibanco (que además utiliza datafonos que también están certificados PCI con la norma específica para este tipo de dispositivos), comercios como Colsubsidio y almacenes Éxito [15], contact

center como Emtelco, siendo la primer entidad del sector en certificarse en el año 2013 [16], y que al atender usuarios finales de empresas del sector financiero, esta certificación además de dar más confianza a los clientes, también les permite ofrecer sus servicios al mercado internacional, posteriormente se certificó el contact center Allus Colombia en el 2014 [17], estas y otras empresas ya certificadas deben hacer el proceso correspondiente para renovar la certificación anualmente. Muchas otras organizaciones de distintos sectores ya emprendieron el camino para obtener esta certificación, y están trabajando arduamente para cumplir con los requisitos necesarios.

El reto está en que el número de empresas certificadas aumente, y así mismo como requisito les exijan el cumplimiento a sus proveedores involucrados con el ambiente PCI, por lo cual se espera que esta cadena se siga ampliando, y que realmente se tenga un cubrimiento de la norma, disminución de índices de fraudes, tarjetahabientes más tranquilos y con la confianza puesta en quienes custodian su información.

Con la velocidad en la que una "nueva" tecnología deja de ser novedad al llegar otra que la supera, es necesario que las entidades fortalezcan sus áreas de investigación y tengan dentro de sus estrategias estar a la vanguardia siempre de la mano de la seguridad, enfocando toda nueva solución tecnológica que desarrollen o adquieran en pro de estar en cumplimiento con las PCI DSS. Este reto no es fácil ya que así como se fortalecen los controles también los delincuentes se ingenian los métodos para vulnerarlas, por lo cual se convierte en un trabajo constante.

Así mismo los responsables de actualizar las normas, estándares y mejores prácticas, están en constante revisión para generar resultados robustos y así enfrentar los retos del día a día en seguridad de la información, que posteriormente se les recomendarán o exigirán a las entidades.

V. CONCLUSIONES

Para comprender por qué nace PCI DSS, es importante conocer sobre la existencia de numerosos y costosos fraudes que fueron los que motivaron al Council (PCI SSC) la generación de unos controles exigentes para la protección de los datos del tarjetahabiente que se ven reflejados en las normas y su exigencia de cumplimiento.

Conocer de qué se trata y cuáles son las actividades generales que implica el cumplimiento de las PCI DSS en una entidad, permite tener una visión del tema para empezar a detallar las actividades y las acciones necesarias para alcanzar y mantener la certificación; así mismo conocer sobre la sinergia existente entre las normas PCI DSS, ISO 27001,COBIT, además de la regulación colombiana que exige controles y condiciones de aseguramiento de la información para las entidades financieras, permiten tener un panorama más completo para generar planes de acción uniendo esfuerzos, optimizando recursos y evitando retrabajo, alineados siempre con la planeación estratégica de la organización.

Se espera que así como aumentan los tarjetahabientes, los canales de servicios y las transacciones con tarjeta, también aumenten las empresas comprometidas con su protección, conllevando a una disminución de los fraudes, menos incidentes de seguridad, más clientes satisfechos, y beneficios en reconocimiento y competitividad.

Si el tarjetahabiente no protege sus propios datos, los controles tecnológicos no serán suficientes para protegerlos por él.

REFERENCIAS

[1] CNN Expansión. (2013, Diciembre). Target reporta robo masivo de datos. *CNN*. [Online] Disponible: http://www.cnnexpansion.com/economia/2013/12/19/target-reporta-robo-masivo-de-datos

[2] M.C. Ramírez. (2014, Abril). A Colombia le falta una regulación para controlar los riesgos en pagos electrónicos. *La Republica*. [Online] Disponible: http://www.larepublica.co/colombia-le-falta-una-

regulaci%C3%B3n-para-controlar-los-riesgos-en-pagos-electr%C3%B3nicos_114431

[3] H.R.Jara. (2015, Mayo). ¿Cómo debe cumplir su empresa el estándar PCI-DSS? *Welivesecurity*. [Online] Disponible: http://www.welivesecurity.com/la-es/2015/05/05/como-cumplir-empresa-pci-dss/

[4] Industria de Tarjetas de Pago (PCI) Normas de Seguridad de Datos (DSS). (Industria de Tarjetas de Pago). Versión 3.1., 2015.

[5] Industria de Tarjetas de Pago (PCI) Normas de Seguridad de Datos (DSS). Glosario de términos, abreviaturas y acrónimos, Versión 1.2 Español. 2008, pp. 2.

[6] Industria de Tarjetas de Pago (PCI) Normas de Seguridad de Datos (DSS). (2015, Mayo). The Prioritized Approach to Pursue PCI DSS Compliance [Online] Disponible: https://www.pcisecuritystandards.org/documents/Prioritized_Approach_for_PCI_DSS_v3-1.pdf

[7] R. Baldecchi (2014, Septiembre) Implementación efectiva de un SGSI 27001. *Isaca*. [Online] Disponible: http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

[8] S. Beissel. (2014, Enero). Cobit Focus Volumen 1. Soportando el cumplimiento de PCI DSS 3.0 con COBIT 5. *Isaca* [Online] Disponible: http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Documents/COBIT-Focus-Volume-1-2014_nlt_Spa_0314.pdf

[9] M.A. Mendoza. (2015,Agosto).COBIT para la seguridad en las organizaciones. *Welivesecurity* [Online] Disponible: http://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/

[10] Superintendencia Financiera de Colombia. Circular Externa 042 de 2012. Capítulo Décimo Segundo, 2012, pp 98.

[11] Superintendencia Financiera de Colombia. Circular Externa 029 de 2014, en la Parte I, Título I, Capítulo IV: Sistema de Control Interno, pp. 4 - 8.

[12] Corporación Colombia Digital. (2013, Abril). Ley de Protección de Datos Personales: una realidad en Colombia. *Colombia Digital Noticias*. [Online] Disponible: http://www.colombiadigital.net/actualidad/noticias/item/4778-ley-de-proteccion-de-datos-personales-una-realidad-en-colombia.html

[13] Incocrédito. Recomendaciones de Seguridad para usuarios de tarjetas [Online] Disponible:http://www.incocredito.com.co/index.php/para-usuarios-tarjetas/recomendaciones-de-seguridad

[14] BBVA. (2015, Enero). BBVA Colombia informe anual 2014 [Online] Disponible: https://www.bbva.com.co/fbin/mult/InformeAnualBBVA2014_1__tcm1304-531314.pdf, p53

[15] Credibanco. (2013,Julio). PCI / DSS. [Online]Disponible: http://ccce.org.co/sites/default/files/biblioteca/normas_pci-dss_-_credibanco_-_abril_2013_0.pdf

[16] La nota económica. (2013, Noviembre). Emtelco obtiene la certificación PCI DSS [Online] Disponible: http://lanotaempresarial.com/business/emtelco-obtiene-la-certificacion-pci-dss-38632.html

[17] Procolombia. (2014, Marzo). Allus Colombia obtuvo la certificación PCI DSS para ingresar a Estados Unidos. *Procolombia Noticias.* [Online] Disponible: http://www.procolombia.co/noticias/allus-colombia-obtuvo-la-certificacion-pci-dss-para-ingresar-a-estados-unidos