GUÍA PARA EL CUMPLIMIENTO DEL ESTÁNDAR PCI DSS V3.2.1 EN UNA PASARELA DE PAGOS

SOFÍA DANIELA CALDERÓN ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA, ECBTI

PROYECTO DE SEGURIDAD INFORMÁTICA

BOGOTÁ, COLOMBIA

2020

GUÍA PARA EL CUMPLIMIENTO DEL ESTÁNDAR PCI DSS V3.2.1 EN UNA PASARELA DE PAGOS

SOFÍA DANIELA CALDERÓN ROMERO

Monografía de Grado requisito para optar al título de:

Especialista en Seguridad Informática

Director (a):
Msc. Katerine Marceles Villaba

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA, ECBTI

PROYECTO DE SEGURIDAD INFORMÁTICA

BOGOTÁ, COLOMBIA

2020

Exclusión de Responsabilidad

La Universidad Nacional Abierta y a Distancia – UNAD no se hace responsable por los conceptos emitidos por el autor(a) de este trabajo de grado. Solo velará porque no se publique nada en contrario al dogma y principios institucionales, ni se atenten contra persona alguna.

Nota de aceptación:

_____
_____
_____
_____
_____

_____
Firma del director:

_____
Firma del jurado

_____
Firma del jurado

Bogotá D. C. (29, Mayo, 2020)

AGRADECIMIENTOS

En primer lugar, agradezco a Dios y a mi madre por el respaldo en la consecución de esta especialización en seguridad informática que permitió dar origen a este proyecto de grado, así mismo, agradezco a las empresas y clientes con los que he trabajado y que me han dotado de experticia en el tema de seguridad de la información para poder merito con criterio a este proyecto. Adicionalmente, se otorga agradecimiento por su colaboración en la construcción de este trabajo de grado de manera directa a:

- ***Msc. Katerine Marceles Villaba – Directora de proyecto de la UNAD***, por su apoyo y asesoramiento continuo como directora de proyecto para la determinación y logro de los resultados de la monografía.
- ***Ing. Julio Cesar Vargas – Docente de la UNAD***, por su participación como tutor en el curso de proyecto de seguridad informática I, el interés por la consecución del proyecto y la atención especializada en temas de seguridad informática orientados a la monografía.
- ***Ing. Yenny Stella Nuñez – Docente de la UNAD***, por su participación como tutora en el curso de proyecto de seguridad informática II y la orientación para el cumplimiento de la estructuración documental del proyecto.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

Activo de Información: Cualquier componente (humano, tecnológico, servicio o documental) que hace parte de los procesos del negocio y que deben protegerse.

Amenaza: Una causa potencial de un evento inesperado, el cual puede resultar en incidente que afecte negativamente a un sistema u organización.[1]

Análisis de los Riesgos: "Proceso para estimar la probabilidad e impacto de los riesgos y determinar el nivel del riesgo."[2]

AoC – (Attestation of Compliance): "Declaración de cumplimiento, es un formulario que resume el estado de cumplimiento por cada uno de los requisitos respecto a los resultados de una evaluación de las PCI DSS; para la validez de esta declaración se debe tener la aprobación de los representantes de la organización auditada y del auditor designado por la QSA"[3] es un formulario para los comerciantes y proveedores de servicios que permite declarar, según está documentado en el Cuestionario de autoevaluación o Informe de cumplimiento.

ASV – (Approved Scanning Vendor): "Proveedor Aprobado de Análisis, es la empresa aprobada por Council de la PCI (PCI SSC) para que pueda hacer los análisis de vulnerabilidades externas."[4]

Código o valor de verificación de la tarjeta: "Permite la validación de la tarjeta y se referencia como código de seguridad de la tarjeta en CAV, CVC, CVV o CSC."[5]

CDE – (Cardholder Data Environment): "Entorno de datos del titular de la tarjeta, es el ambiente lógico o físico que considera los colaboradores, los procesos y los recursos tecnológicos que procesan resguardan o transmiten datos CHD o SAD."[6]

CHD – (Datos del Titular de la Tarjeta): "Información que contiene mínimamente el PAN completo; el nombre o dato de identificación del titular; la fecha de vencimiento y el código de servicio asociado a la tarjeta, etc."[6]

---

[1] ISO – International Organization for Standardization, ISO/IEC 17799:2005. p. 15.

[2] ISO – International Organization for Standardization, ISO 31000:2009 p.13.

[3] PCI SSC. Glosario de términos, abreviaturas y acrónimos de PCI DSS. v3.2, 2016. p. 2.

[4] Ibíd., p. 3.

[5] Ibíd., p. 4.

[6] Ibíd., p. 5.

Establecimiento del contexto: “Especificación de los aspectos internos y externos que se toman en consideración para gestión de los riesgos como la definición del alcance y demás criterios asociados a los riesgos.”[7]

Evento: “Presencia o cambio de un entorno particular; puede darse por una o más situaciones y/o causas; tener o no una consecuencia o convertirse en un incidente.”[8]

Gestión de riesgos: “Actividades definidas para validar y controlar una entidad respecto al riesgo, considerando el establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación del riesgo.”[9]

PAN – (Número de Cuenta Principal): Es conocido como número de cuenta; por ser el número exclusivo de una tarjeta de pago (tarjetas de crédito o débito) que identifica al emisor y la cuenta asignada al titular de la tarjeta.[10]

PS – (Proveedores de Servicios): “Entidad que difieren de las marcas de pago (VISA, MasterCard, entre otras), por lo que estos proveedores no son propiamente una entidad financiera ya que su objetivo es procesar, almacenar o transmitir los datos del titular de la tarjeta (CHD) en nombre de otra entidad; incluyendo también las empresas que controlan u ofrecen servicios tecnológicos y de seguridad para los datos CHD, los proveedores hosting, entre otros; pero, excluyendo de estos las empresas que ofrecen la entrega de acceso a una red pública como los proveedores de telecomunicaciones.”[11] Por lo que las pasarelas de pagos son proveedores de servicio para los objetivos de PCI DSS.

QSA – (Qualified Security Assessor): “Asesor de Seguridad Certificado, que está calificado por las PCI SSC para realizar evaluaciones en un sitio.”[12]

Riesgo: “Efecto de la incertidumbre sobre los objetivos.”[9]

RoC – (Report on Compliance): “Informe de Cumplimiento, es un documento que detalla el estado de cumplimiento de las normas PCI DSS por parte de una entidad, plasmando todos los hallazgos de una auditoría de PCI DSS junto con las evidencias que los soportan.”[13]

---

[7] ISO – International Organization for Standardization, ISO 31000:2009. p. 10.

[8] Ibíd., p. 12.

[9] Ibíd., p. 9.

[10] PCI SSC. Glosario de términos, abreviaturas y acrónimos de PCI DSS. v3.2, 2016. p. 2.

[11] Ibíd., p. 22.

[12] Ibíd., p. 19.

[13] Ibíd., p. 20.

SAD – (Datos Confidenciales de Autenticación): "Información de seguridad que considera los códigos o valores de validación de tarjetas, los datos completos de la pista, el PIN y bloqueos de PIN; información que se usa en la autenticación de titulares de tarjetas o en la autorización de las transacciones ejecutadas."[14]

SAQ – (Self-Assessment Questionnaire): "Cuestionario de Auto-evaluación, es un recurso que permite generar informes con la descripción de los resultados de la autoevaluación a partir de la evaluación del estándar PCI DSS por parte de una entidad siguiendo las indicaciones del PCI SSC."[15] Los cuestionarios SAQ varían al canal usado para la gestión de los datos CHD y la entidad que los gestiona, por lo que los SAQ pueden establecerse como: SAQ A, SAQ A-EP, SAQ B, SAQ B-IP, SAQ C, SAQ C-VT, SAQ D para comercio, SAQ D para proveedores de servicio, SAQ P2PE HW.[16]

Seguridad Informática: También conocida como seguridad de las tecnologías es un aspecto que se asocia o promulga desde la seguridad de la información y que particularmente se enfoca en asegurar los componentes de las Tecnologías de la Información y las Comunicaciones –TIC.

Seguridad de la Información: "Preservación de la confidencialidad, la integridad y la disponibilidad de la información; a lo que puede involucrarse otros pilares como: autenticidad, trazabilidad, no repudio y fiabilidad."[17]

Sistema o Servicio CORE: Correspondiente al servicio que se expone en Internet (plataforma e-commerce) para que interconecte con el comercio muestre el sitio web de la pasarela de pagos para consumo de los tarjetahabientes y que a su vez realice el proceso transaccional con la red de operador de franquicias o procesador de pagos en función de la pasarela de pagos.

Titular de tarjeta o tarjetahabiente: "Cliente o usuario al que se le emite la tarjeta de pago para su consumo o no consumo, o cualquier persona autorizada para utilizar una tarjeta de pago."[18]

---

[14] PCI SSC. Glosario de términos, abreviaturas y acrónimos de PCI DSS. v3.2, 2016. p. 22.

[15] Ibíd., p. 21.

[16] ACOSTA, David. Todo lo que siempre has querido saber acerca de los SAQ de PCI DSS v3.2.1. En: PCIHISPANO. 2018. Disponible en: https://www.pcihispano.com/todo-lo-que-siempre-ha-querido-saber-acerca-de-los-saq-cuestionarios-de-auto-evaluacion/

[17] ISO – International Organization for Standardization, ISO/IEC 17799:2005. p. 14.

[18] PCI SSC, Op. Cit., p. 4.

RESUMEN

La presente monografía titulada “Guía para el cumplimiento del estándar PCI DSS V3.2.1 en una pasarela de pagos”, se plantea el establecimiento del estándar PCI DSS en una pasarela de pago debido a la problemática de garantizar la seguridad y protección a los usuarios/tarjetahabientes en las transacciones de comercio electrónico con las tarjetas de pago a través de las pasarelas de pagos. Por lo que esta monografía permitirá la adaptación y articulación de los requerimientos y consideraciones necesarias para la implementación y certificación de este estándar en este tipo de negocio que también puede adecuarse a cualquier proveedor de servicios (PS) según su alcance; trayéndoles como beneficios la vinculación de nuevos clientes como la seguridad y confianza antes los tarjetahabientes/usuarios finales que hacen consumo continuo de sus compras o transacciones por Internet.

La monografía establece cuatro (4) objetivos específicos que están encaminados en las consideraciones necesarias para la certificación y sostenimiento del estándar PCI DSS a fin de dar solución a la problemática presentada, la cual se solventa con la previa composición de un marco referencial y un diseño metodológico que dará paso a la contextualización del desarrollo de este documento que estructura de manera organizada la especificación de unos requerimientos de PCI DSS v3.2.1 para las pasarelas de pagos; la identificación y análisis de los riesgos las pasarelas de pagos; la definición de unas recomendaciones de seguridad informática para una pasarela de pago y la sustentación del proceso de implementación y certificación en el estándar PCI DSS.

Por lo anterior, esta guía fue estructurada esencialmente para las pasarelas de pagos, pero puede ser adaptada a cualquier organización que tenga características como proveedor de servicio (PS) en el manejo de datos de cuentas (CHD y/o SAD); a fin de que puedan acoplar los requisitos del estándar, las recomendaciones de seguridad y demás aspectos como las fases de evaluación para poder lograr la certificación en el estándar PCI DSS si este es requerido en alguna organización.

Palabras clave:

- Datos de cuentas: CHD – (Datos del Titular de la Tarjeta) y SAD – (Datos Confidenciales de Autenticación)
- Entes de Control como la Superintendencia Financiera de Colombia (SFC)
- Estándar PCI DSS (Payment Card Industry-Data Security Standard)
- Tarjetas de pago: Tarjetas de crédito y débito
- Usuarios / consumidores o tarjetahabientes/ titulares de las tarjetas

INTRODUCCIÓN

Las pasarelas de pago en Colombia buscan ofrecer servicios de autorización dentro del flujo de la transacción a nivel del mercado de la compras apoyando este proceso entre los Usuarios compradores y los diferentes organizaciones que ofrecen sus productos por comercio electrónico, a quienes en algunos casos les exigen que sus ventas se hagan de forma segura y garantizando la protección de la información personal de los propietarios de las tarjetas, lo que genera un impacto importante en sus negocio, por tanto las pasarelas de pago pasan a ser los intermediarios del proceso a fin de tener una disminución significativa en los riesgos de robo y fraude de los datos de la tarjeta.

Por este motivo, los entes regulatorio en Colombia como la Superintendencia de Financiera de Colombia (SFC) dieron pie a requerir compromisos para las pasarelas de pago a fin de que cumplan, certifiquen y mantengan el estándar PCI DSS (Payment Card Industry Data Security Standard); el cual se conoce como el Estándar de Seguridad de Datos de la Industria de la Tarjeta de Pago que en su última versión la V 3.2.1 de mayo de 2018 contempla doce (12) requisitos y 3 Apéndices que se dividen en una serie de sub-requisitos o requisitos de segundo nivel que uno a uno se evalúan en un proceso de cinco (5) fases para obtener la acreditación o certificación en el estándar durante el ciclo anual; aspectos que se sustentaran el desarrollo de esta monografía titulada como: “Guía para el cumplimiento del estándar PCI DSS V3.2.1 en una pasarela de pagos”; la cual fue desarrollada de forma satisfactoria en cuanto a su diseño y contextualización permitiendo obtener el cumplimiento de los objetivos específicos que están enmarcados en unos requerimientos con consideraciones técnicas en materia de seguridad de la información, entregables específicos para el cumplimiento del estándar en una pasarela de pagos, la identificación de unos riesgos de seguridad que se hacen posible en la funcionalidad del servicio que presta la pasarelas de pago frente al manejo de los datos de tarjetas (CHD y SAD) y las estipulaciones que se dan a lugar para la implementación y certificación en el estándar PCI DSS.

Este documento está compuesto estructuralmente por un problema; una justificación; unos objetivos; un marco referencial que contiene marco histórico, marco teórico, marco conceptual, marco normativo; también se especifica un diseño metodológico, la contextualización del desarrollo de los cuatro (4) objetivos definidos en el ámbito de esta monografía, que permitirán obtener unos resultados, unas conclusiones y un anexo para la conformación integral de la guía para el cumplimiento del estándar PCI DSS V3.2.1 en una pasarela de pagos.

1. DEFINICIÓN DEL PROBLEMA

Con el aumento de los usuarios/tarjetahabientes que son poseedores de tarjetas de pagos para el manejo de dinero plástico, así como el alto volumen de los servicios transaccionales para comercio electrónico o en Internet, los cuales entre 2018 y 2019 aumentaron en un 14.974% dentro de las 97 pasarelas de pagos vigentes en Colombia que para el cierre de 2018 crecieron en su cantidad en un 53,9%[19]; especialmente cuando los usuarios/consumidores hacen uso de sus tarjetas de pago por lo que se provee que estas pasarelas de pagos o Gateway de pago seguirán subiendo en su número de transacciones de comercio electrónico con una estimación del 30% para el cierre de 2019[20].

No obstante, el comercio electrónico es mucho más que una plataforma web, ya que considera muchas interacciones entre las cuales se involucran las entidades bancarias como las principales emisores de las tarjetas y que deben efectuar el abono de los recursos monetarios; pero estas entidades no ofrecen la plataforma del pago virtual para garantizar el comercio electrónico, labor que es responsabilidad de las pasarelas de pago y que además para comienzos del año 2018 estas pasarelas de pagos en Colombia todavía no eran vigiladas directamente por la Superintendencia de Financiera de Colombia (SFC) a pesar de su alta demanda operativa[21], haciéndolas vulnerables en sus servicios en Colombia más aún cuando se reportaron alrededor de 40 millones ataques cibernéticos en el sector financiero conforme a la reportado a la SFC[22], más de 6.000 denuncias ante la policía por ciberataques en la cuentas bancarias[23] y que además Colombia está catalogado por la firma Sophos como el país con más ciberataques para 2018[24] por

[19] VENEGAS LOAIZA, Andrés. El número de pasarelas de pago en línea en Colombia ha crecido 53,9%. En: LA REPUBLICA. 2019. Disponible en: https://www.larepublica.co/internet-economy/el-numero-de-pasarelas-de-pago-en-linea-en-colombia-ha-crecido-539-2828821

[20] REVISTA DINERO. Pasarelas de pago se alistan para un verdadero desfile. Sección: Tecnología. 2019. Disponible en: https://www.dinero.com/edicion-impresa/negocios/articulo/pasarelas-de-pago-en-colombia-seguiran-creciendo/268518

[21] RINCÓN CÁRDENAS, Erick. Manual de Buenas Prácticas de las Pasarelas de Pago en Colombia. Bogotá D. C. OE-Observatorio e Commerce. 2018. Disponible en: https://www.observatorioecommerce.com.co/wp-content/uploads/2018/10/Manual-Buenas-Practicas-Pasarelas.pdf

[22] VARGAS, German. Claves para hacerle frente a la amenaza de los ciberataques. En: Portafolio. 2018. Disponible en: https://www.portafolio.co/negocios/claves-para-hacerle-frente-a-la-amenaza-de-los-ciberataques-523223

[23] RODRÍGUEZ, María Carolina. El año pasado se presentaron 12.014 denuncias por ciberataques en Colombia. En: LA REPUBLICA. 2019. Disponible en: https://www.larepublica.co/especiales/informe-tecnologia-junio-2019/el-ano-pasado-se-presentaron-12014-denuncias-por-ciberataques-en-colombia-2879067

[24] COLPRENSA. Colombia fue uno de los países con más ataques cibernéticos el año pasado. En: LA REPUBLICA. 2019. Disponible en: https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

lo que las pasarelas de pagos están crudas y vulnerables en sus obligaciones frente a la seguridad para sus servicios al comercio electrónico.

Teniendo en cuenta el párrafo anterior las entidades bancarias también conocidas como establecimientos de crédito y los administradores de sistemas de pago de bajo valor, que son instituciones financieras vigiladas e inspeccionadas por la SFC, solo podrán vincular pasarelas de pagos que cumplan con los lineamientos del numeral 2.3.8. de la Circular Externa 008 del 05 de junio de 2018; por lo que las pasarelas de pago estarían limitadas en su operación y adquisición de convenios con estas entidades vigiladas sino dan cubrimiento a los lineamientos impartidos por la SFC. En lo que algunas de las pasarelas pago que operan en Colombia como Place to Pay[25], PayU[26]; entre otras en mínima proporción fueron unas de las pioneras en incursionar con estas medidas requeridas por la SFC incluso antes de que comenzaran a regularse por este ente de control; pero, la mayoría de las pasarelas de pago que están en Colombia a la fecha no acreditan la implementación y certificación de los requisitos apropiados de seguridad para la protección de los datos de las tarjetas de pago durante las transacciones de comercio electrónico, ni tampoco han sabido como abordar dichos requisitos considerado para esto las exigencias de la SFC y las necesidades de los clientes/usuarios en sus procesos transaccionales y de comercio electrónico con las tarjetas de pago; por lo que si estos requerimientos no son gestionados a conformidad en una pasarela de pago podrían limitar la seguridad en sus operaciones; provocar la desconfianza de los usuarios al momento de hacer transacciones, la derivación de sanciones o multas según la regulación aplicable y la imposibilidad de vinculación con las entidades vigiladas por la SFC y los clientes.

1.1. FORMULACIÓN

Dada la problemática descrita se plantea la formulación de la situación, la cual se especifica bajo la siguiente pregunta: ¿Cómo establecer apropiadamente los requisitos para la seguridad y protección a los datos de los tarjetahabientes que usan las tarjetas de pago en las transacciones de comercio electrónico desde el año 2018 a través de las pasarelas de pagos cumpliendo con las exigencias normativas de los entes de control y las necesidades de los clientes y usuarios?

[25] CADAVID CORREA, Orlando y GIRALDO OSPINA, Evelio. Plataformas de pagos electrónicas. Disponible en: https://www.eje21.com.co/2018/11/desde-diciembre-se-empezara-a-exigir-a-las-pasarelas-de-pagos-digitales-sistemas-de-proteccion-de-datos/

[26] SANTOS, Jorge. Pagos en línea, más seguros que el comercio tradicional. PAYU. Disponible en: https://www.payulatam.com/blog/dico-velit-delicata-vel-ealia-modus-cum-altera-copiosae/

2. OBJETIVOS

2.1. GENERAL

Diseñar una guía para establecer el estándar PCI DSS V.3.2.1 en una empresa de pasarela de pagos determinado las consideraciones necesarias para su certificación y sostenimiento; en cumplimiento a las exigencias de la Superintendencia Financiera de Colombia y las necesidades de los clientes/usuarios en sus procesos transaccionales y de comercio electrónico.

2.2. ESPECÍFICOS

- Especificar los requerimientos que son necesarios para dar cubrimiento a los requisitos que exige el estándar PCI DSS V.3.2.1 en su proceso de implementación en pasarelas de pagos.

- Analizar los riesgos con sus correspondientes amenazas y vulnerabilidades de seguridad informática que están asociados al cumplimiento del estándar PCI DSS V3.2.1 para una pasarela de pagos.

- Documentar las consideraciones de seguridad informática necesarias en una pasarela de pago para su orientación en el cumplimiento del estándar PCI DSS V3.2.1.

- Compilar las dificultades y amenazas que se pueden presentar durante el proceso de implementación, certificación y sostenimiento del estándar PCI DSS V.3.2.1 en una pasarela de pago.

3. JUSTIFICACIÓN

Las causas que justifican la ejecución de esta monografía basándose en la problemática planteada se sustentan conforme en las siguientes razones:

1. Las tarjetas de pagos son los medios de pagos más utilizados por los usuarios en sus transacciones de comercio electrónico y por tanto son los medios más vulnerables y apetecidos por los ciber-delincuentes para sus ataques.

2. La mayoría de los establecimientos de comercio han adoptado el pago por medio de canales virtuales para que los clientes puedan adquirir sus productos y servicios; para estos se debe garantizar que las transacciones de los usuarios/ tarjetahabientes se realicen de forma segura con el fin de generar confianza e incentivar el uso de sus tarjetas de pago.

3. Las principales franquicias de tarjetas de pago en Colombia (Visa, MasterCard y American Express), que hacen parte del PCI_SSC (Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago) exigen el cumplimiento del estándar PCI DSS en su última versión 3.2.1 a las organizaciones que procesan, transmiten y/o resguardan información relacionada a los datos de las cuentas de estos medios de pago; por lo que las pasarelas de pagos sería una de las empresas objetivo al cumplimiento de este estándar.

4. La implementación del estándar PCI DSS es requerido en su cumplimiento por exigencia de los entes de control colombianos como la Superintendencia Financiera de Colombia que actualmente vigilan los establecimientos de crédito y los administradores de sistemas de pago de bajo valor, los cuales requieren vincular las pasarelas de pagos para su interacción en el comercio electrónico y para ello se rige los lineamientos de la Circular Externa 008 del 05 de junio de 2018 que exige en su numeral 2.3.8.1.1 la implementación y certificación del estándar PCI DSS en su última versión para las pasarelas de pagos; así como, el mantenimiento de esta certificación conforme al numeral 2.3.8.2 de la circular volviéndose una prioridad en el contexto organizacional de estos negocios.

De conformidad con los puntos expuestos anteriormente, se sustentan los motivos para diseñar la guía para el cumplimiento del estándar PCI DSS en su versión actual (V3.2.1) para una pasarela de pagos como solución a la problemática planteada. Por lo que la realización de esta guía permitirá la adaptación y articulación de los requerimientos y consideraciones necesarias para la implementación y certificación del estándar PCI DSS esencialmente en las pasarelas de pago y que también puede adecuarse a cualquier proveedor de servicios (PS) según su alcance; trayéndoles como beneficios los convenios con los establecimientos de crédito y los administradores de sistemas de pago de bajo valor, la vinculación de más comercios

(clientes) a su portafolio de servicio como el reconocimiento de la seguridad y la confianza antes los usuarios finales que hacen consumo continuo de sus compras o transacciones por Internet.

4. ALCANCE

El presente proyecto se delimitará a una guía que brinda orientaciones técnicas en materia de seguridad para el cumplimiento del estándar PCI DSS en su versión actual la 3.2.1 aplicándose sobre el servicio Core que ofrece una pasarela de pagos para los procesos transaccionales; sin desmeritar la oportunidad de su adopción para aquellas entidades u organizaciones que se cataloguen como proveedor de servicios (PS), las cuales pueden adecuar los aspectos tratados en la presente guía para dar cumplimiento al estándar PCI DSS en sus servicios.

Dentro de esta guía se exceptúa la contextualización hacia otras normatividades asociadas a los diferentes estándares de la familia PCI (Payment Card Industry) que son definidos por PCI Security Standards Council (PCI SSC); así mismo, se descartan los protocolos para la adopción el estándar PCI DSS en establecimientos de comercios y demás entidades y/o procesos funcionales que gestionan datos de tarjetas de pago que no estén propiamente relacionadas en el alcance inicial.

5. MARCO REFERENCIAL

5.1. MARCO HISTÓRICO

El estándar PCI DSS fue constituido por PCI SSC (Payment Card Industry Security Standards Council) que constituyó el 07 de septiembre de 2006 por cinco (5) marcas de tarjetas de pago o franquicias: VISA International, American Express, MasterCard, JCB International y Discover Financial Services; quienes establecieron sus propios programas de seguridad y cumplimiento, los cuales se consolidaron para formar un único estándar global que procura la seguridad de los datos estableciendo normatividades que de seguridad de la Industria de Tarjetas de Pago (PCI), entre las más conocidas estan: La Norma de Seguridad de Datos (DSS), la Norma de Seguridad de Datos para las Aplicaciones de Pago (PA-DSS), los Requisitos de Seguridad de Transacciones con PIN (PTS), entre otras.[27]

En lo que respecta a PCI DSS su primera versión se presentó en enero de 2005 como estándar que se fundamentaba en el programa de seguridad y cumplimiento que había establecido por Visa Internacional, el cual fue acogido por las demás marcas de forma particular en los aspectos que les parecía conveniente, por lo que al año 2006 junto con la constitución de PCI_SSC se genera la versión PCI DSS 1.1 como una versión común que aplicaría a todas las marcas asociadas al PCI_SSC; pero, esta versión 1.1 redundaba en aspectos de implementación y procedimientos de auditoría de seguridad por lo que en octubre de 2008 se constituye la versión 1.2 que establece los “Requisitos de las PCI DSS y procedimientos de evaluación de seguridad” como su principal premisa, la cual aún permanece vigente a pesar de las modificaciones o controles de cambios que se le han realizado al estándar en su contexto conforme a lo sustentado en la siguiente tabla, en la que se muestra cada una de las versiones generadas para PCI DSS con las modificaciones que le han creado:

[27] PCI SSC. Requisitos y procedimientos de evaluación de seguridad PCI DSS Versión 3.2.1. 2018. Disponible en: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1-ES-LA.pdf?agreement=true&time=1574494354390

Figura 1. Modificaciones de las versiones del Estándar PCI DSS

Fecha	Versión	Descripción
Octubre de 2008	1.2	Introducir la versión 1.2 de las PCI DSS (Normas de seguridad de datos de la industria de tarjetas de pago) como "requisitos de las PCI DSS y procedimientos de evaluación de seguridad" para eliminar la redundancia entre documentos e implementar cambios generales y específicos de los procedimientos de auditoría de seguridad de la versión 1.1 de las PCI DSS. Para obtener la información completa, consulte el Resumen de cambios de la Normas de seguridad de datos de la PCI de las PCI DSS, versión 1.1 a 1.2.
Julio de 2009	1.2.1	Agregar la oración que se eliminó incorrectamente entre las PCI DSS versión 1.1 y 1.2.
		Corregir "then" por "than" en los procedimientos de prueba 6.3.7.a y 6.3.7.b.
		Eliminar la marca gris para las columnas "Implementado" y "No implementado" en el procedimiento de prueba 6.5.b.
		Para la Hoja de trabajo de controles de compensación - Ejemplo completo, corregir la redacción al principio de la página de modo que diga "Utilizar esta hoja de trabajo para definir los controles de compensación para cualquier requisito indicado como 'implementado' a través de los controles de compensación".
Octubre de 2010	2.0	Actualizar e implementar cambios de la versión 1.2.1. Consulte *PCI DSS: Resumen de cambios de la versión 1.2.1 a 2.0 de las PCI DSS*.
Noviembre de 2013	3.0	Actualización de la versión 2.0. Consulte *PCI DSS: Resumen de cambios de la versión 2.0 a 3.0 de las PCI DSS*.
Abril de 2015	3.1	Actualización de la PCI DSS, versión 3.0. Para obtener los detalles, consulte *PCI DSS - Resumen de cambios de la PCI DSS versión 3.0 a 3.1*
Abril de 2016	3.2	Actualización de la PCI DSS, versión 3.1. Para obtener los detalles, consulte *PCI DSS - Resumen de cambios de la PCI DSS versión 3.1 a 3.2*
Mayo de 2018	3.2.1	Actualización de la PCI DSS, versión 3.2. Para obtener los detalles, consulte *PCI DSS – Resumen de cambios de la PCI DSS versión 3.2 a 3.2.1.*

Fuente: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1-ES-LA.pdf?agreement=true&time=1574494354390 P.2

De la figura 1 se puede percibir que este estándar tiene una tendencia de cambio continua que no supera los 3 años, ya que antes de que pase dicho termino los miembros del PCI_SSC tienen como política el efectuar los 8 foros globales abiertos que pretenden el continuo desarrollo, implementación, almacenamiento, divulgación y mejora de las normas de seguridad para la protección de datos de tarjetahabiente; de ahí que en el año 2018 se reunieron y establecieron la nueva versión 3.2.1 del estándar PCI DSS con fecha de publicación del 17 de mayo de 2018, la cual será fuente principal de la estructuración de esta guía.

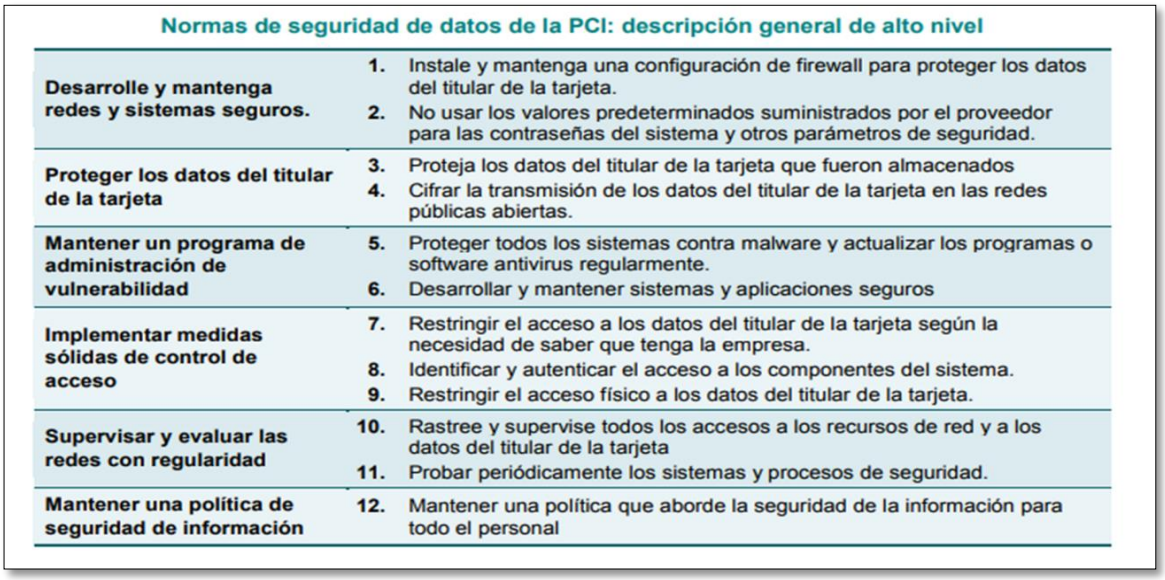
5.2. MARCO TEÓRICO

Dentro del marco teórico se establecerán las generalidades respecto al estándar PCI DSS en su versión 3.2.1 (PCI DSS V3.2.1) y la funcionalidad de las pasarelas de pagos en Colombia.

5.2.1. PCI DSS versión 3.2.1

El estándar PCI DSS V3.2.1 de mayo de 2018, establece 12 requisitos aplicables para su establecimiento los cuales se resumen en:

Figura 2. Contextualización de los 12 requisitos de PCI DSS



Normas de seguridad de datos de la PCI: descripción general de alto nivel		
Desarrolle y mantenga redes y sistemas seguros.	1.	Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta.
	2.	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	3.	Proteja los datos del titular de la tarjeta que fueron almacenados
	4.	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	5.	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.
	6.	Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	7.	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
	8.	Identificar y autenticar el acceso a los componentes del sistema.
	9.	Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	10.	Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta
	11.	Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	12.	Mantener una política que aborde la seguridad de la información para todo el personal

Fuente: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1-ES-LA.pdf?agreement=true&time=1574494354390 P.5

Así mismo, contempla 3 Apéndices adicionales para los diferentes tipos de entidades, que complementan los 12 requisitos:

- Apéndice A1: Requisitos de la PCI DSS adicionales para proveedores de hosting compartido.
- Apéndice A2: Requisitos de la PCI DSS adicionales para las entidades que utilizan SSL/TLS temprana.
- Apéndice A3: Validación suplementaria de las entidades designadas.

Los requisitos y anexos tienen un aproximado entre 245 y 405 sub-requisitos los cuales se determinan por el modo en que se cuenta el número de cláusulas y/o sentencia de cada requisito; por tanto, en la siguiente tabla se especifican los requisitos y el rango de los sub-requisitos de nivel 1 con sus principales aspectos o consideraciones de seguridad informática a desarrollar en esta guía.

Tabla 1. Aspectos de seguridad informática para los Requisitos de PCI DSS

REQUISITO	SUB-REQUISITOS (Nivel 2)	PRINCIPALES ASPECTOS DE SEGURIDAD INFORMÁTICA
1. Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta	**1.1 al 1.5**	• Firewall o cortafuegos • DMZ (zona desmilitarizada) • Traducción de Dirección de Red (NAT)
2. No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad	**2.1 al 2.6**	• Estándar de configuración • Hardening • Contraseñas • SSL • TLS
3. Proteger los datos CHD que fueron almacenados	**3.1 al 3.7**	• Gestión de Llaves • HSM (Modulo de seguridad de Host) • Criptografía - Criptografía solida • Esquemas y algoritmos de Cifrado • Enmascaramiento y Truncamiento de datos • Código o valor Hash • Token
4. Cifrar la transmisión de los datos CHD en las redes públicas abiertas	**4.1 al 4.3**	• Método de criptografía • Protocolos de cifrado • Certificado digital
5. Proteger todos los sistemas contra malware y actualizar los programas o sistema de antivirus regularmente	**5.1 al 5.4**	• Malware o código malicioso y los tipos más conocidos como: Virus informático, Gusano, Troyano, Ramsonware, entre otros. • APTs (Amenazas Persistentes Avanzadas) • EDR (Detección y Respuesta en Endpoints) • EPP (Plataformas de Protección Endpoint) • Antivirus – antimalware

Tabla 1. (Continuación)

REQUISITO	SUB-REQUISITOS (Nivel 2)	PRINCIPALES ASPECTOS DE SEGURIDAD INFORMÁTICA
6. Desarrollar y mantener sistemas y aplicaciones seguros	**6.1 al 6.7**	• Parches de seguridad • Ciclo de vida de desarrollo seguro • Pruebas de seguridad en los desarrollos, Revisión de código - Revisión par • Ambientes de desarrollo seguro • Control de cambios de software • Segregación de funciones • Vulnerabilidades de desarrollo de software, BD y aplicaciones web. • WAF(Firewall de Aplicaciones Web) • Firewall de BD
7. Restringir el acceso a los datos CHD según la necesidad de saber que tenga la empresa	**7.1 al 7.3**	• Sistema de controles de acceso • Asignación de privilegios de acceso
8. Identificar y autenticar el acceso a los componentes del sistema	**8.1 al 8.8**	• Autenticación - Métodos y mecanismos de autenticación • Autorización • Sistema de Gestión de Contraseñas
9. Restringir el acceso físico a los datos del titular de la tarjeta	**9.1 al 9.9**	• Seguridad física en instalaciones • Controles de acceso físico (Sistema Biométrico, Bitácoras, etc.) • CCTV (Circuito cerrado de Televisión) • Copias de respaldo o Backup • Transferencia o distribución de medios físicos • Destrucción de medios e información física • Borrado seguro
10. Rastrear y supervisar todos los accesos a los recursos de red y a los datos del titular de la tarjeta	**10.1 al 10.9**	• Logs o registros de auditoria • Evento de seguridad de la información • Sincronización de relojes en el sistema (Protocolo NTP) • SIEM (Sistema de Gestión de Eventos e Información de Seguridad) •Herramientas de gestión de Logs (Alienvout OSSIM)
11. Pruebe con regularidad los sistemas y procesos de seguridad	**11.1 al 11.6**	• NAC (Control de acceso a redes) inalámbricas • Metodologías y herramientas de Ethical Hacking • Análisis de vulnerabilidades • Pruebas de Intrusión o penetración - Pentesting • Vulnerabilidades de redes y comunicaciones • IPS (Sistema Prevención de Intrusos) • IDS (Sistema de Detección de Intrusos) • Sistema FIM (Supervisión de Integridad de Archivos)

Tabla 1. (Continuación)

REQUISITO	SUB-REQUISITOS (Nivel 2)	PRINCIPALES ASPECTOS DE SEGURIDAD INFORMÁTICA
12. Mantenga una política que aborde la seguridad de la información para todo el personal	**12.1 al 12.11**	• Política de seguridad de la información • Amenaza, Vulnerabilidad, Riesgo Informático, Riesgo de Seguridad de la Información. • Activos de información • Metodologías de gestión de riesgos • Procesos de selección, vinculación y desvinculación seguros para personal • Seguridad en la gestión de proveedores• Gestión de Incidente de seguridad de la información • BIA (Análisis de Impacto de Negocio) • DRP (Plan de Recuperación de Desastre) • BCP (Plan de Continuidad de Negocio) • Procesos de auditoria a la seguridad de la información y sistemas
Apéndice A1: Requisitos de la PCI DSS adicionales para proveedores de hosting compartido	**A1.1 al A1.4**	• Seguridad en los Hosting • Seguridad en la nube • Ataques de seguridad informática
Apéndice A2: Requisitos de la PCI DSS adicionales para las entidades que utilizan SSL/TLS temprana	**A2.1 al A2.3**	Relaciona los aspectos del Requisito 2 y 4 de PCI DSS V3.2.1
Apéndice A3: Validación suplementaria de las entidades designadas (DES)	**A3.1 al A3.5**	• Gobierno de Seguridad • BIA (Análisis de Impacto de Negocio) • Cultura en seguridad • Gestión de Cambios

Fuente: Propia

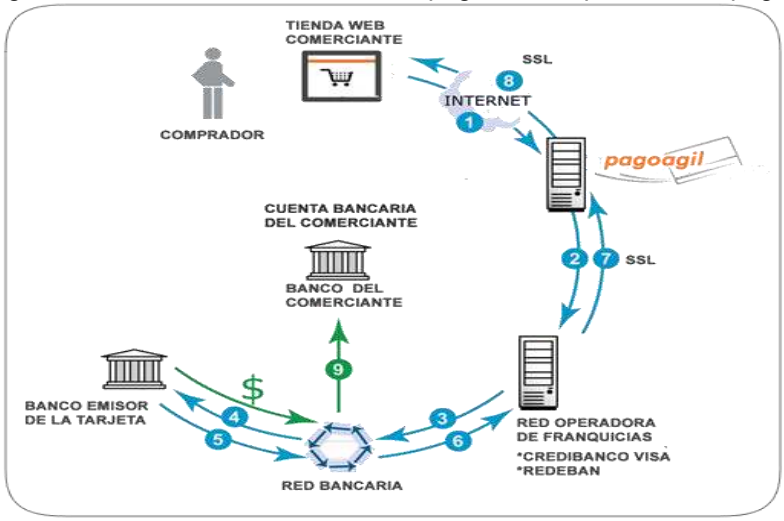
A partir de la Tabla 1 se puede evidenciar aspectos de seguridad informática relacionados con requisitos específicos de PCI DSS V3.2.1, aunque varios de estos aspectos se pueden relacionar con otros requisitos o sub-requisitos del mismo estándar; pero dicha interrelación se soportará en el capítulo 7. Desarrollo de esta guía para los requisitos aplicables a las pasarelas de pagos en Colombia.

5.2.2. Cómo funcionan las Pasarelas de pago en Colombia

Las pasarelas de pagos como proveedores de servicio (PS) suministran un Sistema o Servicio CORE que se expone en Internet bajo una plataforma e-commerce (servidor web) en el que se facilita la gestión de compra virtuales/online por Internet entre los usuarios-tarjetahabientes y los comercios; en el que los comercios son los clientes que contratan los servicios de las pasarelas para que durante una compra puedan gestionar el proceso de traslado del dinero a las cuentas en el banco del comercio.[28] Por lo que las pasarelas de pagos deben tener un adecuado servicio para poder garantizar la seguridad de la transacción al comercio, la cual deberá pagar el proceso transaccional a la pasarela acorde a las condiciones o comisiones establecidas por la pasarela para el comercio, teniendo como punto de prevalencia el cumplimiento de la certificación en PCI DSS de forma efectiva por parte de la pasarela de pago.

Teniendo como referencia a una pasarela de pago como PagoÁgil se describe la ejecución del proceso de pagos con una tarjeta de crédito, la cual constan de 2 fases: una de autorización que contiene ochos (8) pasos y otra de compensación donde se aplica el paso 9, acorde con lo ilustrado en la figura 3; cabe aclarar que en la etapa de autorización se determina si los datos transmitidos para el pago son válidos y si la tarjeta del cliente cuenta con los fondos disponibles y suficientes para la compra; por lo que a continuación se relaciona este proceso en la figura 3:

Figura 3. Proceso de autorización de pago en una pasarela de pagos



Fuente: https://pagoagil.co/pasarela-de-pagos/funcionalidad

[28] URBANO MATEOS, Susana María. Qué es y cómo funciona la pasarela de pago en ecommerce. En: Actualidad ecommerce. 2018. Disponible en: https://www.actualidadecommerce.com/que-es-y-como-funciona-la-pasarela-de-pago-en-ecommerce/

Las pasarelas de pagos dentro del proceso de autorización enrutan los detalles del pago a las redes de tarjetas de crédito en nombre de la tienda, para que luego devuelvan los resultados aprobados o rechazados de la transacción.

Como se había dicho anteriormente, después de la autorización se realiza la compensación que sería el noveno (9) paso donde se efectúa una liquidación, en la que la entidad bancaria emisora de la tarjeta del cliente envía los fondos necesarios para la operación a la entidad bancaria del comerciante. La entidad bancaria deposita los fondos en la cuenta bancaria del comerciante, normalmente dentro de uno a dos días hábiles.

5.3. MARCO CONCEPTUAL

Durante el desarrollo de este trabajo se verán aspectos relacionados a la seguridad informática que se enuncian en el marco teórico y que a continuación se sustenta para una mayor comprensión de los conceptos y consideraciones al momento de efectuar el desarrollo de implementación de esta guía en una pasarela de pagos.

Ataques comunes en seguridad informática:

A. *La Infección por virus y/o código malicioso* hacia los equipos de cómputos, servidores y servicios; lo que generaría captura, manipulación, alteración, fuga, perdida, bloqueo de la información de los sistemas y la información contenida sobre estos. Entre los códigos maliciosos/malware popularmente conocidos está el Ransomware, que se encargada de bloquear con cifrado fuerte el acceso a los archivos critico de los sistemas a cambio de una compensación económica para su recuperación.

B. *La Suplantación de los sitios web*; en la cual un atacante puede simular las aplicaciones y páginas web de la organización para que los usuarios de los servicios de la empresa ingresen a esos sitios que han suplantado y hagan sus las transacciones financiera y de información que venían dirigidas hacia la empresa, generando un fraude económico hacia la empresa y el usuario; como la captura de los datos de los cliente las cuales pueden usar para fines malintencionados como hasta robar las cuentas personales de los usuarios; lo que traería consigo perdidas de imagen, reputación y económicos para el negocio así como problemas legales y sanciones.

C. *Las Infiltraciones a la red de comunicaciones y/o servicios*; en la cual un atacante podrá tener permisos de acceso a la red y de ejecución de acciones

ilícitas sobre los sistemas y red; porque este personaje puede conocer todo lo que hace y se tiene implementado en la infraestructura tecnológica y sistemas de la empresa; permitiéndole tener control total para que pueda cambiar, borrar, copiar, bloquear y hasta dañar los sistemas tecnológicos; sin que la empresa se dé por enterada de quién, cuándo, cómo, dónde y en qué se perpetuo el o los eventos de ataque en los sistemas; lo que traería consigo perdidas de imagen, reputación y económicos para el negocio así como problemas legales y sanciones.

D. *Denegación de los servicios y/o suspensión de los recursos tecnológicos*, esto implica que uno o varios componentes y/o servicios de la infraestructura tecnológica de la organización pueden quedar indisponibles sin poder hacer uso o provecho de ellos, debido a errores de administración, carencias de suministros eléctricos, fallas de los componentes o por acciones deliberadas o accidentales de terceras personas, lo que afectaría representativamente la calidad de servicio ante los clientes, la accesibilidad de los sistemas, productividad y operatividad de la organización.

E. *Perdida, daños o robo de los recursos tecnológicos de la organización*, los cuales pueden ser tomados o afectados de forma arbitraria y sin autorización por parte de terceras personas que hayan podido acceder físicamente a las instalaciones, zonas restringidas o de manera lógicamente a los sistemas de información.

Bombas lógicas, son piezas de código de programa oculto que se activan bajo comando, tecleo, clic o condiciones predeterminadas para las acciones del sistema, como puede acontecer con las bombas de tiempo las cuales se activan al llegar una fecha u hora en particular; por lo que su afectación no se da por sí misma sino se cumple las condiciones prestablecidas. Estas bombas pueden venir de forma inherente en los virus informáticos, gusanos, entre otros malwares, para que se exploten es decir ejecute las acciones de los otros malwares una vez se establezca el tiempo o condición requerida en el sistema.

Certificado digital, es un fichero informático con firma electrónica que se emplea como técnica necesaria para asegurar la intranet y la conexión VPN entre la DMZ y la intranet blindando la comunicación e interacción de los usuarios entre los 2 sitios, ya que permitirá identificar y autenticar la conexión, además cifra los datos transmitidos entre ambas partes. Uno de los certificados a considerar para esta conexión podría hacerse bajo el protocolo de criptográfico SSL (Secure Socket Layer) como el TLS (Transport Layer Security). Los certificados digitales con protocolos de cifrado fuertes son útiles para asegurar especialmente los sitios web del negocio y blindando la comunicación e interacción con los servicios de la red, ya que permitirá identificar y autenticar el servidor, además cifra los datos transmitidos entre el servicio web y el cliente, es útil para el sitio web y las VPN.

DMZ (zona desmilitarizada), es una subred o zona separada de la red LAN (Red de Área Local) que se puede delimitar por medio de un firewall, aunque también se puede hacer con un enrutador doméstico pero esto es poco común y no genera beneficios significativos; la DMZ en las organizaciones se usa para separar la red interna de otra externa; aunque en el contexto organizacional se puede establecer para un entorno de red con accesos permitidos a Internet categorizándose como un ambiente inseguro, de igual forma se puede constituir como una red especial para cosas especificas con condiciones especiales que salen a Internet; por lo que esta subred se puede considerar el entorno con doble capa de seguridad para la red interna, ya que limita los accesos y conexiones de los usuarios/externos desde Internet únicamente hacia los componentes de la DMZ, impidiendo el acceso de estos externos hacia el resto de la red interna u otras subredes constituidas, pero los usuarios o componentes de la red interna si pueden tener interacción con la DMZ mutuamente.

Firewall De Base De Datos, es una solución de software de seguridad que permite filtrar/bloquear las peticiones que llegan al Sistema de Gestión de Bases de Datos (SMBD), gracias al conjunto de reglas preestablecidas; lo que permite la protección de la base de datos contra las solicitudes maliciosa, otorgar permisos de consultas y accesos a los usuarios autorizados con anterioridad y a su vez permite monitorear las actividades efectuadas en la SMBD y la BD (Base de Datos), respectivamente generando registros y análisis de los datos que se almacena en ellas.

Elementos de seguridad física, permiten prevenir la perdida/robo/daño de los componentes tecnológicos, así como acciones deliberadas en los sistemas entre estos elementos se consideran*: Los Sistemas de control de acceso* que procese la autenticación y posterior autorización de las solicitudes tantos físicas como lógicas respectivamente a las instalaciones, por ejemplo: sistema biométrico para acceso a las instalaciones y zonas restringidas de la organización; *CCTV(Circuito cerrado de Televisión)* para vigilancia y control de las acciones efectuadas por los colaboradores y terceros; *Extintores y sistema contra incendios* para mitigar los daños de los componentes tecnológicos y las instalaciones en caso de incendio; *Sistema de alerta y alarma* para descubrir la presencia de intrusos en las instalaciones y en la zona donde se resguardan los componentes tecnológicos.

Firewall De Aplicaciones Web (WAF), Los WAF son un tipo de firewall útiles para blindar, proteger, controlar los accesos y solicitudes que se pueden hacer a las aplicaciones y/o servicios web a nivel de capa 7 de aplicaciones del modelo OSI, a fin de evitar ataques provenidos desde Internet hacia la aplicación /sitio web, como de tipo CrossSite Scripting (XSS), SQL Injection (SQLi), Remote y Local File Inclusion (LFI), etc. Algunas soluciones de WAF opensource que se manejan en software son: Modsecurity, Ironbee; los cuales se pueden encontrar también con soluciones en la nube como Cloudflare, Sucuri Firewall, entre otros. Como componentes físicos se distinguen Barracuda Networks WAF, Fortinet FortiWeb, Citrix Netscaler Application Firewall, entre otros.

Firewall o cortafuego perimetral, para filtrados de contenido, controlar las comunicaciones entre las redes y bloquear los accesos no autorizados; hasta enrutar de forma segura las conexiones. Así mismo permite gestionar la detección y prevención de intrusos a la red y servicios, también permite crear las DMZ/ zonas desmilitarizada, la cual se parametriza de manera trípode en la configuración de este componente si firewall perimetral para que cada red se conecte a un puerto distinto, considerando el Port Address Translation (PAT) ya que la DMZ pretende separar la red interna de otra externa que pueda tener interaccion con conexiones inseguras como la Internet. De la misma manera en el firewall se puede establecer la conexión VPN (Virtual Private Network) que considera un túnel que encapsula toda la información y la cifra durante su transporte, es muy útil para las conexiones entre sede y funciones de teletrabajo.

Gusanos o worm, en informática son unos subtipos de virus que comprende un set de programas que se propagan de equipo a equipo, pero a diferencia de un virus informáticos, se propaga de forma automática sin requerir intervención humana, haciendo uso de un archivo o condiciones del sistema operativo y/o de las conexiones red del sistema de forma oculta; por lo que su réplica es garantizada entre componentes generando pérdida de capacidad de resguardo en el componente y afectaciones de gestión en memoria RAM.

Herramienta de análisis de vulnerabilidades, permite analizar el estado de riesgos y vulnerabilidades de los sistemas y servicios, facilitando la definición de las necesidades o actualizaciones que requieren los sistemas y servicios a fin de que no sean susceptibles a ataques en la red y/o por accesos no autorizados por terceros. Entre las más conocidas se tienen (Nessus, Metasploit, Open vas, etc.)

Herramienta de cifrado con algoritmos de cifrado fuertes, es necesarios para las bases de datos y documentación critica que se almacena y custodia para la organización, a fin de proteger su confidencialidad e integridad, haciéndola accesible solo a las personas autorizada.

Herramienta SIEM (Gestión de eventos e información de seguridad), Son recursos de seguridad informática de soporte y de investigación necesarios para la gestión y correlación de los eventos y logs de los servicios y sistemas críticos; permitiendo tener una información asertiva y oportuna de las acciones ilícitas y ataques que generan a los sistemas y servicios del negocio.

Malware, son conocidos como código malicioso que tiene la intención de hacer afectaciones, daños o infiltraciones a los sistemas de información; los cuales pueden provenir desde la Internet por medio de un archivo/ejecutable descargado de internet, un correo electrónico como también desde un medio removible como USB, CD/DVD; al igual pueden ser transferidos por conexiones red entre componentes o generados desde un código fuentes para ser incorporados al sistema o dispositivo.

Metodologías para la gestión de riesgos *MAGERIT* *(Metodología de Análisis y Gestión de Riesgos de Tecnologías de la Información),* es un metodología cuantitativa, desarrollada por el Consejo superior de Administración Electrónica en España, en la cual se presenta un conjunto de actividades, procedimientos y herramientas para elaborar la gestión de riesgos tecnológicos en una organización, esto con el principal objetivo de identificar posibles amenazas en la infraestructura tecnológica y afrontar los riesgos dependiendo su nivel de criticidad. Es reconocida a nivel mundial porque permite realizar un análisis de riesgos tecnológicos completo, ordenado y de manera efectiva; la herramienta PILAR es la más usada para cumplir con la metodología, no obstante, maneja 4 etapas en el proceso: Caracterización de los activos, de las amenazas y de las salvaguardas como la Estimación del estado del riesgo.

Metodologías para la gestión de riesgos *OCTAVE* *(Operationally Critical Threat, Asset, and Vulnerability Evaluation),* es una metodología definida por la Universidad Carnegie Mellon; Está orientada a la evaluación de los riesgos de seguridad de la información , en la cual se analizan los activos con sus posibles vulnerabilidades y amenazas de seguridad, con el ánimo de que las organizaciones tomen decisiones sobre los activos críticos y a su vez propongan planes y estrategia para el control o tratamiento de los riesgos derivados; Se considera como la más usada para el cumplimiento de la norma ISO 27001.

Pentesting o pruebas de intrusión, son pruebas que comprenden análisis de vulnerabilidades para la identificación de las falencias o brechas de un sistema, la cuales después son explotadas realmente de manera controlada a fin de conocer las consecuencias que derivaría dicho hallazgo en caso de que un ciberdelincuente efectuara el ataque. Los pentesting usualmente son desarrollados por los hackers de sombrero blanco para las organizaciones de forma interna o externa a fin de conocer el estado de reacción de un sistema componente ante un ataque; bien sea con datos de caja negra (sin información) caja gris (con información elemental), caja blanca (con información), las cuales puede abordar en un análisis a nivel de seguridad en redes - comunicaciones, sistema operativos, aplicaciones, herramientas de seguridad, información relacionada o metadatos. Puede aplicar metodólogas como OSSTMM o ISSAF, entre otras. Donde OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad); la cual proporciona un enfoque orientado a la interconexión e interacción de las cosas a través de un proceso de testeo ordenado y de calidad para todos los ámbitos de la seguridad. ISSAF (Frameworks de testeo de la seguridad de las aplicaciones) se orienta en evaluar la Red de trabajo, sistema y control de aplicaciones.

Protocolos criptográficos, son protocolos de seguridad que aplican métodos de cifrado para el intercambio seguro de información, autenticación entre sistemas; gestión y distribución de claves entre los protocolos más conocido se tienen SSL

(Secure Socket Layer) con su última versión 3.0 y TLS (Transport Layer Security) el cual maneja la versión V1.3.

Ransomware, es un tipo de malware que cifra todos los archivos a los que tiene acceso una vez haya ingresado al sistema operativo afecta actualmente a cualquier sistema operativo incluido Windows con el fin de pedir un rescate en Bitcoins u otras criptomonedas para descifrar la información bloqueadas; siendo este el malware de mayor tendencia a nivel mundial en 2017. En Windows este ataque se puedes presentar como Ransom:Win32.WannaCrypt, Petya, entre otros.

Riesgo informático, es la condición que puede presentar un sistema de información, un componente o servicio tecnológico que se deriva de la posibilidad de ocurrencia e impacto que puede ocasionar una o varias amenazas sobre una vulnerabilidad técnica que presenta el sistema /componente. Los riesgos informáticos pueden asociar todos aquellos riesgos que afectan a la seguridad informática a nivel de funcionalidad-disponibilidad de los activos tecnológicos, seguridad física, controles de accesos, protección de la información, proyectos tecnológicos, entre otros; los cuales asocian de alguna forma las tecnologías de la información y las comunicaciones (TIC) y que se pueden gestionar para su control con un Sistema de Administración de Riesgos Informático (SARI).

Para la gestión de los riesgos informáticos se debe aplicar el proceso de identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos conforma a las diferentes metodologías establecidas que permiten dicha ejecución como MAGERIT, Octave, ISO 27005, entre otros.

Entre los riesgos informáticos más conocidos se tienen fraudes informáticos, pérdida o daños de la información, indisponibilidad de los servicios, entre otros. Los cuales se pueden tratar con controles apropiados de seguridad informática y algunos otros estratégicos a nivel organizacional considerando acciones como evitar, disminuir, trasferir/compartir o aceptar el riesgo según sus resultados de evaluación de los riesgos, como el apetito de riesgo que la organización esté dispuesto asumir.

Seguridad Física, se refiere a los implementos usados para proteger la organización frente a las amenazas físicas de la infraestructura tecnológica particularmente el hardware. Este tipo de seguridad se centra en cubrir las amenazas tanto de humanos como de eventos naturales a los que está expuesto el sistema de acuerdo con el medio donde está ubicado. Algunas de las amenazas que se prevén son:

- Desastres naturales o cualquier variación producida por las condiciones del ambiente y el entorno.

- Amenazas de origen externo asociadas a delincuencia común, robo, disturbios, vandalismo, etc.

- Amenazas de origen interno organizacional como, huelgas, accesos físicos no autorizado a zonas restringidas, perdida o daños de activos físicos, etc.

Sistema de control de acceso, es un control de seguridad que procesa la autenticación y posterior autorización de una solicitud, permitiendo el acceso a las instalaciones, los recursos o información requerida por el solicitante, conforme a los permisos asignados. Este control es aplicable a cualquier sistema de información, activo, persona y hasta vehículos.

Los sistemas de control de acceso se clasifican en físico y lógicos. Los físicos, son tangibles y corresponden a aquellos que permiten acceso a zona física y suelen los tipificados como autónomos; mientras que los lógicos son aquellos digitales o intangibles que están inmersos en un software y depende de la conexión a red y los servicios eléctricos para funcionar, estos se tipifican usualmente como los controlados por la red. Los tipos de sistemas de control de acceso comúnmente conocidos son:

- ***Los Autónomos***: Se manejan sin ningún tipo de software para su configuración y descarga. Usa métodos de verificación como contraseñas, tarjetas de proximidad, expresión corporal o biométrica. Este tipo de sistema es uno de los más usados para el registro de control de asistencia.
- ***Los controlados por la red***: Se soportan por medio de una computadora o servidor, ya que necesitan de un software de gestión para que realicen sus operaciones, basada en las configuraciones establecidas. Se pueden jerarquizar a nivel perfiles, roles y privilegios; ya que los accesos los pueden escalonar según la necesidad y los privilegios preestablecidos.

Sistemas de Prevención de Intrusos (IPS), son recursos que salieron de los IDS que se encargan de prevenir y bloquear los ataques que se han presentados a nivel de red, ya que soportan muchas veces las gestiones de los firewalls. Una referencia de IPS es la que presenta Cisco IPS.

Troyanos, son un programa destructivo que se hace pasar por una aplicación o documento auténtico, los cuales se pueden activar por acción humana pero no son replicables de manera autónoma, aun así generan daños a nivel de contenido, además abren puertas traseras en los sistemas lo que facilita el acceso a usuarios y programas maliciosos al mismo para robar información crítica o confidencial, y en casos excepcionales tomar el control del sistema; no obstante su finalidad es causar alteraciones o destrucción en la información almacenada en el sistema como recolectar y transmitir información a tercero o cibercriminales sin permiso.

Sistemas De Detección De Intrusos (IDS), es un recurso de seguridad que permite detectar acciones anómalas, accesos intrusivos o de ataques desde el exterior al interior del sistema informático; de tal forma que detiene y protege de amenazas a los sistemas de los componentes informáticos y a las redes. Los tipos de IDS se categorizan según su función y comportamiento entre los más comunes se encuentran:

- ***H-IDS:*** Considerado como Host-Based IDS que determinan seguridad a nivel de host detectando las acciones maliciosas en este componente a nivel de sistema operativo ya que actúa como daemon en donde analiza los registros almacenado del sistema como las conexiones de red que tiene el host a fin de verificar malware y otro tipo de ataques.
- ***N-IDS:*** Considerado como Network-Based IDS se encarga de verificar los paquetes de información intercambiados en una red para detectar acciones intrusivas y anómalas, usualmente requiere un hardware exclusivo. El N-IDS asigna adaptadores de red exclusivos del sistema en modo "invisible" en el que no tienen dirección IP, permitiendo analizar los posibles ataques y las solicitudes de tráfico que hayan pasado por el firewall o desde interior de la red según su ubicación.

Vulnerabilidad, es una debilidad o carencia que presenta un activo, ser, gobierno, entorno o sistema de información y que puede ser explotada por una amenaza. Las vulnerabilidades pueden ser de origen técnico, ambiental, físicas, económica, entorno, sociopolíticas, humana, entre otras; que en su conjunto o de manera particular pueden afectar directa o indirectamente a los activos de información y a los componentes tecnológicos ocasionando riesgos informáticos.

No obstante para efectos de la seguridad informática la vulnerabilidad se constituye en las brechas o agujeros de seguridad que se derivan por la carencia, falencia o debilidad de los controles de seguridad lo que compromete la confidencialidad, integridad, disponibilidad de los activos tecnológicos y/o sistema de información haciéndolos susceptible a un ataque; comúnmente estas vulnerabilidades son de origen técnico, por lo que se pueden catalogar como vulnerabilidades técnicas entre las que se destacan los errores de configuración, parches desactualizados, resguardo sin protección, contraseñas débiles, entre otros.

Virus informáticos, son programas o un fragmento de código que se alojan en un sistema de cómputo sin consentimiento, cuyo objetivo es infectar y tomar el control de los sistemas vulnerables hasta hacer destrucciones de los mismos. Un virus informático no puede propagarse ni activarse sin la acción humana, por lo que no puede hacer copias de sí mismo, y su activación se puede dar con el acceso o clic sobre su contenido el cual viene oculto en un programa o archivo que se alojara en la memoria atacando directamente al sistema operativo y sus funcionalidades.

5.4. MARCO NORMATIVO

Las pasarelas de pagos como organizaciones que ofrecen “servicios de aplicación de comercio electrónico para almacenar, procesar y/o transmitir el pago correspondiente a operaciones de venta en línea”[29], están regidas o regulada por la Superintendencia Financiera de Colombia (SFC); la cual a través de su Circular Externa 008 del 05 de junio de 2018 exige en su numeral 2.3.8.1.1 la implementación y certificación del estándar PCI DSS; así como, el mantenimiento de esta certificación conforme al numeral 2.3.8.2 de la misma circular. Por lo anterior, estas organizaciones que cuentan con una estructura especifican en recursos tecnológicos, de procesos y personal; han venido gestionando la seguridad de la información para sus servicios financieros certificándolos bajo la Norma ISO 27001 en cumplimiento al numeral 2.3.3.1.2 de la Parte I - Titulo II - Capítulo I de la Circular Básica Jurídica 029 del 03 de octubre de 2014, el cual es extensivo a la Circular Externa 008 de 2018.

Por otra parte, las organizaciones que manejan datos del titular de la tarjeta (CHD) y/o datos confidenciales de autenticación (SAD) deben garantizar el cumplimiento a los artículos 15 y 20 de la Constitución Política de Colombia por lo que se provee para ello de la Ley de 1266 de 2008[30] asociada al Habeas Data en la que se regula los datos personales y financieros de los usuarios que hacen parte de los contextos financieros y crediticios; como también se dispone de la Ley 1581 de 2012[31] asociada a la protección de los datos personales custodiados y/o almacenados en cualquier base de datos que sea objeto de tratamiento por parte de entidades de naturaleza pública o privada. Por lo que las pasarelas de pago de algún modo deben sustentar sus esfuerzos para establecer el cumplimiento del estándar PCI DSS no solo por la exigencia de la Circular Externa 008 de 2018 de la SFC; sino también, para brindar las garantías de seguridad que se requieren en el cumplimiento de las leyes establecidas en pos de los datos personales que sería extensible de algún modo a los datos CHD, los cuales se aplican a los usuarios finales catalogados en su mayoría como personas naturales.

[29] Superintendencia Financiera de Colombia. Circular Externa N° 008, 2018 Parte 1 Titulo II Cap I Literal 2.2.10. P.9.

[30] Congreso de la Republica de Colombia. Ley estatutaria 1266 de 2008. 2008. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[31] Congreso de la Republica de Colombia. Ley estatutaria 1581 de 2012. 2012. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

5.5. ANTECEDENTES

Los proveedores de servicios (PS) que gestionan datos CHD y/o SAD de las tarjetas de pago como lo serían las pasarelas de pagos, se han esforzado por cumplir con los requisitos del estándar PCI DSS para lograr la seguridad y protección de estos datos que hacen parte de sus operaciones o servicios; pero, para esto han acudido al apoyo de algunas QSA (Qualified Security Assessor), a consultores que conocen del estándar y/o a validar los aspectos analizados por el gremio académico; quienes en su experticia han definido diferentes estrategias o teorías para cumplir con el estándar de acuerdo al tipo servicio prestado o gestión de los datos que realizan las organizaciones del sector financiero y/o los PS: Definiciones que a continuación se resumen como antecedentes para dar preámbulo a la constitución de este proyecto:

A. Los especialistas en Seguridad informática Casallas, Perdomo y Vargas de la Universidad Piloto de Colombia en su trabajo de grado del año 2016 denominado "Guía de implementación de herramientas tecnológicas dirigida a las pymes para dar cumplimiento a la norma internacional PCI DSS V3.0"; establecen los costos de la implementación del estándar PCI DSS analizando los pros y contra de implementar herramientas tecnológicas de software libre o licenciada para dar cumplimiento a los requisitos del estándar, concluyendo que las herramientas comerciales/licenciadas pueden salir muy costosa y derivarían una amplia inversión para el proceso de implementación del estándar en una Pyme considerando además que debe invertirse millonarias cuantías para los otros procesos de la implementación de los requisitos del estándar que no implican un tema tecnológico, incluyendo los gastos de la auditoria y evaluación para la certificación del estándar.[32] Por tanto, una pasarela de pagos que no tenga tanto número de transacciones y su operación se categorice como una empresa de tipo Pyme puede verse en apuros si no sabe cómo abordar el costo beneficio de cumplir con este estándar.

B. Los especialistas en auditoría de Sistemas de información Sanabria y Sarmiento de la Universidad Católica de Colombia en su trabajo de grado del año 2018 denominado "Metodología de auditoría para verificar el nivel de cumplimiento del proceso de desarrollo de software frente a los requisitos de la norma PCI DSS en la compañía ABPS"; afirman que ABPS como empresa que ofrece servicios de Contact Center en su ánimo evolutivo quiere incursionar en la prestación de sus servicios al entorno financiero por lo que analizan a través de una auditoria si el proceso de desarrollo de software que

[32] CASALLAS, Hugo; PERDOMO, Javier y VARGAS, Julio. Guía de implementación de herramientas tecnológicas dirigida a las pymes para dar cumplimiento a la norma internacional PCI DSS V3.0. Universidad Piloto de Colombia. 2016. p.140. Disponible en: http://polux.unipiloto.edu.co:8080/00002970.pdf

ellos llevan para sus sistemas de información se encuentra apto en el cumplimiento del estándar PCI DSS especialmente en lo referente al requisito 6 del estándar que se enfoca en desarrollar y mantener sistemas y aplicaciones seguros; a lo que concluyen que a pesar de tener un 96% de cumplimiento del requisito se presentan falencias en un 4% de las medidas requeridas para la empresa por lo que no aprobarían el cumplimiento del estándar,[33] y menos acreditarían la certificación en caso de que se arriesgaran a un proceso de certificación con una QSA. Lo que demuestra que el nivel de exigencia de PCI DSS es muy alto ya que exige un cumplimiento total (100%)

C. La pasarela de pagos Place to Pay, fue una de las primeras organizaciones colombiana de esta industria en lograr la certificación de nivel 1 para PCI DSS desde el año 2013, acreditación que han sostenido en las diferentes versiones del estándar hasta la fecha incluyendo la versión actual la 3.2.1 con el apoyo de la empresa ControlCase, que es la QSA que certifica dicho cumplimiento.[34] Lo anterior con el fin de preservar la seguridad de la información en sus procesos transaccionales y en respaldo a las disposiciones impuestas por la Superintendencia Financiera de Colombia (SFC)[35]a lo cual han tenido resultados positivos frente a sus esfuerzos por cumplir con esta normatividad y que la posicionan en una de las plataformas líder en el país[36] así estén obligados anualmente a certificar el cumplimiento estricto para todos los requisitos indicados por el estándar y asumir el alto costo que esto implique.

D. La multinacional PayU de origen colombiano ofrece sus servicios de pasarela de pago en más de 7 países de Latinoamérica y 16 alrededor del mundo, está catalogada como la pasarela de pagos líder en Colombia con más del 70% del mercado según la Cámara Colombiana de Comercio Electrónico (CCE) cuando existen más de 97 pasarelas operando en el país.[37] No obstante, la compañía durante sus más de 17 años de funcionamiento le tocó vivir en

[33] SANABRIA, Richard y SARMIENTO, Javier. Metodología de auditoría para verificar el nivel de cumplimiento del proceso de desarrollo de software frente a los requisitos de la norma PCI DSS en la compañía ABPS. Universidad Católica de Colombia. 2018. p.39. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/16058/1/Metodolog%C3%ADa%20%20Auditoria%20DS%20PCI%20DSS%20ABPS.pdf

[34] CONTROLCASE. PCICompliant. Disponible en: https://seal.controlcase.com/index.php?page=showCert&cId=3594404955

[35] CADAVID CORREA, Orlando y GIRALDO OSPINA, Evelio. Plataformas de pagos electrónicas. Disponible en: https://www.eje21.com.co/2018/11/desde-diciembre-se-empezara-a-exigir-a-las-pasarelas-de-pagos-digitales-sistemas-de-proteccion-de-datos/

[36] VENEGAS LOAIZA, Andrés. El número de pasarelas de pago en línea en Colombia ha crecido 53,9%. En: LA REPUBLICA. 2019. Disponible en: https://www.larepublica.co/internet-economy/el-numero-de-pasarelas-de-pago-en-linea-en-colombia-ha-crecido-539-2828821

[37] Ibid.

algunos momentos pesadillas con la seguridad, por lo que han aplicado procesos de mejora continua en sus tecnologías para el servicio Core, como la aplicación de la tokenizacion,[38] monitoreo a las transacciones, pruebas de seguridad, entre otras acciones;[39] las cuales van encaminadas a la aplicación del estándar PCI DSS y a la reducción de los fraudes; y que le han permitido acreditar hoy en día el cumplimiento del estándar y posicionarse en el 2018 entre las empresas Fintech del mundo.[40]

E. Las ingenieras de sistemas Calle y Mejía de la Universidad Politécnica Salesiana con sede en Guayaquil para el año 2015 plantearon una tesis en la que analizan "la implementación del estándar PCI DSS en la seguridad de la información en instituciones financiera", en la que practican un muestreo a quince (15) entidades financieras y unas encuestas a los empleados del área de sistemas de estas instituciones; concluyen que el 25% de estas entidades no cuenta con la certificación en el estándar PCI DSS ya que dejan esta responsabilidad a sus proveedores de servicios (PS) y que la mitad del personal encuestado no tiene conocimientos contundentes sobre el estándar y más cuando carecen de campañas para la seguridad de la información.[41]

F. La compañía Microsoft en el año 2017 publicó una guía de planeación para el cumplimiento del Estándar PCI DSS que sustenta las generalidades del estándar encaminadas a su aplicación con el uso de las soluciones tecnológicas que ofrece Microsoft, pero esta orientación es demasiado técnica por lo que va dirigida al personal con rol técnico o de auditor en las diferentes entidades que gestionan datos de las tarjetas de pago; por lo que no entra en detalle frente a las distintas necesidades del estándar en cada organización a lo que lo misma compañía sugiere que dichos detalles deben ser tratados con un asesor jurídico o auditor.[42]

---

[38] PAYU. Tokenización. Disponible en: https://www.payulatam.com/co/caracteristicas/tokenizacion/

[39] FRÍAS, Gabriela. La empresa colombiana que monitorea 850.000 compras en línea al día en todo el mundo. En: CNN ESPAÑOL Disponible en: https://cnnespanol.cnn.com/2017/05/29/la-empresa-colombiana-que-monitorea-850-000-compras-en-linea-al-dia-en-todo-el-mundo/

[40] SCHULTZE, Juan Francisco. Haciendo historia en el mundo Fintech hace 15 años. En: LA REPUBLICA. 2018. Disponible en: https://www.larepublica.co/finanzas-personales/haciendo-historia-en-el-mundo-fintech-hace-15-anos-2591334

[41] CALLE PARRALES Zoila y MEJÍA VILLEGAS, Andrea. "Análisis de la implementación del estándar PCI DSS en la seguridad de la información dentro de una institución financiera". Universidad Politécnica Salesiana Sede Guayaquil. 2015. p. 75-76. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/10317/1/UPS-GT001222.pdf

[42] MICROSOFT. Guía de planeación para el cumplimiento del Estándar de seguridad de datos en la industria de tarjetas de pago. Disponible en: https://docs.microsoft.com/es-es/security-updates/security/guadeplaneacinparaelcumplimientodelestndardeseguridaddedatosenlaindustriadetarjetasdepago

6. DISEÑO METODOLÓGICO

La parte metodológica de esta monografía estará sustentada por la Técnica del Análisis de Contenido que consiste en que pueda definirse como la clasificación de las diferentes partes de un escrito formen categorías especificas en la investigación, a fin de conseguir información relevante con amplia tendencia manifiesta en el documento.

Para esta técnica se requiere que las categorías tengan las cualidades señaladas para otros instrumentos de investigación, tales como la veracidad y la validez, que deben instituirse en un solo principio de clasificación, para que el proceso investigativo sea completo e incluya todas las respuestas esperadas para dar solución a la problemática planteada. Es de ahí que en el curso de esta Guía se aplicará 3 métodos de análisis de contenido:

A. ***Levantamiento de la información,*** en el cual se hará la identificación de los requisitos que exige el estándar PCI DSS V.3.2.1 con los aspectos claves de seguridad informática, para que sean correlacionados con el servicio o funcionalidad que ofrecen las empresas de pasarela de pagos; con el propósito de definir los requerimientos que le son necesarios en implementar a las pasarelas con respecto a este estándar.

   Para la toma de los datos del levantamiento de información que dará cumplimiento al primer (1) objetivo específico se analiza el contenido soportado en el estándar PCI DSS en las versiones reciente que para el caso es la V3.2.1 de 2018; a fin de tomar las variables correspondientes.

B. ***Gestión de riesgos,*** pretende apropiar una metodología para la gestión de riesgos que será aplicable a seguridad informática; a fin de que se puedan presentar los posibles riesgos en seguridad informática asociados al cumplimiento del estándar PCI DSS V3.2.1 para una pasarela de pagos contemplando las bases que la ISO 31000 ofrece como estándar para la gestión de los riesgos en varias etapas que están orientadas a las organizaciones para que sean consideradas en su aplicación como lo son: un establecimiento de contexto, realizar una identificación, análisis, evaluación, tratamiento, monitoreo y revisión de los riesgos con comunicación continua a las partes interesadas; de estas etapas solo se sustentaran las 3 primeras con base a la información proporcionada por algunas pasarelas de pago y las investigaciones técnicas dando cubrimiento con esto al segundo (2) objetivo específico de esta monografía.

   Para ello se toman las buenas prácticas descritas en la siguiente tabla 2 que estable las principales metodologías de riesgos:

Tabla 2. Principales Metodologías de Riesgos

METODOLOGÍA	DETALLES	VENTAJAS	DESVENTAJAS
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	• Es una metodología desarrollada por la Universidad Carnegie Mellon. Está orientada a la evaluación de los riesgos de seguridad de la información, en la cual se analizan los activos con sus posibles vulnerabilidades y amenazas de seguridad, con el ánimo de que las organizaciones tomen decisiones sobre los activos críticos y a su vez propongan planes y estrategia para el control o tratamiento de los riesgos derivados. • Puede establecerse por 3 métodos: El método simplificado OCTAVE -S útil para organizaciones pequeñas de hasta 100 personas; El método OCTAVE ALLEGRO que es intermedio y se centra en los activos de información; y el método OCTAVE convencional que es el más completo y es recomendable en empresa 300 personas que centra visión global de la organización, su seguridad y los activos de información.	• Es un método operativo que se orienta a resultados • Se puede adaptar para cualquier organización grande o pequeña de origen público o privado. • Relaciona las amenazas con las vulnerabilidades • Desarrolla planes y estrategias. • Involucra a todas las partes interesadas incluido el personal, los activos, áreas, procesos y controles.	• Debe tenerse claridad del contexto para establecer idóneamente el método a convenir en la organización a fin de que no se vuelva un proceso complejo e ineficiente. • No considera el principio de no repudio de la información
MAGERIT (Metodología de Análisis y Gestión de Riesgos de Tecnologías de la Información)	• Es una metodología cuantitativa desarrollado por el Consejo Superior de Administración Electrónica, que centra su gestión para los riesgos de los sistemas de información tecnológicos. • Se estructura en 3 libros que definen: 1. El Método, 2. Catálogo de elementos y 3. Guía Técnica; los cuales contempla 4 fases: Planificación, Identificación de activos y amenazas, Análisis de riesgos y Selección de salvaguardas.	• Útil y completa en la gestión de riesgos informáticos y/o tecnológicos bajo un análisis cuantitativo y cualitativo. • Analiza las dependencias de activos. • Existen herramientas para cumplir con la metodología y la más común es PILAR.	• Se orienta más riesgos informáticos y/o de seguridad informática, sin dar cubrimiento a otros elementos de la seguridad de la información. • No involucra procesos, recursos, ni vulnerabilidades

Tabla 2. (Continuación)

METODOLOGÍA	DETALLES	VENTAJAS	DESVENTAJAS
NIST SP 800 – 30	• Es una metodología desarrollada por la National Institute of Standards and Technology bajo la serie SP-800, aplicable en riesgos de seguridad de la información y las tecnologías. • Establece entradas y salidas que se orientan a un flujo de proceso dando respuesta a 9 criterios de evaluación de riesgo que son: Caracterización del sistema; Identificación de amenaza; Identificación de vulnerabilidades; Control de análisis; Determinación del riesgo; Análisis de impacto; Determinación del riesgo; Recomendaciones de control; Documentación del resultado.	• Útil para caracterizar un Sistema de TI y Su entorno operativo • Se recomienda su uso para Análisis de Impacto de Negocios (BIA) • Permite presentar resultados de prueba técnicas proveyendo los resultados de valoración y mitigación de riesgos	• Enfoca su medición de riesgos en un análisis de impacto y controles • Se orienta más riesgos informáticos y/o de seguridad informática, sin dar cubrimiento a otros elementos de la seguridad de la información, ni contemplar a los activos, procesos, dependencias.
ISO 27005	• Es la metodología propuesta por ISO dentro del estándar de la ISO/IEC 27000 en pos de cubrir las expectativas de la ISO/IEC 27001; su antigua versión era la 2011 y recientemente esta la versión en inglés 2018. • Establece el proceso cíclico/ repetitivo asociado a establecimiento de contexto, análisis, evaluación, tratamiento monitoreo y revisión del riesgo con comunicación continua para determinar la aceptación del riesgo y el análisis continuo.	• Es adaptable a cualquier organización que quiere certificarse en ISO/IEC 27001	Esta metodología solo es útil para cumplir ISO/IEC 27000 y necesita complementarse con otras metodologías si se quiere adoptar a para cumplir con otros estándares o normas asociadas a la seguridad.
CRAMM (CCTA Risk Analysis and Management Method)	• Es una metodología diseñada por Agencia Central de Comunicación y Telecomunicación del gobierno británico. • Considera 3 etapas en la cuales la primera acoge un contexto global de la organización a fin de identificar y valorar los activos físicos y software; la segunda etapa analiza los riesgos partiendo de las amenazas y vulnerabilidades identificadas a fin de dar estimación a los riesgos y la tercera etapa gestiona la identificación y selección de medidas de seguridad con el fin de obtener los riesgos residuales.	• Se asemeja a la metodología MAGERIT pero esta considera más de 4000 medidas de seguridad. • Evalúa los impactos empresariales, de forma explícita. • Protege todo el principio de seguridad y se puede adaptar a cualquier servicio TI	• Es útil solo en empresa de gran tamaño. • No considera a los procesos y recursos

Tabla 2. (Continuación)

METODOLOGÍA	DETALLES	VENTAJAS	DESVENTAJAS
MEHERI (Método Armonizado de Análisis de Riesgos)	Es método cuantitativo establecido por el CLUSIF (Club de seguridad de información francés), que se adopta en apoyo a los responsables de la seguridad de una organización en su gestión de las actividades de la seguridad informática; está orientada al análisis de los riesgos a nivel de confidencialidad, integridad y disponibilidad; considerando el enfoque establecido por la ISO 27005. Propone el uso de herramientas, el análisis de intereses y brechas de seguridad derivado de las auditorias y de las evaluaciones a la seguridad; las cuales deben estar sustentada por las políticas de seguridad y estrategias organizacionales. Los temas esenciales de esta metodología son: diseño de un modelo de riesgo, evaluación de la eficiencia de las políticas de seguridad existentes en la organización y capacidad para valorar y simular los niveles de riesgo	• Utiliza método cuantitativo y cualitativo para el análisis. • Se adapta con las del estándar ISO 27000 orientado a un enfoque global para el Sistema de Gestión de Seguridad de la información – SGSI • Maneja un módulo de evaluación rápida y otro detallado	• No considera el principio de no repudio de la información • El impacto se valora en la etapa de evaluación
CORAS (Construct a Platform for Risk Analysis of Security Critical Systems)	Esta metodología surge del proyecto desarrollado desde el año 2001 por Sintef, que se enmarca a sistemas o software críticos que requieren de un alto nivel de seguridad. Su implementación permite detectar fallas de seguridad, inconsistencias, redundancia y el descubrimiento de vulnerabilidades de seguridad. Consta de 7 etapas: presentación, análisis de alto nivel, aprobación, identificación de riesgos, estimación de riesgo, evaluación de riesgo y tratamiento del riesgo.	• Se integra con modelos de leguaje haciendo asequible la interacción entre distintas partes del proceso de análisis de riesgo. • Validas las vulnerabilidades encontradas o semejantes	• No realiza análisis cuantitativo • No contempla los procesos y las dependencias
Ebios (Expresión de las necesidades e identificación de los objetivos de seguridad)	Método francés que analiza y gestiona riesgos para sistemas de información por lo que es útil para los gestores de riesgos TI o desarrollo de software Se establece mediante cinco (5) fases: Fase 1: estudio del contexto; Fase 2: estudio de los eventos peligrosos; Fase 3: estudio de los escenarios de amenazas; Fase 4: estudio de los riesgos; Fase 5: estudio de las medidas de seguridad. Así mismo considera descripciones precisas, retos estratégicos, riesgos detallados con su	• Ofrece los mecanismos para justificar la toma de decisiones. • Se considera una herramienta de negociación y arbitraje. • Se acopla a ISO 27001 y 27005.	• Se considera más como una herramienta de soporte que una metodología de riesgos

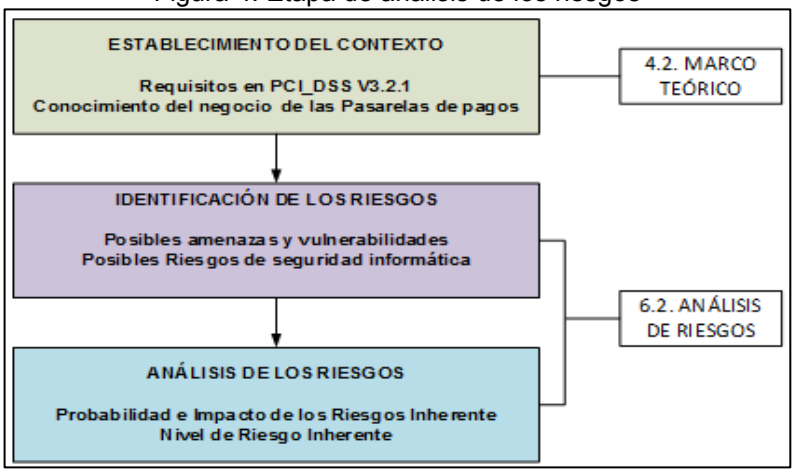
Tabla 2. (Continuación)

METODOLOGÍA	DETALLES	VENTAJAS	DESVENTAJAS
	impacto en el organismo, objetivos y requerimientos de seguridad explícitos.	• Permite la concienciación.	
Método DELPHI	Es un método cualitativo establecido por RandCorporation con el fin de encontrar opiniones fiables de expertos especialmente externos a la empresa. Está orientado a la concertación y criterios de los expertos, cuando no se tiene información o data relacionada para el análisis de los riesgos, el cual se soporta por la generación de cuestionarios que se envían en múltiples fases a terceros anónimos para sus respuestas, las cuales se analizan o concluyen en cada fase; lo que permite la subjetividad dentro de los riesgos reportados.	• Maneja un modelo estadístico e interactivo donde actúan varios actores donde todo va orientados a la experiencia. • Permite el control de influencia y la gestión discreta del análisis	• Puede arrojar datos subjetivos por lo que no tiene una gestión racional sino intuitiva • Requiere de material para cuestionar a los involucrados

Fuente:http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

De conformidad con los anterior para el desarrollo de esta guía se empleará la metodología para gestión de riesgos Octave - Allegro, debido a que esta exige menos recursos o insumos en su consecución, permitiendo con esto un análisis de riesgo de una forma mucho asertivo para el escenario de las pasarelas de pago sobre el cumplimiento del estándar PCI DSS; por lo que desarrollo de esta metodología se efectuará desde el establecimiento del contexto el cual se sustenta con el numeral 4.2. Marco teórico de esta guía hasta la etapa de análisis de los riesgos que se desarrolla en el numeral 6.2. Análisis de Riegos de este documento. Tal y como se representa en la siguiente figura 4:

Figura 4. Etapa de análisis de los riesgos



Fuente: Propia

C. ***Exploración investigativa,*** en el cual se investigarán las variables de los aspectos claves de seguridad informática que deben aplicarse a las pasarelas de pago para el cumplimiento del estándar PCI DSS V3.2.1, de los cuales ya varias de estas organizaciones han implementado exitosamente. Así mismo, bajo este método se investigarán las exigencias e hitos que evalúa una empresa QSA en Colombia para realizar la evaluación en el estándar PCI DSS V3.2.1 y las consideraciones que deben tener las pasarelas de pago para la implementación, certificación y sostenimiento del estándar.

Para poder efectuar las exploraciones investigativas se usa la técnica de recolección de información suministrada por los sitios y páginas web disponibles en Internet que provengan de fuentes de confianza; por lo que los referentes de esta Guía serán de tipo documental o bibliográfico y para ello se ha analizado la información que ofrece PCI_SSC en su página oficial y los sitios web de algunas pasarelas de pago establecidas en Colombia como Place to pay, PayU, Pagos Inteligente, PagoÁgil, MyChoice2Pay, entre otras.

7. DESARROLLO

7.1. REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS

En este numeral se especifican los requerimientos para cumplir con el estándar de PCI DSS V 3.2.1, a los cuales se vinculan los sub-requisitos predefinidos en el estándar que establecen cada uno de los procedimientos a implementar para poder cumplir con todos los requisitos y apéndices de esta normatividad y que serán objeto de prueba o evaluación según el alcance de cualquier organización. No obstante, como aporte a las pasarelas de pagos en los siguientes ítems de este numeral se determina la aplicabilidad efectiva de los requerimientos de PCI DSS V3.2.1 para estas organizaciones; que se pueden apoyar de las consideraciones para una pasarela de pago, las cuales serán de soporte o guía de estos requerimientos junto con los entregables y las dependencias entre sub-requisitos para la implementación coherente del estándar en este tipo de organizaciones; soportes que en su conjunto se encontrarán detallados en el ***Anexo A*** que soporta este documento.

7.1.1. Requisito 1: Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta

7.1.1.1. *Sub-requisito 1.1:* Se debe establecer e implementar estándares de configuración en los firewall y enrutadores, por lo que tiene que ejecutarse los procedimientos 1.1.1 al 1.1.7 que están asociados a este sub-requisito perteneciente al requisito 1; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.1.2. *Sub-requisito 1.2:* Se debe desarrollar parametrizaciones en los firewalls y routers que limiten las conexiones con redes inseguras y cualquier componente del sistema en el CDE, por lo que tiene que implementarse el o los procedimiento(s) 1.2.1 al 1.2.3 que están asociados a este sub-requisito perteneciente al requisito 1; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.1.3. *Sub-requisito 1.3:* Se debe prohibir el acceso abierto a Internet con todos los componentes del sistema en el CDE, por lo que tiene que implementarse el o los procedimiento(s) 1.3.1 al 1.3.7 que están asociados a este sub-requisito perteneciente al requisito 1; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.1.4. *Sub-requisito 1.4:* Se debe instalar herramientas de firewall personal o su equivalencia en los dispositivos móviles (corporativos y/o personales de los empleados) que tengan acceso a Internet cuando no están en la red corporativa, por lo que tiene que implementarse el o los procedimiento(s) 1.4 que están asociados a este sub-requisito perteneciente al requisito 1; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.1.5. *Sub-requisito 1.5:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos operacionales para administrar los firewalls, por lo que tiene que implementarse el o los procedimiento(s) 1.5 que están asociados a este sub-requisito perteneciente al requisito 1; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.2. Requisito 2: No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad

7.1.2.1. *Sub-requisito 2.1:* Se debe cambiar los valores por defecto del fabricante y suprimir o inhabilitar las cuentas predefinidas no necesarias previamente a la instalación de un sistema en la red., por lo que tiene que implementarse el o los procedimiento(s) 2.1 incluyendo 2.1.1 que están asociados a este sub-requisito perteneciente al requisito 2; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.2.2. *Sub-requisito 2.2:* Se debe generar estándares de configuración para todos los componentes del sistema que hagan parte del CDE, asegurándose de que estos estándares contemplen las vulnerabilidades de seguridad conocidas y sean consistentes con los sistemas aceptados por la industria; por lo que tiene que implementarse el o los procedimiento(s) 2.2 incluyendo 2.2.1 al 2.2.5 que están asociados a este sub-requisito perteneciente al requisito 2; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.2.3. *Sub-requisito 2.3:* Se debe cifrar toda conexión administrativa que no sea de consola aplicando un esquema de cifrado seguro, por lo que tiene que implementarse el o los procedimiento(s) 2.3 que están asociados a este sub-requisito perteneciente al requisito 2; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.2.4. *Sub-requisito 2.4:* Se debe tener un inventario de los componentes que hacen parte del alcance de PCI DSS, por lo que tiene que implementarse el o los procedimiento(s) 2.4 que están asociados a este sub-requisito perteneciente al requisito 2; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.2.5. *Sub-requisito 2.5:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos operacionales para administrar los parámetros por defecto del fabricante y otras configuraciones de seguridad, por lo que tiene que implementarse el o los procedimiento(s) 2.5 que están asociados a este sub-requisito perteneciente al requisito 2; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.2.6. *Sub-requisito 2.6:* Sí se proveen de un hosting compartido deben proteger el entorno y los datos CHD que aloja la entidad. Aplicando los requerimientos definidos en el Apéndice A1, por lo que tiene que implementarse el o los procedimiento(s) 2.6 que están asociados a este sub-requisito perteneciente al requisito 2; los cuales son unos de los requerimientos condicionados en su cumplimiento para una pasarela de pagos que sería aplicable en el caso de tener su entorno CDE en un hosting compartido con un tercero.

7.1.3. Requisito 3: Proteger los datos CHD que fueron almacenados

7.1.3.1. *Sub-requisito 3.1:* Se debe mantener reducido el almacenamiento de datos CHD ejecutando políticas, procedimientos y procesos de conservación y supresión de datos, por lo que tiene que implementarse el o los procedimiento(s) 3.1 que están asociados a este sub-requisito perteneciente al requisito 3; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.3.2. *Sub-requisito 3.2:* No se debe almacenar datos SAD después de recibir la autorización (Aunque estén cifrados), convertirlos en datos en irrecuperables una vez culminada la autorización, por lo que tiene que implementarse el o los procedimiento(s) 3.2 incluyendo 3.2.1 al 3.2.3 que están asociados a este sub-requisito perteneciente al requisito 3; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.3.3. *Sub-requisito 3.3:* Se debe enmascarar el PAN, en el que únicamente el personal autorizado por temas comerciales pueda acceder a los primeros 6 o los últimos 4 números del PAN, por lo que tiene que implementarse el o los procedimiento(s) 3.3 que están asociados a este sub-requisito

perteneciente al requisito 3; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.3.4. *Sub-requisito 3.4:* Se debe volver ilegible el PAN en cualquier lugar donde sea almacenado, por lo que tiene que implementarse el o los procedimiento(s) 3.4 incluyendo 3.4.1 que están asociados a este sub-requisito perteneciente al requisito 3; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.3.5. *Sub-requisito 3.5:* Se debe documentar e implementar procedimientos que aseguren las claves usadas para la protección de los datos CHD que se almacenan a fin de evitar una divulgación o uso indebido, por lo que tiene que implementarse el o los procedimiento(s) 3.5 incluyendo 3.5.1 al 3.5.4 que están asociados a este sub-requisito perteneciente al requisito 3; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.3.6. *Sub-requisito 3.6:* Se debe documentar e implementar todos los procesos y procedimientos para administrar las claves de las llaves de cifrado que se usan para cifrar de datos CHD, por lo que tiene que implementarse el o los procedimiento(s) 3.6 incluyendo 3.6.1 al 3.6.8 que están asociados a este sub-requisito perteneciente al requisito 3; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.3.7. *Sub-requisito 3.7:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos operacionales para proteger los datos CHD almacenados, por lo que tiene que implementarse el o los procedimiento(s) 3.7 que están asociados a este sub-requisito perteneciente al requisito 3; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos

7.1.4. Requisito 4: Cifrar la transmisión de los datos CHD en las redes públicas abiertas

7.1.4.1. *Sub-requisito 4.1:* Se debe usar cifrado fuerte y protocolos de seguridad para la protección de los datos CHD confidenciales durante transacción por redes públicas abiertas, por lo que tiene que implementarse el o los procedimiento(s) 4.1 incluyendo 4.1.1 que están asociados a este sub-requisito perteneciente al requisito 4; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.4.2. *Sub-requisito 4.2:* No se debe enviar el PAN desprotegido a través de las tecnologías de mensajería del usuario final como el correo electrónico, mensajes de texto, entre otros; por lo que tiene que implementarse el o los procedimiento(s) 4.2 que están asociados a este sub-requisito perteneciente al requisito 4; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.4.3. *Sub-requisito 4.3:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos operacionales para cifrado de las transmisiones de los datos CHD., por lo que tiene que implementarse el o los procedimiento(s) 4.3 que están asociados a este sub-requisito perteneciente al requisito 4; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.5. Requisito 5: Proteger todos los sistemas contra malware y actualizar los programas o sistema de antivirus regularmente

7.1.5.1. *Sub-requisito 5.1:* Se debe implementar un software antivirus/ antimalware en todos los sistemas que puedan verse vulnerables a códigos malicioso, por lo que tiene que implementarse el o los procedimiento(s) 5.1 incluyendo 5.1.1 al 5.1.2 que están asociados a este sub-requisito perteneciente al requisito 5; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.5.2. *Sub-requisito 5.2:* Se debe garantizar que las herramientas de antivirus cumplan las exigencia de PCI DSS, se mantenga actualizada, haga análisis periódicos y genere logs de auditoria, por lo que tiene que implementarse el o los procedimiento(s) 5.2 que están asociados a este sub-requisito perteneciente al requisito 5; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.5.3. *Sub-requisito 5.3:* Se debe garantizar que las herramientas de antivirus funcionen activamente y que no permitan su inhabilitación, ni alteración por los usuarios no autorizados sin previa aprobación gerencial delimitada, por lo que tiene que implementarse el o los procedimiento(s) 5.3 que están asociados a este sub-requisito perteneciente al requisito 5; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.5.4. *Sub-requisito 5.4:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos

operacionales para proteger los sistemas contra código malicioso, por lo que tiene que implementarse el o los procedimiento(s) 5.4 que están asociados a este sub-requisito perteneciente al requisito 5; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.6. Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros

7.1.6.1. *Sub-requisito 6.1:* Se debe establecer un proceso de detección de las vulnerabilidades de seguridad haciendo uso de fuentes externas conocidas para su información y asignándoles una clasificación de riesgo a las recientemente descubiertas., por lo que tiene que implementarse el o los procedimiento(s) 6.1 que están asociados a este sub-requisito perteneciente al requisito 6; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.6.2. *Sub-requisito 6.2:* Se debe garantizar a todos los software y componentes del sistema tengan instalados los parches de seguridad proporcionados por los fabricantes que otorgan protección contra vulnerabilidades conocidas, las remediaciones importantes se deberían hacer el primer mes del lanzamiento parche, por lo que tiene que implementarse el o los procedimiento(s) 6.2 que están asociados a este sub-requisito perteneciente al requisito 6; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.6.3. *Sub-requisito 6.3:* Se debe desarrollar aplicaciones de software de forma segura siguiendo las directrices de PCI DSS, por lo que tiene que implementarse el o los procedimiento(s) 6.3 incluyendo 6.3.1 al 6.3.2 que están asociados a este sub-requisito perteneciente al requisito 6; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.6.4. *Sub-requisito 6.4:* Se debe aplicar los procesos y procedimientos de control de cambios en los componentes del sistema, por lo que tiene que implementarse el o los procedimiento(s) 6.4 incluyendo 6.4.1 al 6.4.6 que están asociados a este sub-requisito perteneciente al requisito 6; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.6.5. *Sub-requisito 6.5:* Se debe tratar las vulnerabilidades comunes de código fuente en los procesos de desarrollo de software considerando capacitaciones anuales en los desarrolladores en técnicas y directrices para desarrollo seguro de software , por lo que tiene que implementarse el o los procedimiento(s) 6.5 incluyendo 6.5.1 al 6.5.10 que están

asociados a este sub-requisito perteneciente al requisito 6; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.6.6. *Sub-requisito 6.6:* Se debe tratar las nuevas amenazas y vulnerabilidades continuamente y garantizar que las aplicaciones web públicas se aseguren contra ataques, por lo que tiene que implementarse el o los procedimiento(s) 6.4 incluyendo 6.4.1 al 6.4.6 que están asociados a este sub-requisito perteneciente al requisito 6; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.6.7. *Sub-requisito 6.7:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos operacionales para desarrollar y mantener de forma segura los sistemas y las aplicaciones, por lo que tiene que implementarse el o los procedimiento(s) 6.7 que están asociados a este sub-requisito perteneciente al requisito 6; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.7. Requisito 7: Restringir el acceso a los datos CHD según la necesidad de saber que tenga la empresa

7.1.7.1. *Sub-requisito 7.1:* Se debe limitar el acceso a los componentes del sistema y a los datos CHD a las personas autorizadas, por lo que tiene que implementarse el o los procedimiento(s) 7.1 incluyendo 7.1.1 al 7.1.4 que están asociados a este sub-requisito perteneciente al requisito 7; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.7.2. *Sub-requisito 7.2:* Se debe establecer un sistema de control de acceso para los componentes del sistema que limite la accesibilidad según sea requerido y que se parametrice para “negar todo”, por lo que tiene que implementarse el o los procedimiento(s) 7.2 incluyendo 7.2.1 al 7.2.3 que están asociados a este sub-requisito perteneciente al requisito 7; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.7.3. *Sub-requisito 7.3:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos operacionales para restringir el acceso a los datos CHD, por lo que tiene que implementarse el o los procedimiento(s) 7.3 que están asociados a este sub-requisito perteneciente al requisito 7; los cuales son unos de los

requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.8. Requisito 8: Identificar y autenticar el acceso a los componentes del sistema

7.1.8.1. *Sub-requisito 8.1:* Se debe definir e implementar las políticas y procedimientos para la adecuada administración de la identificación de los usuarios (ID) en los diferentes perfiles de todos los componentes del sistema, por lo que tiene que implementarse el o los procedimiento(s) 8.1 incluyendo 8.1.1 al 8.1.8 que están asociados a este sub-requisito perteneciente al requisito 8; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.8.2. *Sub-requisito 8.2:* Se debe asignar una ID exclusiva al usuario y garantizar una adecuada administración de autenticación de usuarios en los diferentes perfiles de todos los componentes del sistema, aplicando los método de autenticación sugeridos por PCI DSS, por lo que tiene que implementarse el o los procedimiento(s) 8.2 incluyendo 8.2.1 al 8.2.6 que están asociados a este sub-requisito perteneciente al requisito 8; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.8.3. *Sub-requisito 8.3:* Se debe garantizar que el acceso administrativo individual no sea por consola y todo el acceso remoto al CDE se haga con múltiples factores de autenticación, mínimo dos de estos conforme a los propuestos por PCI DSS , por lo que tiene que implementarse el o los procedimiento(s) 8.3.1 al 8.3.2 que están asociados a este sub-requisito perteneciente al requisito 8; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.8.4. *Sub-requisito 8.4:* Se debe documentar y comunicar los procedimientos y políticas de autenticación a todos los usuarios, en la que se incluyan las directrices de PCI DSS relacionada a la autenticación, por lo que tiene que implementarse el o los procedimiento(s) 8.4 que están asociados a este sub-requisito perteneciente al requisito 8; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.8.5. *Sub-requisito 8.5:* No se debe permitir el uso de ID, ni claves grupales, ni compartidas ni genéricas, ni otros métodos de autenticación diferentes a los configurados, por lo que tiene que implementarse el o los procedimiento(s) 8.5 incluyendo 8.5.1 que están asociados a este sub-requisito perteneciente al requisito 8; los cuales son unos de los

requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.8.6. *Sub-requisito 8.6:* Se debe aplicar las directrices de PCI DSS para el uso de otros métodos de autenticación como tokens, tarjetas, certificados, entre otros; por lo que tiene que implementarse el o los procedimiento(s) 8.6 que están asociados a este sub-requisito perteneciente al requisito 8; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.8.7. *Sub-requisito 8.7:* Se debe restringir los accesos a cualquier base de datos que contenga datos CHD, por lo que tiene que implementarse el o los procedimiento(s) 8.7 que están asociados a este sub-requisito perteneciente al requisito 8; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.8.8. *Sub-requisito 8.8:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos operacionales de identificación y autenticación de usuarios, por lo que tiene que implementarse el o los procedimiento(s) 8.8 que están asociados a este sub-requisito perteneciente al requisito 8; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.9. Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta

7.1.9.1. *Sub-requisito 9.1:* Se debe usar controles de ingreso a las instalaciones apropiados para restringir y supervisar el acceso físico a los sistemas en el CDE, por lo que tiene que implementarse el o los procedimiento(s) 9.1 incluyendo 9.1.1 al 9.1.3 que están asociados a este sub-requisito perteneciente al requisito 9; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.9.2. *Sub-requisito 9.2:* Se debe establecer procedimientos que permitan diferenciar de manera fácil a los empleados de los visitantes, por lo que tiene que implementarse el o los procedimiento(s) 9.2 que están asociados a este sub-requisito perteneciente al requisito 9; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.9.3. *Sub-requisito 9.3:* Se debe controlar el acceso físico de los empleados a las áreas confidenciales, por lo que tiene que implementarse el o los procedimiento(s) 9.3 que están asociados a este sub-requisito

perteneciente al requisito 9; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.9.4. *Sub-requisito 9.4:* Se debe implementar procedimientos para la identificación y autorización de acceso físico de los visitantes a las instalaciones, por lo que tiene que implementarse el o los procedimiento(s) 9.4 incluyendo 9.4.1 al 9.4.4 que están asociados a este sub-requisito perteneciente al requisito 9; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.9.5. *Sub-requisito 9.5:* Se debe proteger físicamente todos los medios, por lo que tiene que implementarse el o los procedimiento(s) 9.5 incluyendo 9.5.1 que están asociados a este sub-requisito perteneciente al requisito 9; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.9.6. *Sub-requisito 9.6:* Se debe tener un control riguroso de la distribución de todos los tipos de medios, por lo que tiene que implementarse el o los procedimiento(s) 9.6 incluyendo 9.6.1 al 9.6.3 que están asociados a este sub-requisito perteneciente al requisito 9; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.9.7. *Sub-requisito 9.7:* Se debe tener un control riguroso del almacenamiento y la accesibilidad de los medios, por lo que tiene que implementarse el o los procedimiento(s) 9.7 incluyendo 9.7.1 que están asociados a este sub-requisito perteneciente al requisito 9; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.9.8. *Sub-requisito 9.8:* Se debe destruir los medios cuando ya no sea necesario conservarlos, por lo que tiene que implementarse el o los procedimiento(s) 9.8 incluyendo 9.8.1 al 9.8.2 que están asociados a este sub-requisito perteneciente al requisito 9; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.9.9. *Sub-requisito 9.9:* Se debe proteger los dispositivos que capturan información de las tarjetas de pago mediante la interacción física directa con el plástico de una tarjeta para evitar alteraciones y sustituciones sobre esta, por lo que tiene que implementarse el o los procedimiento(s) 9.9 incluyendo 9.9.1 al 9.9.3 que están asociados a este sub-requisito perteneciente al requisito 9; los cuales son unos de los requerimientos

que no aplicarían en su cumplimiento para una pasarela de pagos debido a que su servicio Core no interactúa con las tarjetas de pago físicamente.

7.1.9.10. *Sub-requisito 9.10:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos operacionales para limitar el acceso físico a los datos CHD, por lo que tiene que implementarse el o los procedimiento(s) 9.10 que están asociados a este sub-requisito perteneciente al requisito 9; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.10. Requisito 10: Rastrear y supervisar todos los accesos a los recursos de red y a los datos del titular de la tarjeta

7.1.10.1. *Sub-requisito 10.1:* Se debe implementar logs de auditoría para asociar todo acceso a los componentes del sistema por cada usuario, por lo que tiene que implementarse el o los procedimiento(s) 10.1 que están asociados a este sub-requisito perteneciente al requisito 10; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.10.2. *Sub-requisito 10.2:* Se debe implementar logs de auditoría automáticos en todos los componentes del sistema a tener registros de los evento que requiere PCI DSS, por lo que tiene que implementarse el o los procedimiento(s) 10.2 incluyendo 10.2.1 al 10.2.7 que están asociados a este sub-requisito perteneciente al requisito 10; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.10.3. *Sub-requisito 10.3:* Se debe llevar registro de las especificaciones que requiere PCI DSS en logs de auditoría de los componentes del sistema, por lo que tiene que implementarse el o los procedimiento(s) 10.3 incluyendo 10.3.1 al 10.3.6 que están asociados a este sub-requisito perteneciente al requisito 10; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.10.4. *Sub-requisito 10.4:* Se debe hacer uso de métodos tecnológicos para la sincronización de los tiempos y relojes críticos y se apliquen al momento de adquirir, distribuir y almacenar tiempos, por lo que tiene que implementarse el o los procedimiento(s) 10.4 incluyendo 10.4.1 al 10.4.3 que están asociados a este sub-requisito perteneciente al requisito 10; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.10.5. *Sub-requisito 10.5:* Se debe proteger los logs de auditoría para que sean inmodificables, por lo que tiene que implementarse el o los procedimiento(s) 10.5 incluyendo 10.5.1 al 10.5.5 que están asociados a este sub-requisito perteneciente al requisito 10; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.10.6. *Sub-requisito 10.6:* Se debe revisar los logs de auditoria y los eventos de seguridad en todos los componentes del sistema para identificar irregularidades o acciones sospechosas., por lo que tiene que implementarse el o los procedimiento(s) 10.6.1 al 10.6.3 que están asociados a este sub-requisito perteneciente al requisito 10; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.10.7. *Sub-requisito 10.7:* Se debe conservar el historial de los registros de auditorías mínimamente por un año, con posibilidad de acceso rápido para análisis de los registros de los últimos tres meses, por lo que tiene que implementarse el o los procedimiento(s) 10.7 que están asociados a este sub-requisito perteneciente al requisito 10; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.10.8. *Sub-requisito 10.8:* Se debe establecer un proceso para detectar oportunamente y presentar los informes de falencias de los sistemas críticos de control de seguridad, incluyendo mínimamente los componentes establecidos por el estándar PCI DSS, por lo que tiene que implementarse el o los procedimiento(s) 10.8 incluyendo 10.8.1 que están asociados a este sub-requisito perteneciente al requisito 10; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.10.9. *Sub-requisito 10.9:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos operacionales para monitorear los accesos a los recursos de la red y a los datos CHD, por lo que tiene que implementarse el o los procedimiento(s) 10.9 que están asociados a este sub-requisito perteneciente al requisito 10; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.11. Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad

7.1.11.1. *Sub-requisito 11.1:* Se debe implementar procesos para validar la presencia de puntos de acceso inalámbrico (802.11), detectando e identificando trimestralmente estos puntos estén o no autorizados, por lo que tiene que implementarse el o los procedimiento(s) 11.1 incluyendo 11.1.1 al 11.1.2 que están asociados a este sub-requisito perteneciente al requisito 11; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.11.2. *Sub-requisito 11.2:* Se debe realizar análisis internos y externos de las vulnerabilidades de la red, mínimamente cada trimestre y después de cada cambio significativo en la red, por lo que tiene que implementarse el o los procedimiento(s) 11.2 incluyendo 11.2.1 al 11.2.3 que están asociados a este sub-requisito perteneciente al requisito 11; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.11.3. *Sub-requisito 11.3:* Se debe establecer una metodología para las pruebas de penetración que cumpla las directrices de PCI DSS, por lo que tiene que implementarse el o los procedimiento(s) 11.3 incluyendo 11.3.1 al 11.3.4 que están asociados a este sub-requisito perteneciente al requisito 11; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.11.4. *Sub-requisito 11.4:* Se debe usar y mantener actualizados los mecanismos de prevención y detección de intrusos para que controle las intrusiones en la red, realice monitoreo al tráfico presente en el perímetro del CDE y en los puntos críticos del CDE y genere alertas al personal en caso de sospechar riesgos; por lo que tiene que implementarse el o los procedimiento(s) 11.4 que están asociados a este sub-requisito perteneciente al requisito 11; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.11.5. *Sub-requisito 11.5:* Se debe implementar una solución de detección de cambios para alertar al personal sobre alteraciones no autorizadas de archivos críticos del sistema, de archivos de configuración o de contenido, y que esta solución permita realizar comparaciones de archivos críticos, como mínimo una vez a la semana, por lo que tiene que implementarse el o los procedimiento(s) 11.5.a al 11.5.b; 11.5.1 que están asociados a este sub-requisito perteneciente al requisito 11; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.11.6. *Sub-requisito 11.6:* Se debe documentar, implementar y apropiar por las partes interesadas las políticas de seguridad y los procedimientos operacionales para monitorear y comprobar la seguridad, por lo que tiene que implementarse el o los procedimiento(s) 11.6 que están asociados a este sub-requisito perteneciente al requisito 11; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12. Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal

7.1.12.1. *Sub-requisito 12.1:* Se debe establecer, publicar, mantener y distribuir una política de seguridad., por lo que tiene que implementarse el o los procedimiento(s) 12.1 incluyendo 12.1.1 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12.2. *Sub-requisito 12.2:* Se debe implementar un proceso de evaluación de riesgos que cumpla las directrices de PCI DSS, por lo que tiene que implementarse el o los procedimiento(s) 12.2 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12.3. *Sub-requisito 12.3:* Se debe establecer políticas de uso para las tecnologías críticas y determine el cómo para su uso adecuado, por lo que tiene que implementarse el o los procedimiento(s) 12.3 incluyendo 12.3.1 al 12.3.10 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12.4. *Sub-requisito 12.4:* Se debe garantizar que en las políticas y los procedimientos de seguridad se establezcan las responsabilidades de seguridad de la información para todo el personal., por lo que tiene que implementarse el o los procedimiento(s) 12.4 incluyendo 12.4.1 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12.5. *Sub-requisito 12.5:* Se debe designar una persona o a un equipo de trabajo las responsabilidades de administración de seguridad de la información que establecen PCI DSS en este requerimiento, por lo que tiene que implementarse el o los procedimiento(s) 12.5 incluyendo 12.5.1

al 12.5.5 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12.6. *Sub-requisito 12.6:* Se debe implementar un programa de concienciación sobre seguridad para que todo el personal en el que se concienticen de la importancia de la seguridad de los datos CHD., por lo que tiene que implementarse el o los procedimiento(s) 12.6 incluyendo 12.6.1 al 12.6.2 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12.7. *Sub-requisito 12.7:* Se debe evaluar al personal calificado antes de su contratación a fin de reducir el riesgo de ataques internos, por lo que tiene que implementarse el o los procedimiento(s) 12.7 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12.8. *Sub-requisito 12.8:* Se debe implementar y mantener políticas y procedimientos para administrar los proveedores de servicios con quienes se compartirán datos CHD, o que podrían afectar la seguridad de estos datos., por lo que tiene que implementarse el o los procedimiento(s) 12.8 incluyendo 12.8.1 al 12.8.5 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12.9. *Sub-requisito 12.9:* Se debe aceptar por escrito y ante los clientes, las responsabilidades de la seguridad de los datos CHD que como proveedores de servicios poseen y gestionan en nombre del cliente, o en la medida en que pudiesen afectar la seguridad del CDE del cliente., por lo que tiene que implementarse el o los procedimiento(s) 12.9 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12.10. *Sub-requisito 12.10:* Se debe implementar un plan de respuesta ante incidentes y estar listos para responder inmediatamente ante una violación del sistema., por lo que tiene que implementarse el o los procedimiento(s) 12.10 incluyendo 12.10.1 al 12.10.6 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.12.11. *Sub-requisito 12.11:* Se debe ejecutar revisiones como mínimo cada trimestre para confirmar que el personal sigue las políticas de seguridad y los procedimientos operacionales, dando cubrimiento a las estipulaciones establece PCI DSS en este requerimiento, por lo que tiene que implementarse el o los procedimiento(s) 12.11 incluyendo 12.11.1 que están asociados a este sub-requisito perteneciente al requisito 12; los cuales son unos de los requerimientos obligatorios en su cumplimiento para una pasarela de pagos.

7.1.13. Apéndice A1: Requisitos de la PCI DSS adicionales para proveedores de hosting compartido

Si es proveedor de hosting debe proteger el entorno y los datos alojados de cada entidad por lo que deberá implementar los procedimientos A.1.1 a A.1.4 que están asociados a este apéndice junto con las demás secciones pertinentes de la PCI DSS; por lo que estos requerimientos estarían condicionados en su cumplimiento para una pasarela de pagos, que sería aplicable en el caso de tener su entorno CDE en un hosting compartido con tercero.

7.1.14. Apéndice A2: Requisitos de la PCI DSS adicionales para las entidades que utilizan SSL/TLS temprana

Las entidades que utilizan SSL y TLS temprana para conexiones de terminal de POS POI deben aplicar los procedimientos A.2.1 al A.2.3 mientras logran migrar a un protocolo de criptografía fuerte prontamente; los cuales son unos de los requerimientos que no aplicarían en su cumplimiento para una pasarela de pagos debido que su servicio Core no requieren conexiones de terminal de POS POI por lo que no tienen justificación para utilizar SSL y TLS temprana.

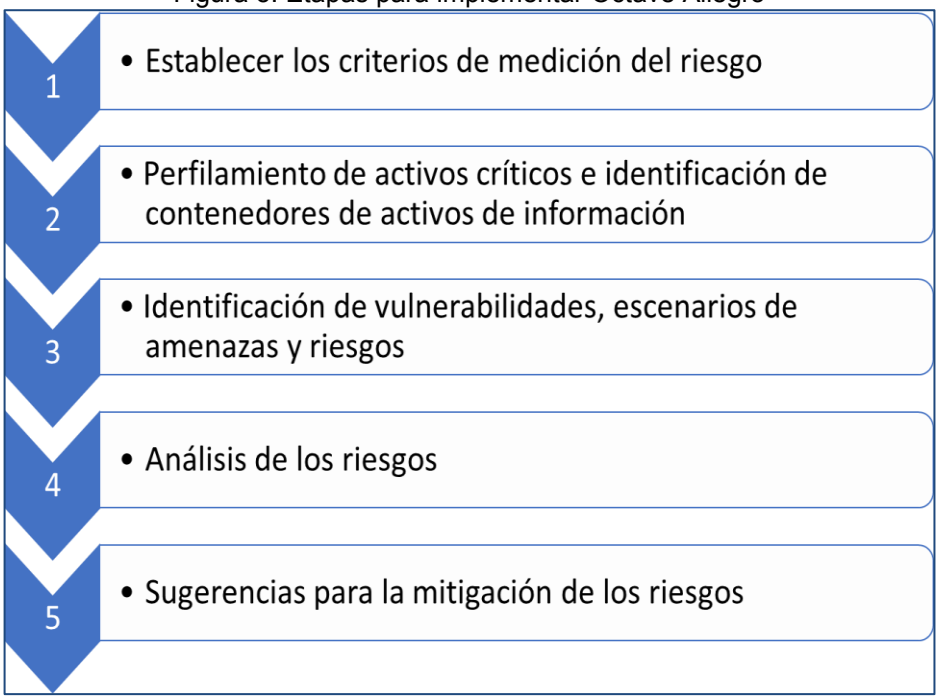
7.1.15. Apéndice A3: Validación suplementaria de las entidades designadas (DES)

Se debe realizar la validación suplementaria destinada a la corroboración de los controles de la PCI DSS en cuanto su eficacia y mejora continua a través de los procesos de validación habituales (BAU), apéndice que es aplicable únicamente a las entidades designadas por una marca de pago o adquirente, los cuales pueden exigir una validación adicional de los requisitos de la PCI DSS existentes con la QSA, conforme a los procedimientos A.3.1 al A.3.5 de este apéndice, por lo que estos requerimientos estarían condicionados en su cumplimiento para una pasarela de pagos, en el caso de que una marca de tarjeta de pago o adquirente se lo exija formalmente mediante su QSA autorizada para la evaluación de certificación.

7.2. IDENTIFICACIÓN Y ANÁLISIS DE LOS RIESGOS LAS PASARELAS DE PAGOS

Los riesgos, amenazas y vulnerabilidades que están asociados al cumplimiento del estándar PCI DSS V3.2.1 para una pasarela de pagos, se pueden sustentar con cualquier metodología que este orientada a la gestión de riesgos informático como las sustentadas en el capítulo 6. Diseño metodológico de esta guía; no obstante, para este objetivo se aplicaría la metodología de riesgos Octave Allegro que está enfocada a los activos de información y reduce significativamente la recolección de datos para el análisis, ya que no se cuenta con todos los insumos para el mismo; por lo que esta derivación de la metodología octave se puede implementar en 8 pasos[43] los cuales para este numeral se considerarán de forma compilada dentro las siguientes etapas:

Figura 5. Etapas para implementar Octave Allegro



Fuente: Propia

[43] SOTO SUAREZ, Andrés. Exposición octave. En: SlideShare. 2018. Disponible en: https://www.slideshare.net/AndresSotoSuarez1/exposicion-octave

7.2.1. Establecer los criterios de medición del riesgo

Para establecer los criterios de medición de los riesgos se determinan los parámetros posibles de probabilidad de un evento de riesgo frente al impacto en el cumplimiento en el estándar y los efectos en la certificación en PCI DSS conforme a la siguiente tabla 3:

Tabla 3.Criterios de medición de los riesgos

CRITERIO	PROBABILIDAD	IMPACTO
Alto	Más de una vez al año	• Perdida en la seguridad y protección para los datos CHD y/o SAD, generando la suspensión temporal o permanente en la certificación en PCI DSS por parte del PCI_SSC; considerando paralelamente el retraso en la evaluación de recertificación anual en PCI DSS por parte de la QSA
Medio	Una vez al año	• Perdida en la seguridad y protección para los datos CHD, generando investigaciones, auditorias continuas y mayores exigencias en los requisitos por parte de las marcas de pago, de los adquirientes y/o clientes con el posible retraso en la evaluación de recertificación anual en PCI DSS por parte de la QSA.
Bajo	Cada varios años	• Perdida en la seguridad y protección para algunos datos CHD en el que toca reportar el incidente a las marcas de pago afectadas y demás partes interesadas; pero no afecta la certificación vigente en PCI DSS ni el proceso de evaluación por parte de la QSA.

Fuente: Propia

De conformidad con los criterios anteriores se establece el nivel de riesgo el cual se sustenta con el siguiente mapa de calor:

Tabla 4. Nivel de riesgo

MAPA DE CALOR					
PROBABILIDAD (P)	Alto	3	Medio	Alto	Alto
	Medio	2	Bajo	Medio	Alto
	Bajo	1	Bajo	Bajo	Medio
NIVEL DE RIESGO			1	2	3
			Bajo	Medio	Alto
			IMPACTO (I)		

Fuente: Propia

7.2.2. Perfilamiento de activos críticos e identificación de contenedores de activos de información

Se prioriza los activos que son parte esencial dentro del proceso de las pasarelas de pagos en los que se derivan los siguientes activos críticos:

A. *Sistema o Servicio CORE*: Correspondiente al servicio que se expone en Internet (plataforma e-commerce) para que interconecte con el comercio muestre el sitio web de la pasarela de pagos para consumo de los tarjetahabientes y que a su vez realice el proceso transaccional con la red de operador de franquicias o procesador de pagos en función de la pasarela de pagos.

B. *Los controles de seguridad críticos*: Estos se asocian acorde al requisito 10.8 de la PCI DSS entre los que se destacan el Firewall, antivirus, IDS/IPS, entre otros.

C. *Códigos fuentes de aplicaciones/servicio Core*: Corresponde a los programas desarrollados que están expuestos en el entorno productivo para funcionamientos del Sistema o servicio Core.

D. *Canal de comunicaciones*: Son los mecanismos como MPLS (Multiprotocol Label Switching), VPN (Virtual Private Network) Site to Site, entre otros; que permiten la conexión con los comercios como también de forma separada interconecta con la Red de operador de franquicias o procesadores de pagos como Redeban Multicolor, CrediBanco, entre otras; permitiendo protocolizar el proceso de autorización de la transacción.

E. *Áreas confidenciales*: Corresponde al centro de datos o DataCenter donde se aloja la infraestructura física que hacen parte del CDE (Entorno de datos del titular de la tarjeta).

F. *Recursos tecnológicos o componentes TI del CDE*: Son los activos tecnológicos, componentes del CDE que permiten la funcionalidad integrada del sistema o servicio CORE, entre los que se destacan servidores, switches, router, equipos de cómputos, entre otros.

7.2.3. Identificación de vulnerabilidades, escenarios de amenazas y riesgos

Se realiza la identificación de las vulnerabilidades, escenarios de amenazas y riesgos aplicables de forma genérica a las pasarelas de pagos que están asociados directamente con el cumplimiento del estándar PCI DSS; teniendo en cuenta tanto las exigencias o recomendaciones que establece el estándar, la información suministradas por algunas pasarelas de pagos (Pagos Inteligentes, Place to Pay, MyChoice2Pay, PayU) como unas fuentes de referencias asociadas a riesgo operacional en los sistemas de pagos[44] y de ataques de las pasarelas de pago en los últimos años[45,46]; de los cuales se obtuvieron los siguientes resultados:

Tabla 5. Identificación de vulnerabilidades, escenarios de amenazas y riesgos

VULNERABILIDADES	ESCENARIOS DE AMENAZAS	RIESGOS
• Tener firewalls obsoletos, sin la configuraciones y actualizaciones pertinentes para el CDE. • Carecer de los controles de seguridad críticos para el CDE • Desconocimiento técnico en la configuración y administración de los recursos tecnológicos del CDE y los controles de seguridad críticos por parte del personal encargado	• Falla o daño de los equipos firewall • Inadecuado gestión de la restricciones y acciones filtrado por parte del firewall • Ataques externos o internos contra las redes y canales de comunicaciones (Hombre en el medio, Sniffing, Spoofing, entre otros)	Las Infiltraciones a las redes y/o canales de comunicaciones que conforman el CDE
• Carecer de los controles de seguridad críticos y seguridad física/ambiental para el CDE • Usar Hardening con estándares de configuraciones desactualizados para los componentes del CDE y los controles de seguridad críticos • Uso de recursos tecnológicos obsoletos para el CDE • Tener valores predeterminados en los recursos tecnológicos que componen el CDE • Carencias en la capacidad de la comunicaciones y recursos para el servicio Core	• Ataques externos o internos contra los componentes del CDE (DoS, Botnet, Malware, Desastres Naturales/industriales, entre otros) • Falla o daño de los recursos, suministros o de cualquier dispositivo TI crítico para el sistema Core. • Saturación del sistema o Servicio Core	Denegación de los servicios CORE y/o suspensión/daño de los recursos tecnológicos

[44] Rodríguez, Ana Cecilia; Rodríguez, Ana Karina & Liñares, Verónica. Riesgo operacional en los sistemas de pagos - Metodología VaR. 2013. Disponible en: http://www.bvrie.gub.uy/local/File/doctrab/2013/4.2013.pdf

[45] Malca, Solange. Los 5 mayores ataques de seguridad en los medios de pagos digitales durante el 2016. Alignet. 2017. Disponible en: https://www.alignet.com/blog/seguridad/los-5-mayores-ataques-de-seguridad-en-los-medios-de-pagos-digitales-durante-el-2016/

[46] Towers Watson, Willis. "E-commerce-riesgos-ciberneticos". 2018. Disponible en: https://willistowerswatsonupdate.es/ciberseguridad/e-commerce-riesgos-ciberneticos/

Tabla 5. (Continuación)

VULNERABILIDADES	ESCENARIOS DE AMENAZAS	RIESGOS
• No tener vigente o activos los controles de seguridad física y sistemas de control de acceso • Los controles de acceso físico existente son manuales o están desactualizados con los usuarios autorizados para el acceso al CDE. • Las áreas confidenciales están ubicadas en zonas de mucha circulación de personas • Carecer de zonas restringidas para el personal que gestiona el procesamiento de datos CHD	• Circulación de personas cercanamente al entorno CDE • Falla o daño de uno o varios de los controles de seguridad física y sistemas de control de acceso • Cambio continuo del personal autorizado para acceder al CDE	Acceso físico no autorizado a las zonas del CDE
• Uso de Códigos fuentes de aplicaciones/servicio Core desactualizados o en ambiente productivo inefectivo • No ejecutar análisis de vulnerabilidades y pruebas de intrusión a los sistemas de forma continua, remediando inmediatamente las brechas • Desconocimiento técnico y del proceso para la configuración y administración de los recursos tecnológicos del CDE incluido el servicio Core por parte del personal encargado • Errores en el ciclo de vida del desarrollo y administración del sistema (Bugs) • Carencias en las funcionalidades del servicio Core incluyendo acciones manuales o de gestión humana	• Generación continua de nuevos códigos maliciosos y métodos ataques contra los servicios web y sistemas transaccional-financiero • Renovación permanente de las tecnologías de la información y parches de seguridad para los sistemas • Error Humano	Falla funcional del sistema o servicio Core
• Definición de procesos inadecuados o equipos para el ciclo de vida del desarrollo y administración del sistema (Bugs) • Inadecuada protección y/o debilidad en el cifrado de los datos CHD durante la transmisión y/o el almacenamiento • Desconocimiento técnico y del proceso para la configuración y administración de los recursos tecnológicos del CDE incluido el servicio Core por parte del personal encargado • Carencias en la capacidad de las BD y esquemas de almacenamientos para el sistema Core • Debilidades o falencias en los controles de acceso físico o lógico al CDE • Carencias en las funcionalidades del servicio Core incluyendo acciones manuales o de gestión humana	• Ataques externos o internos contra el servicio Core y las BD (Malware, Inyección de código, entre otros) • Error humano y/o del sistema Core en la gestión del procesamiento y custodia de los datos CHD y las transacciones • Llenado de los registros en las BD o de los esquemas de almacenamiento del sistema Core • Acceso físico o lógico no autorizado al CDE	Alteración/ Supresión de los datos CHD

Tabla 5. (Continuación)

VULNERABILIDADES	ESCENARIOS DE AMENAZAS	RIESGOS
• No tener debidamente segmentadas las redes y el ambiente CDE que usara el servicio CORE. • Carecer de los controles de seguridad críticos para el CDE a nivel de seguridad física y tecnológica. • Inadecuada protección y/o debilidad en el cifrado de los datos CHD durante la transmisión y/o el almacenamiento • Uso de contraseñas débiles y sin la debida parametrización para su gestión • Errores en el ciclo de vida del desarrollo y administración del sistema (Bugs)	• Ataques externos o internos contra los componentes del CDE (Malware, Drown, Heartbleed, entre otros) • Acceso físico o lógico no autorizado al CDE • Mal funcionamiento del sistema Core y demás los componentes del CDE • Error humano y/o del sistema Core en la gestión transmisión y almacenamiento de los datos CHD y las transacciones	Exposición de los datos CHD
• No tener establecido o debidamente configurado el borrado seguro de los datos SAD para después de una autorización • Inadecuada protección y/o debilidad en el cifrado de los datos SAD durante la transmisión • Carencias en las funcionalidades del servicio Core incluyendo acciones manuales o de gestión humana • Desconocimiento técnico y del proceso para la configuración y administración de los recursos tecnológicos del CDE incluido el servicio Core por parte del personal encargado	• Error Humano • Fallas en el proceso transaccional y del sistema para el borrado seguro de datos SAD • Ataques externos o internos contra las redes y canales de comunicaciones (Hombre en el medio, Sniffing, Spoofing, entre otros)	Exposición o almacenamiento de datos SAD después de una autorización transaccional

Fuente: Propia

7.2.4. Análisis de los riesgos

Para realizar el análisis de los riesgos se tuvieron en cuenta las mismas referencias que permitieron la identificación de los riesgos obtenidos en el subcapítulo 6.2.3 de la guía adicionando circunstancialmente las evaluaciones de las pasarelas de pago[47] y los ataque recibidos en Colombia asociados al sector financiero[48]; los cuales en cierta medida permiten determinar el siguiente análisis para los riesgos:

[47] MYCHOICE2PAY. “Guía para saber elegir una pasarela de pago adaptada a tu negocio en 2019”. 2019. Disponible en: https://www.mychoice2pay.com/es/blog/elegir-una-pasarela-de-pago

[48] COLPRENSA. Colombia fue uno de los países con más ataques cibernéticos el año pasado. En: LA REPUBLICA. 2019. Disponible en: https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

Tabla 6. Análisis de riesgos en las pasarelas de pagos

RIESGOS	PROBABILIDAD	IMPACTO	NIVEL DE RIESGOS
Las Infiltraciones a las redes y/o canales de comunicaciones que conforman el CDE	MEDIO	ALTO	ALTO
Denegación de los servicios CORE y/o suspensión/daño de los recursos tecnológicos	MEDIO	ALTO	ALTO
Falla funcional del sistema o servicio Core	ALTO	ALTO	ALTO
Acceso físico no autorizado a las zonas del CDE	ALTO	BAJO	MEDIO
Alteración/ Supresión de los datos CHD	ALTO	ALTO	ALTO
Exposición de los datos CHD	ALTO	ALTO	ALTO
Exposición o almacenamiento de datos SAD después de una autorización transaccional	MEDIO	ALTO	ALTO

Fuente: Propia

7.2.5. Sugerencias para la mitigación de los riesgos

Teniendo en cuenta que los riesgos analizados en el subcapítulo 6.2.4. establecen un nivel alto u medio se hace imprescindible el tratamiento de estos, para lograr su reducción o mitigación por lo que se sugiere las siguientes medidas de tratamiento para la mitigación de los riesgos:

Tabla 7. Medidas de tratamiento para mitigación de los riesgos

RIESGOS	MEDIDAS DE TRATAMIENTO
Las Infiltraciones a las redes y/o canales de comunicaciones que conforman el CDE	• Proteger las comunicaciones con protocolos de seguridad aprobados y aceptados para PCI DSS que garantizan la seguridad de los datos durante el tránsito de los mismos en la redes y/o canales de comunicaciones. • Aplicar adecuadas plantillas de hardening para los firewall y enrutadores involucrados con el CDE de forma directa o indirecta. • Capacitar y concientizar en la mejores prácticas de seguridad y gestión de comunicaciones seguras a los colaboradores que apoyan la gestión de seguridad e infraestructura en la redes de la empresa.
Denegación de los servicios CORE y/o suspensión/daño de los recursos tecnológicos	• Implementar controles de seguridad críticos y seguridad física/ambiental para el CDE • Establecer y configurar los componentes TI del CDE incluyendo los controles de seguridad críticos con estándares de configuración propiamente definido que consideren adecuadas plantillas de Hardening para parametrizar cada componente con las mejores prácticas de tecnología y de seguridad informática

Tabla 7. (Continuación)

RIESGOS	MEDIDAS DE TRATAMIENTO
Falla funcional del sistema o servicio Core	• Adoptar procesos de ciclo de vida de desarrollo de software seguro que implique los análisis de las aplicaciones considerando para ellos criterios como TOP Ten OWASP, TOP 25 SANS entre otros • Capacitar y concientizar en la mejores prácticas de seguridad y desarrollo de software seguro a los colaboradores que apoyan la gestión de requerimientos-diseño, desarrollo, pruebas, implementación y soporte de los software/aplicaciones establecidos/adquiridos en la empresa. • Ejecutar Test de intrusión y análisis de vulnerabilidades preferiblemente con un proveedor AVS o en su defecto con herramientas avaladas para PCI DSS
Acceso físico no autorizado a las zonas del CDE	• Ubicar las áreas confidenciales en lugares estratégico, con limitación de acceso y circulación de personas y que a su vez considere los estándares y mejores prácticas para su diseño e implementación de estas áreas. • Implementar sistemas de control de acceso automatizados que garanticen un adecuado proceso de autenticación y autorización de acceso físico a las instalaciones donde custodie componente TI físicos del CDE o se haga procesamiento de datos CHD.
Alteración/ Supresión de los datos CHD	• Implementación de los controles de seguridad críticos (Antivirus, Firewall, IDS/IPS, FIM, SIEM, entre otros) con estándares de configuración apropiados de seguridad y funcionalidad. • Aplicar sistema de gestión de contraseñas con políticas de manejo de contraseña fuerte y adecuadamente parametrizadas.
Exposición de los datos CHD	• Uso de cifrado fuerte con algoritmos de cifrado, Hash y protocolos de seguridad aprobados y aceptados para PCI DSS • Implementación de los controles de seguridad críticos (Antivirus, Firewall, IDS/IPS, FIM, SIEM, entre otros) con estándares de configuración apropiados de seguridad y funcionalidad. • Aplicar sistema de gestión de contraseñas con políticas de manejo de contraseña fuerte y adecuadamente parametrizadas.
Exposición o almacenamiento de datos SAD después de una autorización transaccional	• Aplicar técnicas de borrado seguro para los datos SAD después de una autorización • Uso de cifrado fuerte con algoritmos de cifrado, Hash y protocolos de seguridad aprobados y aceptados para PCI DSS • Implementación de los controles de seguridad críticos (Antivirus, Firewall, IDS/IPS, FIM, SIEM, entre otros) con estándares de configuración apropiados de seguridad y funcionalidad.

Fuente: Propia

La estructuración técnica asociada para la mitigación de los riesgos se detallará con el capítulo 7.3 de esta guía, en el cual se establece las recomendaciones de seguridad informática necesarias en una pasarela de pago para su orientación en el cumplimiento del estándar PCI DSS V3.2.1.

7.3. RECOMENDACIONES DE SEGURIDAD INFORMÁTICA PARA UNA PASARELA DE PAGO

Las recomendaciones de seguridad informática necesarias en una pasarela de pago para su orientación en el cumplimiento del estándar PCI DSS V3.2.1 no solo están orientadas en el tratamiento de los riesgos analizados en el capítulo 7.2; sino también en dar cubrimiento a las consideraciones que se detallan en este ítem, las cuales están directamente relacionadas con las definidas en el Anexo A de esta guía para su adecuada implementación en los requisitos obligatorios del estándar.

A continuación, se detallan las consideraciones para los estándares de configuración en los recursos tecnológicos o componentes TI que hacen parte del CDE incluyendo los controles de seguridad a los que toca adaptarle fuerte parámetros de configuración y/o hardening para que no sean violentados por los atacantes y sean resistentes durante su función de protección y seguridad.

- En el Requisito N° 1 de PCI DSS para los Firewall deben habilitarse una a una las reglas o políticas y activar los siguientes parámetros: IPS/IDS, Stateful inspection, AntiSpoofing, Copias de Configuración (protegidas), NAT/PAT, Regla del Deny all /CleanUp para que rechace lo que no está autorizado/permitido, Egress Filtering (Filtrado de tráfico de salida). Así mismo; se debe restringir el acceso a Internet a cualquier componente del CDE; permitiendo conectividad únicamente a los sitios web hacen parte de la interacción funcional con el servicio CORE y a los necesarios para las actualizaciones de seguridad propias de cada componente (Ej.: La actualización de la base de datos del Antivirus).

- Para los requisitos N° 1 y 2 de PCI DSS se debe limitar el uso y bloquear los siguientes puertos catalogados como inseguros entre esos: 110 - POP3; 12345 - NetBus (troyano/virus) / Italk Chat System; 1337 - menandmice DNS; 137 - NETBIOS Name Service; 138 - NETBIOS Datagram Service; 139 - NETBIOS Session Service; 143/220 - IMAP; 1433 - Microsoft-SQL-Server; 1434 - Microsoft-SQL-Monitor; 1521 - nCube License Manager; 161/162 - SNMP V1 y V2; 20 - FTP data; 21 - FTP; 23 - Telnet; 31337 - Back Orifice herramienta de administración remota (por lo general troyanos); 3389 - MS WBT Server; 445 - Microsoft DS; 5060(UDP) - Session Initiation Protocol (SIP); 5631/5632 - PC-Anywhere protocolo de escritorio remoto; 80/8080 - http; 98-98 - Gusano Dabber (troyano/virus) / MonkeyCom.

- En el requisito N° 2 de PCI DSS se debe establecer los estándares de configuración de cada uno de los componentes TI implementados conforme a los diagramas de red y de flujo de los datos, los cuales deben ser consecuente con el CDE y el servicio Core; para ello se sugiere utilizar plantillas de hardening con altos niveles de seguridad aceptados por la industria como: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), Institute National Institute of Standards

Technology (NIST), entre otros; y a la vez considerar referentes de PCI DSS para estándares de configuración que sean vigente y/o aplicables al negocio como el del siguiente link: https://www.pcihispano.com/estandares-de-configuracion-segura-hardening-en-pci-dss/. También restringir las conexiones de tipo Plug-and-Play o PnP; bloqueando el acceso a los puertos USB y entradas que permitían la lectura y/o escritura de medios extraíbles.

- En el Requisito N° 3 de PCI DSS se debe parametrizar el proceso de Tokenización establecido por PCI DSS conforme a las guías que establece como: "Tokenization Product Security Guidelines – Irreversible and Reversible Tokens"[49] y "PCI DSS Tokenization Guidelines"[50] considerando para esto el uso de clave criptográfica de al menos 128 bits en el sistema de Tokenización.

- Para los requisitos N° 3 y 4 de PCI DSS se deben usar algoritmos de cifrados aprobados y aceptados por la NIST Special Publication 800-57 Part 1, con longitud de clave superior a 112 bits (Ver sugeridos en la figura 6)

Figura 6. Algoritmos de encriptación y firma digital y longitudes de clave aceptados por PCI DSS

Algoritmo	Longitud de clave mínima
AES	128 bits y superior (192 y 256)
TDES/TDEA (Triple Data Encryption Algorithm)	Obligatorio el uso de tres claves (Three-key TDEA): 112 bits y superior
RSA	2048 bits y superior
ECC (Elliptic Curve Cryptography)	224 bits y superior
DSA (Digital Signature Algorithm)	2048/224 bits y superior
DH (Diffie–Hellman)	2048/224 bits y superior
Cualquier otro algoritmo aprobado y aceptable con clave > 112 bits	Ver NIST Special Publication 800-57 Part 1

Fuente: https://www.pcihispano.com/que-algoritmos-criptograficos-se-deben-emplear-para-cumplir-con-pci-dss/

- En el requisito N° 4 de PCI DSS se debe usar Hash aprobados y aceptados por la NIST Special Publication 800-57 Part 1, con longitud de clave superior a 112 bits (Ver sugeridos en la figura 7). Adicionalmente, deberían implementar protocolo de seguridad TLS V1.2 en adelante para asegurar las conexiones durante la transferencia de datos y WPA2 en conexiones inalámbricas manteniendo actualizadas las librerías de OpenSSL.

[49] PCI SSC. Tokenization Product Security Guidelines. 2015. Disponible en: https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

[50] Scoping SIG, Tokenization Taskforce PCI SSC. "PCI DSS Tokenization Guidelines". 2011. Disponible en: https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

Figura 7.Algoritmos de hash aceptados por PCI DSS

Familia	Algoritmo
SHA-2	SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 y SHA-512/256
SHA-3	SHA3-224, SHA3-256, SHA3-384 y SHA3-512
Whirpool	Whirpool-512
Cualquier otro algoritmo aprobado y aceptable de hash	Ver NIST Special Publication 800-57 Part 1

Fuente:https://www.pcihispano.com/que-algoritmos-criptograficos-se-deben-emplear-para-cumplir-con-pci-dss/

- En el requisito N° 5 de PCI DSS se debe tener activo y funcionando la actualización automática de la Base de Datos (BD) y/o firmas de los antivirus-antimalware.

- En el requisito N° 8 de PCI DSS se debe eliminar o inhabilitar las cuentas de usuario inactivas preferiblemente el día que se retira o desvincule el usuario; así mismo, mantener adecuadamente parametrizado y con las mayores restricciones los sistemas de gestión de contraseñas y/o de autenticación de usuarios especialmente el que está vinculado con el directorio activo corporativo y el del servicio Core, a los cuales se recomienda que hagan el bloqueo del ID de un usuario a los tres (3) intentos fallidos de autenticación.

- En el requisito N° 9 de PCI DSS se debe aplicar las mejores prácticas para las áreas confidenciales como los Data Center, para los que se recomiendan los criterios del estándar ANSI/TIA-942 y la NFPA 75 como normas para la protección de equipos electrónicos procesadores de datos por computadora.

- En el requisito N° 10 de PCI DSS se debe considerar los escenarios de logs definidos en la tabla 8 y su estructuración respectiva con los campos mínimos definidos en la tabla 9.

Para los logs de evento que se determinan en el requisito 10 del estándar se sugieren tener en cuenta los despliegues de gestión de eventos sugerido por la NIST 800-92 «Guide to Computer Security Log Management»[51] y para esto se puede tener en cuenta los siguientes parámetros como mínimo:

a) Los escenarios a los que se les debe determinar logs de eventos dentro del sistemas pueden tipificar de la siguiente forma:

[51] ACOSTA, David. Controles técnicos de PCI DSS parte VI: Registro de eventos (logs). En: PCIHISPANO. 2016. Disponible en: https://www.pcihispano.com/controles-tecnicos-de-pci-dss-parte-vi-registro-de-eventos-logs/

Tabla 8. Escenarios para los logs de eventos

ESCENARIOS POR EVENTO	FUNCIONALIDAD
Acceso a un componente IT/Aplicación	Puede ser exitoso con autenticación de credenciales correcta o incorrecta cuando ingresa mal los datos de autenticación
Bloqueo de usuario	Se aplica cuando se registren 3 intentos fallidos en el acceso de autenticación o Log-in
Acciones de Administración o actualización del componente IT/ Aplicación	Se aplica para los casos en que el administrador o superusuario, hace algunas gestiones sobre el componente IT /Aplicación ejemplo cambio de contraseña, restablecimiento de usuario/contraseña, consultas, eliminaciones, inhabilitación, ajuste a privilegios/perfil de los usuarios, creación de usuarios, ajuste de configuración, etc.
Acceso de consulta, Cambios o acciones de Inicialización, detención o pausa de los logs	Cuando se presenten acciones frente a los logs (Journal o un SysLog) de los componentes IT
Alertamientos de los sistemas por fallas/anomalías	Cuando se presenten alarma en el sistema, alertas por posibles ataques o accesos no autorizados.
Trazabilidad en el sistema y la BD	Se puede aplicar a nivel servicio de la aplicación o en BD donde se valida la traza en la creación, modificación, consulta y eliminación de objetos o datos en el sistema

Fuente: Propia

b) Los campos para los logs de auditorías componentes TI sugerido como mínimo serian:

Tabla 9. Campos para los logs de auditorías componentes TI

CAMPO LOG	DESCRIPCIÓN
ID DE USUARIO	ID Usuario que origina el evento
TIPO DE EVENTO	Creación, mantenimiento/cambio, consulta, eliminación - formateo, backup, encendido - boot, apagado, falla del dispositivo, error funcional, etc.
FECHA Y HORA	DD/MM/AAAA HH:MM:SS o formato similar; con la fecha y hora en que se origina el evento y finaliza
ORIGEN DEL EVENTO	Desde que máquina y/o herramienta se origina el evento (IP Y/O HERRAMIENTA)
PROCESO DE ENTRADA	En los casos que aplique indicar la entrada que origina el evento (EJ: Comando; Herramienta, etc.)
COMPONENTE AFECTADO	MAC/ Identificador o dato de referencia del componente; permitiendo identificar con facilidad en que componente se presentó el evento
RESULTADO	Indicación de EXITOSO O FALLIDO del evento efectuado
DATO INICIAL	Información o proceso previo al evento
DATO RESULTANTE	Información o proceso resultante a causa del evento

Fuente: Propia

En cuanto a las herramientas de seguridad que se recomiendan como controles de seguridad críticos[52] se pueden establecer los asociados en la siguiente tabla 10 en la que también se detalla las mejores soluciones técnicas basada los ofrecimientos de los fabricantes y las calificaciones en el Reporte de Gartner (Sitio web: https://www.gartner.com/reviews/home).

Tabla 10. Herramientas de seguridad

REQ	TIPO DE HERRAMIENTAS	CRITERIOS PARA CUMPLIR CON PCI DSS[39]	MEJORES SOLUCIONES TÉCNICAS
1	**Firewall**	• Considerar una amplia cantidad puertos/interfaces de red para establecer los segmentos de red requeridos por el CDE para la funcionalidad apropiada en las conectividades del servicio CORE, incluyendo las DMZ, la red interna, las redes inalámbricas, entre otros entornos de red de la pasarela; donde se gestionen/conserven datos de tarjetas de pago. • Permitir la configuración de IPS/IDS para los intrusos, así como de la opción del Anti-Spoofing contra la suplantación de identidad (Req. 1.3.4) • Debe ser mínimamente una solución de FW de tercera generación que considere a su vez el Stateful Inspection para el manejo de estados en el filtrado de tráfico (Req. 1.3.6) • Debe tener las funciones que prevengan la divulgación de la IPs privadas y los datos de enrutamiento desde redes internas a Internet considerando para ello las funcionalidades: NAT, Proxies y la eliminación de publicación de enrutamiento interno. • Se sugiere que la solución permita seguir con los lineamientos de la guía "Methodology for Firewall Reviews for PCI Compliance" del SANS Institute. • Tener presente que la solución Firewall Personal para los dispositivos móviles o de propiedad de los colaboradores que se conecten al CDE deben cumplir con las siguientes características: - No permitir que pueda ser deshabilitada, ni modificada por el usuario - Debe habilitarse automáticamente en el componente y funcionar en todo momento con o sin conexión al CDE.	Algunas de las mejores soluciones Firewall (Reporte de Gartner 2018) • Fortinet: FortiGate - Firewall de próxima generación (NGFW) • Cisco: ASA; Meraki MX • Palo Alto: Serie PA-3000 (Legacy)
1	**IDS/IPS**	• Deben permitir la detección basadas en firmas, en análisis de anomalías y facilitar el soporte para inspección de estados, considerando a su vez el análisis perimetral de la red del entorno CDE. • La herramienta designada debe facilitar la caracterización de las alertas y criterios de detección, para poder validar los falsos positivos y adaptar otros controles de detección/prevención a los que provee por defecto.	• Cisco (Sourcefire) • McAfee Network Security Platform (NSP)

[52] ACOSTA, David. Controles técnicos de PCI DSS. En: PCIHISPANO. 2014. Disponible en: https://www.pcihispano.com/category/controlespcidss/

Tabla 10. (Continuación)

REQ	TIPO DE HERRAMIENTAS	CRITERIOS PARA CUMPLIR CON PCI DSS[39]	MEJORES SOLUCIONES TÉCNICAS
1	**IDS/IPS**	• La solución debe poderse actualizar tanto en sus componentes como las firmas; por lo que se hace necesario protocolizar el proceso de control de cambios considerando las especificaciones del requisito 6.4.5. previniendo cualquier indisponibilidad o incidente en el entorno. •Si la solución es appliances, se debe considerar la escalabilidad del dispositivo y la densidad de puertos de red, incluyendo los de gestión; y en los casos de soluciones de virtualización, contemplar la necesidad de monitorizar los segmentos de red en este tipo de plataformas anexando los virtual switch. • Se recomienda que el IPS/IDS aplique la totalidad o mayor cantidad de los criterios mencionados en el «Special Publication 800-94» del NIST y que la solución acople los criterios para el registro de eventos conforme a los requisitos 10.6 y 10.7 de PCI DSS.	• Radware DefensePro IPS • StoneSoft (McAfee) • IBM Security Network Intrusión Prevention System
5	**Soluciones antivirus / antimalware Endpoint Security**	• Permitir su instalación en cualquier sistema operativo, especialmente en los que hacen parte del CORE y sean vulnerables a Malware; considerando que no solo se debe tratar los virus informáticos sino también otros tipos de malware como gusanos,troyanos, ransomware, rootkits, entre otros. • Optar por tener una única opción de antivirus, pero sí los sistemas del entorno CDE no convergen para trabajar integradamente con el mismo se debe considerar la opción de manejar varios sistemas de antivirus o antimalware en el CDE que deben cumplir con el requisito 5 de PCI DSS. • La solución establecida debe detectar y eliminar todos los tipos de malware. Por lo que se sugiere que esta solución se valide en cuanto su detección completa a los malware presentados en las listas «Wildlist» (virus) y «Extended wildlist» (malware adicional) suministrada por WildList Organization International. • Permitir su configuración para actualización automática tanto de firmas como de componentes; ya que no se admite el proceso manual por el requisito 5 de PCI DSS • Facilitar la realización de escaneos periódicos-programados; en tiempo real con funcionamiento de manera activa. Debe evitar que un usuario pueda inactivar/suspender la protección de la solución sin autorización. Por lo que la solución debe permitir la configuración de contraseña maestra, control a nivel de sistema operativo, restricciones centralizadas, etc. • Permitir el despliegue de las configuraciones de seguridad previamente determinadas por el antimalware. • Debe lograr la generación de los registros de eventos, cumpliendo con las estipulaciones que exige el requisito 10.6 y 10.7 de PCI DSS.	Algunas de las mejores soluciones Endpoint Security (Reporte de Gartner 2018) • Kaspersky Endpoint Security para empresas • McAfee Endpoint Security • Trend Micro Apex One

Tabla 10. (Continuación)

REQ	TIPO DE HERRAMIENTAS	CRITERIOS PARA CUMPLIR CON PCI DSS[39]	MEJORES SOLUCIONES TÉCNICAS
6	**Analizadores de seguridad sobre las aplicaciones desarrolladas**	• Facilite la ejecución de análisis estático durante todo el ciclo de vida de desarrollo en el que se permite analizar todo código fuente sin tener ejecutables • Facilite la ejecución de Análisis dinámico que se debe aplicar sobre la fase final o de prueba del desarrollo antes de puesta a producción, ya que requiere del ejecutable para hacer una valoración completa sobre el sistema de forma general • Se debe tener los lenguajes de programación actualizados y que sea consiste a lo manejado por la entidad. • Permita analizar los desarrollos/aplicaciones y arrojar informes mínimamente con respecto al Top Ten de OWASP y a su vez considere análisis desde la perspectiva del ciclo de vida desarrollo seguro y los informes de cumplimiento con PCI DSS.	• Veracode • Kiuwan • Qualys
6.6	**WAF (Firewall de aplicaciones web)**	• Tener componente independiente para la funcionalidad del WAF y no combinarlo con las del Firewall perimetral, Firewall interno, un IDS/IPS y demás firewall usados por la organización; ya que son soluciones diferente que se manejan conjuntamente sin ser excluyentes, pero estas no pueden remplazar a un WAF y viceversa. • Mínimamente, debe detectar las vulnerabilidades detalladas en el Top ten de OWASP y considerar CWE/SANS Top 25. • Permitir el aprendizaje del entorno evaluado; adaptando y personalizando al mismo para facilitar la creación de forma dinámica y la edición de nuevas reglas. • Ser adaptable que considere los parámetros necesarios para interactuar y analizar distintas tecnologías asociadas con aplicaciones web (XML, SOAP, JSON, etc.) • Permitir las actualizaciones continuas y automatizadas, tanto de la solución como de las firmas si estas aplican. • Adecuar la solución WAF apropiadamente al entorno CDE para que pueda tener un control contra los falsos positivos, a fin de no bloquear peticiones legitimas sin afectar el servicio CORE ni a la pasarela. • Aplicar la solución WAF dentro del flujo HTTP, considerando las pruebas de interoperabilidad y desempeño frente a las aplicaciones y/o servicio CORE para definir las acciones a implementar en caso de comportamiento inesperados de esta solución. • Se sugiere que la solución WAF permita seguir con las guías "OWASP Best Practices: Use of Web Application Firewalls" y " Los criterios de evaluación de WAF" del Web Application Security Consortium".	Algunas de las mejores soluciones WAF (Reporte de Gartner 2018) • Fortinet: FortiWeb • Signal Sciences WAF • Imperva WAF

Tabla 10. (Continuación)

REQ	TIPO DE HERRAMIENTAS	CRITERIOS PARA CUMPLIR CON PCI DSS[39]	MEJORES SOLUCIONES TÉCNICAS
10	**SIEM (Gestión de eventos de seguridad e información)**	• Facilite el descubrimiento e inventario de elementos. • Cumpla con todas los requerimientos que establece el requisito 10 de PCI DSS, facilitando la integralidad entre varios tipos de dispositivos de diferentes fabricantes. • La correlación de eventos descartando falsos positivos • Permite controlar la gestión de los registros y monitoreo de los eventos garantizando la integración con el plan de respuesta a incidentes. • Genere informes de Cumplimiento de PCI DSS e impida la alteración de los registros analizados o en custodia.	Algunas soluciones SIEM (Reporte de Gartner 2019) • Elastico • LogPoint SIEM • Splunk
11.5	**FIM (File Integrity Monitoring)**	• Alertar cambios, adiciones y eliminaciones en los archivos supervisados. Usar algoritmos de hash con criptografía fuerte y con poca posibilidad de colisión (ver NIST SP 800-57 Part 1 y la FIPS 180-4) • Permitir la protección de los cambios en la línea base de hash y sus propios programas y componentes. • Ser configurable a fin de identificar modificaciones en archivos cuando se inserta contenido (como sucede en los logs) y facilitar la ejecución de revisiones periódica. • Tener características agentless que faciliten el monitoreo de plataformas en donde los agentes no están disponibles • Permitir la integración de reportes con las herramientas de registro de eventos y el sistema centralizado de logs • Generar alertas a diferentes canales de comunicación o de contacto cuando se requiera • La solución deberá identificar las partes del archivo que han sido alteradas, mostrar el antes y el después de los contenidos cambiados para una comparación efectiva.	• TripWire File Integrity Monitor • McAfee Integrity Control • CimTrak File Integrity Monitoring

Fuente: Propia

7.4. PROCESO DE IMPLEMENTACIÓN Y CERTIFICACIÓN EN EL ESTÁNDAR PCI DSS

En primer lugar, una pasarela de pago antes de considerar la opción de certificarse en PCI DSS debe hacer la gestión con una empresa acreditada como Asesor de Seguridad Certificado (QSA – Qualified Security Assessor) para que le practique este proceso y a su vez debe tener el aval con al menos una de las franquicias asociadas al PCI SSC a fin de que determine su nivel como proveedor de servicio (PS) considerando para ello uno o varios de los criterios aplicables que establece cada franquicia o marca de tarjeta de pago como el número de transacciones anuales; por lo que los requerimientos exigibles en la validación o auditoria de cumplimiento en PCI DSS estarían establecidos bajo los siguientes niveles para cada una las marcas:

Tabla 11. Requerimientos aplicables a un PS para la certificación en PCI DSS

Nivel/ Marca	Visa	MasterCard	American Express (AMEX)	Discover	JCB
1	**Criterios:** ✓ Más de 300 mil transacciones. ✓ Todos los procesadores VisaNet ✓ Los PS incluidos en la lista global de proveedores de servicios **Requerimientos de cumplimiento:** **• Auditoria Anual por una QSA** • Escaneos de Vulnerabilidades Trimestrales por ASV* • AoC** • Remitir el RoC*** anual.	**Criterios:** ✓ Más de 300 mil transacciones. ✓ Cualquier TPP**** ✓ PS o TPP comprometidos en alguna brecha. **Requerimientos de cumplimiento:** **• Auditoria Anual por una QSA** • Escaneos de Vulnerabilidades Trimestrales por ASV • AoC • Remitir el RoC anual.	**Criterios:** ✓ Más de 2.5 millones de transacciones. ✓ PS asignados a ser Nivel 1. **Requerimientos de cumplimiento:** **• Auditoria Anual por una QSA** • Escaneos de Vulnerabilidades Trimestrales por ASV • AoC.	**Criterios:** ✓ Más de 300 mil transacciones. ✓ PS asignados a ser Nivel 1. **Requerimientos de cumplimiento:** **• Auditoria Anual por una QSA** • Escaneos de Vulnerabilidades Trimestrales por ASV • AoC • Remitir el RoC anual	**Criterios:** Cualquier PS sin importar la cantidad de transacciones. **Requerimientos de cumplimiento:** **• Auditoria Anual por una QSA** • Escaneos de Vulnerabilidades Trimestrales por ASV.
2	**Criterios:** Menos de 300 mil transacciones **Requerimientos de cumplimiento:** • Llenado SAQ anual ***** con firma del QSA • Escaneos de Vulnerabilidades trimestrales ASV • AoC.	**Criterios:** Menos de 300 mil transacciones **Requerimientos de cumplimiento:** • Llenado SAQ anual con firma del QSA • Escaneos de Vulnerabilidades trimestrales ASV. Los PS en incumplimiento deben enviar plan de remediación.	**Criterios:** De 50 mil a 2.5 millones de transacciones. **Requerimientos de cumplimiento:** • Llenado SAQ anual con firma del QSA • Escaneos de Vulnerabilidades trimestrales ASV.	**Criterios:** Menos de 300 mil transacciones **Requerimientos de cumplimiento:** • Llenado SAQ anual con firma del QSA • Escaneos de Vulnerabilidades trimestrales ASV. Los PS en incumplimiento deben enviar plan de remediación.	

* ASV – (Approved Scanning Vendor): Proveedor Aprobado de Escaneo

** AoC – (Attestation of Compliance): Declaración de cumplimiento

*** RoC – (Report on Compliance): Informe de cumplimiento

**** TPP – (Third Party Processors): Procesador de terceros, conectadas directamente a las redes de pago de MasterCard.

***** SAQ – (Self-Assessment Questionnaire): Cuestionario de Auto-evaluación

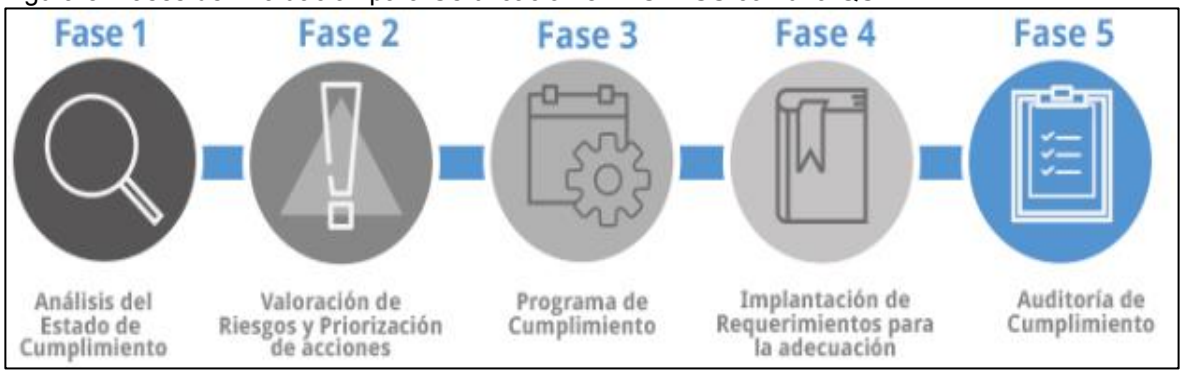
Tabla 11. (Continuación)

Nivel/ Marca	Visa	MasterCard	American Express (AMEX)	Discover	JCB
3	N/A	N/A	**Criterios:** Menos de 50.000 transacciones anuales **Requerimientos de cumplimiento:** No requiere enviar documentos de validación, pero se recomienda rellenar (SAQ) y ejecutar el escaneo de vulnerabilidades trimestral	N/A	

Fuente: https://www.isecauditors.com/sites/default/isecauditors.com/files//files/2-ISecAuditors_ACDECC-PCI-DSS_Justificacion_del_Cumplimiento.pdf

Teniendo en cuenta la tabla 11 lo necesario para adecuar o implementar estructuralmente los requerimientos de cumplimiento para la certificación en PCI DSS, se obtendrían mediante una evaluación de cumplimiento que sería el proceso que ejecutaría una entidad (En este caso la pasarela de pagos) con el apoyo de la QSA (ISECAuditors)[53] para lograr la acreditación de la certificación en PCI DSS y para eso se debería proceder mínimamente con las siguientes fases sugeridas por una QSA:

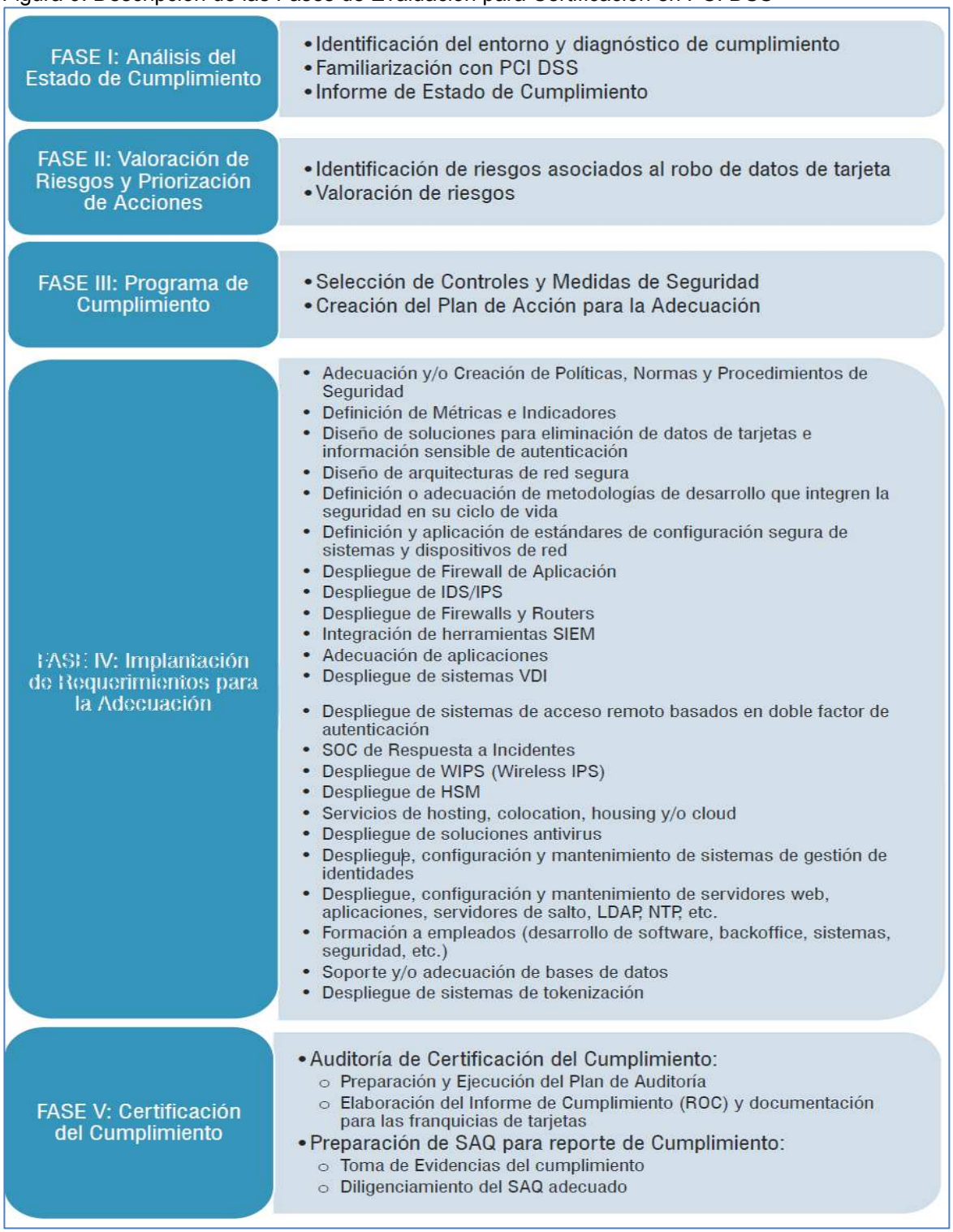
Figura 8. Fases de Evaluación para Certificación en PCI DSS con una QSA



Fuente: https://www.isecauditors.com/implantacion-pci-dss

[53] Internet Security Auditors - ISECAuditors. Adecuación y Certificación PCI DSS. 2018. Disponible en: https://www.isecauditors.com/implantacion-pci-dss

Figura 9. Descripción de las Fases de Evaluación para Certificación en PCI DSS



Fuente: https://www.isecauditors.com/sites/default/isecauditors.com/files//files/2-ISecAuditors_ACDECC-PCI-DSS_Justificacion_del_Cumplimiento.pdf

Una vez llegada la fase 5 se establecen 7 etapas para el proceso de certificación del cumplimiento las cuales se pueden aplicar para dar cubrimiento al informe RoC o a la preparación del informe SAQ; en los cuales se requiere el apoyo y aprobación de una QSA para acreditar la certificación de cumplimiento en el estándar PCI DSS. Por lo que estas etapas conforme a la QSA ISec Auditors[54] serian:

Etapa I - Lanzamiento de proyecto: Que determina el proyecto y alcance para la certificación de la entidad. *Tiempo duración estimado por la QSA 1 día hábil.*

Etapa II - Revisión del Entorno de Cumplimiento: Se valida los procesos rutinarios del cliente con relación a la transmisión, procesamiento o almacenamiento de datos de tarjetas de crédito (CHD), con el objetivo de comprobar la pertinencia de la y/o cambios en el entorno CDE asociado con el cumplimiento desde la implantación inicial de PCI DSS o desde la última auditoría realizada. *Tiempo duración mínimo por la QSA 5 días hábiles.*

Etapa III - Revisión Documental: Recopilación de información relacionada en la etapa 2 y que se sustenta con los soportes documentados y/o entregables que exige PCI, las cuales serán objeto de revisión por la QSA; por lo que se recomienda tener soportado los entregables definidos en el Anexo A. Requerimientos de PCI DSS V3.2.1 para las pasarelas de pagos de esta guía. *Tiempo duración estimado por la QSA 20 días hábiles.*

Etapa IV – Preparación del Plan de Auditoría: Se determina el plan de trabajo para las reuniones y ejecución de pruebas de cumplimiento necesarias para la obtención de evidencias que sustentaran la auditoría. Además, se define puntos como personal específico que se requieran durante la auditoría o para labores específicas. *Tiempo duración estimado por la QSA 5 días hábiles.*

Etapa V - Ejecución de la Auditoría: Se ejecuta el Plan de Auditoria validando el cumplimiento de los requerimientos del estándar PCI DSS, incluyendo la evaluación de controles compensatorios; considerando en ello el análisis de la documentación, las pruebas con muestreo y las entrevistas al personal de la entidad auditada. *Tiempo duración estimado por la QSA 30 días hábiles.*

Etapa VI - Presentación de Resultados: Cada QSA presenta los resultados de su proceso de auditoria con la entidad auditada detallando los aspectos y hallazgos que se dieron a lugar como los términos que se presentaran en el resultado final

[54] Internet Security Auditors - ISECAuditors. Auditoría de Certificación del Cumplimiento de PCI DSS. 2018. Disponible en: https://www.isecauditors.com/auditoria-certificacion-cumplimiento-pcidss

que se soportaran en el informe de cumplimiento (RoC) o en el informe (SAQ). *Tiempo duración estimado por la QSA 1 día hábil al final la etapa V.*

Etapa VI - Elaboración del Informe de Cumplimiento: Elaboración del informe RoC que acreditara el cumplimiento de los requisitos además de soportar los requerimientos de cumplimiento para sustentarlos ante la marcas de tarjetas de pago y el PCI SSC; quienes oficializaran la certificación de cumplimiento en el estándar PCI DSS a la entidad auditada (Si fue exitoso, sin ningún hallazgo) en un término aproximado de 45 días hábiles después de radicado por la QSA los requerimientos de cumplimiento de forma completa y pertinente. *Tiempo duración para la elaboración del informe sujeto a cada QSA según el alcance de la entidad auditada.*

Cabe resaltar que también se puede certificar el cumplimiento en el estándar mediante el Cuestionario de Auto-Evaluación (SAQ) el cual debe estar firmado por el QSA para su validez por el PCI SSC y las marcas de tarjeta de pago asociadas; pero esta opción solo sería aplicable solamente sí los criterios establecidos por la marcas de tarjetas de pagos convenidas con el proveedor de servicio (PS) están sujetas a un nivel 2 o 3 según corresponda, de lo contrario la certificación se avalaría bajo los requerimientos que establece cada franquicia para el nivel 1. No obstante como existen varios formatos para el SAQ, el que se aplicaría para los proveedores de servicios como a las pasarelas de pagos seria SAQ – D-SP para proveedores de servicio[55], ya que este considera 369 preguntas que conforman el subconjunto de controles de PCI DSS aplicados al escenario específico que se maneja para un proveedor de servicio, por lo que este formato se encuentra disponible para PCI DSS V.3.2.1 en el siguiente link: https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-D_ServiceProvider.pdf.

Algunas organizaciones avaladas al 2019 por PCI SSC como QSA para que apoyen en la gestión de implementación y certificación en PCI DSS a las pasarelas de pago en Colombia son: Auditores de seguridad de Internet (ISEC Auditors), IQ Information Qualty, ControlCase, entre otras. (Ver QSA vigentes/permitidas por el PCI SSC en: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors)

[55] ACOSTA, David. Todo lo que siempre has querido saber acerca de los SAQ (Cuestionarios de Auto-evaluación) de PCI DSS v3.2.1. En: PCIHISPANO. 2018. Disponible en: https://www.pcihispano.com/todo-lo-que-siempre-ha-querido-saber-acerca-de-los-saq-cuestionarios-de-auto-evaluacion/

7.4.1. Dificultades y amenazas durante el proceso de implementación, certificación y sostenimiento de PCI DSS en una pasarela de pago

Dificultades

- Las Fases de Evaluación para Certificación en PCI DSS con una QSA son dispendiosas y las empresas QSA pueden cobrar elevadas cuantías y demandar un desgaste institucional por el proceso y más cuando este se debe ejecutar anualmente, por lo que la organización debe estar preparada para efectuar esta labor y considerar un equipo de trabajo dispuesto para este proceso de forma continua.

- Las exigencias de los requisitos del estándar PCI DSS exigen amplios procesos para la seguridad del servicio por lo que la organización debe contar con recursos económicos para garantizar una adecuada implementación y sostenimiento del servicio de forma segura y en cubrimiento de los requisitos del estándar. Más aún si se opta por soluciones tecnológicas licenciadas en vez de herramientas de software libre para la implementación del estándar.[56]

- Limitaciones de solo diez (10) empresas de la categoría QSA con asesores acreditados en Colombia para la realización de la evaluación del estándar en una entidad; ya que al 2019 se ha incrementado la exigencia u obligatoriedad de tener la certificación en el estándar PCI DSS a las entidades que gestionan datos CHD para que se certifiquen; los que hace que hoy sea complejo tramitar este proceso de certificación y su costo pueda ser elevado ante una QSA dependiendo la dimensión de la infraestructura TI, servicios ofrecidos para la gestión datos CHD, cantidad de transacciones, marcas de pagos convenidas, entre otros para las entidad solicitante. Ya que únicamente una empresa con categoría QSA está autorizada para efectuar el proceso de auditoría de certificación sustentado en un Informe de Auditoría (ROC) o para certificar el cumplimiento del Cuestionario de Autoevaluación (SAQ)

- No tener personal en la organización con la experticia para apoyar la labor de la certificación en el estándar; por lo que se pueden cometer errores durante las fases de evaluación o en la gestión de la documentación y registros de evidencias para los informes SAQ.

[56] CASALLAS, Hugo; PERDOMO, Javier y VARGAS, Julio. Guía de implementación de herramientas tecnológicas dirigida a las pymes para dar cumplimiento a la norma internacional PCI DSS V3.0. Universidad Piloto de Colombia. 2016. P.171. Disponible en: http://polux.unipiloto.edu.co:8080/00002970.pdf

Amenazas

- El PCI SSC considera dentro de sus políticas que al menos cada 3 años se actualiza la versión de su estándar PCI como proceso cíclico de mejora continua, en el que tienen en cuenta las tendencias tecnológicas y los riesgos de seguridad que se derivan de las constante amenazas y vulnerabilidades que surgen para las tecnologías y el sector financiero; por lo que esos cambios pueden exigir renovaciones y cambios sustanciales o brusco a cualquier organización que tenga el deber de certificarse y sostener el estándar PCI DSS en pos de sus objetivos organizacionales.

- Incumplir con algún requisito o sub-requisito durante la fase 5 de certificación del cumplimiento que puede dilatar el proceso de la auditoria de certificación y en su defecto generar la negación de la certificación del cumplimiento en el estándar por parte de la QSA; ya que esta PCI SSC en sus estatus no admite hallazgos o no conformidades para el cumplimiento de los requisitos o sub-requisitos del estándar y por eso es exigente en su total cumplimiento ya que el resultado cumplimiento se acredita en una 100% o no se admite.

- No ser aceptado por una o varias marcas de tarjetas de pago bien sea por sanciones impuestas en el pasado, la perdida temporal o permanente de los permisos para gestionar datos de tarjetas por parte del proveedor de servicio; como el hecho de no ser admitido por la marca de tarjetas de pago en el nivel deseado por el proveedor de servicio limitando su negocio a las imposiciones establecidas por las franquicias para dar cumplimiento a los requerimientos en la certificación de PCI DSS.

- Los resultados de los escaneos de vulnerabilidades trimestrales por el ASV arrojen vulnerabilidades con resultados elevados que sean complejos de remediar o parchar; ante la falencia operativa para una posible remediación a la(s) brecha(s) presentada(s) acorde a los requerimientos del requisito 11 del estándar; lo que retrasaría el proceso de evaluación y certificación del estándar y hasta generaría incumplimientos contractuales con los clientes y con las marcas de tarjetas de pago en caso de una recertificación.

- Tener multas de incumplimiento por parte de las marcas de tarjetas de pago a los proveedores de servicio por no cumplir los plazos en los compromisos para la entrega de los requerimientos de cumplimiento o diligenciar los informes SAQ no pertinentes para la entidad o en su defecto con información incorrecta sin las validaciones pertinentes.

8. RESULTADOS Y DISCUSIÓN

De conformidad con los resultados del capítulo 7.1 de esta guía se puede decir que para las pasarelas de pagos se excluye un (1) Apéndice más un (1) sub-requisito dentro de la cobertura que establece el estándar PCI DSS V3.2.1 y estarían condicionados dos (2) requisitos más un (1) sub-requisito; información que se alinea con los colores sombreados establecidos dentro de la ***Anexo A***. de este documento y como se evidencia en la siguiente tabla 12:

Tabla 12. Resumen de aplicabilidad requisitos PCI DSS en pasarelas de pagos

REQUERIMIENTOS OBLIGATORIOS	REQUERIMIENTOS EXCLUIDOS	REQUERIMIENTOS CONDICIONADOS
Requisitos 1 al 12 (Excluyendo los sub-requisitos 2.6 y 9.9)	Sub-requisito 9.9 Apéndice 2	Sub-requisito 2.6 Apéndice 1 Apéndice 3

Fuente: Propia

Cabe aclarar que la estipulación que determina la exclusión del sub-requisito 9.9 se da porque este rige en los dispositivos de lectura de tarjetas físicas como lo señala el estándar PCI DSS, lo cual no hace parte del servicio Core de las pasarelas de pagos y en cuanto al Apéndice 2 es porque el estándar sustenta que este apéndice es un requisito adicional que se tendrá en cuenta en entidades que usan SSL/TLS temprana, lo cual no está admitido en su manejo por parte de las pasarelas de pagos por tratarse de protocolos de seguridad inseguros para el servicio Core. De igual forma los requisitos condicionados están sujetos a las consideraciones de seguridad y de implementación de la arquitectura del servicio Core de la pasarela como de la interacción del CDE, por lo que si el servicio Core está en un entorno CDE con hosting compartido con un tercero deberá aplicarse respectivamente el sub-requisito 2.6 y Apéndice 1 de forma obligatoria; mientras que el Apéndice 3 se aplicaría de forma obligatoria si lo exige formalmente una marca de tarjeta de pago o un adquiriente teniendo como premisas la densidad de datos CHD que gestiona la pasarela de pago y/o los incidentes de seguridad presentados por esta.

Por otra parte los capítulos 7.2 y 7.3 de esta guía permite ver que el principal riesgo está sobre la información de cuentas que incluyen los datos de titulares de tarjetas (CHD) y los datos confidenciales de autenticación (SAD), porque la obtención de esta información permite la ejecución de fraudes financieros con las tarjetas de los usuarios/tarjetahabientes y es por eso que es muy apetecido el atentar con las infraestructuras o sistemas financieros por los ciberdelincuente lo que lleva a que la organizaciones del sector financiero incluyendo entre estas las pasarelas de pago a que tengan esquemas seguridad fuerte y actualizado regidos por un estándar como PCI DSS que es bastante riguroso a la hora de evaluarse para dar su acreditación ante las marcas de pago o franquicias quienes son las que finalmente

representan la globalización de la red o interconexión para uso extensivo de la tarjetas de pago a nivel mundial y en diferentes tecnologías/medios.

Respecto al capítulo 7.4 se puede decir que el proceso de implementación y certificación en el estándar es bastante dispendioso, que incluso puede generar grandes costos más aún cuando es una labor continua que anualmente se debe evaluar independientemente del nivel en que se encuentra la pasarela de pago como proveedor de servicio (PS); pero esta labor es retribuidle en la seguridad del servicio CORE que a su vez permitirá vincular más clientes (Comercio) y obtener la confianza en los usuarios/tarjetahabientes para que hagan sus compras por los portales de comercio electrónico.

En cuanto a los antecedentes del capítulo 5.5. se puede observar que estos arrojan un compendio de información útil a nivel del estándar PCI DSS para diferentes los sectores interesados en la normatividad, pero no se enfoca explícitamente en como implementar y certificar con éxito el cumplimiento de este estándar en las pasarelas de pagos; considerando la tesis de las ingenieras Calle y Mejía de la Universidad Politécnica Salesiana con sede en Guayaquil en la que alude la carencia de las competencias en el personal y la falta de preparación para este propósito en el sector financiero, que también puede hacerse extensible a los proveedores de servicios (PS) que incluye a las pasarelas de pagos. Así exista la opción de contratar la asesoría de un QSA o de un profesional PCI (PCIP) para este proceso, no todas las pasarelas de pagos cuentan con los recursos financieros suficientes para proveer y mantener este apoyo indefinidamente o en su defecto acreditar a su personal con ese perfil; más aún cuando esta normatividad está en constante cambio en pos de la mejora continua y tendencia del mercado y las tecnologías, por lo que sería un gran esfuerzo e inversión para estas empresas especialmente en aquellas que quieren aumentar su cobertura, la cantidad de transacciones o poner en marcha esta línea de negocio en el país y que de entrada se verían abocadas en cumplir con el estándar PCI DSS; sumado a los altos costos que se les demandaran en la implementación al 100% de los requisitos del estándar con sus herramientas tecnológicas más el proceso de certificación que anualmente se hace ante la QSA.

Por lo anterior, esta guía puede ser una primera opción de consulta en las pasarelas de pago para que conozcan el estándar PCI DSS y se orientaren respecto a su proceso de implementación y certificación en el cumplimiento del estándar, guía que puede ser acogida en su gran mayoría de aspectos por otros Proveedores de Servicios (PS); pero no todos los aspectos relacionados están orientados a los distintos PS, ya que cada uno de ellos abordan temas propios y diferenciales en un amplio universo de acciones para las tarjetas de pago; por lo que el enfoque de esta guía se limita más a las pasarelas de pagos, más aún cuando la tendencia va en crecimiento tanto en el número de transacciones por comercio electrónico como en la constitución de este tipo de organizaciones a nivel nacional y hasta mundial; que han derivado sobre estas una mayor regulación con controles de seguridad que incitan al cumplimiento del estándar PCI DSS.

9. CONCLUSIONES

Los comercios al momento de elegir una pasarela de pago tienen en cuenta los esquemas de seguridad que presta su sistema y que a su vez estén certificados en la última versión del estándar PCI DSS; ya que paralelamente los usuarios o tarjeta habientes que tienen cierta conciencia para usar de forma segura sus medios de pagos verifican que puedan su por lo que tendrán confianza en hacer una compra segura y de ahí la importancia de mantener implementadas las medidas de seguridad como establece el estándar.

El estándar no exige literalmente tener la última generación de los componentes tecnológicos para el CDE ni el servicio Core, pero si es bastante riguroso en requerir que la pasarela de pago haya considerado para su servicio cuente con las actualizaciones, parches de seguridad y medidas protección efectivas, y que no estén lista de ser violentadas porque cualquier incumplimiento o falencia en al menos un (1) requisito del estándar es causal de dilatación y/o perdida del proceso de evaluación para la certificación en PCI DSS, por lo que se sugiere asesorarse muy bien con la QSA cuando se gestione por primera vez el proceso de evaluación para la certificación en PCI DSS o se tengan cambios significativos en el servicio.

Esta guía fue estructurada esencialmente para las pasarelas de pagos, pero puede ser adaptada a cualquier organización que tenga características como proveedor de servicio (PS) en el manejo de datos de cuentas (CHD y/o SAD); a fin de puedan acoplar los requisitos del estándar, las recomendaciones de seguridad y demás aspectos como las fases de evaluación para poder lograr la certificación en PCI DSS si este es requerido. Sin embargo, es bueno tener presente que el estándar evoluciona por diverso factores que establecen las marcas de tarjetas de pagos asociadas al PCI SSC; por tanto, los requisitos y demás exigencias de las marcas de pagos pueden cambiar entre versiones; de ahí que las organizaciones deben estar monitoreando las actualizaciones que presente el PCI SSC y adaptar los cambios al negocio conforme a las actualizaciones normativas y mantener en mejora continua lo que este funcionado de manera pertinente, admisible y segura.

10. RECOMENDACIONES

Como recomendaciones de seguridad informática se sugiere seguir a cabalidad las estipulaciones documentadas en el Anexo A y el capítulo 7.3 que se alienan con los aspectos de seguridad informática para los requisitos de PCI DSS definidos en la tabla #1 del capítulo 5.2 de marco teórico de esta guía; ya que estas recomendaciones sustentan las especificaciones necesarias para dar cubrimiento a los 12 requisitos primordiales del estándar, entre las que se destacan los estándares de configuraciones de los componentes TI y las herramientas de seguridad que son necesarias como controles de seguridad críticos para el cumplimiento del estándar contemplando en estos los criterios esenciales para su selección e implementación.

Se le recomienda a los proveedores de servicio (PS) incluyendo en estos a las pasarelas de pago validar la contratación de una preauditoria o preevaluación cuando se quieren certificar por primera vez en PCI DSS, asesorándose muy bien de la QSA con que se haría esta labor, más aún si no tuvieron un apoyo calificado durante el proceso de implementación del estándar; por lo que las fases 1 a 4 de una evaluación para lograr la certificación en PCI DSS con una QSA podrían considerarse como Análisis de Brechas (GAP) que resultan como una preauditoria para la empresa, lo que podría servir para orientar el personal en su compromiso y mejorar las falencias con el apoyo de los asesores internos o externos según recomiende la QSA; pero todo esto es previo al examen de auditoria (Fase 5) que si se considerará la rigurosidad en el proceso para poder obtener la certificación.

Por último, a las pasarelas de pago que están interesadas en lograr esta certificación se les recomienda no limitar únicamente su negocio a cumplir el estándar PCI DSS exclusivamente en pos de efectuar una normatividad de la Superintendencia Financiera o la exigencia de un cliente; sino también deben alinear la aplicación de este estándar con las demás parte involucradas, los sistemas integrados de gestión de la organización y las diferentes estrategias tecnologías del negocio; todo esto en pos de optimizar el sistema, facilitar su administración en materia documental y tecnológica controlando a la vez posibles riesgos e incidentes y a hasta las vulnerabilidades/exploit como las zero-day en la que suelen perpetrase amenazas persistentes avanzadas (APTs) nuevas o recién salidas que de algún modo afectan los servicios Core y la credibilidad de cualquier sistema. Por lo que la gestión del estándar PCI DSS, se puede adecuar con buenos procesos de negocio, acompañado de una buena y segura gestión/infraestructura de TI y con la integración con otros estándares como SGSI- Sistema de Gestión de Seguridad de la Informacion, COBIT - Control Objectives for Information and related Technology, entre otros que aportarían unas buenas prácticas en términos de tecnología y seguridad para la adaptación apropiada del estándar PCI DSS en el negocio y que se deben mejorar continuamente de manera organizada y periódica.

11. DIVULGACIÓN

La divulgación de la presente monografía se efectúa en la biblioteca virtual de la Universidad nacional Abierta y a Distancia (UNAD) ubicada en el link http://bibliotecavirtual.unad.edu.co

BIBLIOGRAFÍA

ACOSTA, David. “¿Qué es PCI DSS?” En: PCIHISPANO. 30 de mayo de 2019. {En línea}. {19 septiembre de 2018} disponible en: https://www.pcihispano.com/que-es-pci-dss/

--------. “Controles técnicos de PCI DSS”. En: PCIHISPANO. 2014. {En línea}. {27 octubre de 2019} disponible en: https://www.pcihispano.com/category/controlespcidss/

--------. “Controles técnicos de PCI DSS parte VI: Registro de eventos (logs)”. En: PCIHISPANO. 05 de Julio de 2016. {En línea}. {27 octubre de 2019} disponible en: https://www.pcihispano.com/controles-tecnicos-de-pci-dss-parte-vi-registro-de-eventos-logs/

--------. “Estándares de configuración segura (hardening) en PCI DSS (actualización v3.2)”. En: PCIHISPANO. 04 de junio de 2016. {En línea}. {27 octubre de 2019} disponible en: https://www.pcihispano.com/estandares-de-configuracion-segura-hardening-en-pci-dss/

--------. “Listado de documentación para cumplir con el estándar PCI DSS”. En: PCIHISPANO. 20 de junio de 2016. {En línea}. {27 octubre de 2019} disponible en: https://www.pcihispano.com/estas-buscando-listado-documentacion-cumplir-pci-dss-aqui-lo-tienes/

--------. “Niveles de cumplimiento y requerimientos de las marcas para comercios y proveedores de servicio en PCI DSS”. En: PCIHISPANO. 30 de septiembre de 2014. {En línea}. {27 octubre de 2019} disponible en: https://www.pcihispano.com/niveles-de-cumplimiento-y-requerimientos-de-las-marcas-para-comercios-y-proveedores-de-servicio-en-pci-dss/

--------. “Todo lo que siempre has querido saber acerca de los SAQ de PCI DSS v3.2.1”. En: PCIHISPANO. 29 de junio de 2018. {En línea}. {27 octubre de 2019} disponible en: https://www.pcihispano.com/todo-lo-que-siempre-ha-querido-saber-acerca-de-los-saq-cuestionarios-de-auto-evaluacion/

ASOBANCARIA. “Pasarelas de pago, un aliado para el comercio electrónico”, may 2016. {En línea}. {01 octubre de 2018} disponible en: http://www.asobancaria.com/sabermassermas/pasarelas-pago-aliado-comercio-electronico/

BARTOLOMÉ, Laura. “Historia de los medios de pago con tarjeta. Los riesgos asumidos por empresas de retail y estudio de hábitos de compra con tarjeta”, 2014. {En línea}. {01 octubre de 2018} disponible en: https://www.comercioexterior.ub.edu/tesina/Proyectos13-14/proyecto_modificado/Proyecto2_BartolomeLaura.pdf

CADAVID CORREA, Orlando y GIRALDO OSPINA, Evelio. “Plataformas de pagos electrónicas”. En: Eje21. 07 de noviembre 2018 {En línea}. {07 marzo de 2020} disponible en: https://www.eje21.com.co/2018/11/desde-diciembre-se-empezara-a-exigir-a-las-pasarelas-de-pagos-digitales-sistemas-de-proteccion-de-datos/

CALLE PARRALES Zoila y MEJÍA VILLEGAS, Andrea. “Análisis de la implementación del estándar PCI DSS en la seguridad de la información dentro de una institución financiera”. Tesis de Ingeniera de Sistemas. Ecuador. Universidad Politécnica Salesiana Sede Guayaquil. 2015. 175p. {En línea}. {07 marzo de 2020} disponible en: https://dspace.ups.edu.ec/bitstream/123456789/10317/1/UPS-GT001222.pdf

CASALLAS LARROTTA, Hugo A.; PERDOMO VALDERRAMA, Javier y VARGAS FERNÁNDEZ, Julio Alberto. “Guía de implementación de herramientas tecnológicas dirigida a las pymes para dar cumplimiento a la norma internacional PCI DSS V3.0”. Trabajo de grado Especialista en Seguridad Informática. Bogotá D.C. Universidad Piloto de Colombia. 2016. 171p. {En línea}. {07 marzo de 2020} disponible en: http://polux.unipiloto.edu.co:8080/00002970.pdf

COLPRENSA. “Colombia fue uno de los países con más ataques cibernéticos el año pasado”. En: LA REPUBLICA. 21 de julio de 2019 {En línea}. {06 octubre de 2019} disponible en: https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

CONGRESO DE LA REPUBLICA DE COLOMBIA. “Ley estatutaria 1266 de 2008”. 31 de diciembre de 2008. {En línea}. {27 octubre de 2019} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

--------. “Ley estatutaria 1581 de 2012”. 18 de octubre de 2012. {En línea}. {27 octubre de 2019} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

CONSEJO SOBRE NORMAS DE SEGURIDAD DE LA PCI, LLC. (PCI SSC) “Enfoque priorizado para PCI DSS V3.2.1”. Jun 2018 {En línea}. {01 octubre de 2018} disponible en: https://www.pcisecuritystandards.org/document_library

CONSEJO SOBRE NORMAS DE SEGURIDAD DE LA PCI, LLC. (PCI SSC). “Glosario de términos, abreviaturas y acrónimos de PCI DSS Versión 3.2”. Abr 2016 {En línea}. {01 octubre de 2018} disponible en: https://www.pcisecuritystandards.org/document_library

--------. “Resumen de cambios de PCI DSS V3.2.1”. May 2018 {En línea}. {01 octubre de 2018} disponible en: https://www.pcisecuritystandards.org/document_library

--------. “Requisitos y procedimientos de evaluación de seguridad PCI DSS Versión 3.2.1”. May 2018. {En línea}. {01 octubre de 2018} disponible en: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1-ES-LA.pdf?agreement=true&time=1574494354390

--------. “Self-Assessment Questionnaire D and Attestation of Compliance for Service Providers para PCI DSS V3.2.1”. Jun 2018 {En línea}. {27 octubre de 2019} disponible en: https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-D_ServiceProvider.pdf.

--------. “Tokenization Product Security Guidelines – Irreversible and Reversible Tokens”. Abr 2015 {En línea}. {01 octubre de 2018} disponible en: https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

CONTROLCASE. “PCICompliant of Place to Pay”. 31 de enero de 2020. {En línea}. {07 marzo de 2020} disponible en: https://seal.controlcase.com/index.php?page=showCert&cId=3594404955

DATAPAGA. “Formas de prevenir el fraude online con tu pasarela de pago”, firelionsolutions”. 2018. {En línea}. {01 octubre de 2018} disponible en: https://medium.com/@datapagaoficial/formas-de-prevenir-el-fraude-online-con-tu-pasarela-de-pago-7d4dda2ad98a

EL TIEMPO. “Denuncias por delitos informáticos crecieron el 31 % el año pasado”. Sección: Justicia. 17 de enero de 2018. {En línea}. {01 octubre de 2018} disponible en https://www.eltiempo.com/justicia/delitos/denuncias-por-delitos-informaticos-crecieron-en-2017-172294

--------. “Intermediario de pagos en internet, negocio que crece con poco control”. Sección: Economía y Negocios. 26 de enero 2018. {En línea}. {01 octubre de 2018}

disponible en https://www.eltiempo.com/economia/sector-financiero/intermediarios-de-pagos-por-internet-en-colombia-no-estan-muy-controlados-175320

FERNÁNDEZ BLEDA, Daniel. “PCI DSS, justificación del cumplimiento”. En Internet Security Auditors. 2018. {En línea}. {27 octubre de 2019} disponible en: https://www.isecauditors.com/sites/default/isecauditors.com/files//files/2-ISecAuditors_ACDECC-PCI-DSS_Justificacion_del_Cumplimiento.pdf

FRÍAS, Gabriela. La empresa colombiana que monitorea 850.000 compras en línea al día en todo el mundo. En: CNN ESPAÑOL. 29 de mayo de 2017 {En línea}. {07 marzo de 2019} disponible en: https://cnnespanol.cnn.com/2017/05/29/la-empresa-colombiana-que-monitorea-850-000-compras-en-linea-al-dia-en-todo-el-mundo/

Internet Security Auditors - ISECAuditors. “Adecuación y Certificación PCI DSS”. 2018. {En línea}. {27 octubre de 2019} disponible en: https://www.isecauditors.com/implantacion-pci-dss

--------. “Auditoría de Certificación del Cumplimiento de PCI DSS”. 2018. {En línea}. {27 octubre de 2019} disponible en: https://www.isecauditors.com/auditoria-certificacion-cumplimiento-pcidss

ISO – International Organization for Standardization. ISO/IEC 27000:2016. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario. Edición Instituto Colombiano de Normas Técnicas Internacional – ICONTEC del 2017.

--------. ISO/IEC 27001:2013. Técnicas de Seguridad, Requisitos del Sistema de Gestión de Seguridad de la Información. Edición Instituto Colombiano de Normas Técnicas Internacional – ICONTEC del 2013.

--------.ISO 31000:2018. Gestión de riesgos - Directrices. Edición Instituto Colombiano de Normas Técnicas Internacional – ICONTEC del 2018.

MALCA, Solange. “Los 5 mayores ataques de seguridad en los medios de pagos digitales durante el 2016”. Alignet. 2017. {En línea}. {27 octubre de 2019} disponible en: https://www.alignet.com/blog/seguridad/los-5-mayores-ataques-de-seguridad-en-los-medios-de-pagos-digitales-durante-el-2016/

MICROSOFT. “Guía de planeación para el cumplimiento del Estándar de seguridad

de datos en la industria de tarjetas de pago". Octubre 2017. {En línea}. {08 marzo de 2020} disponible en: https://docs.microsoft.com/es-es/security-updates/security/guadeplaneacinparaelcumplimientodelestndardeseguridaddedatosenlaindustriadetarjetasdepago

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. "MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método". Gobierno de Madrid. 2012. {En línea}. {19 Septiembre de 2018} disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

---------. "MAGERIT – versión 3.0 Libro II - Catálogo de Elementos". Gobierno de Madrid. 2012. {En línea}. {19 Septiembre de 2018} disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

---------. "MAGERIT – versión 3.0 Libro III - Guía de Técnicas". Gobierno de Madrid. {En línea}. 2012 {19 Septiembre de 2018} disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

MYCHOICE2PAY. "Guía para saber elegir una pasarela de pago adaptada a tu negocio en 2019". 2019 {En línea}. {27 octubre de 2019} disponible en: https://www.mychoice2pay.com/es/blog/elegir-una-pasarela-de-pago

PAGOÁGIL. "Funcionalidad de la pasarela de pagoágil". 2017 {En línea}. {01 octubre de 2018} disponible en: https://pagoagil.co/pasarela-de-pagos/funcionalidad

PARDO J. Y RODRÍGUEZ S. "Análisis de la problemática de los medios de pago en el comercio electrónico aplicado al caso colombiano", Tesis de Universidad Javeriana, 2005. {En línea}. {01 octubre de 2018} disponible en: http://javeriana.edu.co/biblos/tesis/ingenieria/Tesis211.pdf

PAYU. Tokenización. {En línea}. {07 marzo de 2020} disponible en: https://www.payulatam.com/co/caracteristicas/tokenizacion/

REVISTA DINERO. "Nuevas reglas de la Superfinanciera para proteger las transacciones digitales". Sección: Ciberseguridad. 05 de junio de 2018 {En línea}. {01 octubre de 2018} disponible en: https://www.dinero.com/pais/articulo/nuevos-controles-de-la-superfinanciera-a-transacciones-digitales/259052

REVISTA DINERO. “Pasarelas de pago se alistan para un verdadero desfile”. Sección: Tecnología. 26 de marzo de 2019 {En línea}. {06 octubre de 2019} disponible en: https://www.dinero.com/edicion-impresa/negocios/articulo/pasarelas-de-pago-en-colombia-seguiran-creciendo/268518

RINCÓN CÁRDENAS, Erick, “Manual de Buenas Prácticas de las Pasarelas de Pago en Colombia”. Bogotá D. C. OE- Observatorio e Commerce. 2018. {En línea}. {06 octubre de 2019} disponible en: https://www.observatorioecommerce.com.co/wp-content/uploads/2018/10/Manual-Buenas-Practicas-Pasarelas.pdf

RODRÍGUEZ, Ana Cecilia; RODRÍGUEZ, Ana Karina & LIÑARES, Verónica. “Riesgo operacional en los sistemas de pagos - Metodología VaR”. 2013 {En línea}. {27 octubre de 2019} disponible en: http://www.bvrie.gub.uy/local/File/doctrab/2013/4.2013.pdf

RODRÍGUEZ, Herbert. “Por qué no aprender un poco de Pasarelas de pago y el Fraude en Comercio Electrónico”, 2014 {En línea}. {01 octubre de 2018} disponible en: https://blogcomercioelectronico.com/por-que-aprender-un-poco-de-pasarelas-de-pago-y-el-fraude-en-comercio-electronico/

RODRÍGUEZ, María Carolina “El año pasado se presentaron 12.014 denuncias por ciberataques en Colombia”. En: LA REPÚBLICA. 28 de junio de 2019 {En línea}. {06 octubre de 2019} disponible en: https://www.larepublica.co/especiales/informe-tecnologia-junio-2019/el-ano-pasado-se-presentaron-12014-denuncias-por-ciberataques-en-colombia-2879067

SANABRIA BELLO, Richard M. y SARMIENTO PIÑEROS, Javier A. Metodología de auditoría para verificar el nivel de cumplimiento del proceso de desarrollo de software frente a los requisitos de la norma PCI DSS en la compañía ABPS. Trabajo de grado de especialista en auditoría de Sistemas de información. Bogotá D.C. Universidad Católica de Colombia. 2018. 42p. {En línea}. {07 marzo de 2020} disponible en: https://repository.ucatolica.edu.co/bitstream/10983/16058/1/Metodolog%C3%ADa%20%20Auditoria%20DS%20PCI%20DSS%20ABPS.pdf

SANTOS, Jorge. “Pagos en línea, más seguros que el comercio tradicional.” PAYU. 13 abril de 2014. {En línea}. {07 marzo de 2020} disponible en: https://www.payulatam.com/blog/dico-velit-delicata-vel-ealia-modus-cum-altera-copiosae/

SCHULTZE, Juan Francisco. Haciendo historia en el mundo Fintech hace 15 años. En: LA REPUBLICA. 23 de enero de 2018 {En línea}. {07 marzo de 2020} disponible en: https://www.larepublica.co/finanzas-personales/haciendo-historia-en-el-mundo-fintech-hace-15-anos-2591334

SCOPING SIG, TOKENIZATION TASKFORCE PCI SECURITY STANDARDS COUNCIL. “PCI DSS Tokenization Guidelines”. Ago 2011 {En línea}. {01 octubre de 2018} disponible en: https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

SOTO SUAREZ, Andrés. “Exposición octave”. En: SlideShare. 26 de mayo de 2018 {En línea}. {27 octubre de 2019} disponible en: https://www.slideshare.net/AndresSotoSuarez1/exposicion-octave

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. “Circular Externa N° 008”, 2018 {En línea}. {01 octubre de 2018} disponible en: https://www.superfinanciera.gov.co/inicio/circulares-externas-2018_10096745

TOWERS WATSON, Willis. “E-commerce-riesgos-cibernéticos”. 27 de noviembre de 2018. {En línea}. {27 octubre de 2019} disponible en: https://willistowerswatsonupdate.es/ciberseguridad/e-commerce-riesgos-ciberneticos/

URBANO MATEOS, Susana María. “Qué es y cómo funciona la pasarela de pago en ecommerce”. En: ACTUALIDAD ECOMMERCE. 2018. {En línea}. {01 octubre de 2018} disponible en: https://www.actualidadecommerce.com/que-es-y-como-funciona-la-pasarela-de-pago-en-ecommerce/

VARGAS, German. “Claves para hacerle frente a la amenaza de los ciberataques”. En: Portafolio. 09 de noviembre de 2018 {En línea}. {06 octubre de 2019} disponible en: https://www.portafolio.co/negocios/claves-para-hacerle-frente-a-la-amenaza-de-los-ciberataques-523223

VENEGAS LOAIZA, Andrés. “El número de pasarelas de pago en línea en Colombia ha crecido 53,9%”. En: LA REPUBLICA. 16 de febrero de 2019 {En línea}. {06 octubre de 2019} disponible en: https://www.larepublica.co/internet-economy/el-numero-de-pasarelas-de-pago-en-linea-en-colombia-ha-crecido-539-2828821

ANEXOS

Anexo A. Requerimientos de PCI DSS V3.2.1 para las pasarelas de pagos[57]

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
1	1.1	1.1.1	• Considerar que se debe habilitar y que no • Lo que se deje por default se debe sustentar en materia de negocio • Separar la red corporativa de los acceso al Core del Negocio • Tener habilitado el IPS/IDS; Stafull del firewall • Considerar 1 a 1 las reglas del firewall • Tener como regla del CleanUp para que rechacé todo aquello que no se haya considerado • Si se hacen cambios dejarlo documentado en el estándar de configuración. • Formalizar y dejar registros de los cambios hechos los cuales deben ser aprobados y probados	1. Estándar de configuración para las reglas y otro de Administración del equipo de Firewall Pasarelas de pagos 2. Estándares de configuración de todos los componentes de red de Pasarelas de pagos 3. Procedimiento de control de cambios de infraestructura IT 4. Formatos y registros de control de cambios	N/A
		1.1.2	• Tener el diagrama vigente y coherente con lo que está en funcionamiento • Solicitar a los proveedores tecnológicos o proveedores IAAS información clara y precisa de cada componente, su distribución, Uso y configuración Hardening justificada.	1. Diagrama de red de Pasarelas de pagos contemplando los nuevos cambios para el Core del Negocio y la red corporativa	1.1.1; 1.2; 1.3.7
		1.1.3	• Muestra del recorrido de los datos CHD entre los sistemas y las redes. • Se lleva actualizado el flujo de los datos conforme a los cambios establecidos en el entorno.	1. Diagrama de flujo de datos	1.1.1; 1.1.2

[57] Propia (Autor)

[58] Para mayor detalle de los requerimientos del estándar PCI DSS V3.2.1 consultar el archivo “Requerimientos de PCI DSS V3.2.1 para las pasarelas de pagos.pdf” de autoría propia (Autor). Tomando como referente el Estándar PCI DSS V3.2.1 del PCI SSC.

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
		1.1.4	• Los estándares de configuración del firewall deben incluir los requisitos de cada firewall establecido con conexión a Internet, entre una DMZ y la red interna. • Se debe segmentar las redes con firewalls y estas deben quedar claramente identificada en el diagrama de red y el estándar de configuración.	1. Estándar de configuración para las reglas y otro de Administración del equipo de Firewall Pasarelas de pagos	1.1.1; 1.1.2
		1.1.5	• Considerar en los estándares de configuración los grupos, roles y responsabilidades para el manejo de los componentes de red. • Documentar en el manual de funciones de gestión humana los roles y responsabilidades asignadas al funcionario de IT de forma consecuente con lo del estándar de configuración e informar al funcionario el detalle de sus asignaciones.	1. Matriz de roles y responsabilidades de IT	1.1.1
		1.1.6	• Listar en el estándar de configuración todos los servicios, protocolos y puertos, teniendo en cuenta la justificación de negocio y la autorización de uso para cada componente de la red. • Identificar los servicios, protocolos y puertos inseguros permitidos en los componentes, dejarlos documentados y establecerles medidas de seguridad para sus funciones las cuales de quedar documentadas e implementadas en firewall y en el componente correspondiente.	1. Estándares de configuración de todos los componentes de red de Pasarelas de pagos	1.1.1
		1.1.7	• Establecer como política la revisión de las reglas del Firewall y enrutador cada seis meses; dejar la política establecida en el estándar de configuración. • Tener registros con la ejecución de revisión semestral, relacionando al responsable de esta tarea y que este tenga clara la labor gestionada; dejando constancia de aprobación y aceptación de resultados.	1. Política de revisión de las reglas del Firewall y enrutador cada seis meses de Pasarelas de pagos 2. Registros de revisión de la infraestructura y firewall de Pasarelas de pagos	1.1.1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	1.2	1.2.1	• Separar la red corporativa de Pasarelas de pagos con lo que involucra a la red del Core del Negocio • Los estándares de configuración deben estar documentados con la información de entrada y salidas del tráfico de la red; los cuales deben ser consecuentes a lo que esta implementado en los dispositivos. • Denegar aquellos permisos, ruta de red o reglas de firewall con una política de “Deny all” / "Cleanup" que no se contemplen para el tráfico del Core del Negocio	1. Política de “Deny all” / "Cleanup" para limitar el tráfico y reglas de firewall que no se contemplen en el Core del Negocio	1.1.1
		1.2.2	• Los archivos de configuración del router deben estar protegidos contra el acceso no autorizado; por tanto, deben cifrarse y almacenarse en una ruta segura los documentos. • Los Routers cuando se reinician deben dejar la misma configuración que tenían cuando estaban activos; en caso de no ser posible debe documentarse en el estándar de configuración como queda después de un reinicio y como se procede a dejarlo en el estado deseado.	1. Evidencias de las configuraciones estipuladas en este sub-requisito	1.1.1
		1.2.3	• Los firewalls deben negar el tráfico que no sea necesario para el CDE y no permitir conexiones inalámbricas que no sean sustentables para el servicio del Core del Negocio. • Confirmar que lo documentado corresponda totalmente con lo implementado en los componentes y conexiones de firewall. • Configurar DMZ, Router perimetrales y el Firewall; para que no permitan acceso directo de los datos de tarjeta habiente a Internet, ni siquiera a través de otros componentes red.	1. Evidencias de las configuraciones estipuladas en este sub-requisito	1.2.1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	1.3	1.3.1 - 1.3.6	• Cifrar los datos de tarjeta habiente que se transmiten a través de VPN o usan Internet entre el CDE y Pasarelas de pagos o entre el CDE de Producción y Contingencia • Impedir cualquier conexión de entrada /salida a Internet entre los componentes que hacen parte del CDE • Las configuraciones de firewalls y routers, deben contemplar controles contra la suplantación, como el hecho de que las direcciones internas no se pueden interconectar desde Internet a la DMZ. • Las configuraciones de firewalls y routers, deben dejar claramente definido que datos de tarjetahabiente van a salir a internet y se debe dejar autorizado dicho proceso de forma documentada. • Las configuraciones de firewalls y routers solo debe permitir conexiones relacionadas en la red interna y rechazar cualquier conexión entrante que no está parametrizada como una sesión previamente establecida. • Separar el CDE con una DMZ; a fin de aislar de cualquier otro ambiente o componente de los datos de tarjetahabiente y así delimitar el alcance de PCI DSS.	1. Estándar de configuración del Firewall y Routers.	1.3
		1.3.7	• Se debe evitar la exposición de direcciones IP privadas y datos de enrutamiento desde redes internas a Internet. • Cifrar los diagramas y documentos asociados que puedan tener enunciada direcciones IP privada y datos de enrutamiento a entidades externas.	1. Diagrama de red cifrado 2. Estándar de configuración con direcciones IP cifradas; y relacionando el mecanismo para ocultar la dirección.	1.2
	1.4	1.4	• Se debe aplicar herramientas de firewall personal o una funcionalidad semejante en todos los dispositivos móviles (de propiedad de la compañía y/o de los funcionarios) que tengan conexión a Internet cuando están fuera de la red (Ej.: Smartphone, laptops, Tabletas que usan los funcionarios), y que tengan habilitado el acceso al CDE. La funcionalidad habilitada no puede permitir administración o alteración por parte del funcionario o usuario del dispositivo. • Documentar la política para uso de dispositivos móviles	1. Documentar la política para uso de dispositivos móviles	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	1.5	1.5	• Las personas que administren el Firewall deben conocer su documentación y tener claramente el paso a paso definido para atender cualquier requerimiento de PCI DSS	1. Procedimiento para uso y administración del Firewall 2. Políticas para uso y administración del Firewall 3. Estándar de configuración del Firewall	1.1.1
2	2.1	2.1.a - 2.1.c	• Garantizar el cumplimiento de la política de contraseñas en TODOS los componentes del CDE y aquellos que sean parte del alcance de PCI. En la cual se debe cambiar las contraseñas que vienen por default, antes de instalar un sistema en la red. • Eliminar o Inhabilitar las cuentas prestablecidas como innecesarias, antes de colocar un sistema en la red.	1. Política de contraseñas	N/A
		2.1.1.a - 2.1.1.e	Implementar y soportar con la documentación y formatos de control de cambios correspondientes las siguientes tareas: • Cambio de las contraseñas de cifrado prestablecidas en la instalación • Cambio de las contraseñas siempre que una persona conozca esta y deja su empleo o cambia de cargo. • Las contraseñas / frases de contraseña prestablecidas en los puntos de acceso deben modificarse durante la instalación. • Las cadenas de comunidad SNMP prestablecidas para ser modificadas durante la instalación. • La documentación del proveedor debe contemplar procesos para la configuración inalámbrica de los dispositivos inalámbricos en la cual se admita un cifrado fuerte para la Autenticación a través de redes inalámbricas, la Transmisión a través de redes inalámbricas, que las cadenas de comunidad SNMP prestablecidas no se utilicen y que Las contraseñas / frases de contraseña prestablecidas en los puntos de acceso no se usen. • Garantizar que se hayan cambiado los valores prestablecidos del proveedor inalámbrico relacionado con la seguridad y dejar esto soportado con control de cambios.	1. Formato de control de cambios 2. Documentación del proveedor de insumos inalámbricos 3. Procedimientos para administración de dispositivos inalámbricos	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	2.2	2.2.a - 2.2.d	• Dejar documentados todos los estándares de configuración para todos los tipos de componentes del CDE que hacen parte del servicio core definido en el alcance PCI DSS de la organización y estos deben ser consistentes con los modelos de alta seguridad aceptados en la industria. • Los estándares de configuración del servicio se deben actualizar conforme a los resultados de identificación de nuevas vulnerabilidades, conforme a lo definido en el Requisito 6.1; dejando registro de control de cambios de esta actualización. • Los estándares de configuración del servicio se deben implementar cuando se configuran nuevos componentes y se verifican que están en su lugar previa a la instalación de un sistema en la red del CDE. Los estándares de configuración deben incluir las siguientes instrucciones para cualquier componente del sistema CDE: ◘ Cambio de todos los valores prestablecidos por el proveedor del componente y eliminación de cuentas prestablecidas que sean innecesarias ◘ Efectuar solo una función principal por servidor para evitar que las funciones que requieren otros niveles de seguridad coexistan en el mismo servidor ◘ Activar solo los servicios necesarios, protocolos, daemons, etc., según la necesidad para el función del sistema ◘ Implementación de características de seguridad agregadas para cualquier servicio requerido, protocolo o daemons que se crean inseguros. ◘ Configurar las opciones de seguridad del sistema previniendo su uso inapropiado ◘ Eliminación de toda funcionalidad innecesaria, como scripts, controladores, características, subsistemas, sistemas de archivos y servidores web no necesarios.	1. Estándares de configuración de todos los componentes del CDE que están involucrados directamente o indirectamente con datos de tarjeta habiente.	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
		2.2.1.a - 2.2.1.b	• Si se usan los métodos de virtualización, dejen una única función principal por componente del sistema virtual. • Garantizar que solo se implemente una función principal por servidor o sino usar técnicas de virtualización y garantizar que se deje una función principal por cada componente o dispositivo del sistema virtual. • Dejar documentado el estándar de configuración de cada componente creado detallando su respectiva función y niveles de seguridad establecidos según necesidad.	1. Estándar de configuración de cada componente o sistema virtual creado detallando su respectiva función y niveles de seguridad.	2.2
		2.2.2 - 2.2.3	• Garantizar que en el CDE solo estén habilitados los servicios, los daemons y los protocolos necesarios y que están soportados en un estándar de configuración documentado. • Identificar los servicios, daemons y protocolos; que pueden ser inseguros pero que requieren estar habilitados en el sistema del CDE, los cuales deben justificarse a nivel de negocio el porqué de su uso dentro del estándar de configuración y deben contar con un proceso de autorización y aprobación para su habilitación o manejo dentro del CDE (EJ.: TELNET). • Establecer, implementar y documentar los controles compensatorios que puedan darse a lugar para permitir el uso o implementación de los Servicios, daemons y protocolos inseguros • No usar SSL / TLS temprana, porque se considera inseguro para los servicios ofrecidos en la pasarela de pago acorde a Las especificaciones emitidos por el estándar PCI DSS en su nueva versión 3.2.1.	1. Estándar de configuración de cada Servicios, daemons y protocolos inseguros que este habilitado en el CDE con su respectiva justificación de negocio y controles compensatorios. 2. Registro de autorización y aprobación del uso de los Servicios, daemons y protocolos inseguros	2.2
		2.2.4	• Los administradores del servicio y/o administradores de seguridad deben tener conocimiento de la configuración común de las medidas de seguridad para los componentes del servicio. • En los estándares de configuración del sistema deben incluirse las configuraciones de parámetros de seguridad comunes. • Los componentes del servicio deben tener configurados adecuadamente los lineamientos de seguridad comunes, los cuales deben estar conforme a lo documentado en los estándares de configuración.	1. Documentar Las especificaciones de seguridad en los Estándar de Configuración	2.2

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
		2.2.5	• Eliminar de todos los componentes del sistema asociados al CDE toda funcionalidad innecesaria. • Documentar y habilitar los lineamientos de seguridad, garantizando una configuración segura de los componentes del servicio y que lo documentado sea lo implementado.	1. Documentar Las especificaciones de seguridad en los Estándar de Configuración	2.2.4
	2.3	2.3 incluye 2.3.a - 2.3.d	• En el proceso ingreso de cada sistema, al administrador se le debe invocar un procedimiento de cifrado fuerte antes de solicitar la contraseña del administrador. • Garantizar que los servicios y archivos de configuraciones en los sistemas como Telnet y otros comandos inseguros ingreso remoto no están disponibles para el acceso fuera de la consola. (En caso de requerirse se debe sustentar el motivo de negocio para este servicio y establecer los controles compensatorios para el uso del Telnet) • El administrador que inicie sesión en cada sistema debe tener el acceso a la interfaz de administración de la Web mediante una criptografía fuerte. • Tener soportada la documentación del proveedor referente a la criptografía fuerte de la tecnología en uso, la cual se debe implementar de conformidad con las buenas prácticas de la industria y/o las sugerencias de los proveedores. Esta documentación debe ponerse en conocimiento de los administradores del sistema y personal de seguridad. • No usar SSL / TLS temprana, porque se considera inseguro para los servicios ofrecidos en la pasarela de pago acorde a Las especificaciones emitidos por el estándar PCI DSS en su nueva versión 3.2.1.	1. Documentación del proveedor referente a la criptografía fuerte de la tecnología en uso 2. Procedimiento de ingreso seguro a los sistemas	N/A
	2.4	2.4.a - 2.4.b	• Realizar un inventario con todos los componentes del sistema CDE a nivel de hardware y software el detalle del objeto funcional de cada componente. • Mantener el inventario actualizado, cada vez que se adquiera o actualice un componente.	1. Matriz de Inventario de activos de todos los componentes del CDE.	5.1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	2.5	2.5	• Las políticas de seguridad y los procedimientos operativos deben estar actualizados con lo realmente implementado y debe ponerse en conocimiento de todas las partes interesadas.	1. Políticas y procedimientos operacionales del servicio del Core del Negocio	N/A
	2.6	2.6	• Este requisito se aplicaría si la pasarela de pago maneja su servicio Core en un entorno CDE con hosting compartido con tercero, a lo cual le aplicarían los procedimientos de prueba A.1.1 a A.1.4 detallados en el Apéndice A1. En caso contrario, se excluiría del alcance para las pasarelas de pagos.	1. Entregables del Apéndice A1 del Estándar PCI DSS	N/A
3	3.1	3.1.a - 3.1.c	• Limitar el resguardo de datos y llevar la retención en los tiempos y cantidad permitida por los requisitos regulatorios y del negocio. • Se debe relacionar todos sitios donde se resguardan los datos CHD relacionándolos en el procedimiento de retención y eliminación de datos. • Se debe definir y aplicar una política que permita trimestralmente de forma automática o manual la gestión para identificar y eliminar de forma segura, los datos CHD almacenados; labor que se debe efectuar en todas las ubicaciones de datos del titular de la tarjeta.	1. Procedimiento de retención y eliminación de datos de los datos CHD 2. Políticas y requisitos correspondientes para la retención y eliminación de datos de los datos CHD	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	3.2	3.2.a - 3.2.d	• Las pasarelas de pagos, ni ninguna otra entidad regida por PCI DSS puede almacenar los datos de autenticación confidenciales (SAD) posteriormente de un proceso de autorización transaccional, acción que ni siquiera se puede hacer de forma cifrada así no se tengan el PAN en el CDE, no obstante esta restricción se puede excluir si las marcas de pago lo autorizan lo que algunas veces es avalado solo para las empresas que emiten tarjetas prepagos o virtuales, de resto no suele ser aprobado; por lo que se debe aplicar procedimientos de borrado seguro para eliminar esta información del CDE después de la autorización. • Si se contempla el proceso de emisión de tarjetas (tarjetas prepagos o virtuales) por parte de la pasarela pago dentro de su portafolio de servicios o que se respalda a las empresas que brindan servicios de emisión y pueden resguardar datos SAD, toca revisar las políticas en las cuales se justifique a nivel de negocio de forma documentada el ¿por qué? se almacena datos de autenticación confidenciales; y estas políticas deben ser avaladas por las respectivas marca de pagos y conocida únicamente por las personas que manejan este servicio. • Acorde con la política los datos confidenciales de autenticación almacenados y la configuración del sistema se debe garantizar que los datos SAD están protegidos.	1. Política para los datos confidenciales de autenticación 2. Política y procedimientos de borrado seguro	3.1
		3.2.1	• Las fuentes de datos de cualquier pista de la banda magnética en la parte posterior de la tarjeta o datos equivalentes en un chip no se almacena después de la autorización: - Datos de transacciones entrantes - Todos los registros (por ejemplo, transacciones, historiales, depuración, error) - Archivos de historial - Archivos de seguimiento - Esquemas de bases de datos - Contenidos de bases de datos • Para minimizar riesgos de reproducción de tarjetas de pago ilegales con las que ejecuten transacciones fraudulentas, se debe almacenar solamente los datos que sean estrictamente necesarios para el negocio.	1. Evidencias de las configuraciones estipuladas en este sub-requisito	3.1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
		3.2.2	El código de verificación de las tarjetas brinda protección para las no presenciales ejecutada en cualquiera de los canales como Internet o MO/TO (correo o teléfono), por lo que el consumidor ni el plástico está presente, por tanto, este código está representado con tres o cuatro dígitos impresos en el anverso de la tarjeta pero dicho dato no debe almacenarse después de una autorización; porque cualquiera que tenga acceso a este dato y demás información asociada a la tarjeta podrá suplantar un transacción ilícita. De igual forma tampoco se debe almacenar después de una autorización los siguientes datos: - Información de ingreso de transacciones - Todos los registros transaccionales, históricos, entre otros - Registro del Historial - Registros de seguimiento - Esquemas de BD - Contenidos de BD	1. Evidencias de las configuraciones estipuladas en este sub-requisito	N/A
		3.2.3	Garantizar que en las fuentes de datos se incluya lo siguiente, pero que los PIN y los bloques PIN cifrados no se resguarden después de la autorización: - Información de ingreso de transacciones - Todos los registros transaccionales, históricos, entre otros - Registro del Historial - Registros de seguimiento - Esquemas de BD - Contenidos de BD	1. Evidencias de las configuraciones estipuladas en este sub-requisito	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	3.3	3.3.a - 3.3.c	• En las configuraciones de los sistemas se debe garantizar que el número de PAN completo solo se muestre para usuarios / roles con una necesidad comercial que esté aprobada y documentada para dicho fin; y aquí mismo que el Número de cuenta principal (PAN) esté enmascarado para todas las demás solicitudes. • Tener presente que en las pantallas, recibos de papel y cualquier otro elemento donde se pueda visualizar los datos CHD se permita únicamente ver los primeros seis / últimos cuatro dígitos del PAN justificándose documentalmente con una necesidad empresarial valida y aprobada.	1. Políticas y los procedimientos para enmascarar el numero PAN	N/A
	3.4	3.4.a - 3.4.e	• Se debe mostrar el numero PAN de forma ilegible u oculta en las tablas o archivos de los repositorios de datos; en los medios removibles (como copias de respaldo), en los registros de Logs incluidos los registros de la aplicación de pago; entre otros. • Si la pasarela de pagos lleva versiones en valores hash y truncadas del mismo PAN, deben implementar medidas complementarias para certificar que estas versiones no se puedan correlacionar permitiendo la reconstrucción del PAN original.	1. Políticas para la protección del PAN	N/A
		3.4.1.a - 3.4.1.c	• Si se usa el cifrado de disco se debe llevar un proceso de autenticación que valide el acceso lógico a los sistemas de archivos cifrados y que además se establezca desde un mecanismo separado al de autenticación del sistema operativo nativo. • Las llaves criptográficas se salvaguarden de forma segura (como en medios removibles protegidos, proceso que debe ser conocido por los encargados. • Los datos CHD almacenados en medios removibles se cifren en cualquier lugar donde se salvaguarden. • Si no se usa el cifrado de disco para cifrar medios extraíbles, los datos salvaguardados en estos medios deberán quedar ilegibles mediante algún otro método.	1. Evidencia del proceso de cifrados de los medios removibles y/o del método de hacer ilegibles los datos almacenados	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	3.5	3.5	• Limitar el acceso a las claves al mínimo de custodios posibles. • Las claves de cifrado de las llaves deben ser fuertes como las claves de cifrado de datos que protegen, además deben resguardarse de forma segura, separadas de las claves de cifrado de datos y en pocas ubicaciones y formas posibles.	1. Políticas y los procedimientos de administración de claves 2. Procesos para cifrar datos	N/A
		3.5.1	• Este requisito es aplicable para las pasarelas de pagos porque estas son proveedores de servicio de los comercios, por tanto, deben tener soportada la administración de claves y procesos de cifrado; considerando para esto la documentación de la arquitectura criptográfica, la cual debe ser claramente conocida por el personal responsable. • Incluir las especificaciones requeridas por este requisito entre los que se destaca los detalles de todos los algoritmos, protocolos y claves usados, incluyendo la complejidad de la clave y la fecha de expiración; la sustentación del uso de la clave para cada tecla; el inventario de los elementos utilizados para la gestión de claves como un HSM, SMS y entre otros.	1. Manual o procedimientos con la arquitectura criptográfica	N/A
		3.5.2	• Establecer las listas de acceso de usuarios para restringir el acceso a las claves al mínimo de custodios posibles.	1. Matriz de acceso de usuarios	N/A
		3.5.3	No es necesario conservar las claves públicas si se cumple los siguientes lineamientos: • Siempre que se usen claves de cifrado de llaves, validar las configuraciones del sistema y las ubicaciones de resguardo de estas considerando que las claves de cifrado de llaves son fuertes como las claves de cifrado de datos usadas y se resguardan de forma independiente a las claves de cifrado de datos.	1. Procedimiento de configuración y resguardo de las llaves criptográficas	3.5
		3.5.4	• Las ubicaciones de resguardo de claves y los procesos de resguardo para las claves están en el mínimo de sitios posibles.	1. Políticas y los procedimientos de administración de claves	3.5.3

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	3.6	3.6.a - 3.6.b incluye 3.6.1 a 3.6.8	• Este requisito es aplicable para las pasarelas de pagos porque estas son proveedores de servicio de los comercios, por tanto, debe tenerse un procedimiento de administración y generación de claves con los siguientes ítems: - Crear claves fuertes. - Repartir las claves de forma segura - Resguardar claves de forma segura. - Aplicar un período de cifrado para cada tipo de clave usada y que concreten un proceso para las modificaciones de clave al terminar el período de cifrado establecido. - Quitar o cambiar claves cuando se haya bajado la integridad de la clave, se presuma de un riesgo, inclusive cuando los funcionarios se retiran o cambian de puesto en la empresa. - Las claves que se registran después de quitarlas o cambiaras no se usan para operaciones de cifrado. - Para los *procesos manuales con claves de texto claro* se debe tener: Comprensión de la división de claves, de tal forma que los componentes de las claves queden controladas por 2 personas que únicamente conocen su propio componente de la clave. - Para los *procesos manuales con claves de texto claro* se debe tener: dualidad de controles de claves, al punto de 2 personas puedan ejecutar las operaciones de administración de claves y que no conozcan ni tengan permitiendo el acceso al material de las otra persona. - Procesos para impedir el reemplazo indebido de claves. - Procesos para requerir que los custodios de claves formalicen sus compromisos como custodios de claves. • Los aspectos anteriores se deben implementar, dejar evidencia y aplicar acordemente al procedimiento y deben ser conocidos en su manejo por el personal encargado.	1. El procedimiento de administración y generación de claves	3.5
	3.7	3.7	• Se debe dejar referenciado los puntos y documentos implementados en el requisito 3 • Se debe actualizar anual esta documentación antes de cada evaluación PCI • Poner en conocimiento en sensibilizaciones a las partes interesadas.	1. Políticas de seguridad para proteger los datos CHD. 2. Procedimientos operativos para proteger los datos CHD.	3; 4.3

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
4	4.1	4.1.a - 4.1.g	• Establecer que los estándares documentados y las configuraciones del sistema usen los protocolos de seguridad y criptografía fuerte para todas las ubicaciones. • Las políticas y los procedimientos documentados deben especificar que: - Solo aceptan claves o certificados de confianza. - El protocolo en uso únicamente permita versiones y configuraciones seguras. - Para la implementación del cifrado fuerte se establece según la metodología de cifrado en uso. • Las comunicaciones de entrada y salida a medida que ocurren con los datos CHD deben estar cifrados con un método de cifrado fuerte durante la transmisión. • Las claves y los certificados deben ser de confianza. • Para establecer la intensidad de cifrado adecuada se recomienda ver mejores prácticas de los proveedores. • Considerar que algunos protocolos como SSL, SSH 1.0 y TLS temprana tienen vulnerabilidades conocidas que pueden ser aprovechables; por lo que no se debe estos protocolos al considerarlos inseguros para los servicios ofrecidos en la pasarela de pago acorde a Las especificaciones emitidos por el estándar PCI DSS en su nueva versión 3.2.1; al 2019 se recomienda establecer TLS V1.2 en adelante validando que este último no haya sido vulnerado.• “HTTPS” debe mostrarse como protocolo de la URL .• Los datos CHD se deben solicitar únicamente si “HTTPS” sale como parte de la URL.• Las redes públicas abiertas incluyen: Internet; Tecnologías inalámbricas; incluso 802.11y Bluetooth; Tecnología celular como GSM, CDMA; o Servicio (GPRS)	1. Políticas de seguridad en la transmisión por redes públicas abiertas. 2. Procedimientos para la transmisión por redes públicas abiertas.	A2
		4.1.1	• Identificar todas las conexiones inalámbricas que transmitan datos CHD o que estén conectados al CDE. • Los estándares documentados de redes inalámbricas deben ser coherentes con las configuraciones del sistema las cuales deben contemplar: - El uso de buenas prácticas de la industria para realizar un cifrado fuerte en la autenticación y la transmisión. - No usar cifrado débil (Ej: WEP, SSL) como medida de seguridad para la autenticación o la transmisión.	1. Los estándares de configuración de las redes inalámbricas	2.2; 4.1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	4.2	4.2.a - 4.2.b	• En las políticas debe quedar especificado que los PAN no protegidos, no se pueden enviar a través de mecanismos tecnológicos en la mensajería para el usuario final	1. La política para el uso de mecanismos tecnológicos en la mensajería para el usuario final	N/A
	4.3	4.3	• Se debe dejar referenciado los puntos y documentos implementados en el requisito 3 y 4 • Se debe actualizar anual esta documentación antes de cada evaluación PCI • Poner en conocimiento en sensibilizaciones a las partes interesadas.	1. Políticas de seguridad para proteger los datos CHD. 2. Procedimientos operacionales para cifrar las transmisiones de los datos CHD.	3.7; 4
5	5.1	5.1	• Ningún componente del CDE con sistema operativo debe estar sin antivirus en caso, de alguna excepción se debe dejar soportada documentalmente con las aprobaciones correspondientes. • Se debe tener controles compensatorios para aquellos casos en los cuales se deje soportado la imposibilidad de instalación de un antivirus para alguno(s) de los componentes.	1. Matriz de Inventario de activos de todos los componentes del CDE; con las consideraciones correspondientes.	2.4
		5.1.1	• La documentación del proveedor de referencia de los antivirus debe garantizar las siguientes configuraciones, las cuales deben quedar habilitadas en la implementación de la herramienta: - Detección de todos los tipos de códigos maliciosos comunes. - Eliminación de todos los tipos de códigos maliciosos comunes - Protección del sistema contra todos los tipos de códigos maliciosos comunes. Entre los ejemplos de tipos de código maliciosos, considerando entre esto a los virus, troyanos, gusanos, spyware, adware y rootkits.	1. Documentación del proveedor de referencia de los antivirus implementados	N/A
		5.1.2	• Dejar evidencia y en conocimiento del personal encargado los procesos para la supervisión y evaluación de las amenazas por códigos maliciosos para los sistemas que no suelen verse afectados por malware.	1. Registros de revisión y evaluación de amenazas	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	5.2	5.2.a - 5.2.d	• Las configuraciones de los sistemas de antivirus deben: - Permitir actualizaciones automáticas. - Realizar análisis periódicos. • Todos los sistemas que componen el CDE, para cualquier tipo de sistemas operativos común pueden verse usualmente afectados por código malicioso, por lo que deben tener los siguientes parámetros establecidos: - Las configuraciones debidas y las actualizaciones oportunas en el sistema de antivirus. - Ejecute los análisis periódicos. • Las configuraciones de los sistemas antivirus, incluida la administración maestra del sistema y en los componentes del CDE, deben: - Tener habilitada la reproducción de los registros logs del sistema de antivirus. - Permitir conservar los registros logs conformemente con el Requisito 10.7 del estándar PCI DSS.	1. Políticas del sistema de antivirus 2. Procedimientos para la implementación y administración de los sistemas de antivirus	5.1; 10.7
	5.3	5.3.a - 5.3.c	• El sistema de antivirus funcione activamente y que los usuarios no puedan inhabilitar, ni cambiar el sistema de antivirus; desde las configuraciones de antivirus, incluida la administración maestra del sistema y en los componentes del CDE. • El personal responsable de la administración y custodia de los antivirus de conocer y aplicar apropiadamente las políticas y procesos para que los usuarios no puedan inhabilitar, ni cambiar el sistema de antivirus, contemplando las autorizaciones gerenciales para aquellos casos excepcionales los cuales deben ser justificados en el pro del negocio y aprobados por el Gerente.	1. Políticas del sistema de antivirus	5.2
	5.4	5.4	• Se debe dejar referenciado los puntos y documentos implementados en el requisito 5 • Se debe actualizar anual esta documentación antes de cada evaluación PCI • Poner en conocimiento en sensibilizaciones a las partes interesadas.	1. Políticas del sistema de antivirus 2. Procedimientos para la implementación y administración de los sistemas de antivirus	5

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
6	6.1	6.1.a - 6.1.b	• Contemplar las directrices para la gestión de riesgos definidos organizacionalmente en el manual de riesgos para la articulación de los riesgos exigidos en este requisito. • Capacitar al personal sobre la gestión de riesgos incluyendo a los dueños de los riesgos estructurandolos para que puedan aplicar la metodología de riesgos y tengan claramente apropiados sus riesgos. • Las clasificaciones de riesgo deben basarse en las buenas prácticas de la industria, así como en la consideración del impacto potencial. Para esto se puede aplicar los criterios para catalogar las vulnerabilidades pueden incluir la consideración del puntaje base de CVSS, y / o la clasificación del proveedor, y / o el tipo de sistemas afectados. Los métodos para valorar vulnerabilidades y fijar clasificaciones de riesgo difieren según el entorno de una organización y la estrategia de valoración de los riesgos. La clasificación de riesgos debe, como mínimo, identificar todas las vulnerabilidades consideradas de "alto riesgo" para el medio ambiente. Además de la clasificación de riesgos, las vulnerabilidades pueden considerarse "críticas" si representan una amenaza inminente para el medio ambiente, impactan sistemas críticos y / o resultarían en un compromiso potencial si no se abordan.	1. Manual de gestión de riesgos 2. Política de Riesgos 3. Matriz de riesgos 4. Mapa de riesgos 5. Política de gestión de vulnerabilidades técnicas 6. Procedimientos de gestión de vulnerabilidades técnicas	11.2.1
	6.2	6.2.a - 6.2.b	• Los parches de seguridad catalogados como importantes que sean suministrados por el proveedor se deben instalar máximo un mes después de su lanzamiento; los demás que no esté en un alto nivel de criticidad se podrán instalar en un período específico, al cual se sugiere no supere el plazo de tres meses. • Los parches de seguridad catalogados como importantes se deben identificar y catalogar dentro del proceso de clasificación de riesgos definido en el Requisito 6.1.	1. Políticas para la instalación de parche de seguridad 2. Procedimientos para la instalación de parche de seguridad	1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	6.3	6.3.a - 6.3.d	• Los procesos de desarrollo de software se deben estructurar con las normas y buenas prácticas de la industria; contemplando la seguridad de la información en todo el ciclo de vida. • Garantizar que los software o aplicaciones se desarrollen de conformidad con las PCI DSS. • Se debe poner en conocimiento los procesos de desarrollo a todo el personal que se involucra con los proyectos directamente, evaluar y exigirle que cumplan los procesos y directrices.	1. Política de Desarrollo de Software Seguro	N/A
		6.3.1	• Los procedimientos de desarrollo de software deben garantizar que la producción preliminar y las cuentas de aplicaciones estén personalizadas, las ID de usuarios y las claves se eliminen previamente a la puesta en producción o antes de disponerlas a los clientes. • El personal encargado de aplicar este proceso debe tener claro cómo se ejecuta y tener conocimiento de la documentación asociada.	1. Procedimientos de desarrollo de software	N/A
		6.3.2.a - 6.3.2.b	• El personal encargado de aplicar este proceso debe tener claro cómo se ejecuta y tener conocimiento de la documentación asociada. • Dotar con herramientas de verificación de código y en capacitación al personal que efectuara las revisiones a fin de maneje técnicas de codificación segura y pueda presentar resultados / informes al respecto. • Establecer Las especificaciones y manuales para el manejo de la herramientas y metodologías de verificación de códigos. • Documentar los resultados de las revisiones con los respectivos controles de cambios de las acciones de mejora o correctivas y dejando constancia de las aprobaciones por parte de la dirección de proyectos. • Cumplir las especificaciones del requisito y los procesos documentados para efectuar y articular las revisiones de los códigos. • Nota: Este requisito de revisión de códigos se aplica a todos los códigos personalizados (tanto internos como públicos) como parte del ciclo de vida de desarrollo del sistema. Las revisiones de los códigos pueden ser realizadas por terceros o por personal interno con conocimiento. Las aplicaciones web también están sujetas a controles adicionales a los efectos de tratar las amenazas continuas y vulnerabilidades después de la implementación, conforme al Requisito 6.6 de las PCI DSS.	1. Manual de uso de la herramienta de revisión de códigos. 2. Políticas para revisión de código. 3. Procedimiento de revisión por Pares en los proyectos/PMO. 4. Formatos de aplicación de cambios a los desarrollos. 5. Formatos de ejecución de revisiones a los códigos fuentes.	6.5

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	6.4	6.4 incluye 6.4.1 - 6.4.5	• Aplicar las políticas y procedimientos en los componentes de sistema conforme a lo documentado y que sea de conocimiento por las partes interesadas el cómo está la configuración y arquitectura de los componentes en los ambientes de desarrollo de Software. • La configuración de los controles de acceso deben garantizar la independencia entre los ambientes de desarrollo/prueba y el ambiente de producción. • Definir los roles y responsabilidades para el personal de desarrollo a fin de que tenga injerencia separada en los ambiente desarrollo/prueba Vs Producción; capacitar al personal con sus correspondientes asignaciones. • Garantizar que los cambios asociados con la documentación del control de cambios queden registrados documentalmente y soportados con su aprobación en el formato correspondiente considerando los siguientes parámetros: - Detalle de la incidencia - Firmas de aprobación - Evidencias de la ejecución de las pruebas de funcionalidad - Cundo se presneten cambios del código personalizado, se deben probar todas las actualizaciones aplicando el Requisito 6.5 de las PCI DSS antes de la puesta en producción. - Aplicar los procedimientos de desinstalación para cada muestra de cambio.	1. Políticas para la administración de los ambientes de desarrollo 2. Procedimientos para la administración de los ambientes de desarrollo 3. Procedimientos de control de cambios (Desarrollo; Infraestructura TI; organizacional) 4. Formatos para control de cambios 5. Matriz de roles y responsabilidades	6.5
		6.4.6	• Conservar los registros de cambios significativos de los componentes del sistema, los cuales deben ser comunicados a las partes interesadas y que a su vez los sistemas/redes afectados en el cambio se le aplicaron los requisitos correspondientes a la PCI DSS y que se registró la actualización en el formato correspondiente al control de cambios.	1. Registros de los formatos de control de cambios	N/A
	6.5	6.5.a - 6.5.c	• Los Requisitos 6.5.1 al 6.5.6 de la PCI DSS, aplican para todas las aplicaciones de pago (internas o externas). • Los Requisitos 6.5.7 al 6.5.10 de la PCI DSS, aplican para las aplicaciones web y las interfaces de las aplicaciones (internas o externas).	1. Políticas de desarrollo de software seguro 2. Procedimientos de desarrollo de software	N/A

		6.5.1 - 6.5.10	• El personal encargado de aplicar técnicas de codificación en las pruebas para las prevenciones y/o mitigaciones a estas vulnerabilidades debe tener claro cómo se ejecutan estas pruebas y tener conocimiento de la documentación asociada. Y se debe dejar evidencias de las verificaciones/pruebas realizadas de manera documentada y el plan de remediación de las brechas detectadas. • Las técnicas de codificación deben abordar las brechas definidas por PCI DSS y el TOP 10 de OWASP cumpliendo con lo siguiente: - Validar los datos de entrada para evidenciar que los datos de los usuarios no puedan cambiar el significado de los comandos, ni de las consultas. - Aplicar consultas establecidas en parámetros. - Validar los límites del buffer. - Truncamiento de cadenas de entrada. - Prevenga errores de cifrado. - Utilice claves y algoritmos criptográficos fuerte. - Las posibles comunicaciones inseguras o vulnerables cuenten con técnicas de codificación que autentiquen y cifren idóneamente todas las comunicaciones confidenciales. - Se mitigue el manejo inadecuado de errores con el uso de técnicas de codificación que no filtran datos por medio de mensajes de error (Ej.: mostrando pormenores genéricos del error, en lugar de mostrar pormenores específicos). - Controles contra vulnerabilidades de “alto riesgo” - Validar todos las medidas antes de la inclusión. - Usar técnicas de salida sensibles al contexto. - Autenticación exitosa de usuarios. - Desinfectar las entradas. - No exponer detalles de los objetos internos a los usuarios. - Restringir el acceso de las interfaces de usuarios a las funciones no autorizadas. - No permitir que las aplicaciones crean en las credenciales de autorización ni en los tokens que los navegadores ofrecen automáticamente. - Marcas de tokens de sesión como cookies “seguros”. - No exponer las ID de la sesión en la URL. - Establecer tiempos de espera adecuados considerando la seguridad y conformidad de usuario con la aplicación; generando la rotación de las ID de la sesión después de iniciar sesión exitosamente.	1. Políticas de desarrollo seguro de software 2. Procedimientos de pruebas del desarrollo de software 3. Procedimiento de la metodología OWASP 4. Informe de pruebas 5. Plan de remediación de las brechas detectadas	6.1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	6.6	6.6	• El personal encargado de aplicar este proceso debe tener claro cómo se ejecuta y tener conocimiento de la documentación asociada. • Esta evaluación no está relacionada con el análisis de vulnerabilidades requerido en el Requisito 11.2 de PCI DSS	1. Procedimiento de análisis de vulnerabilidades de códigos fuentes 2. Informe de análisis de vulnerabilidades de códigos fuentes 3. Plan de remediación de las brechas detectadas	6.5
	6.7	6.7	• Se debe dejar referenciado los puntos y documentos implementados en los requisitos 6 y 11. • Se debe actualizar anual esta documentación antes de cada evaluación PCI. • Poner en conocimiento en sensibilizaciones a las partes interesadas.	1. Políticas de desarrollo de software seguro 2. Procedimientos de desarrollo de software	6
7	7.1	7.1 incluye 7.1.1 - 7.1.4	• Las personas responsables de asignar los accesos, la administración de los servicios y la de recursos humanos deben ser conscientes y justificar la asignación de los accesos y los privilegios otorgados al personal; con el fin de que estos sean limitados los accesos privilegiados y se habiliten según la clasificación y labor de cada rol. • La Identificación de los privilegios requeridos de cada cargo para que puedan laborar en su rol. (Ej: usuario, administrador, etc.) • Se otorga accesos únicamente a los cargos que específicamente requieren el privilegio. • Limita al mínimo el número de privilegios otorgados para cumplir con las responsabilidades del trabajo. • Debe existir de forma documentada la aprobación para los privilegios asignados, por las personas competentes para dicha autorización, los cuales deben ser facilitados al rol autorizado, cumpliendo con las políticas de PCI DSS.	1. Política de control de acceso a los sistemas de información 2. Procedimiento control de acceso a los sistemas de información 3. Matriz de roles y perfiles de acceso los componentes del Sistema CDE. 4. Formato de autorización de acceso privilegiados. 5. Procedimiento control de acceso físico a las instalaciones	9

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	7.2	7.2 incluye 7.2.1 - 7.2.3	• Aplicar Las especificaciones definidos • Implementar técnicas en los sistemas y herramientas a nivel de acceso físico; para dar cumplimiento a este requisito.	1. Procedimiento control de acceso a los sistemas de información 2. Procedimiento control de acceso físico. 3. Formato de control de acceso físico 4. Formato de autorización de acceso a los sistemas de información	7.1
	7.3	7.3	• Se debe dejar referenciado los puntos y documentos implementados en los requisitos 7 • Se debe actualizar anual esta documentación antes de cada evaluación PCI • Poner en conocimiento en sensibilizaciones a las partes interesadas.	1. Política de control de acceso a los sistemas de información 2. Procedimiento control de acceso a los sistemas de información 3. Procedimiento control de acceso físico.	7; 9
8	8.1	8.1.a - 8.1.b; 8.1.1 - 8.1.2	• La personas que tengan acceso a los componentes de sistema del CDE deben tener ID exclusiva para ello y conocer de PCI, estar capacitados en esta norma y las políticas establecidas por las pasarelas de pagos para tal fin. • Se debe documentar la matriz de acceso correspondiente a los usuarios con ID exclusivas y accesos privilegiados; los cuales deben tener la correspondiente autorización para los accesos requeridos.	1. Política de control de acceso a los sistemas de información 2. Procedimiento control de acceso a los sistemas de información 3. Formato de capacitación y evaluación 4. Matriz de acceso de usuarios	7.3
		8.1.3 - 8.1.4	• Se debe cancelar los accesos a los usuarios retirado/cesantes el mismo día del retiro, y validar que efectivamente ya no tenga accesos tanto local como remoto. Así mismo, se debe pedir la devolución de los activos como los métodos de autenticación físicos, las tarjetas inteligentes, tokens, etc.; y desactivarlos los correspondientes. • Cada 90 días se debe verificar que las personas retiradas del último semestre no tengan acceso tanto local como remoto, y que sus ID se hayan inhabilitado o suprimido de las listas de acceso. Así mismo que las cuentas inactivas se eliminen o inhabiliten.	1. Formato de seguimiento y control de revisión de derechos de accesos de los usuarios a los sistemas de información	8.1.a; 8.1.b

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
		8.1.5 incluye 8.1.5.a - 8.1.5.b	• Realizar procesos de auditoria a los proveedores considerando la gestión de administración de cuentas que manejan los terceros sobre los componentes del CDE y los privilegios de acceso, respaldo o mantenimiento sobre los componentes a fin de verificar que las cuentas que usan de forma remota cumplen con lo siguiente: - Se desactivan cuando no se reporta uso. - Se activan cuando es requerido por el proveedor y se desactivan cuando están sin uso. - Dejar soportado los procesos de monitoreo de las cuentas de acceso remoto de los proveedores mientras se utilizan.	1. Formato de autorización de acceso a terceros 2. Formato seguimiento y control de revisión de derechos de accesos de los usuarios a los sistemas de información 3. Plan - Informe de Auditoria a proveedores	8.1.a; 8.1.b
		8.1.6 - 8.1.8	• En el caso de que hallan limitaciones con Las especificaciones de autenticación y configuraciones de las cuentas los componentes del sistema CDE se puede permitir que: - Las cuentas de usuarios se bloqueen cuando hay 6 intentos de ingreso fallidos; incluyendo esta limitación tanto para los procesos internos como en los clientes/usuarios por el hecho de que las pasarelas de pagos son proveedores de servicios de los comercios. - Los accesos de usuario al sistema CDE después de haberse bloqueado deben restablecerse por el administrador del sistema en primera instancia sino deben esperar mínimamente 30 minutos de bloqueo para que se les permita un nuevo intento de autenticación de acceso. - Los componentes de sistemas CDE al estar con inactividad deben bloquearse antes de cumplir los 15 minutos de inactividad. • Garantizar que los proveedores de servicios EJ.: Proveedores IaaS o Tecnológicos apliquen los límites que exige PCI para la gestión de contraseñas y autenticación en las cuentas de usuarios a los componentes de servicio que hagan parte del CDE.	1. Políticas de uso de las tecnologías críticas y activos 2. Política de control de acceso 3. Política de gestión y uso de contraseñas 4. Procedimientos de ingreso seguro a los sistemas y aplicaciones	8.1.a; 8.1.b
	8.2	8.2	• Se deben establecer y documentar coherentemente a su uso todos los tipos de método de autenticación implementados para cada tipo de componente del sistema.	1. Procedimientos ara los métodos de autenticación 2. Políticas de autenticación de usuarios	7; 8.1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
		8.2.1 incluye 8.2.1.a - 8.2.1.e	• Garantizar que el o los proveedores IaaS o tecnológicos parametricen la configuración de sus sistemas para que puedan proteger las contraseñas durante la transmisión y el resguardo mediante un cifrado fuerte; de tal manera que las contraseñas no sean visibles durante su transferencia y en los archivos almacenados. • En los archivos y componentes de sistema CDE las contraseñas deben ser ilegibles durante el resguardo y la transmisión respectiva; por el hecho de que las pasarelas de pagos son proveedores de servicios de los comercios.	1. Política para las Llaves criptográficas 2. Política de la gestión y uso de contraseñas	N/A
		8.2.2	• Sensibilizar a las personas acerca del proceso de autenticación para cambiar las credenciales de autenticación • Establecer el procedimiento de cómo se gestiona la recuperación de una credencial de autenticación considerando el canal de contacto para esta solicitud y la validación de los datos de identidad del usuario previo al cambio de la credencial de autenticación.	1. Procedimiento para la gestión de los medios removibles 2. Política para las Llaves criptográficas 3. Política de la gestión y uso de contraseñas	N/A
		8.2.3 - 8.2.6	• Se debe aplicar todos los procedimientos establecidos por PCI DSS en los sub-requisitos 8.2.3 a 8.2.6 considerando las especificaciones agregadas para los proveedores de servicios por el hecho de que las pasarelas de pagos son proveedores de servicios de los comercios; de igual forma se debe solicitar la parametrización de las contraseñas con las especificaciones requeridas en la Política de la gestión y uso de contraseñas definida por las pasarelas de pagos para que sean aplicables por parte de los proveedores que soportan el servicio Core. • Se debe sensibilizar a las partes interesadas acerca de las políticas definidas para gestión y uso de contraseñas.	1. Política de la gestión y uso de contraseñas 2. Formato de capacitación y evaluación	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	8.3	8.3.1 - 8.3.2	• La autenticación de múltiples factores contempla el uso de 2 de los 3 métodos de autenticación que sugiere el Requisito 8.2 respecto a estos métodos. Por lo que no se pueden repetir el mismo método (por ejemplo, el uso de 2 claves individuales) no permitiría considerar una autenticación de múltiples factores. • Tener presente que los colaboradores que se conectan de forma remota al CDE deben usar 2 de los 3 métodos de autenticación. • Las configuraciones en los componentes del CDE por medio de sistemas de acceso remoto debe requerir la autenticación de múltiples factores de autenticación en los siguientes casos: - Para los accesos por parte del personal, incluido el administrador. - Para los accesos de todos los terceros/proveedores (incluyendo al proveedor propietario de los servicios u fabricante de los componentes)	1. Política de control de acceso 2. Política de gestión y uso de contraseñas 3. Procedimientos de ingreso seguro a los sistemas y aplicaciones 4. Formato de capacitación y evaluación 5. Procedimientos ara los métodos de autenticación 6. Políticas de autenticación de usuarios	8.1; 8.2
	8.4	8.4.a - 8.4.c; 8.5.a - 8.5.c	• Validar que en las listas de ID de Usuarios de los componentes de sistema CDE se cumplan las políticas definidas para las ID. • En las políticas y procedimientos de autenticación debe quedar explícito y soportarse en su implementación la prohibición del uso de métodos de autenticación, ID y contraseña de tipo genérico, grupal y/o compartida para el acceso al Core del Negocio y demás elementos que puedan ser parte del CDE del alcance PCI. • Capacitar a todo el personal y terceros acerca de las políticas y procedimientos de autenticación definidas y acerca de que sus credenciales de autenticación no se compartan, incluso si se solicitan por los mismos compañeros de trabajo, un jefe o por un proveedor.	1. Política de gestión y uso de contraseñas 2. Procedimientos de ingreso seguro a los sistemas y aplicaciones 3. Procedimientos ara los métodos de autenticación 4. Políticas de autenticación de usuarios	8.1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	8.5	8.5.1	• Este requisito es aplicable para las pasarelas de pagos porque estas son proveedores de servicio de los comercios, por tanto, deben tener soportada políticas y procedimientos de autenticación ampliamente conocidos por el personal en las que se utilicen distintas credenciales de autenticación para tener acceso a cada cliente. Lo anterior se da para que las pasarelas de pago puedan acceder a su propio entorno de hosting, donde se alojan numerosos entornos de clientes y no es de responsabilidad de los proveedores de servicios de hosting compartido aplicar este requisito.	1. Política de gestión y uso de contraseñas 2. Procedimientos de ingreso seguro a los sistemas y aplicaciones 3. Procedimientos ara los métodos de autenticación 4. Políticas de autenticación de usuarios	8.4
	8.6	8.6.a - 8.6.c	• El personal de seguridad debe tener claro los mecanismos de autenticación, los cuales se asignan a una única cuenta y que no se comuniquen entre varias. • Evalué las especificaciones de configuración del sistema y los controles físicos, para confirmar que solo la cuenta autorizada usa esos mecanismos de autenticación para su acceso.	1. Procedimientos ara los métodos de autenticación 2. Políticas de autenticación de usuarios	8.1
	8.7	8.7.a - 8.7.d	• Las especificaciones de configuración de los servicios del CORE que incluye a las aplicaciones y las bases de datos deben: - Garantizar la previa autenticación de todos los usuarios antes de otorgar el acceso. - Confirmar la autorización para el acceso de los usuarios como los privilegios en términos de consultas y acciones como de mover, copiar, eliminar que le son permitidas en el servicio. - En la base de datos se realicen cambios en los registros mediante métodos programáticos los cuales debe hacerse por alguien con privilegios autorizados para ello. - El acceso directo o de consulta a la base de datos este permitido solamente a los administradores de la base de datos - DBA. • Las aplicaciones deben usar las ID de la aplicación que deben ser acopladas de forma particular y no estar asociadas como credenciales de usuario de red comunes o por defectos, ni otras credenciales de otros procesos.	1. Política de control de acceso 2. Procedimientos de ingreso seguro a los sistemas y aplicaciones	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	8.8	8.8	• Se debe dejar referenciado los puntos y documentos implementados en los requisitos 8 • Se debe actualizar anual esta documentación antes de cada evaluación PCI • Poner en conocimiento en sensibilizaciones a las partes interesadas.	1. Política de control de acceso 2. Política de gestión y uso de contraseñas 3. Procedimientos de ingreso seguro a los sistemas y aplicaciones 4. Procedimientos ara los métodos de autenticación 5. Políticas de autenticación de usuarios	7; 8
9	9.1	9.1	• Considerar que las “Áreas confidenciales” aplican para los centros de datos, cuarto de servidores o cualquier otra instalación que alojen los componentes físicos del CDE o en que se resguarden documentos que contengan datos CHD.	1. Política de control de acceso físico a las instalaciones 2. Procedimiento control de acceso físico a las instalaciones.	7
		9.1.1 - 9.1.3	• Los circuitos cerrados de Televisión (CCTV) y/o los mecanismos de control de acceso físico deben: - Ubicarse en puntos estratégicos que supervisen las entradas y salidas de las áreas confidenciales. - Estar en una posición segura que impida su alteración, vulneración física o desactivación. - Los videos de las cámaras y registros de los controles de acceso deben conservarse, al menos, durante tres meses. • Para las conexiones de red disponibles en áreas públicas en la que se permite a acceso de personas no autorizadas como los visitantes se debe restringir el acceso a la red en los casos que sean requeridos o en su defecto para tener la conexión permanente se debe acompañar al visitante en todo momento en estas áreas mientras las conexiones de red estén activas.	1. Políticas para áreas seguras	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	9.2	9.2.a - 9.2.c	• Se consideran "Colaboradores nuevos" aquellos a quienes aún no se les ha entregado formalmente el carnet con los respectivos accesos físicos; y a ellos se le debe otorgar acceso diariamente a las instalaciones por lo tanto deben portar un carnet que los distinga como colaboradores nuevos y no como visitantes. • Los carnet de colaboradores desvinculados y de visitantes deben tener caducidad de tal forma que si el visitante o el empleado a desvincular se llevan el carnet fuera de las instalaciones no se le permita un nuevo acceso a las instalaciones después de haberse retirado de esta.	1. Política de control de acceso físico a las instalaciones 2. Procedimiento control de acceso físico a las instalaciones.	9.1
	9.3	9.3.a - 9.3.c	• Mantener actualizada las listas de acceso y bitácoras para que no hayan dentro de este personal retirado de la organización con permisos habilitados para el acceso a las áreas confidenciales.	1. Formato - Registro Bitácora de acceso a las áreas confidenciales 2. Matriz de listado de acceso a las áreas confidenciales	N/A
	9.4	9.4 incluye 9.4.1 - 9.4.4	• Capacitar al personal administrativo que apoya la gestión de recepción acerca del proceso de identificación y autorización de visitantes a las instalaciones. • Se debe tener en cuenta para el manejo de los carnet se debe aplicar el requisito 9.2 aplicando los protocolos exigidos entre carnet de visitantes y de colaboradores antiguos y nuevos. • Los registros de visitantes como Logs de acceso físico a las instalaciones y áreas confidenciales deben conservarse físicamente durante un periodo mínimo de tres meses y componerse por los siguientes datos: - Nombre del visitante - Tipo y Numero de Identificación - Empresa representada - Empleado que autoriza el acceso físico - Motivo de la Visita - Fecha y Hora de ingreso y salida • Solicitar al visitante un documento de identificación propio con foto, basado en este documento diligenciar el formato de registro de acceso de visitantes y conservar este documento como garantía para la devolución del carnet de visitante.	1. Formato de registro de acceso de visitantes a las instalaciones 2. Política de control de acceso físico a las instalaciones 3. Procedimiento control de acceso físico a las instalaciones.	9.2

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	9.5	9.5 incluye 9.5.1	• El lugar de resguardo (Proveedor de Almacenamiento) se debe auditar o supervisar en su proceso de resguardo de cintas por lo menos anualmente para validar que el resguardo de medios de copia de respaldo sea seguro.	1. Procedimiento para la gestión de los medios removibles 2. Política de dispositivos móviles 3. Política de copias de respaldo 4. Procedimiento de copias de respaldo	N/A
	9.6	9.6 incluye 9.6.1 - 9.6.3	• Se debe aplicar esta clasificación y etiquetado conforme a las políticas definidas especialmente a todos los componentes del sistema de CDE. • Garantizar que el personal efectué y conozca el proceso de transferencia de información en la cual se evidencie los registros de todos los medios transportados por fuera de la empresa, los cuales deben llevar registros de si se transportan por mensajería segura u otro método de transporte que se pueda rastrear. • Se debe llevar registros de monitoreo externos de todos los medios y dejarse soportado documentalmente los detalles de seguimiento; en los cuales se evidencie la correcta autorización de la gerencia cuando sea necesario enviar los medios desde una instalación segura (incluso, cuando los medios se entregan a personas internas para que hagan el mandado). • Sensibilizar al personal encargado para que conozca sus procesos y políticas relacionados.	1. Manual de Clasificación, Etiquetado, Manejo y Disposición de la información 2. Políticas de transferencia de información 3. Procedimientos de transferencia de información. (Medios físicos en tránsito) 4. Formato de transferencia de medios físicos en tránsito. (EJ. entrega de cintas de respaldos)	9.5
	9.7	9.7 incluye 9.7.1	• Aplicar las consideraciones de clasificación y evaluación para riesgos dentro del inventario de activos • Llevar registro con el inventario de las cintas magnéticas usadas en las copias de respaldo - Backup	1. Procedimiento para el plan de mantenimiento de activos del Core del Negocio 2. Procedimiento de inventario de activos 3. Matriz de Inventario de activos de todos los componentes del CDE - Core del Negocio 4. Registro con el inventario de las cintas magnéticas usadas en las copias de respaldo	2.4; 9.6

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	9.8	9.8 incluye 9.8.1 - 9.8.2	Sí en la pasarela de pagos se conservan medios con registros de transacciones o con información de tarjetahabiente se debe: • Establecer las herramientas requeridas para la disposición y/o destrucción de medios • Ratificar que no hayan datos de tarjetas habientes o que hagan parte del Core del Negocio sin destruir y que estén protocolizados para tal fin. • Dejar formalizado en registros los datos que se pretendieron destruir con la respectiva autorización y aprobación para hacer dicho proceso.	1. Procedimiento para la Destrucción, Disposición o reutilización de Medios y Equipos 2. Formato de disposición de activos 3. Formato de Borrado seguro	9.6
	9.9	9.9 incluye 9.9.1 - 9.9.3	Este requisito queda completamente excluido del alcance de su implementación para una pasarela de pago; ya que está estructurado para uso de tarjetas de pago físicas en dispositivos terminales con interacción física del plástico de la tarjeta, lo cual no haría parte del servicio Core de una pasarela de pago.	N/A	N/A
	9.10	9.10	• Se debe dejar referenciado los puntos y documentos implementados en los requisitos 9 • Se debe actualizar anual esta documentación antes de cada evaluación PCI • Poner en conocimiento en sensibilizaciones a las partes interesadas.	1. Políticas para áreas seguras 2. Política y Procedimiento de control de acceso físico a las instalaciones 3. Procedimiento para la gestión de los medios removibles 4. Política de dispositivos móviles 5. Política y procedimiento de copias de respaldo 6. Políticas y Procedimiento de transferencia de información (Medios físicos en tránsito) 7. Procedimiento para la Destrucción, Disposición o reutilización de Medios y Equipos 8. Procedimiento para el plan de mantenimiento de activos del Core del Negocio 9. Procedimiento de inventario de activos 10. Política de manejo e inventario de activos	7; 9

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
10	10.1	10.1	• Los Logs de auditoría deben estar habilitados para los componentes del servicio. CORE. • El acceso a los componentes del servicio CORE debe estar asociado a usuarios determinados.	1. Manual de Logs de Auditoria	2
	10.2	10.2 incluye 10.2.1 - 10.2.7	• Realizar prueba para comprobar si se cumple cada una las implementaciones exigidas	1. Manual de Logs de Auditoria	10.1
	10.3	10.3 incluye 10.3.1 - 10.3.6	• Esta parametrización se debe aplicar a cada componente que dé cumplimiento al requisito 10.2 • Se debe considerar para dar cumplimiento a este requisito la incorporación de los siguientes datos: - Componente donde se presentó la actividad - Usuario que hizo la actividad - Tipo de evento efectuado (Cambio, Consulta, Descarga, Eliminación, Re-inicialización, Creación, Detección o pausa, ingreso fallidos, Mejora de privilegios, Adicciones, etc.) - Detalle de los datos origen EJ.: Dato inicial o previo al cambio o eliminación, origen de la acción, búsqueda realizada; etc. - Detalle de la actividad resultante Ej.: Dato alterado, dato del cambio efectuado o dato de la consulta realizada - IP Origen o elemento donde se originó la actividad - Fecha y hora de la actividad - Resultado de la actividad : Exitosa o Fallida	1. Manual de Logs de Auditoria 2. Registros de Logs de Auditoria	10.2
	10.4	10.4 incluye 10.4.1 - 10.4.3	• La hora parametrizada en los componente y registrada en los Logs de auditoria debe ser coherente con la hora local de zona que en Colombia la controla el Instituto Nacional de Metrología o en su defecto con el que designe la Superintendencia de Industria y Comercio. • Dejar establecido en los estándares de configuración y los procesos que la técnica de sincronización se aplique y sostenga actualizada, según los Requisitos 6.1 y 6.2 de las PCI DSS. • Considerar el uso de tecnologías o protocolos para sincronización de la hora local en los sistemas como es el NTP (protocolo de tiempo de red). • El proceso para obtener, repartir y almacenar el horario exacto en la organización debe considerar los siguientes ítems, los cuales se parametrizan en la configuración del sistema de los	1. Procedimiento de sincronización de relojes de los sistemas	6.1; 6.2

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
			componentes del sistema CDE: - Únicamente los servidores de horario central que están para recibir señales de tiempo de origen externo junto con las señales de tiempo de origen externo se deben conformar sobre la hora atómica internacional o UTC. - En el caso de tener más de servidor de horario designado, estos se deben empatar sistemáticamente para mantener la hora exacta. - Los sistemas aceptan el dato horario local únicamente de los servidores de horario central establecidos.		
	10.5	10.5 incluye 10.5.1 - 10.5.5	• Los Logs de auditoria se debe conservar 3 meses en los servidores para consulta inmediata y 1 año en cinta (la Circular 042 de la Superintendencia Financiera de Colombia exige 2 años de conservación en cinta) • Tener en cuenta en la configuración del sistema, los archivos supervisados y los registros de las labores de supervisión se deben sustentar o aplicar con el uso de herramientas de Supervisión de Integridad de Archivos (FIM) o de herramientas que permitan las detección de cambios en los registros.	1. Registros de ejecución de las copias de seguridad de los Logs de auditorias 2. Registros de supervisión de integridad de archivos o de detección de cambios 3. Registro de centralización de los Logs desagregado por componente.	10.2; 10.3
	10.6	10.6.1 - 10.6.3	• Se pueden implementar herramientas de recolección, análisis y alerta de registros; para ello se debe considerar la implementación de la herramienta SIEM como centralizador de Logs. • Tener en cuenta dentro de la valoración de riesgos de la organización las revisiones que se realicen con respecto a las políticas y la estrategia de gestión de riesgos de la organización, las cuales los dueños de los riesgos deben conocer a claridad según sus riesgos. • Capacitar a las partes involucradas en los procesos y políticas establecidas; así como en la toma de conciencia acerca de los resultados obtenidos debido a esta implementaciones de este requisito.	1. Políticas de centralización, retención y monitoreo de Logs de Auditoria 2. Manual de Logs de Auditoria 3. Procedimiento de gestión de debilidades, eventos e incidentes	10.2; 10.3
	10.7	10.7.a - 10.7.c	• Se deben probar las copias de respaldo de los Logs y que efectivamente la consulta en línea pueda ofrecer los registros filtrados por fecha diaria y hora durante los últimos tres meses.	1. Políticas de centralización, retención y monitoreo de Logs de Auditoria 2. Manual de Logs de Auditoria	10.5

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	10.8	10.8.a - 10.8.b	• Revisar las actividades de detección y de alerta para confirmar que los procesos se aplican para todas las medidas de seguridad críticas, y que la falla de una de estas medidas da lugar a la generación de una alerta. • Este proceso debe ser conocido por el rol encargado de la administración de estos componentes. • Los informes de fallas de las medidas de seguridad críticas para los servicios del CORE; no solo deben aplicarse en los controles enunciados por PCI DSS en estos requisitos si no en todos los implementados por la organización incluyendo aquellos que puedan considerarse como complementarios.	1. Políticas de monitoreo y alertas de componentes2. Procedimiento de monitoreo y alertas de componentes	N/A
		10.8.1	• Este requisito es aplicable para las pasarelas de pagos porque estas son proveedores de servicio de los comercios, por tanto, debe tenerse documentados los registros con las fallas del control de seguridad de conformidad a los lineamientos establecidos en este requisito.	1. Políticas de gestión de debilidades, eventos e incidentes. 2. Procedimiento de gestión de debilidades, eventos e incidentes. 3. Informes de fallas de las medidas de seguridad críticas	12.10
	10.9	10.9	• Se debe dejar referenciado los puntos y documentos implementados en los requisitos 10 • Se debe actualizar anual esta documentación antes de cada evaluación PCI • Poner en conocimiento en sensibilizaciones a las partes interesadas.	1. Políticas de centralización, retención y monitoreo de Logs de Auditoria 2. Manual de Logs de Auditoria 3. Políticas de gestión de debilidades, eventos e incidentes. 4. Procedimiento de gestión de debilidades, eventos e incidentes 5. Procedimiento de sincronización de relojes de los sistemas 6. Políticas de monitoreo y alertas de componentes 7. Procedimiento de monitoreo y alertas de componentes	10

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
11	11.1	11.1.a - 11.1.d; 11.1.1 - 11.1.2	• Los métodos aplicados en este proceso incluyen, entre otros, análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC (control de acceso a la red) o IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) inalámbricos. Si se usa proceso automatizado la configuración debe generar alertas para notificar al personal. • La metodología establecida para detección e identificación de cualquier conexión inalámbrica no autorizada, debe al menos cumplir lo siguiente: - Tarjetas WLAN implantadas en los componentes del servicio CORE - Dispositivos portátiles o móviles conectados a los componentes del servicio CORE para crear conexiones inalámbricas como una USB. - Elementos inalámbricos habilitados a un puerto o a un equipo de red. • Se debe evitar tener conexiones inalámbricas para el proceso del Core del Negocio y transacciones con datos de tarjeta habiente, pero si en el negocio se requiere este proceso con conexiones inalámbricas se debe dejar soportado por la Gerencia General dicha sustentación. •En la validación de la seguridad del plan de respuesta a incidentes de la organización (Requisito 12.10) se debe verificar que está establecido documentalmente y probado las acciones de respuesta en caso de detección de una conexión inalámbrica no autorizada. • El personal encargado de la inspección de los análisis inalámbricos recientes y las respuestas correspondientes deben conocer el esquema inalámbrico y aplicar medidas cuando se encuentren conexiones inalámbricas no autorizados.	1. Políticas para acceso inalámbricos (Política de dispositivos móviles) 2. Procedimiento de análisis a los servicios inalámbricos 3. Procedimiento de gestión de debilidades, eventos e incidentes.	12.10

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	11.2	11.2 incluye 11.2.1 - 11.2.3	• Se pueden concertar diferentes informes de análisis para el proceso de análisis trimestral a fin de sustentar la labor de análisis sobre todos los sistemas y que se trataron todas las vulnerabilidades. • Los análisis externos se efectúan para los componentes con acceso a Internet o se asocian a una IP Publica; los análisis internos se aplican a componente de red privada. • Se debe considerar documentación adicional que certifique que las vulnerabilidades no remediadas están en proceso de tratamiento bajo un plan específico de tratamiento. • Para la primera certificación en PCI DSS, no es necesario tener análisis 4 para el último año con corte trimestral aprobados si el evaluador de la QSA confirma que: 1) los resultados del último análisis fueron positivos, 2) la empresa ha documentado las políticas y los procedimientos que definen la realización de análisis trimestrales y 3) las vulnerabilidades detectadas en los resultados del análisis se han remediado y que deben corroborarse en su último retest a la fecha de corte. En los años posteriores a la evaluación inicial o de acreditación de las PCI DSS, se debe tener los 4 análisis trimestrales ejecutados y aprobados. • Tener los informes de análisis de vulnerabilidades trimestrales internos y externos en los últimos 12 meses y por cada control de cambios en la red; los cuales se retestean los análisis hasta que se corrijan todas las brechas “de alto riesgo”, conforme al Requisito 6.1 de PCI DSS; y no se registren brechas con puntuaciones CSVV de 4.0 o superior en el análisis externos. • El análisis interno puede ser realizado por personal interno o externo calificado pero debe ser ajeno a la gestión de los procesos que se manejan en el CDE y los servicios CORE de la empresa (no es necesario que sea un QSA o ASV si lo hace un externo, en caso contrario si es necesario). • Los análisis externos deben cumplir con la Guía del programa de ASV (proveedor aprobado de escaneo) para obtener un análisis aprobado (EJ: que no haya brechas con una puntuación CVSS de 4.0 o superior y que no haya fallas automáticas); y debe ser efectuado por una persona externa sea un QSA o ASV; que esté certificado por el PCI SSC.	1. Política de gestión de vulnerabilidades técnicas 2. Manual de gestión de vulnerabilidades técnicas 3. Registro de Informes de vulnerabilidades 4. Plan de remediación de vulnerabilidades técnicas	6.1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	11.3	11.3 incluye 11.3.1 - 11.3.3	• Están basada en los enfoques de pruebas de intrusión aceptados por la industria como la NIST SP800- 115. • Contenga la totalidad del perímetro del CDE y de los sistemas críticos. • Incluya pruebas del entorno interno y externo de la red. • Aplique pruebas para verificar cualquier segmentación y medidass de reducción del alcance. • Establezca las pruebas de intrusión de la capa de la aplicación para que contemple como mínimo las vulnerabilidades enunciadas en el Requisito 6.5. • Defina las pruebas de intrusión de la capa de la red para que contenga los componentes que permiten las funciones de red y los sistemas operativos. • Aplique la exploración y valoración de las amenazas y vulnerabilidades presentadas el último año. • Defina la conservación de los resultados de las pruebas de intrusión y de las tareas de remediación. • Si la prueba la realiza por una persona interna debe ser calificado y capacitado como QSA o ASV; pero si la realiza un externo no es necesario dicho rango .	1. Política de gestión de vulnerabilidades técnicas 2. Manual de gestión de vulnerabilidades técnicas 3. Registros de Informes de pruebas de penetración 4. Plan de remediación de vulnerabilidades técnicas	6.5
		11.3.4	• Validar si efectivamente se aplicaron controles de segmentación en la red, con el fin de establecerlos en la metodología y cumpliendo con el requisito aplicable (11.3..4.1) ya que este sub-requisito es aplicable para las pasarelas de pagos porque estas son proveedores de servicio de los comercios, por tanto, se debe ejecutar las pruebas de intrusión para cada seis meses garantizando que los procedimientos estén determinados para evidenciar todos los métodos de segmentación. • La prueba de intrusión deben ejecutarse semestralmente para los controles de segmentación que se tienen establecidos y después de cualquier cambio en los controles o métodos de segmentación. • La prueba de intrusión debe considerar todos los controles o métodos de segmentación implementados. • La prueba de intrusión debe velar porque los métodos de segmentación sean operativos y eficaces, y que cubren independientemente todos los sistemas fuera de alcance de los sistemas dentro del CDE. • Si la prueba la realiza por un recurso interno debe ser calificado	1. Política de gestión de vulnerabilidades técnicas 2. Manual de gestión de vulnerabilidades técnicas 3. Registros de Informes de pruebas de penetración 4. Plan de remediación de vulnerabilidades técnicas	6.1; 6.5; 11.3

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
			y capacitado como QSA o ASV; pero si la realiza un externo no es necesario dicho rango.		
	11.4	11.4.a	• Monitorear todo el tráfico de red: - En el perímetro del CDE. - En los puntos críticos del CDE. • El personal encargado de la administración de los IDS e IPS debe conocer sus procesos y mantenerse informado de las alertas generadas. • La documentación del proveedor tecnológicos o IAAS debe contemplar las técnicas de intrusión-detección y de intrusión-prevención se parametricen, registren y conserven según las indicaciones del proveedor para obtener una protección óptima.	1. Políticas de monitoreo y alertas de componentes 2. Procedimiento de monitoreo y alertas de componentes	10.8
	11.5	11.5.a - 11.5.b; 11.5.1	• Se debe dejar soportado que las alertas se investiguen y resuelven.	1. Políticas de monitoreo y alertas de componentes 2. Procedimiento de monitoreo y alertas de componentes 3. Procedimiento de gestión de debilidades, eventos e incidentes.	11.4
	11.6	11.6	• Se debe dejar referenciado los puntos y documentos implementados en los requisitos 11 • Se debe actualizar anual esta documentación antes de cada evaluación PCI • Poner en conocimiento en sensibilizaciones a las partes interesadas.	1. Políticas de monitoreo y alertas de componentes 2. Procedimiento de monitoreo y alertas de componentes 3. Procedimiento de gestión de debilidades, eventos e incidentes. 4. Política de gestión de vulnerabilidades técnicas 5. Manual de gestión de vulnerabilidades técnicas 6. Políticas para acceso inalámbricos (Política de dispositivos móviles) 7. Procedimiento de análisis a los servicios inalámbricos	11

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
12	12.1	12.1 incluye 12.1.1	• Se debe dar a conocer la política a todas las partes interesadas incluyendo el personal de la organización, quiénes deben ser conscientes de la confidencialidad de los datos y de sus responsabilidades para asegurarlos. • Realizar los cambios a la política de seguridad de la información anualmente cada vez que se requiera teniendo en cuenta que las amenazas y mediadas de protección avanzas continuamente y se debe establecer una política consistente que se alinee con las estrategias de negocio y las medidas de control para las actuales amenazas. • Se debe aprobar por la Gerencia general.	1. Política de seguridad de la información	N/A
	12.2	12.2.a - 12.2.b	• La gestión de riesgos considera etapas de identificación, valoración, tratamiento y monitoreo de los riesgos; las cuales se deben hacer consecutivamente y de forma estructural para ello se recomienda seguir los lineamientos del marco de referencia de la ISO 31000 a fin de aplicar asertivamente la metodología en la gestión de riesgos. • Identificación de los activos críticos, amenazas y vulnerabilidades. • Resultados en un gestión formal y documentada.	1. Manual de gestión de riesgos con metodología establecida 2. Matriz de riesgos 3. Mapa de riesgos 4. Planes de tratamiento de riesgos	6.1
	12.3	12.3 incluye 12.3.1 - 12.3.10	• Las tecnologías críticas dan cubrimiento a las tecnologías de tipo inalámbrico, de acceso remoto, las computadoras, las tabletas, los medios extraíbles, el uso del correo electrónico y de Internet, entre otros. • En la configuración de las tecnologías para acceso remoto debe permitir que las sesiones de acceso remoto se desctiven automáticamente después de un tiempo de inactividad. • Si se tiene un requerimiento comercial avalado, las políticas de uso de las tecnologías criticas deben considerar la protección de los datos personales siguiendo la regulación vigente y los requisitos asociados en el estándar PCI DSS.	1. Políticas de uso de las tecnologías críticas	8.1

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	12.4	12.4.a - 12.4.b; 12.4.1	• Estas políticas, estatutos y responsabilidades deben ser aprobadas por la Gerencia General, en la cual busque mantener el cumplimiento de la PCI DSS de la entidad. • La responsabilidad de la protección de los datos CHD y el programa de cumplimiento de la PCI DSS debe ser asignada y aprobada por la gerencia general o la junta directiva debido a que las pasarelas de pagos son proveedores de servicio de los comercios	1. Programa de cumplimiento de la PCI DSS aprobado 2. Formatos de capacitación y evaluación de las políticas de seguridad de la información - PCI DSS 3. Presentación de la capacitación	12.2
	12.5	12.5 incluye 12.5.1 - 12.5.5	Tener formalmente asignado la responsabilidad de: • Definir, documentar y comunicar las políticas y los procedimientos de seguridad. • Monitorear y analizar las alertas de seguridad y de distribuir la información al personal de las unidades comerciales y de seguridad • Establecer, documentar y distribuir los procedimientos de escalamiento y de respuesta ante incidentes de seguridad, para garantizar una respuesta oportuna y efectiva cualquier situación. • Administrar las cuentas de usuario y los procesos de autenticación. • Monitorear y controlar todo acceso a los datos.	1. Roles y responsabilidades en seguridad de la información	12.1
	12.6	12.6.a - 12.6.b; 12.6.1 - 12.6.2	• Contemplar los programas de inducción y reinducción anual que consideren temas de seguridad, los cuales al final de cada sesión deben evaluar en su interiorización por parte de los asistentes. • Abarcar espacios de sensibilizaciones para refuerzos • Aplicar varios métodos para la concienciación (por ejemplo, carteles, cartas, notas, capacitación en línea, reuniones y promociones). • Preparar a los colaboradores en los aspectos de seguridad de la organización como conocimiento y cumplimiento en políticas, buenas prácticas, ejecución de procedimientos, sus roles y responsabilidades frente a la seguridad; solicitándoles anualmente la firma de compromiso con el cumplimiento de Las especificaciones establecidos para la seguridad.	1. Matriz de Programa de capacitaciones 2. Formatos de capacitación y evaluación de las políticas de seguridad de la información - PCI DSS 3. Presentación de la capacitación	12.1; 12.4

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	12.7	12.7	• Confirmar dentro de la valoración de antecedentes los soportes entregados como constancias de estudios y experiencia laboral, los registros de antecedentes penales, reportes en centrales de riesgo financiero y referencias personales-laborales-familiares. • Considerar como alternativa complementaria la ejecución de pruebas de polígrafos o test especializados para validar la fiabilidad de la información suministrada por los candidatos preseleccionados para vinculación contractual.	1. Procedimiento de selección y contratación de personal	N/A
	12.8	12.8 incluye 12.8.1 - 12.8.5	• Se deben pactar acuerdos para la confidencialidad y transferencia segura de los datos CHD que va gestionar o custodiar el proveedor. • Se debe realizar una auditoría adecuada previa a la contratación formal con cualquier proveedor de servicios; considerando dentro del acuerdo contractual la ejecución de auditoria de seguimiento ciclo de al menos 1 vez al año para la validación de la conformidad en los requisitos de PCI DSS y la seguridad sobre el servicio suministrado que hace parte del alcance PCI DSS. • Distinguir claramente los requisitos de PCI DSS que administra cada proveedor que interactúa con el Core del Negocio en el que se contemple datos CHD o tenga acceso al CDE, delimitando los requisitos que le son aplicables a las pasarela de pagos; teniendo en cuenta el alcance al nivel de cumplimiento requerido para PCI DSS.	1. Política para gestión de los proveedores 2. Lista de proveedores 3. Acuerdos de confidencialidad y de transferencia con los proveedores 4. Matriz con los Requisitos de seguridad y de PCI DSS aplicables a cada proveedor 5. Soportes de Auditoria preliminares a la contratación y de seguimiento a los proveedores	N/A
	12.9	12.9	• Este requisito es aplicable para las pasarelas de pagos porque estas son proveedores de servicio de los comercios, por tanto, debe tenerse acordado, documentado y firmado con los clientes los acuerdos pertinentes convenidos entre las partes para asumir la responsabilidad frente a la seguridad de los datos CHD que se gestionan en el servicio Core de la pasarela de pago.	1. Acuerdo contractual con cada cliente con las responsabilidades frente a la seguridad de los datos CHD	12.8

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	12.10	12.10 incluye 12.10.1 - 12.10.6	• El plan de respuesta ante incidentes debe incluir todos los aspectos requerido por PCI DSS que serían: Roles, responsabilidades y estrategias de comunicación incluyendo la notificación a las marcas de pago en caso de riesgo; Procedimientos específicos de respuesta a incidentes, de recuperación y continuidad de negocio, de copia de seguridad de datos; Análisis de requisitos legales para el informe de riesgos conforme a la legislación aplicable a cada país; Tener cobertura y respuestas para todos los componentes críticos del sistema; Referencia o inclusión de acciones de respuesta ante el escenario de un incidentes de las marcas de pago. • Considerar en el plan de respuesta ante incidentes los escenarios comunes en el sector, los desarrollos -medida reciente en la industria-tecnología; como los casos frecuentes en la organización teniendo en cuenta las lecciones aprendidas que se registran y permiten actualizar oportunamente el plan de respuesta; para que este permita a la organización la actuación de forma efectiva en caso de un fallo en el sistema que pueda afectar los datos CHD o al CDE. • Dentro de las revisiones y pruebas anuales al plan de respuesta ante incidentes, considerar no solo lo requerido por PCI DSS en el requisito 12.10.1 sino también todos aquellos procedimientos-escenarios adicionales, cambios o mejoras que hagan parte de la organización y afecten directa o indirectamente a los datos CHD o al CDE. • Todo el personal designado para respuesta ante incidentes debe estar capacitado y fácilmente disponible; para los casos en que la organización no trabaje ordinariamente en fines de semana, festivos y horario nocturno se debe proveer personal para estos espacios con asignaciones específicas de forma permanente o por turnos rotativos a fin de que puedan atender oportunamente todos los incidentes que se den de cualquier escenario o cliente que este asociado a los datos CHD o al CDE. • En caso de registrarse un incidente, se debe notificar del mismo a las marcas de pago , seguirme adecuadamente los lineamientos del plan y los procedimiento dentro de los tiempos establecidos y que hacen parte de las pruebas ejecutadas al plan, como también registrarse el evento dentro de la bitácora que se lleve de lecciones aprendidas.	1. Plan de respuesta ante incidentes 2. Procedimiento de gestión de debilidades, eventos e incidentes 3. Plan de recuperación de desastre (DRP) Y Plan de continuidad de negocio (BCP) 4. Procedimientos de copia de seguridad de datos 5. Bitácora de lecciones aprendidas	10.6; 10.8

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
	12.11	12.11.a 12.11.b 12.11.1	• Este requisito es aplicable para las pasarelas de pagos porque estas son proveedores de servicio de los comercios, por tanto, debe ejecutarse auditorias interna periódica y de seguimiento y control permanente para monitorear el cumplimiento efectivo de las políticas de seguridad y los procedimientos operativos; labor que debe hacerse por el área de control interno o auditoria permitiendo la segregación de funciones o por cualquier personal interno o externo que no esté involucrado con los procesos del Core, ni con la implementación directa de los requisitos de PCI DSS, ni con la administración de los datos CHD o del CDE. • Debe aplicarse este requisito como medida previa o de evaluación interna preliminar antes de efectuarse la evaluación de PCI DSS por la QSA; para realizar acciones correctivas o de mejora pertinentes y se aplique los requisitos de PCI como se esperaba.	1. Informes de auditoría interna y de seguimiento y control 2. Plan de gestión de acciones correctiva y de mejora	Todos

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
APÉNDICE 1	A.1	A.1.1 - A.1.4	• Este requisito se aplicaría si la pasarela de pago maneja su servicio Core en un entorno de hosting por medio de un proveedor hosting compartido, por lo que deberá exigirle a su proveedor de hosting / alojamiento web compartido el cumplimiento de este requisito adicional de PCI DSS en caso contrario se excluiría del alcance este requisito para la pasarela de pago. • Si el servicio de la pasarela de pago está en un entorno de hosting por medio de un proveedor hosting compartido; debe tener su propia ID de usuario de servidor Web compartido y a la vez permitir que todas las secuencias de comandos CGI se generen y usen únicamente con la ID de usuario única establecida. • La pasarela de pago contratante debe ser la única autorizada para poder acceder a su propio entorno y ningún otro cliente del proveedor hosting compartido puede tener acceso a este entorno sin que se amerite para ello como parte del servicio Core o del CDE de la pasarela de pago; por lo que se debe considerar los privilegios y permisos otorgados y asignados a nivel de ID usuario de servidor web del hosting, así mismo el proveedor hosting debe tener los controles necesarios para evitar que ninguno de sus clientes monopolice, altere o desborde los recursos del sistema hosting afectando los demás clientes como las pasarelas de pago. • Tener en cuenta los acuerdos contractuales convenidos con el proveedor de hosting / alojamiento web compartido para que se cumpla con este requisito adicional A1 junto con los demás requisitos que sean considerados por PCI DSS aplicables para el servicio contratado.	1. Acuerdo contractual con el proveedor de hosting compartido con las especificaciones del cumplimiento de los requisitos de PCI DSS y del establecimiento de los lineamientos requeridos por la pasarela de pago en materia de seguridad. 2. Evidencias del cumplimiento por parte del proveedor de hosting compartido	1; 2.6; 7; 8; 10; 12.8; 12.9
APÉNDICE 2	A.2	A.2.1 - A.2.3	• Este requisito queda completamente excluido del alcance de su implementación para una pasarela de pago; ya que está estructurado para su implementación en un terminal de POS POI de tarjeta el cual no es implementado dentro del servicio Core de la pasarela de pago, además de que los lineamientos considerados en este requisito adicional se orienta al uso de SSL o TLS temprana que son protocolos poco seguros y que no son admisible en ninguno de los procesos del servicio Core de la pasarela de pago por lo que no se considera el análisis de este requisito A2 en esta guía.	N/A	N/A

ANEXO A. (Continuación)

REQUERIMIENTOS DE PCI DSS V3.2.1 PARA LAS PASARELAS DE PAGOS[58]					
Requisito	**Sub-Requisito**	**Procedimientos. a implementar**	**Consideraciones para una pasarela de pagos**	**Entregables**	**Dependencias**
APÉNDICE 3	A.3	A.3.1 - A.3.5	• La pasarela de pago debe cumplir y acreditar este requisito adicional sí una marca de tarjeta de pago o adquirente se lo exige formalmente mediante su QSA autorizado para la evaluación de certificación; por lo que este requisito adicional no es necesario en su implementación, si previa a una evaluación de acreditación no fue estipulado su exigencia en su cumplimiento por parte de una marca de tarjeta de pago o adquirente. No obstante, con el pasar del tiempo se le pude exigir a una entidad o pasarela de pago especifica su aplicabilidad teniendo en cuenta lo siguientes criterios: 1. Almacene, procese y/o transmite grandes cantidades de datos CHD. 2. Proporcionen puntos de agregación a los datos CHD 3. Tenga muchos reportes de vulnerabilidades significativos o reiterados incidentes asociados al servicio Core. • La gerencia general y la junta directiva deben estar muy pendientes de la gestión de cumplimiento e incitativas que se orientan a PCI DSS, volviendo este estándar una rutina estratégica del negocio al cual deben considerar recursos (económicos, tecnológicos, de personal, de capacitación y supervisión) para establecer, implementar y mejorar el programa formal de cumplimiento de la PCI DSS. • Tener presente el alcance que se ha definido para el cumplimiento del estándar; por lo que si se consideran nueva líneas de negocio, ajustes o ampliaciones de los servicios, cambios en la infraestructura TI y demás cambios significativos se debe reevaluar el alcance y analizar todas las variables del estándar PCI DSS para su adecuada aplicabilidad poniendo estos cambios en conocimiento de la QSA cada trimestre a fin de que la acreditación PCI DSS existente sea aceptada como estaba o renovada con los cambios sobre el servicio Core y/o el CDE según el impacto generado; ya que de no hacerlo el PCI_SSC podría revocar la acreditación o certificación PCI DSS existente y hasta emitir una sanción/suspensión para la pasarela de pagos y/o la QSA si se omite la notificación de los cambios sobre el Alcance PCI DSS y el CDE dentro los plazos definidos.	1. Evidencias de las configuraciones y de los registros documentados estipulados en este requisito (Incluyendo entre estos las actas de gestión/reuniones por la gerencia general y la junta directiva; programa de cumplimiento de la PCI DSS; reporte de validación al alcance PCI DSS con los soportes correspondientes y la notificación de los cambios presentados sobre el servicio Core y/o el CDE)	Todos

Fuente: Propia