DECANATO DE INGENIERÍA EN INFORMÁTICA

ESCUELA DE INFORMÁTICA

PROPUESTA DE UN AUTODIAGNÓSTICO DEL NIVEL DE MADUREZ PARA LOGRAR EL CUMPLIMIENTO PCI DSS ENERO - ABRIL 2021

TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE INGENIERO DE SOFTWARE

Sustentantes:

Diana Joa 2017-0983

Yasser Jorge 2017-1036

Asesor:

Ing. Patricia Cao

Santo Domingo, Rep. Dom.

Abril, 2021

DEDICATORIA

Le dedico esta tesis a mi familia, amigos y maestros por apoyarme en esos momentos donde he necesitado apoyo para cumplir mis metas, incluyendo esta. Su apoyo marcó este éxito y los que están por venir.

Diana Joa

Agradezco a Dios por la vida, por la oportunidad de permitirme cumplir una meta más en mi vida, por la fuerza otorgada para mantenerme en pie, a pesar de las dificultades. Gracias a los directivos deportivos de voleibol de APEC por haberme ayudado a obtener la beca con la cual estudie. Gracias a mis familiares, amigos, a aquellos que en el transcurso de la carrera fueron un soporte para mí y gracias a APEC por el privilegio de hacer nuevos amigos.

Yasser Jorge

AGRADECIMIENTOS

Agradezco primeramente a Dios por poner en mi camino situaciones y personas claves que de una forma u otra aportaron a mi crecimiento personal y profesional duramente mi trayecto en la universidad.

A nuestra asesora de tesis, Patricia Cao, por estar siempre dispuesta y en buena actitud en hacer de esta tesis un entregable de calidad.

A mi familia por siempre estar dispuesta a tenderme la mano y apoyarme.

A mis amigos y maestros que siempre estuvieron ahí para animarme cuando lo necesitaba.

Diana Joa

Este trabajo de tesis lo dedico a Dios, a cada uno de mis familiares, a cada uno de los amigos que me brindaron su apoyo en la universidad, a cada profesor que me brindo su apoyo y a aquellos que no creen posible en la vida cumplir sus sueños.

Yasser Jorge

INDICE GENERAL

INDICE DE FIGURAS

RESUMEN EJECUTIVO

Debido a la pandemia actual en la que vivimos, ocasionada por el virus COVID-19, hemos sido testigo de la transformación digital de muchos negocios, lo cual ha incrementado exponencialmente las ventas on-line y estas su vez las transacciones comerciales electrónicas. Este crecimiento por un lado es bueno, pero trae consigo nuevos riesgos, como el aumento de fraudes a través de medios de pago, estafas por Internet, clonación digital, suplantación de identidad, etc. No obstante, existen alternativas de prevención para los comercios dedicados a operar a través de medios digitales, consistentes en adoptar normas de cumplimiento internacionales, fortalecimiento de la seguridad de los datos u optar por certificaciones que los preparen para enfrentar escenarios nuevos y dentro de las opciones existentes, está certificarse como entidad que cumple con los lineamientos PCI-DSS.

Basados en lo planteado en el párrafo anterior, la presente investigación tiene como objetivo proponer una herramienta automatizada, a nivel de prototipo, que permita a los comercios que operan a través de transacciones comerciales electrónicas, realizar un Auto-Diagnóstico de su nivel de madurez operacional y prepararse para obtener la certificación PCI-DSS.

La herramienta tiene el propósito de guiar al Comercio de la siguiente manera: primero en identificar la categoría de la operación comercial, segundo, de manera automática le muestra, acorde a su categoría, cuales controles internos debe tener implementados, tercero, pide indicar si el control existe o no, por último, proporciona un informe del nivel de cumplimiento. Finalmente, con el resultado del Auto-Diagnóstico, el Comercio conocerá su nivel de madurez y cual control fortalecer o implementar para dar respuesta satisfactoria ante una revisión de los requisitos que exige la PCI DSS.

INTRODUCCIÓN

Los Comercios que operan usando medios de pagos digitales, deben renovarse y convertirse en alternativas de proporcionar servicios o productos más seguros, en vista de que cada día son más las vulnerabilidades que están siendo explotadas por malhechores que buscan siempre aprovecharse de la debilidad de las empresas. Hoy en día se les hace difícil contratar un servicio externo para confiarle sus datos confidenciales, debido a esto muchas veces al no tener ni contratar una empresa que ofrezca estos servicios, se quedan abiertas muchas brechas que hacen las transacciones inseguras.

Los Comercios certificados PCI DSS aportan a la reducción de los fraudes causados con medios de pagos como tarjetas de crédito, tarjetas de débito, transferencias por internet, entre otros, lo que contribuyen en gran manera a proteger tanto los datos de los consumidores, como la reputación de las entidades certificadas.

Es por esto que decidimos dedicar nuestro trabajo de grado al desarrollo de una propuesta para automatizar la evaluación de los formularios que deben completar las entidades que procesan y transmiten datos de las transacciones realizadas con tarjetas de pago. Para el desarrollo de esta propuesta realizamos diferentes pasos los cuales agrupamos en 4 capítulos contenidos en este trabajo:

Dedicamos el primer capítulo a desarrollar los aspectos generales del PCI DSS, para así tener una visión general de estos.

En el segundo capítulo detallamos los diferentes métodos de investigación que implementamos para el desarrollo de este trabajo.

En el tercer capítulo abarcamos el proceso agotado por las entidades certificadas y el proceso que deben agotar las entidades para aplicar a la certificación PCI DSS.

Finalmente, en el cuarto capítulo damos a conocer los detalles de nuestra propuesta de evaluación automatizada del formulario que evalúa el nivel de madurez de las entidades aplicantes para obtener la certificación PCI DSS.

CAPÍTULO I

ASPECTOS GENERALES DEL PCI DSS (ESTÁNDAR DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO)

Introducción

En este capítulo se estará abarcando los aspectos generales del PCI DSS para así poder tener una visión general de en qué consisten estas normas y que estas pretenden lograr con su implementación en las entidades que procesas y transmiten datos y transacciones de tarjeta de pago.

Proponemos el formulario de evaluación automatizada para facilitar y a su vez motivar a que más entidades apliquen y se critiquen bajo los lineamientos PCI DSS y de esta forma reducir los fraudes electrónicos.

Los aspectos generales contemplados en este capítulo abarcan un marco teórico donde hacemos referencia a varios estudios y artículos relacionados al PCI DSS, la definición de los conceptos utilizados en esta tesis para que sirvan de soporte al lector, la historia y origen del PCI DSS, criterio de evaluación que se utilizan en la evaluación PCI DSS, los roles que intervienen en la evaluación y la responsabilidad de cada uno.

1.1. Marco teórico

La seguridad informática es un campo que requiere de inversión, ya que un descuido podría ser hasta 100 veces más costoso que la inversión a realizar en seguridad. Rosario Sang, presidenta de la Cámara Dominicana de las Tecnologías de la Información y la Comunicación (Cámara TIC), empresaria del sector financiero en una conferencia de la OEA en el 2016 expresó lo siguiente: "La seguridad de la información es una de las preocupaciones de mayor peso en el empresariado en general, ahora bien, las altas finanzas, sector que durante los últimos años ha mejorado sus niveles de eficiente por medio de las nuevas tecnologías, es sensible a las vulnerabilidades, porque de esto depende en parte la confianza de los usuarios, la satisfacción de sus clientes y su rentabilidad, sin contar con el efecto que tiene la ciberseguridad en los costos de los servicios financieros."

"Las entidades financieras invierten al menos el 4% de la cifra de sus gastos totales en mantener fortalecidas sus estructuras de seguridad informática, puesto que flagelos como el "phishing" o robo de identidad digital comprenden las principales amenazas que enfrentan de cara a garantizar el patrimonio de sus clientes y sostener la rentabilidad" (Morrison, 2016). Vemos que los bancos sienten interés en fortalecer la estructura de seguridad en su empresa, ya que de ella depende la confianza que brinda a sus clientes.

En el artículo 2 del decreto 230-18 realizado en el mandato del Sr. Danilo Medina: "La Estrategia Nacional de Ciberseguridad 2018-2021 tiene como misión establecer los mecanismos de ciberseguridad adecuados para la protección del Estado, sus habitantes y, en general, del desarrollo y la seguridad nacional". Es notable el interés del gobierno en brindar apoyo para fomentar la seguridad informática.

Según Walter Cervoni, Chief Technology Officer de GM Sectec (2020) "El PCI DSS consta de pasos de sentido común que coinciden con las mejores prácticas de

seguridad de datos ampliamente aceptadas. Los objetivos de los estándares PCI DSS son ayudar a los comerciantes a procesar de forma segura las transacciones con tarjeta de crédito y prevenir el fraude."

"Los comercios al no ser compatible con PCI podrían exponer sus sistemas a un robo de datos. En 2019, el costo promedio por robo de datos en los EE. UU. Superó los 8 millones de dólares. Para la mayoría de las pequeñas empresas, eso significa cerrar las puertas. También hay multas por parte de las marcas de tarjetas que en los Estados Unidos pueden alcanzar los 100,000 dólares por incidente. El monto de la multa depende del volumen de transacciones de una empresa, la cantidad de requisitos de PCI DSS robados y otros factores." según un informe de IBM (2019).

Según Visa, "En el primer trimestre de 2020 más de 13 millones de sus tarjetahabientes realizaron una transacción de comercio electrónico por primera vez. En las primeras semanas de la cuarentena en Latinoamérica, dos de cada 10 usuarios de la tarjeta de crédito realizaron compras en línea por primera vez."

"Las principales debilidades que se reportan en el 2019 Payment Security Report atañen a la efectividad de las tecnologías de protección de los datos ante vulnerabilidades y ataques del exterior en los sistemas críticos de las empresas; así como en el cumplimiento de programas continuos de evaluación de los procesos de gestión de datos", informa Alberto España, Vicepresidente Senior de GM Security Techologies (2019).

"Estamos convencidos de que la manera más eficaz de mejorar la postura de seguridad general en los sistemas de pago, es continuar evangelizando sobre la importancia del cumplimiento de los PCI-DSS y asesorando a los comerciantes", destaca Alberto España, Vicepresidente Senior de GMST (2019).

1.2. Marco conceptual

1.2.1. PCI-DSS:

Los estándares de seguridad PCI son requerimientos técnicos y operativos establecidos por el Consejo de Normas de Seguridad de Tarjetas de Pago para proteger datos del titular de la tarjeta**.** (Payment Card Industry Security Standards, 2008).

1.2.2. Nivel de madurez

Un nivel de madurez es una meseta evolutiva bien definida que establece un nivel de capacidad para mejorar la capacidad de la fuerza laboral; cada nivel de madurez especifica ciertas características para los procesos, niveles de madurez más altos implican características más avanzadas y es un paso hacia el logro de un proceso maduro, proporcionando un conjunto de metas que, cuando se cumplen, coloca a una organización en el siguiente nivel de madurez. (Cruz-Cunha et al., 2013, pp. 1–3).

1.2.3. Pandemia

Se llama pandemia a la propagación mundial de una nueva enfermedad. (World Health Organization, 2013).

1.2.4. Ciberseguridad

La ciberseguridad se define como una capa de protección para los archivos de información, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo. Lanz, L. (2020, 27 mayo).

1.2.5. COVID-19

La COVID-19 es la enfermedad infecciosa causada por el coronavirus que se ha descubierto más recientemente. (*Preguntas y respuestas sobre la enfermedad por coronavirus (COVID-19)*, 2020).

1.2.6. Coronavirus

Los coronavirus son una extensa familia de virus que pueden causar enfermedades tanto en animales como en humanos. En los humanos, se sabe que varios coronavirus causan infecciones respiratorias que pueden ir desde el resfriado común hasta enfermedades más graves como el síndrome respiratorio de Oriente Medio (MERS) y el síndrome respiratorio agudo severo (SRAS). (Preguntas y respuestas sobre la enfermedad por coronavirus (COVID-19), 2020).

1.2.7. Entidades adquirientes

Una entidad adquirente es una institución financiera que procesa pagos de determinadas tarjetas de crédito y débito. (¿Qué es una entidad adquirente?, 2021)

1.2.8. Entidades emisoras

Son las entidades económicas que requieren de financiamiento para la realización de diversos proyectos. Además de requerir de financiamiento, cumplen con los requisitos de inscripción y mantenimiento establecidos por las autoridades para garantizar el sano desempeño del mercado. (Gobierno de México, 2016)

1.2.9. Cifrado

Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger. (RAE, 2020)

1.2.10. Ocultamiento

Esconder, tapar, disfrazar, encubrir a la vista. (RAE, 2020)

1.2.11. Truncamiento

Es el término usado para referirse a reducir el número de dígitos a la derecha del separador decimal, descartando los menos significativos. (Spivak, 2008)

1.2.12. Hashing

Una función criptográfica hash- usualmente conocida como “hash”- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud. (Donohue, 2021)

1.2.13. Software malicioso

Se trata de un tipo de software o de aplicación que tiene como objetivo hacer daño al dispositivo en el que se ha conseguido alojar, instalar o infiltrar, ya sea un ordenador, un teléfono móvil o cualquier otro aparato. (Fernández, 2020)

1.2.14. Software antivirus

Un antivirus es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora. (Verizon, s. f.)

1.2.15. Parches de seguridad

Son parches que solucionan problemas de seguridad y, en la medida de lo posible, no modifican la funcionalidad del sistema. (Proffitt, 2016)

1.3. Historia y origen de PCI DSS

El PCI Security Standards Council (PCI SSC) es un foro mundial que reúne a las partes interesadas del sector de los pagos para desarrollar e impulsar la adopción de normas y recursos de seguridad de datos para realizar pagos seguros en todo el mundo (Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards, 2021).

La misión del PCI SSC es mejorar la seguridad de los datos de las cuentas de pago a nivel mundial mediante el desarrollo de normas y servicios de apoyo que impulsen la educación, la concienciación y la aplicación efectiva por parte de las partes interesadas.

Para ello, contamos con un marco estratégico que guía nuestro proceso de toma de decisiones y garantiza que todas las iniciativas estén en consonancia con nuestra misión y respalden las necesidades del sector de los pagos a nivel mundial (Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards, 2021).

El Consejo fue fundado en 2006 por American Express, Discover, JCB International, MasterCard y Visa Inc. Los miembros fundadores comparten a partes iguales la propiedad, la gobernanza y la ejecución del trabajo de la organización. Cada uno de ellos incorpora la norma de seguridad de datos de la PCI (PCI DSS) como parte de los requisitos técnicos de sus respectivos programas de cumplimiento de la seguridad de los datos. Los miembros fundadores también reconocen a los evaluadores cualificados por el PCI SSC (Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards, 2021).

1.4. Roles y responsabilidades en el cumplimiento con PCI DSS

Los estándares de seguridad PCI DSS surgieron de la necesidad de que todas las tarjetas de pago siguieran un mismo lineamiento ya que anterior a la PCI DSS, cada una de estas definían sus propios estándares y controles de seguridad. Esto resultaba en un problema de duplicidad y solapamiento de implementación de controles en las entidades que almacenaban, procesaban y/o transmitía datos de tarjeta perteneciente a cualquiera de las marcas de tarjetas de pago ya que debía regirse bajo los controles de cada una de estas.

A pesar de la publicación e implementación de los estándares de seguridad PCI DSS, las marcas de tarjeta de pago mantienen ciertas responsabilidades para asegurar la seguridad en sus procesos, entre las cuales podemos citar: definición de las entidades que tienen que cumplir con el estándar, la gestión de los reportes de cumplimiento, la

publicación de las listas de entidades certificadas, las acciones en caso de compromiso de datos de tarjetas y los criterios de multas y sanciones siguen siendo administrados por cada marca de forma independiente a través de dichos programas (Acosta, 2020a).

Figura 1.1

Roles y responsabilidades en el cumplimiento con PCI DSS

1.5. Alcance de cumplimiento de PCI DSS

Para determinar el alcance del cumplimiento de PCI DSS es necesario segmentar los diferentes sistemas, procesos, entidades, etc. a evaluar ya que, dependiendo de esto el alcance puede variar. La determinación del alcance se basa en identificar las personas, procesos y tecnologías que interactúan o que pudiesen de alguna forma impactar los datos del tarjetahabiente.

"Ejemplos de métodos de segmentación comúnmente utilizados para reducir el alcance de la PCI DSS incluyen cortafuegos y configuraciones de enrutadores para evitar que el tráfico pase entre las redes fuera del alcance y el CDE, configuraciones de red que impiden las comunicaciones entre diferentes sistemas y/o subredes, y controles de acceso físico.

Tenga en cuenta que cuando se utilizan tecnologías para gestionar el acceso entre sistemas y redes con el fin de cumplir los requisitos de la PCI DSS, esto no se considera una segmentación que reduzca el alcance de la PCI DSS. Aunque todavía en el ámbito de la PCI DSS, estas comunicaciones son potencialmente más seguras que los canales de comunicación no controlados." (Guidance for PCI DSS Scoping and Network Segmentation, 2017)

La entidad a ser evaluada es la encargada de, anualmente definir y documentar la segmentación y el alcance de su evaluación PCI DSS mientras que el evaluador PCI DSS debe validar que estos fueron propiamente definidos, documentados, así como validar el proceso que la entidad llevó a cabo o el razonamiento detrás de la definición del alcance y segmentación.

Según la guía para definir el alcance y segmentación de la evaluación PCI DSS proporcionada por esta misma institución, estos son algunos ejemplos de definición de alcance:

1.5.1. Identificar cómo y dónde la organización recibe los datos del tarjetahabiente

Identificar todos los canales y métodos de pago para aceptar los datos de los tarjetahabientes, desde el punto en que se reciben hasta el punto de destrucción, eliminación o transferencia.

1.5.2. Localizar y documentar donde los datos de la cuenta son almacenados, procesados y transmitidos

Documentar todos los flujos de los datos del tarjetahabiente e identificar a las personas, los procesos y tecnologías que intervienen en el almacenamiento, el procesamiento y/o la transmisión de los datos del tarjetahabiente. Estas personas, procesos y tecnologías forman parte del ambiente de los datos del tarjetahabiente.

1.5.3. Mantener y supervisar

Implementar procesos para garantizar que los controles PCI DSS sigan siendo efectivos cada día, día tras días. (PCI Security Standards Council, 2017)

1.6. Descripción de los controles de Seguridad de Datos de PCI DSS

Aquellas entidades que aceptan o procesan pagos con tarjetas, pueden regirse bajo los estándares de Seguridad de Datos PCI DSS.

Estos estándares abarcan componentes tantos técnicos como operacionales incluidos o relacionados a la data del tarjetahabiente:

Figura 1.2

Controles de Seguridad de Datos de PCI DSS

Objetivo	Requerimiento PCI DSS
Construir y mantener una red segura	1. Instalar y mantener una configuración de cortafuegos para proteger los datos de los titulares de las tarjetas
	2. No utilice los valores predeterminados proporcionados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad
Proteger los datos de los titulares de las tarjetas	3. Proteja los datos de los titulares de las tarjetas almacenados
	4. Encriptar la transmisión de los datos de los titulares de las tarjetas a través de redes abiertas y públicas
Mantener un programa de gestión de la vulnerabilidad	5. Desarrollar y mantener sistemas y aplicaciones seguros
	6. Implantar fuertes medidas de control de acceso
Implementar fuertes medidas de control de acceso	7. Restringir el acceso a los datos de los titulares de las tarjetas según la necesidad de conocimiento de la empresa
	8. Asignar una identificación única a cada persona con acceso a los ordenadores
	9. Restringir el acceso físico a los datos de los titulares de las tarjetas
Supervisar y probar regularmente las redes	10. Rastrear y supervisar todos los accesos a los recursos de la red y a los datos de los titulares de las tarjetas
	11. Probar periódicamente los sistemas y procesos de seguridad
Mantener una política de seguridad de la información	12. Mantener una política que aborde la seguridad de la información para empleados y contratistas

1.7. Criterio de evaluación de PCI DSS

Aquellas entidades que deseen o requieran evaluarse bajo los estándares PCI DSS, según el tipo de evaluación que le corresponda pueden en el mismo documento de evaluación que proporciona la PCI DSS validar cuáles son los requisitos, procedimiento a seguir para evaluarse. Este documento también incluye guías con detalles adicionales que sirve de apoyo para delimitar el alcance de la evaluación.

Cada cuestionario cuenta con diferentes opciones de respuestas que el evaluado debe seleccionar según corresponda. Estas respuestas son cerradas y concretas y el mismo documento de evaluación da a conocer más en detalle el equivalente a cada respuesta seleccionada.

Resumen CAPÍTULO I

Los estándares de seguridad PCI DSS surgieron de la necesidad de que todas las tarjetas de pago siguieran un mismo lineamiento ya que anterior a la PCI DSS, cada una de estas definían sus propios estándares y controles de seguridad. Esto resultaba en un problema de duplicidad y solapamiento de implementación de controles en las entidades que almacenaban, procesaban y/o transmitía datos de tarjeta perteneciente a cualquiera de las marcas de tarjetas de pago ya que debía regirse bajo los controles de cada una de estas.

Para determinar el alcance del cumplimiento de PCI DSS es necesario segmentar los diferentes sistemas, procesos, entidades, etc. a evaluar ya que, dependiendo de esto el alcance puede variar. La determinación del alcance se basa en identificar las personas, procesos y tecnologías que interactúan o que pudiesen de alguna forma impactar los datos del tarjetahabiente.

Los formularios que la PCI DSS pone a disposición para que las entidades se evalúen cuenta con el criterio correspondiente para que le sirva de guía a estas a la hora de evaluarse.

CAPÍTULO II

DISEÑO METODOLÓGICO

Introducción

En este capítulo se dará a conocer los tipos y métodos de investigación utilizados para el desarrollo de este trabajo de grado, así como los tipos fuente de documentación utilizadas.

Nos apoyamos de técnicas y fuentes de investigación que nos facilitarán ver tanto desde una perspectiva a alto nivel así como a una perspectiva a bajo nivel en base a los recursos que pone a disposición de forma totalmente online, en inglés y español, la PCI DSS y las diferentes instituciones y organizaciones que sirve de soporte para dar a conocer estas normas y que sirven como soporte brindando sus servicios de asesoría a las diferentes entidades para que estas puedan prepararse y aplicar a la certificación PCI DSS.

2.1. Conceptos y tipos de Investigación

"La investigación es un conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema" (Sampieri et al., 2014, p. 4).

Dicho esto, podríamos deducir que la investigación es una herramienta que utilizamos con el objetivo de obtener nuevos conocimientos o ampliar el conocimiento existente, de un determinado problema o tema de investigación, siendo este parte fundamental del método científico.

2.1.1. Investigación exploratoria

"Los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes. Es decir, cuando la revisión de la literatura reveló que tan sólo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio, o bien, si deseamos indagar sobre temas y áreas desde nuevas perspectivas" (Sampieri et al., 2014, p. 91).

Implementamos este método de investigación como soporte para poder identificar cuáles son los puntos más importantes a tratar, para a partir de estos, desarrollar el tema de investigación.

2.1.2. Investigación descriptiva

"Con los estudios descriptivos se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refiere, esto es, su objetivo no es indicar cómo se relacionan éstas" (Sampieri et al., 2014, p. 92).

Su finalidad en este trabajo de investigación es describir la situación o fenómenos que están involucrados en el campo de estudio. En este tipo de investigación más que describir el "¿por qué?" se busca describir otras cuestionantes como el "¿qué?", "¿cómo?", "¿cuándo?" y "¿dónde?".

2.1.3. Investigación explicativa

"Los estudios explicativos van más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; es decir, están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta o por qué se relacionan dos o más variables" (Sampieri et al., 2014, pp. 95-96).

Su finalidad en ese trabajo de investigación es definir el "¿por qué?" y el "¿para qué?" del objeto de estudio, con el fin de ampliar los resultados obtenidos de la investigación descriptiva y exploratoria. En nuestro caso, utilizaremos esta investigación para determinar y definir el "¿por qué?" y el "¿para qué?". Es necesario saber el nivel de madurez con el que cuenta la empresa, la que a groso modo busca reducir y erradicar los fraudes a través de tarjetas de crédito o débito.

2.2. Métodos de investigación

2.2.1. Observación

"Se define observación como la inspección y estudio realizado por el investigador, mediante el empleo de sus propios sentidos, con o sin ayuda de aparatos técnicos, de las cosas o hechos de interés social, tal como son o tienen lugar espontáneamente" (Caceres, 2016).

Se utilizará para identificar los conflictos que puede ocasionar la falta de aplicación de las normas de la PCI, con la finalidad de crear una guía que sirva de apoyo para identificar el nivel de madurez para poder cumplir con las normas PCI DSS.

2.2.2. Deductivo

"Es una estrategia de razonamiento empleada para deducir conclusiones lógicas a partir de una serie de premisas o principios" (7Graus, 2019).

Se utilizará este método porque este comienza analizando el problema general, que es la seguridad por las cuales se efectúan las transacciones a través de las plataformas tecnológicas, para poder determinar cuál es el grado de vulnerabilidad de cada transacción.

2.2.3. Analítico-Sintético

"El método analítico o método empírico-analítico es un modelo de estudio científico basado en la experimentación directa y la lógica empírica." (etecé, 2020)

Utilizando este método, se procede a descomponer el objeto de estudio con la finalidad de analizarlos por separado de manera individual y luego hacer una integración donde se analice el todo como conjunto.

2.3. Fuentes de documentación

2.3.1. Fuentes primarias

Se emplearán el uso de libros y artículos referentes a las normas PCI DSS publicados en el sitio web de esta entidad.

2.3.2. Fuentes secundarias

Se realizarán investigaciones en los portales web de las instituciones principales del Distrito Nacional relacionadas al sector bancario.

Resumen CAPÍTULO II

Para dar inicio al resumen de este capítulo, deducimos que la investigación es una herramienta que utilizamos con el objetivo de obtener nuevos conocimientos o ampliar el conocimiento existente, de una determinado problema o tema de investigación, siendo este parte fundamental del método científico.

Luego de evaluar los diferentes métodos de investigación que existen, decimos utilizar como métodos de investigación para el desarrollo de este proyecto el método deductivo, la observación, y analítico-sintético con el objetivo de poder implementar los parámetros de obtención de información que estos ofrecen.

Como fuente primaria de documentación nos basamos en diferentes libros digitales para el desarrollo de los diferentes conceptos utilizados en este proyecto y en el sitio web oficial de PCI DSS como fuente principal, para desarrollar todo lo relacionado a esta.

Como fuente secundaria utilizamos los diferentes sitios web que están disponible en internet, de entidades que ofrecen servicios de asesoría para esas entidades que deseen prepararse para aplicar y certificarse PCI DSS.

CAPÍTULO III

ANÁLISIS DE ENTIDADES CERTIFICADAS Y APLICANTES PARA CERTIFICACIÓN PCI DSS

Introducción

En este capítulo abarcamos dos puntos principales a tomar en cuenta a la hora decidir prepararse y aplicar a la certificación PCI DSS.

Como primer punto desarrollamos el proceso agotado por las entidades ya certificadas PCI DSS. Este proceso a nivel general abarca la evaluación de los riesgos y los diferentes planes de acción que se deben tener en cuenta para mitigar dichos riegos. Una vez esto ha sido cubierto se debe hacer una evaluación general para identificar cuales otros aspectos aún faltan por cubrir para poder cumplir con los requerimientos que exige la PCI DSS. Una vez hecho esto se debe desarrollar un plan de acción para llevar a cabo el cumplimiento de lo identificado.

Como segundo punto desarrollamos los 12 requerimientos exigidos por la PCI DSS para que las entidades puedan aplicar y obtener su certificación. Se recomienda que todas las entidades que procesan y almacenan datos de tarjetas de pago y de sus tarjetahabientes sigan estos lineamientos.

A nivel general estos requerimientos persiguen evaluar que tan seguro son los sistemas y aplicaciones que intervienen en las diferentes operaciones de las entidades que transmiten y almacenan datos de tarjetas de pago.

3.1. Levantamiento de proceso agotado por entidades certificadas PCI DSS

El proceso que deben agotar las entidades para analizar cuáles aspectos necesita o no están implementado de forma adecuada para cumplir con los lineamientos PCI DSS, el certificador independiente PCI DSS Internet Security Auditors lo dividió en 5 fases:

Figura 3.1

Fases del cumplimiento de PCI DSS

Una vez identificados estos aspectos se deben definir un plan de acción para que la entidad en cuestión pueda implementar o adecuar los puntos identificados.

3.1.1. Fase 1: Análisis del Estado de Cumplimiento

En esta fase se estudia a nivel general el estado actual de la entidad a ser evaluada, se da a conocer el equipo involucrado, como la entidad está manejando actualmente la información de las tarjetas de pago y las del tarjetahabiente, el tiempo designado para llevar a cabo la certificación y el presupuesto disponible para en base a esto definir cuáles aspectos necesitan ser abordados.

3.1.2. Fase 2: Valoración de Riesgos y Priorización de Acciones

En esta fase se identifican y evalúan los riesgos detectados para en una etapa posterior definir plan de acción para mitigar dichos riesgos en base a la priorización asignada a cada riesgo en esta misma fase.

Estas son las etapas para llevar a cabo la priorización según la guía de Enfoque Priorizado para Lograr el Cumplimiento de PCI DSS:

Etapa 1: Eliminar la información relativa a la autenticación y limitar la retención de información. Esta etapa hace referencia a las entidades que han estado en riesgo y recomienda no almacenar datos confidenciales de autenticación ni otros datos que sean innecesarios almacenar para evitar así que se den escenarios donde se vean comprometidos datos sensitivos.

Etapa 2: Proteger sistemas y redes, y estar listos para responder ante violación del sistema. Esta etapa hace referencia a los diferentes controles que deben existir para proteger los diferentes sistema y redes y poder responder ante alguna violación a estos.

Etapa 3: Aplicaciones de tarjeta de pagos seguras. Esta etapa hace referencia a los diferentes controles que deben existir para proteger las diferentes aplicaciones, servidores de la aplicación y procesos de la aplicación.

Etapa 4: Monitorización y control de acceso a las aplicaciones. Esta etapa busca identificar los controles que la entidad tiene implementado para llevar registros de quién, qué, cuándo y cómo acceden a sus aplicaciones.

Etapa 5: Proteger la información almacenada de los tarjetahabientes. En esta etapa se enfoca en los protocolos que las entidades utilizan para proteger los datos del tarjetahabiente, que por alguna razón u otra decidieron almacenar.

Etapa 6: Finalizar los esfuerzos de cumplimiento restantes y asegurarse de que todos los controles están en marcha. En esta etapa se identifican cuáles son los requisitos faltantes para el cumplimiento PCI DSS para que estos puedan ser desarrollados y así cumplir con la certificación.

3.2. Levantamiento de proceso actual que están agotando entidades aplicantes para obtener certificación PCI DSS

La PCI DSS definió 12 requerimientos que deben cumplir las entidades para considerar que cumplen con lo necesario para poder obtener esta certificación. Se recomienda que todas las entidades que procesan y almacenan datos de tarjetas de pago y de sus tarjetahabientes sigan estos lineamientos.

A continuación, se listan los Requisitos y procedimientos de evaluación de seguridad según la guía de Normas de Seguridad de Datos PCI DSS. Estos requerimientos fueron agrupados en diferentes módulos para que sirva como referencia a que aspectos hace referencia cada requerimiento:

3.2.1. Desarrollar y mantener sistemas y redes seguros

Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los tarjetahabientes. Firewall es una red de seguridad que de cierta forma filtra/monitorea el tráfico de red entre las redes internas y externas según los parámetros definidos en este. Por esto la PCI DSS requiere se tenga instalado y en constante mantenimiento, la implementación de un firewall que asegure los tarjetahabientes.

Requisito 2: No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores. Estas contraseñas ya son conocidas por terceros que pueden hacer uso de esta de forma malintencionada por lo que es un requisito de la PCI DSS que estas sean cambiadas inmediatamente para proteger los sistemas de acciones que puedan comprometer los sistemas.

3.2.2. Proteger los datos del titular de la tarjeta

Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados. La PCI DSS recomienda métodos como el cifrado, el ocultamiento, truncamiento y hashing

para proteger los datos del tarjetahabiente. De ser necesario se podrían implementar otros métodos que apoyen este requerimiento.

Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas. Para esos casos en que es necesario la transmisión de data sensitiva como los datos del tarjetahabiente, es requerido que estos sean cifrados para protegerlos del acceso a estos datos por personas malintencionadas.

3.2.3. Mantener un programa de administración de vulnerabilidad

Requisito 5: Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente. El termino malware es utilizado como nombre colectivo para hacer referencia a un conjunto de variantes de software malicioso. Para proteger todos los sistemas de estos, se recomienda la implementación y mantenimiento de forma regular de software antivirus para proteger todos los sistemas.

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras. El acceso y uso malintencionado de los sistema y aplicaciones se pueden mitigar con la implementación de parches de seguridad. Estos deben ser implementados de forma tal que no intervengan con la configuración de seguridad actual.

3.2.4. Implementar medidas sólidas de control de acceso

Requisito 7: Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. Se requiere que se implementen los protocolos y controles necesarios para limitar el acceso a los datos del tarjetahabiente para que solo el personal autorizado tenga acceso a estos.

Requisito 8: Identificar y autenticar el acceso a los componentes del sistema. Se requiere asignar a cada persona que tendrá acceso a los diferentes componentes del sistema,

le sea asignado un ID y contraseña única para así poder identificarlas en el registro actividades y acciones realizadas en los diferentes sistemas.

Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta. Es requerido que el acceso físico a datos o sistemas que alojan los datos del tarjetahabiente a los diferentes sistemas de todo el personal sea restringido y que el personal que deba tener acceso sea propiamente identificado.

3.2.5. Supervisar y evaluar las redes con regularidad

Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas. Los mecanismos de registro y la posibilidad de rastrear las actividades del usuario son críticos para la prevención, detección o minimización del impacto de los riesgos de datos. La presencia de los registros en todos los entornos permite el rastreo, alertas y análisis cuando algo no funciona bien. Determinar la causa de un riesgo es muy difícil, si no imposible, sin los registros de la actividad del sistema.

Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad. Es requerido que se prueben con regularidad los sistemas y procesos de seguridad para garantizar que los diferentes sistemas y aplicaciones mantienen los protocolos, controles y configuraciones implementadas para su protección.

3.2.6. Mantener una política de seguridad de información

Requisito 12: Mantener una política que aborde la seguridad de la información de todo el personal. Una política de seguridad sólida establece el grado de seguridad para toda la entidad e informa al personal lo que se espera de ellos. Todo el personal debe estar al tanto de la confidencialidad de los datos y de su responsabilidad para protegerlos.

Resumen CAPITULO III

En este capítulo se abarcó a nivel específico el proceso agotado por las entidades para certificarse PCI DSS, detallando las diferentes etapas que debe agotar la entidad en cuestión, según la guía de Enfoque Priorizado para Lograr el Cumplimiento de PCI DSS, para priorizar los riesgos identificados durante el proceso de preparación para certificarse.

También a nivel específico, detallamos los 12 requerimientos estipulados por PCI DSS que debe agotar las entidades correspondientes para certificarse. Dichos requerimientos fueron agrupados en diferentes módulos para que sirva como referencia a que aspectos hace referencia cada requerimiento.

CAPITULO IV

PROPUESTA DE UN AUTODIAGNÓSTICO DEL NIVEL DE MADUREZ PARA LOGRAR EL CUMPLIMIENTO PCI DSS

Introducción

A continuación, se muestran nuestra propuesta de un formulario automatizado para que las entidades que transmiten y procesan transacciones de tarjetas de pago puedan determinar su nivel de madurez para poder aplicar a la certificación PCI DSS.

Tomamos como base 4 de los 9 formularios indicados por la PCI DSS para el desarrollo de esta propuesta para plasmar en esencia como funcionaría para todos los formularios.

El tipo de formulario a llenar dependerá del tipo de comercio al que pertenezca la entidad postulante. Este formulario puede ser completado por el mismo comercio o por el asesor que esté dando apoyo al comercio en su proceso de certificación.

Este formulario automatizado pretende servir de soporte para dar a conocer al comercio su nivel de madurez de cara a la certificación PCI DSS, sin embargo, no es el objetivo de este formulario que se use fuente oficial ya que no cuenta con la aprobación de la entidad oficial certificadora PCI DSS. Obtener esta aprobación podría ser considerarse como siguiente paso en el desarrollo de este formulario.

Estos formularios ya existes y la PCI DSS los pone a disposición en su sitio web oficial, https://www.pcisecuritystandards.org/, sin embargo, estos formularios están disponibles para ser evaluados de forma manual. Con nuestra propuesta estos formularios podrán ser evaluados de forma automática, agilizando el proceso de evaluación, motivando así a que cada vez más comercios se certifiquen y contribuyan a la reducción de fraudes electrónicos asociados a las tarjetas de pago.

4.1. Guía Propuesta - Descripción

Diariamente se realizan millones de transacciones con tarjetas de crédito, ya sean compras por internet, retiros de dinero de cajeros automáticos, pagos realizados con esta vía telefónica, entre otras formas de uso. Solamente en República Dominicana de enero 2018 a septiembre 2020, en promedio, se realizaron 3 millones de transacciones mensuales (Banco Central de la República Dominicana, 2020).

Debido a esto, se hace necesario que los Comercios que emiten y gestionan las transacciones hechas con tarjetas de crédito, estén certificadas con algo que avale la seguridad que los tarjetahabientes esperan recibir al momento de utilizar un instrumento de pago.

Es por esto que decidimos desarrollar una Propuesta de un Autodiagnóstico del Nivel de Madurez para lograr el Cumplimiento PCI DSS, con el objetivo de que las entidades financieras correspondiente puedan utilizarla para certificarse y pueda así reducir la cantidad de fraudes de tarjeta de crédito.

4.2. Objetivos de la guía

4.2.1. Objetivo General

Realizar una guía de Autodiagnóstico para determinar el Nivel de Madurez con el fin de lograr el Cumplimiento PCI DSS en el Distrito Nacional durante el periodo enero-abril 2021.

4.2.2. Objetivos específicos

- Determinar el nivel de madurez que requiere una entidad de servicios para realizar transacciones electrónicas.
- Identificar las vulnerabilidades de mayor impacto de cara al usuario.
- Analizar el riesgo que corren los usuarios cuando existen vulnerabilidades en el proceso de transmisión, procesamiento o almacenamiento de datos de tarjetas de crédito o débito.
- Analizar los requisitos y el nivel de madurez que se necesita para cumplir con el estándar PCI DSS.
- Determinar el riesgo de no cumplir con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI).
- Diseñar una guía básica para auto determinar el nivel de madurez para el cumplimiento de las normas PCI DSS.

4.3. Diseño del formulario automatizado

Para el diseño del formulario automatizado propuesto utilizamos las siguientes herramientas:

4.3.1. Draw.io

Herramienta en línea que sirve para crear diferentes diagramas. Este fue utilizado para el diseño de los diagramas de arquitectura, de clase, entidad relación, de cumplimiento y de estado.

4.3.2. Visual Use Case

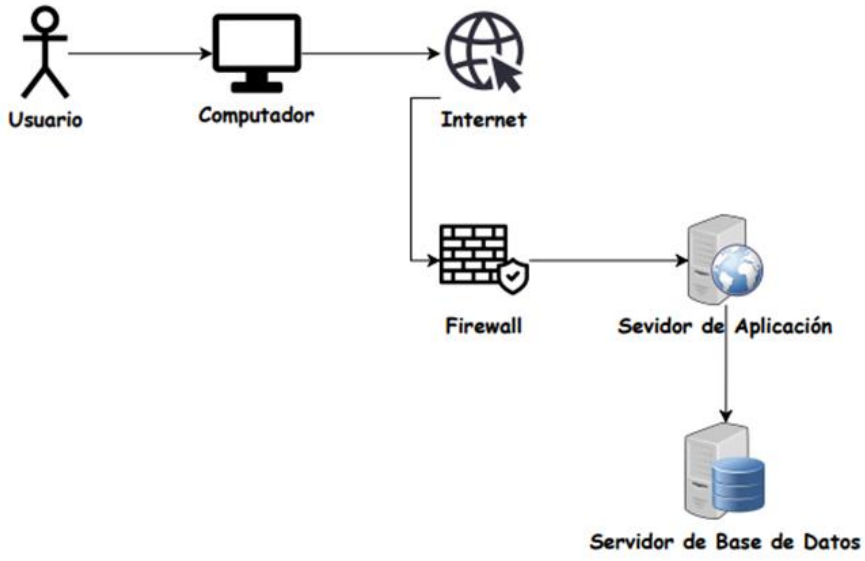
Herramienta descargable utilizada para el desarrollo de caso de uso.

4.4. Diagramas del sistema

4.4.1. Diagrama de arquitectura

Figura 4.1

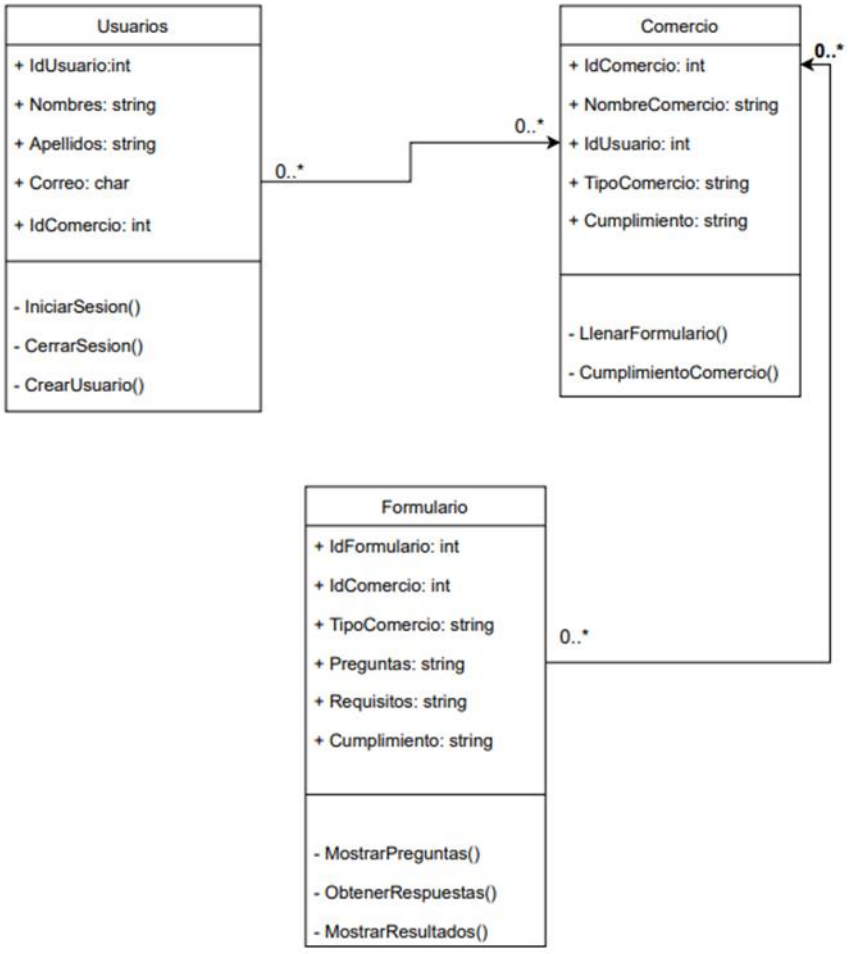
Esquema de arquitectura del sistema



4.4.2. Diagrama de clases

Figura 4.2

Esquema de clases del sistema



4.4.3. Diagramas de estado

Figura 4.3

Diagrama de estado del usuario

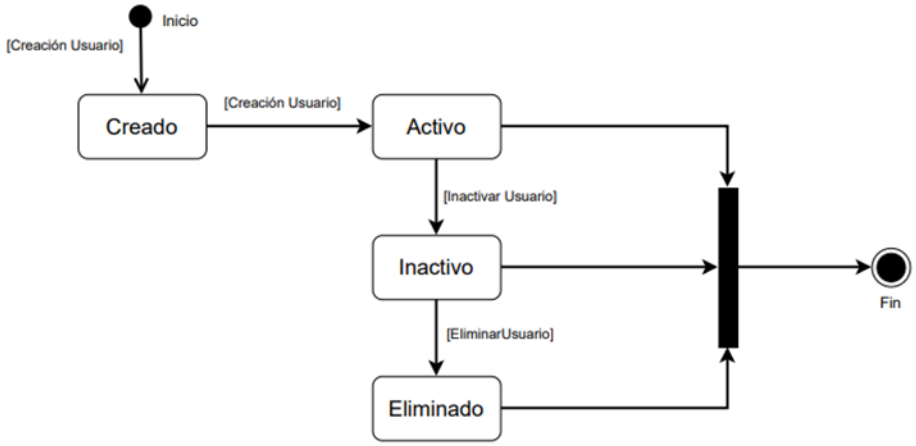
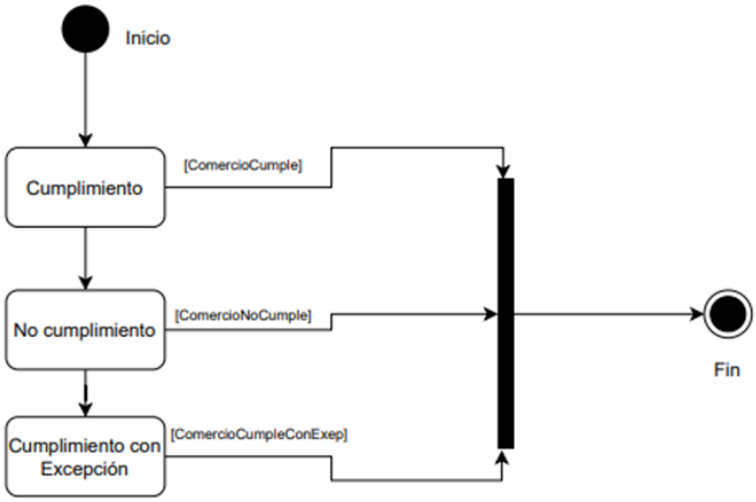


Figura 4.4

Diagrama de estado de cumplimiento

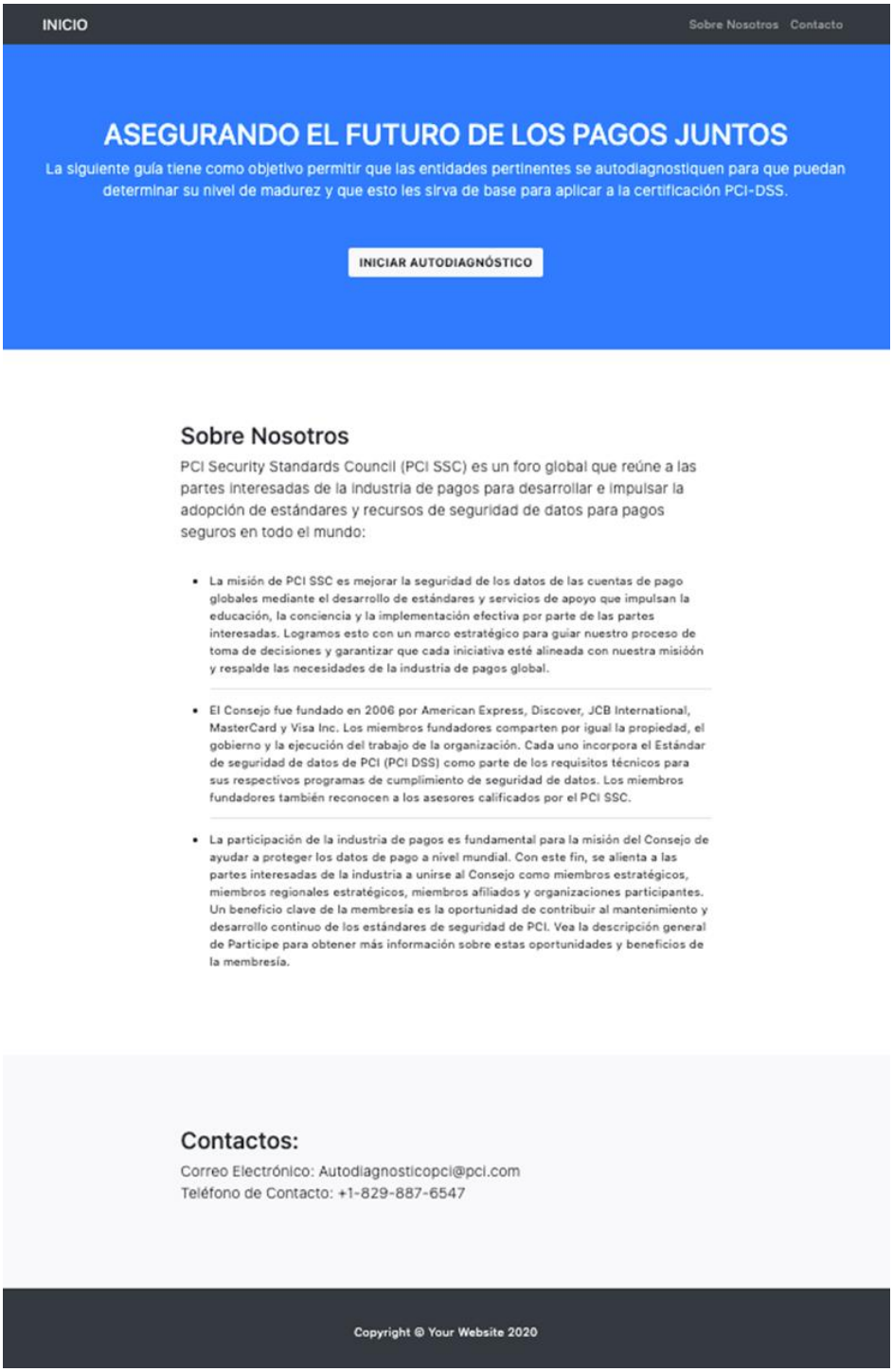


4.5. Diseño preliminar de la interfaz gráfica de usuario

4.5.1. Diseño de la pantalla de inicio

Figura 4.5

Diseño de la pantalla de inicio



4.5.2. Diseño de la pantalla de selección del tipo de comercio

Figura 4.6

Diseño de la pantalla de selección del tipo de comercio

4.5.3. Diseño de la pantalla para ingresar datos del comercio y asesor de seguridad certificado

Figura 4.7

Diseño de la pantalla para ingresar datos del comercio

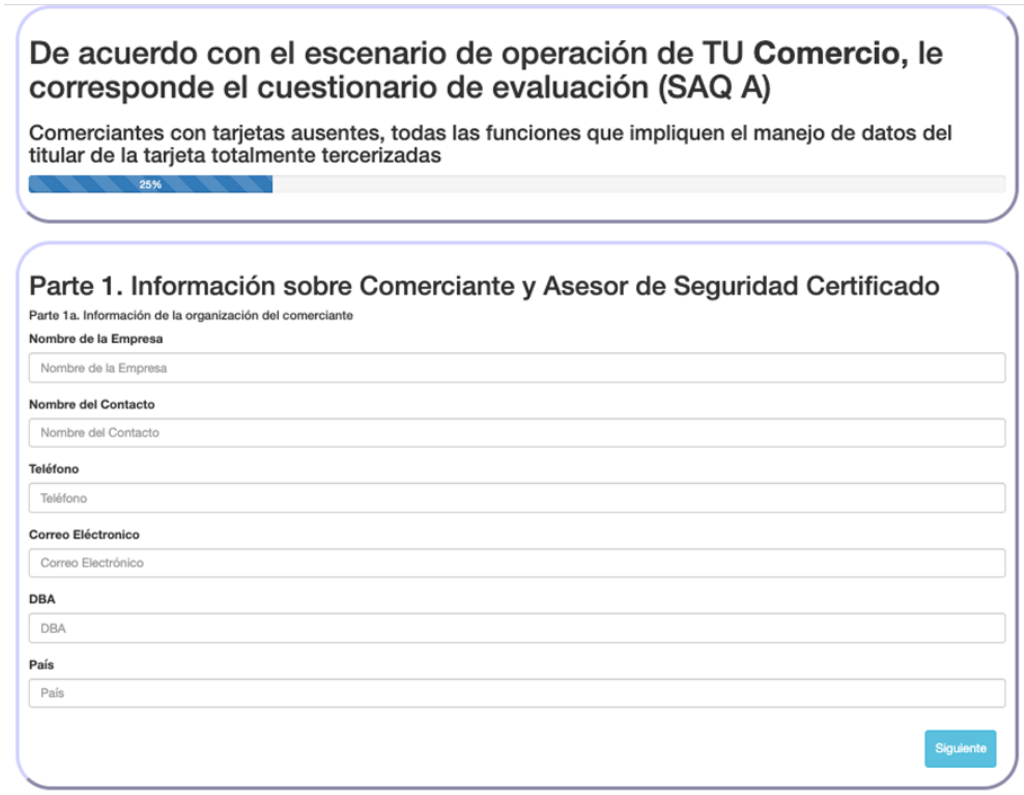
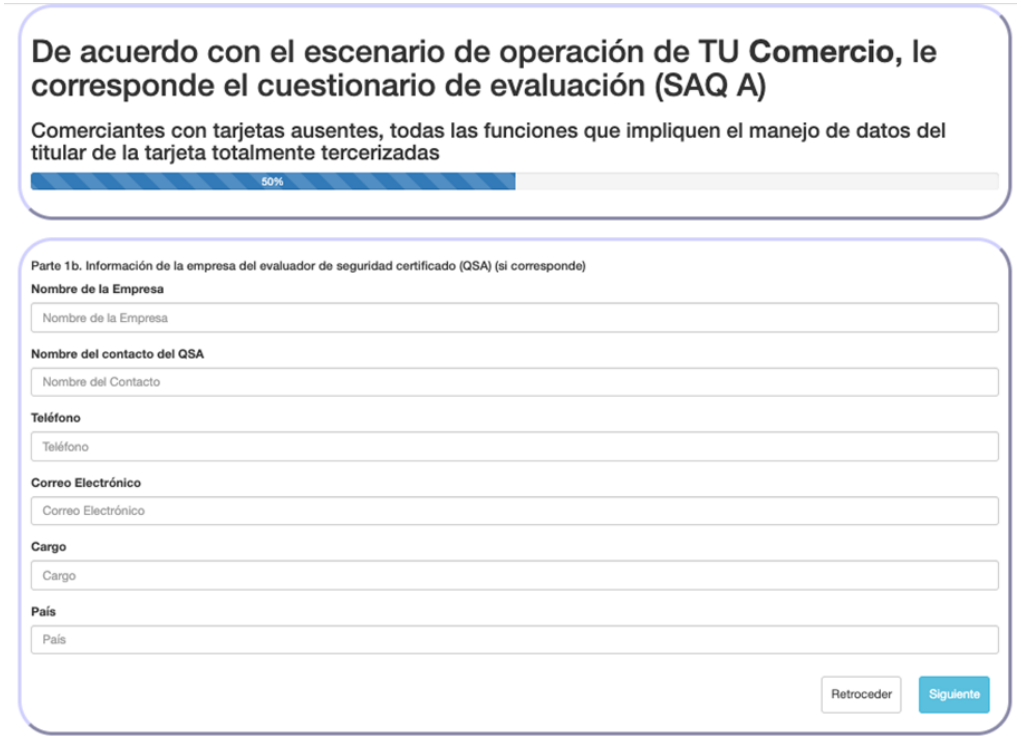


Figura 4.8

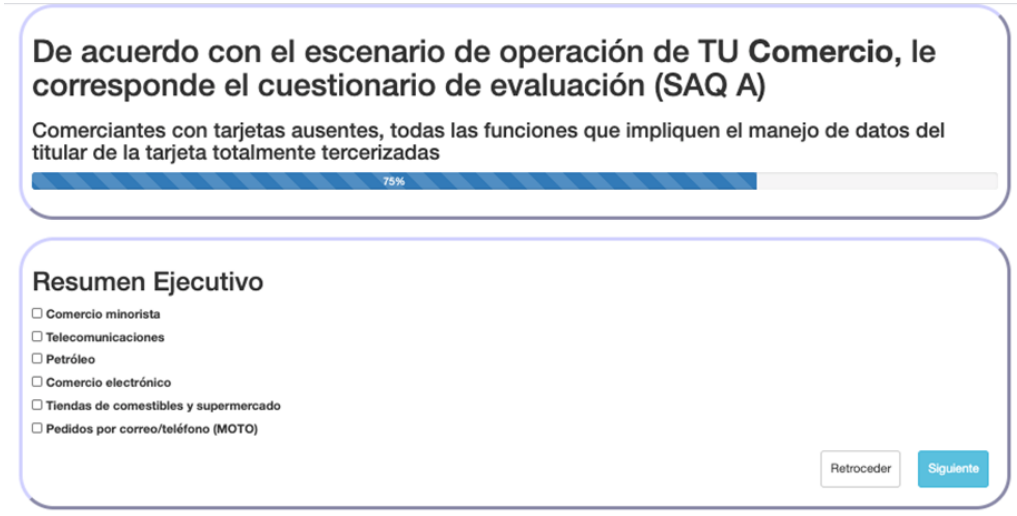
Diseño de la pantalla para ingresar datos del asesor



4.5.4. Diseño de pantalla para seleccionar el tipo de resumen ejecutivo

Figura 4.9

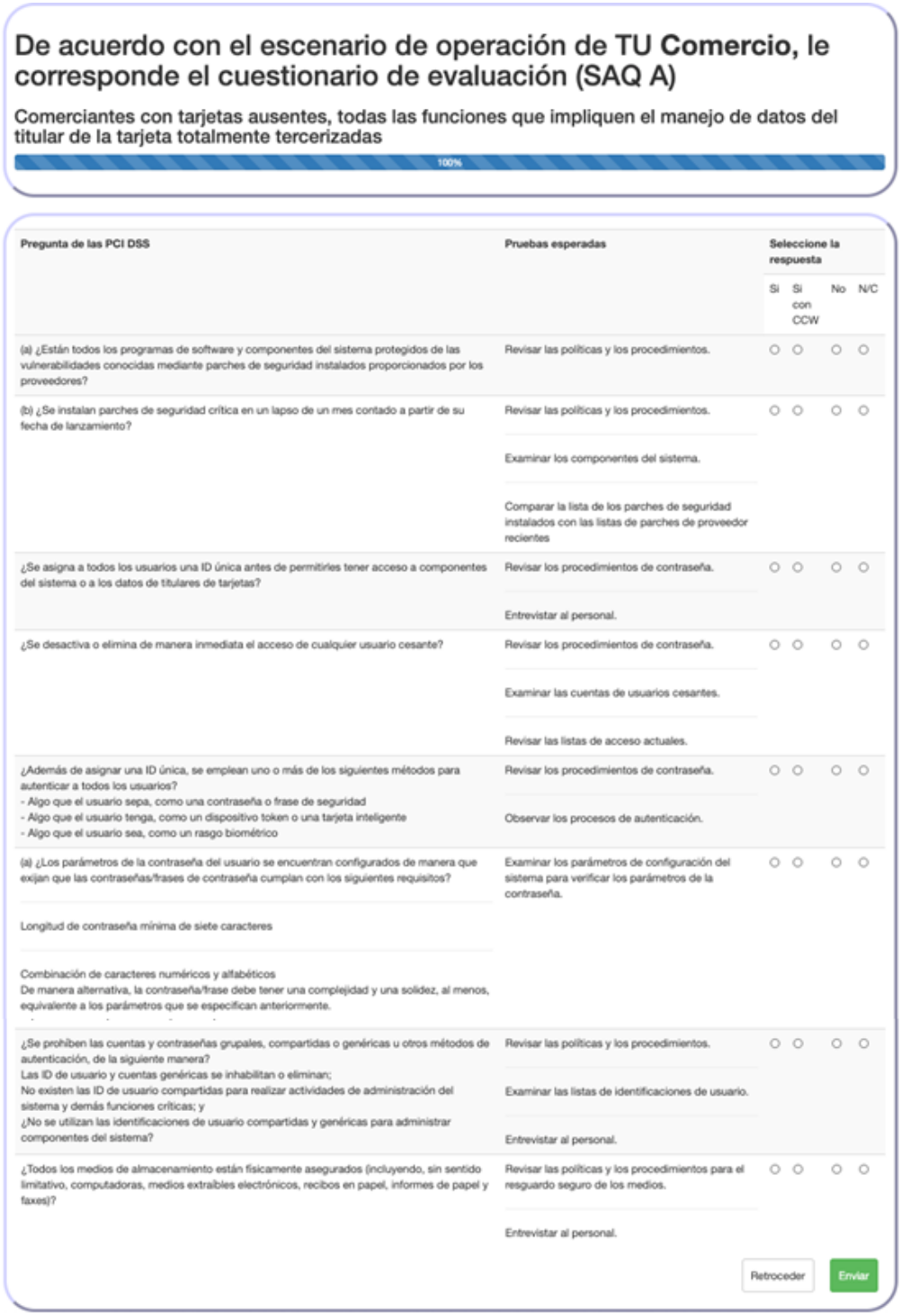
Diseño de la pantalla para seleccionar el tipo de resumen ejecutivo



4.5.5. Diseño de la pantalla del formulario PCI DSS

Figura 4.10

Diseño de la pantalla del formulario PCI DSS



4.5.6. Diseño de la pantalla de Falta de Cumplimiento

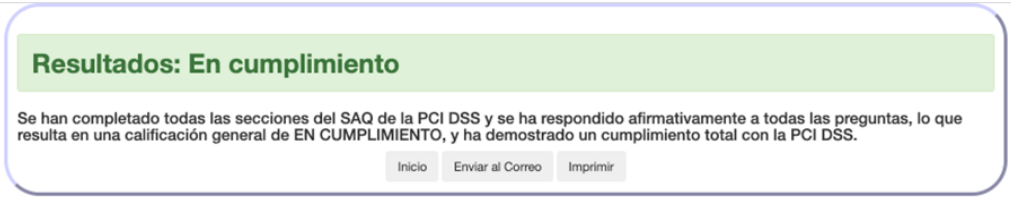
Figura 4.11

Diseño de la pantalla de Falta de Cumplimiento

4.5.7. Diseño de la pantalla En Cumplimiento

Figura 4.12

Diseño de la pantalla En Cumplimiento



4.5.8. Diseño de la pantalla En Cumplimiento con Excepción Legal

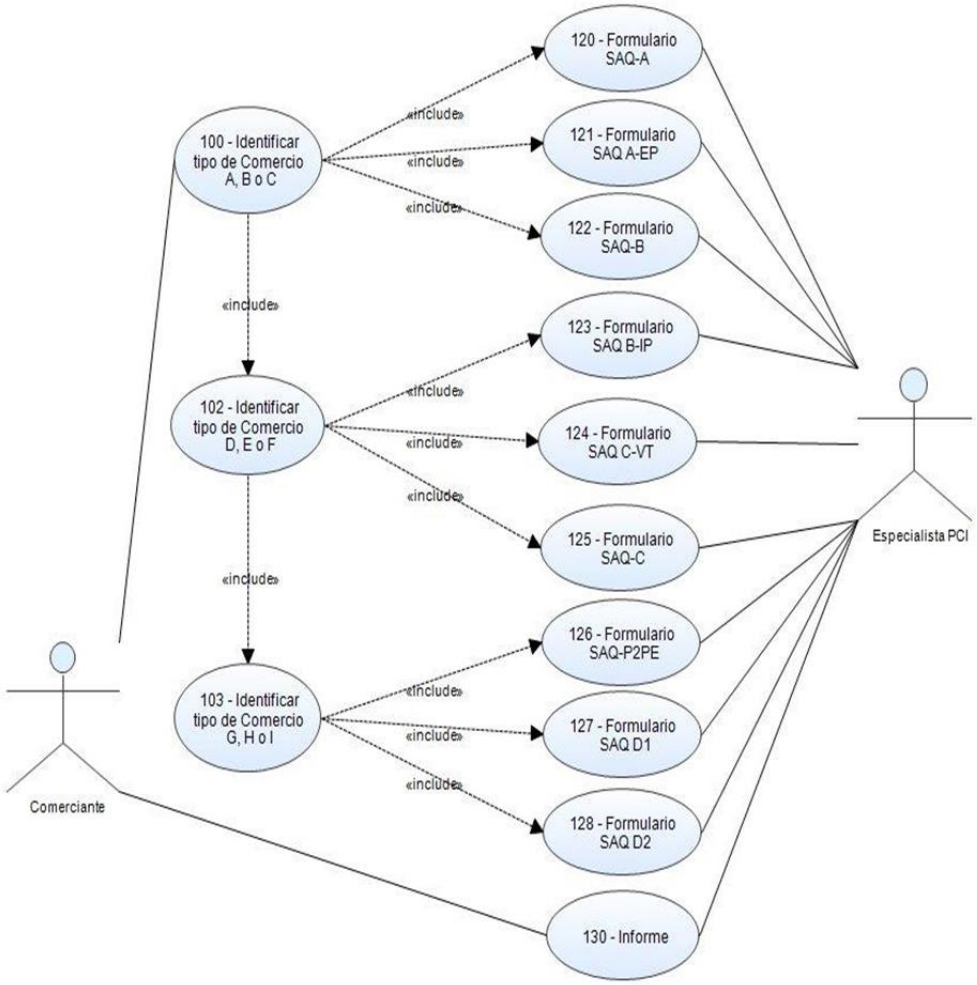
Figura 4.13

Diseño de la pantalla En Cumplimiento con Excepción Legal

4.6. Diseño de Caso de uso

Figura 4.14

Esquema de casos de uso



Resumen CAPÍTULO IV

Los diferentes diagramas incluidos en este capítulo tienen como objetivo plasmar la estructura que proponemos se utilice para el desarrollo del formulario automatizado. Para esto nos apoyamos de diagramas de arquitectura, de clase y de estados.

También, incluimos un caso de uso que abarca de manera general las diferentes actividades que se llevarán a cabo en el formulario automatizado propuesto y capturas de pantallas que recomendamos tenga la solución final. Estas contemplan lo necesario para cumplir con el objetivo de la solución propuesta, dar a conocer el nivel de madurez del comercio que complete este formulario.

Estas representaciones gráficas entendemos sirven de apoyo para que el equipo de desarrollo las pueda utilizar de apoyo en el desarrollo e integración del resto de los formularios.

CONCLUSIÓN

Cabe recalcar que lo que nos motivó a desarrollar este trabajo de grado en base a una propuesta para automatizar la evaluación de los formularios que debe llenar las entidades que procesan y transmiten datos de tarjeta de pago, fue agilizar el proceso de evaluación de estas para incentivar a las entidades a que se preparen, apliquen y se certifiquen bajo las normas PCI DSS ya que a largo plazo esto aportará a la reducción de fraudes electrónicos asociado a las transacciones que se realizan con tarjetas de pago.

Para el desarrollo de esta propuesta nos apoyamos de diferentes métodos de investigación como la observación para identificar los conflictos que puede ocasionar el no aplicar las normas PCI DSS, la investigación deductiva para analizar el problema que puede y que ocasiona el hecho de que las entidades o comercios no se rijan bajo los lineamientos PCI DSS desde un punto de vista general y el analítico-sintético para descomponer el objeto de estudio con la finalidad de analizarlos por separarlos para su posterior integración donde se analizamos como interactúan en conjunto.

Nos aseguramos de basarnos en informaciones que consideramos confiable, disponible en el sitio web oficial de la PCI DSS, sitios web de entidades que sirven de soporte ofreciendo servicios de asesoría para apoyar a las entidades que quiera aplicar a la certificación y otras fuentes digitales y libros para conceptos generales utilizados en el desarrollo de este trabajo de grado.

RECOMENDACIONES

Después de entender el proceso para que un Comerciante obtenga la Certificación PCI DSS, es más que justificable y recomendable la automatización de los formularios que actualmente sirven como guía y herramienta para determinar el nivel de madurez del comercio aplicante.

De acuerdo con nuestra propuesta, la automatización del proceso debe iniciar con permitir que el Comercio identifique su escenario operativo, para que la herramienta le permita acceder al formulario que le corresponde según la imagen que compartimos a continuación:

Figura 4.15

Asociación del formulario con el comercio según su escenario operativo

1	**SAQ A**	Comerciantes con tarjetas ausentes, todas las funciones que impliquen el manejo de datos del titular de la tarjeta totalmente tercerizadas
2	**SAQ A-EP**	Comerciantes dedicados al comercio electrónico parcialmente tercerizados que emplean un sitio web externo para el procesamiento de pagos
3	**SAQ B**	Comerciantes con validadoras manuales o terminales independientes con discado externo solamente. Sin almacenamiento electrónico de los datos de los titulares de tarjetas
4	**SAQ B-IP**	Comerciantes con terminales de punto de interacción (POI) aprobados por PTS con conexión IP. Sin almacenamiento electrónico de los datos de los titulares de tarjetas
5	**SAQ C-VT**	Comerciantes con terminales de pago virtuales basadas en la Web – Sin almacenamiento electrónico de datos de titulares de tarjetas
6	**SAQ C**	Comerciantes con sistemas de aplicación de pago conectado a Internet – Sin almacenamiento electrónico de los datos del titular de la tarjeta
7	**SAQ P2PE**	Comerciantes que usan terminales de pago de hardware en una solución únicamente P2PE publicada por la PCI SSC. Sin almacenamiento electrónico de datos de los titulares de tarjetas
8	**SAQ D - Comerciantes**	Todos los demás comerciantes elegibles para el SAQ
9	**SAQ D - Proveedores de servicios**	Proveedores de servicio elegibles para el SAQ

- Implementar la solución con el apoyo de un equipo de trabajo con experiencia en desarrollo web (preferiblemente con gran experiencia en JavaScript), con experiencia en desarrollo de Web Responsive.
- Almacenar la solución en un servidor confiable, que este activo en todo momento y que el alojamiento de información sea seguro, para esto se recomiendo Azure o AWS.
- Se requiere la creación de guías, y tutoriales donde se den explicaciones y demostraciones de manera sencilla sobre el uso de la guía de Autodiagnóstico PCI DSS.

BIBLIOGRAFÍA

1. Acosta, D. (2020, 19 agosto). ¿Qué es PCI DSS? PCI Hispano. https://www.pcihispano.com/que-es-pci-dss/

2. Dahn, M. (2020). Guía para cumplir con la normativa PCI. Stripe. https://stripe.com/es-us/guides/pci-compliance

3. Guijarro, H. (2018, 15 julio). Tarjetas bancarias: los 12 requisitos PCI DSS. IT Governance Blog ES. https://www.itgovernance.eu/blog/es/tarjetas-bancarias-los-12-requisitos-pci-dss

4. Internet Security Auditors. (2019). Auditoría de Certificación del Cumplimiento de PCI DSS | Internet Security Auditors. isecauditors. https://www.isecauditors.com/auditoria-certificacion-cumplimiento-pcidss

5. Internet Security Auditors. (2020a). Análisis de cumplimiento de PCI DSS | Internet Security Auditors. isecauditors. https://www.isecauditors.com/analisis-cumplimiento-y-plan-accion

6. Internet Security Auditors. (2020b). Implantación Requerimientos de PCI DSS | Internet Security Auditors. isecauditors. https://www.isecauditors.com/implantacion-requerimientos-para-adecuacion-pcidss

7. Internet Security Auditors. (2021). Adecuación y Certificación PCI DSS | Internet Security Auditors. isecauditors. https://www.isecauditors.com/implantacion-pci-dss

8. Morrison, I. H. (2016, 16 junio). Ciberseguridad es carga pesada para los bancos de RD. Audiencia Electrónica. https://www.audienciaelectronica.net/noticias-de-republica-dominicana/ciberseguridad-es-carga-pesada-para-los-bancos-de-rd

9. Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. (2021, 1 enero). PCI Security Standards Council. https://www.pcisecuritystandards.org/

10. Oswal, P. (2020, 26 noviembre). What are the 12 requirements of PCI DSS Compliance? ControlCase. https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/

11. PCI Security Standards Council. (2013, noviembre). Requisitos y procedimientos de evaluación de seguridad (Versión 3.0). https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

12. PCI Security Standards Council. (2017, mayo). Guidance for PCI DSS Scoping and Network Segmentation (Version 1.1). pcisecuritystandards. https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf

13. PCI Security Standards Council. (2018, mayo). Requirements and Security Assessment Procedures (Version 3.2.1). https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

14. PCI Security Standards Council, LLC. (2016a, mayo). El Enfoque Prioritario para Lograr el Cumplimiento de la PCI DSS (Version 3.2). https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.esla.pdf

15. PCI Security Standards Council LLC. (2016, mayo). El Enfoque Prioritario para Lograr el Cumplimientode la PCI DSS (Version 3.2).

https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2_3.esla.pdf

16. PCI Security Standards Council, LLC. (2016b, mayo). The Prioritized Approach to Pursue PCI DSS Compliance (Version 3.2). https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf?agreement=true&time=1469037392985#:~:text=What%20Is%20the%20Prioritized%20Approach%3F&text=The%20Prioritized%20Approach%20provides%20a,and%2For%20transmitting%20cardholder%20data

17. PCI Security Standards Council, LLC. (2018). Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. Pcisecuritystandards. https://www.pcisecuritystandards.org/document_library

18. PCI Security Standards Council, LLC. (2020, octubre). Card Production and Provisioning Security Requirements (Version 2.0). https://www.pcisecuritystandards.org/documents/Card_Prod_Security_Rqrmts_FAQs_v2_Oct_2020.pdf?agreement=true&time=1617243799558

19. PCI Security Standards Council, LLC. (2021). Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. Assessing the Security of Your Cardholder Data. https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

20. ¿Qué es una entidad adquirente? (2021). Support Site - ePayments. https://epayments-support.ingenico.com/es/direct/faq/-qu-es-una-entidad-adquirente

21. RAE. (2020). Cifrado. En Diccionario de la lengua española. https://dle.rae.es/cifrar

22. Gobierno de Mexico. (2016, 25 octubre). Emisoras. cnbv. https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/BURS%C3%81TIL/Descripci%C3%B3n/Paginas/Emisoras.aspx

23. RAE. (2020). Ocultamiento. En Diccionario de la lengua española. https://dle.rae.es/ocultar

24. Spivak, M. (2008). Calculus. Publish or Perish, Inc.

25. Donohue, B. (2021, 11 marzo). ¿Qué Es Un Hash Y Cómo Funciona? Blog oficial de Kaspersky. https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

26. Fernández, Y. (2020, 2 junio). Malware: qué es, qué tipos hay y cómo evitarlos. Xataka. https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos

27. Verizon. (s. f.). What is Antivirus - Definition, Meaning & Explanation. Verizon Fios. https://espanol.verizon.com/info/definitions/antivirus/

28. Proffitt, B. (2016). Introducing Ubuntu. Thomson Course Technology.

29. PCI Security Standards Council, LLC. (s. f.). Official PCI Security Standards Council Site - Verify PCI Compliance, Credit Card Security Standards. https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

30. Sampieri, R. H., Collado, C. F., Lucio, P. B., Valencia, S. M., & Torres, C. P. M. (2014). Metodología de la investigación. McGraw-Hill Education.

31. Caceres, G. L. J. (2016). Tecnicas De Investigacion En Sociedad Cultura Y Comunicacion (1.a ed.). ADDISON WESLEY LONGMAN/PEARSON.

32. 7Graus. (2019). Método deductivo. En Significados.com

33. etecé. (2020). Método analítico. En concepto.de. https://concepto.de/metodo-analitico/

ANEXOS

Anexo 1. Anteproyecto

Decanato de Ingenierías e Informática

Escuela de Informática

Anteproyecto para trabajo de grado

Título:

Propuesta de un Autodiagnóstico del Nivel de Madurez para lograr el Cumplimiento PCI DSS Enero – Abril 2021.

Sustentantes:

Diana Joa	2017-0983
Yasser Antonio Jorge	2017-1036

Asesor:

Ing. Patricia Cao

Santo Domingo, D.N.

República Dominicana Noviembre, 2020

ÍNDICE DE CONTENIDO

TÍTULO:

Propuesta de un Autodiagnóstico del Nivel de Madurez para lograr el

Cumplimiento PCI DSS Enero - Abril 2021

INTRODUCCIÓN

Las empresas del sector financiero cada día deben renovarse y hacerse más segura, en vista de que cada día son más las vulnerabilidades que están siendo explotadas por malhechores que buscan siempre aprovecharse de la debilidad de las empresas. Hoy en día se les hace difícil contratar un servicio externo para confiarle sus datos confidenciales, debido a esto muchas veces al no tener ni contratar una empresa que ofrezca estos servicios, se quedan abiertas muchas brechas que hacen las transacciones inseguras.

La entidades financieras certificadas PCI DSS aportan a la reducción de los fraudes causados con tarjeta de crédito lo que contribuyen en gran manera a proteger tanto como los datos de los consumidores así como la reputación de las entidades certificadas.

1. JUSTIFICACIÓN

La presente investigación tiene como objetivo plantear una guía que sirva como referencia para aquellas entidades que necesiten o deseen autodiagnosticarse para aplicar a la certificación PCI-DSS.

Debido a la pandemia actual en la que vivimos, ocasionada por el virus COVID-19, hemos sido testigo de cómo muchos negocios han pasado a convertirse en negocios virtuales, lo que es igual a más personas realizando transacciones utilizando tarjetas de crédito. Este crecimiento aumenta la probabilidad de que se lleven a cabo fraudes de tarjetas de crédito y uno de tantos métodos utilizados para prevenir esto, es certificarse como entidad que cumple con los lineamientos PCI-DSS.

Una guía que permita a las entidades pertinentes autodiagnosticarse para determinar su nivel de madurez para aplicar a la certificación PCI-DSS abre paso a que más entidades se preparen, apliquen y se certifiquen, reduciendo así los casos de fraudes atados a las transacciones con tarjetas de crédito e incrementando la seguridad de los datos utilizados para estas transacciones.

2. DELIMITACIÓN DEL TEMA Y PLANTEAMIENTO DEL PROBLEMA

2.1. Delimitación del tema

La guía propuesta podrá ser utilizada por cualquier entidad que de servicio de autorización electrónica, que transmita, procese o almacene datos de tarjetas de crédito o débito. Esta será desarrollada durante el periodo Enero-Abril del año 2021.

2.2. Planteamiento del problema

Diariamente se realizan millones de transacciones con tarjetas de crédito, ya sean compras por internet, retiros de dinero de cajeros automáticos, pagos realizados con estas, vía telefónica, entre otras formas de uso. Solamente en República Dominicana de Enero 2018 a Septiembre 2020, en promedio, se realizaron 3 millones de transacciones mensuales (Banco Central de la República Dominicana, 2020).

Debido a esto, se hace necesario que las entidades bancarias o de servicios que emiten y gestionan las transacciones hechas con tarjetas de crédito, demuestren estar en cumplimiento con normas de seguridad que avale la privacidad y buen manejo de los datos que los tarjetahabientes esperan recibir al momento de utilizar este instrumento financiero.

Es por esto que decidimos desarrollar una Propuesta de un Autodiagnóstico del Nivel de Madurez para lograr el Cumplimiento PCI DSS, con el objetivo de que las entidades de servicios que transmitan, procesen o almacenen datos de tarjetas

de crédito o débito puedan utilizarla para certificarse y así reducir la cantidad de fraudes a través de las mismas.

2.3. Formulación del problema

¿A qué se deben las vulnerabilidades que presentan las transacciones realizadas a través de medios electrónicos de pago?

2.4. Sistematización del problema

- ¿El problema recae en la falta de información disponible?
- ¿Se debe a la dificultad para acceder a esa información?
- ¿Se debe a la falta de una guía para corregir las vulnerabilidades?

3. OBJETIVOS DE LA INVESTIGACIÓN

3.1. Objetivo general

Realizar una guía de Autodiagnóstico para determinar el Nivel de Madurez con el fin de lograr el Cumplimiento PCI DSS. Esta guía se desarrollará desde el Distrito Nacional durante el periodo Enero-Abril 2021.

3.2. Objetivos específicos

1. Determinar el nivel de madurez que requiere una entidad de servicios para realizar transacciones electrónicas.
2. Identificar las vulnerabilidades de mayor impacto de cara al usuario.

3. Analizar el riesgo que corren los usuarios cuando existen vulnerabilidades en el proceso de transmisión, procesamiento o almacenamiento de datos de tarjetas de crédito o débito.
4. Analizar los requisitos y el nivel de madurez que se necesita para cumplir con el estándar PCI DSS.
5. Determinar el riesgo de no cumplir con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI).
6. Diseñar una guía básica para autodeterminar el nivel de madurez para el cumplimiento de las normas PCI DSS.

4. MARCO TEÓRICO REFERENCIAL

4.1. Marco teórico

La seguridad informática es un campo que requiere de inversión, ya que un descuido podría ser hasta 100 veces más costoso que la inversión a realizar en seguridad. **Rosario Sang, presidenta de la Cámara Dominicana de las Tecnologías de la Información y la Comunicación (Cámara TIC)**, empresaria del sector financiero en una conferencia de la **OEA en el 2016** expresó lo siguiente: *"La seguridad de la información es una de las preocupaciones de mayor peso en el empresariado en general, ahora bien, las altas finanzas, sector que durante los últimos años ha mejorado sus niveles de eficiente por medio de las nuevas tecnologías, es sensible a las vulnerabilidades, porque de esto depende en parte la*

confianza de los usuarios, la satisfacción de sus clientes y su rentabilidad, sin contar con el efecto que tiene la ciberseguridad en los costos de los servicios financieros."

"Las entidades financieras invierten al menos el 4% de la cifra de sus gastos totales en mantener fortalecidas sus estructuras de seguridad informática, puesto que flagelos como el "phishing" o robo de identidad digital comprenden las principales amenazas que enfrentan de cara a garantizar el patrimonio de sus clientes y sostener la rentabilidad." **(Carlos Guisarre, 2016).** Vemos que los bancos sienten interés en fortalecer la estructura de seguridad en su empresa, ya que de ella depende la confianza que brinda a sus clientes.

En el artículo 2 del decreto 230-18 realizado en el mandato del Sr. Danilo Medina: *"La Estrategia Nacional de Ciberseguridad 2018-2021 tiene como misión establecer los mecanismo de ciberseguridad adecuados para la protección del Estado, sus habitantes y, en general, del desarrollo y la seguridad nacional."* Es notable el interés del gobierno en brindar apoyo para fomentar la seguridad informática.

Según **Walter Cervoni, Chief Technology Officer de GM Sectec(2020)** *"El PCI DSS consta de pasos de sentido común que coinciden con las mejores prácticas de seguridad de datos ampliamente aceptadas. Los objetivos de los estándares PCI DSS son ayudar a los comerciantes a procesar de forma segura las transacciones con tarjeta de crédito y prevenir el fraude.*"

"Los comercios al no ser compatible con PCI podrían exponer sus sistemas a un robo de datos. En 2019, el costo promedio por robo de datos en los EE. UU. Superó los 8 millones de dólares. Para la mayoría de las pequeñas empresas, eso significa cerrar las puertas. También hay multas por parte de las marcas de tarjetas

que en los Estados Unidos pueden alcanzar los 100,000 dólares por incidente. El monto de la multa depende del volumen de transacciones de una empresa, la cantidad de requisitos de PCI DSS robados y otros factores." según un informe de IBM (2019).

Según **Visa, multinacional de servicios financieros(2020)** *"En el primer trimestre de 2020 más de 13 millones de sus tarjetahabientes realizaron una transacción de comercio electrónico por primera vez. En las primeras semanas de la cuarentena en Latinoamérica, dos de cada 10 usuarios de la tarjeta de crédito realizaron compras en línea por primera vez."*

"Las principales debilidades que se reportan en el 2019 Payment Security Report atañen a la efectividad de las tecnologías de protección de los datos ante vulnerabilidades y ataques del exterior en los sistemas críticos de las empresas (Requisito 6 del estándar); así como en el cumplimiento de programas continuos de evaluación de los procesos de gestión de datos", informa **Alberto España, Vicepresidente Senior de GM Security Technologies.**

"*Estamos convencidos de que la manera más eficaz de mejorar la postura de seguridad general en los sistemas de pago, es continuar evangelizando sobre la importancia del cumplimiento de los PCI-DSS y asesorando a los comerciantes*", destaca **Alberto España, Vicepresidente Senior de GMST.**

4.2. Marco conceptual

- **PCI-DSS:** Los estándares de seguridad PCI son requerimientos técnicos y operativos establecidos por el Consejo de Normas de Seguridad de Tarjetas

de Pago para proteger datos del titular de la tarjeta**.** (*Payment Card Industry Security Standards*, 2008).

- **Nivel de madurez:** Un nivel de madurez es una meseta evolutiva bien definida que establece un nivel de capacidad para mejorar; cada nivel de madurez específica ciertas características para los procesos, niveles de madurez más altos implican características más avanzadas y es un paso hacia el logro de un proceso maduro, proporcionando un conjunto de metas que, cuando se cumplen, coloca a una organización en el siguiente nivel de madurez.(Cruz-Cunha et al., 2013, pp. 1–3).
- **Pandemia:** Se llama pandemia a la propagación mundial de una nueva enfermedad. (World Health Organization, 2013)
- **Ciberseguridad:** La ciberseguridad se define como una capa de protección para los archivos de información, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo. Lanz, L. (2020, 27 mayo)
- **COVID-19:** es la enfermedad infecciosa causada por el coronavirus que se ha descubierto más recientemente. (*Preguntas y respuestas sobre la enfermedad por coronavirus (COVID-19)*, 2020).
- **Coronavirus:** Los coronavirus son una extensa familia de virus que pueden causar enfermedades tanto en animales como en humanos. En los humanos, se sabe que varios coronavirus causan infecciones respiratorias que pueden ir desde el resfriado común hasta enfermedades más graves como el

síndrome respiratorio de Oriente Medio (MERS) y el síndrome respiratorio agudo severo (SRAS). (*Preguntas y respuestas sobre la enfermedad por coronavirus (COVID-19)*, 2020).

4.3. Marco Espacial

Esta investigación será realizada en el Distrito Nacional, República Dominicana.

4.4. Marco Temporal

Una vez expuesto el tema "Propuesta de un Autodiagnóstico del Nivel de Madurez para lograr el Cumplimiento PCI DSS Enero-Abril 2021", se debe definir el tiempo donde se enmarca la investigación propuesta, la cual tendrá duración de cuatro meses en el periodo Enero-Abril del 2020.

5. HIPÓTESIS

5.1. Primer Grado

- Las entidades financieras o de servicios emisoras o procesadoras de pagos electrónicos a través de tarjetas de crédito o débito, no cuentan con un guía que les permita diagnosticar su nivel de madurez para lograr el cumplimiento PCI DSS.

5.2. Segundo Grado

- Las entidades financieras o de servicios emisoras o procesadoras de pagos electrónicos a través de tarjeta de crédito o débito, no cuentan con una guía que les permita saber si cumple con los parámetros de seguridad definidos por PCI DSS, debido a esto no pueden determinar el grado de seguridad de sus transacciones.

6. DISEÑO METODOLÓGICO

6.1. Tipos de Investigación

6.1.1. Investigación exploratoria

Su finalidad es identificar cuáles son los puntos más importantes a tratar, para a partir de estos, desarrollar el tema de investigación.

6.1.2. Investigación descriptiva

Su finalidad es describir la situación o fenómenos que están involucrados en el campo de estudio. En este tipo de investigación más que describir el "¿por qué?" se busca describir otras cuestionantes como el "¿qué?", "¿cómo?", "¿cuándo?" y "¿dónde?".

6.1.3. Investigación explicativa

Su finalidad es definir el "¿por qué?" y el "¿para qué?" del objeto de estudio, con el fin de ampliar los resultados obtenidos de la investigación descriptiva y

exploratoria. En nuestro caso, utilizaremos esta investigación para determinar y definir el "¿por qué?" y el "¿para qué?" Es necesario contar con la certificación PCI DSS, la que a groso modo busca reducir y erradicar los fraudes a través de tarjetas de crédito o débito.

6.2. Métodos de Investigación

6.2.1. Observación

Se utilizará para identificar los conflictos que puede ocasionar la falta de aplicación de las normas de la PCI, con la finalidad de crear una guía para saber que le hace falta tener a la empresa para poder cumplir con las normas PCI DSS.

6.2.2. Deductivo

Se utilizará este método porque este comienza analizando el problema general, que es la seguridad por la cuales se efectúan las transacciones a travès de las plataformas tecnológicas, para poder determinar cual es el grado de vulnerabilidad de cada transacción.

6.2.3. Analítico-Sintético

Utilizando este método, se procede a descomponer el objeto de estudio con la finalidad de analizarlos por separado de manera individual y luego hacer una integración donde se analice el todo como conjunto.

6.3. Técnicas de investigación

Para el desarrollo de la tesis se pretende realizar entrevistas y encuestas a las autoridades y personal encargado de ser auditado por las entidades certificadoras PCI DSS y a los que auditan para aprobar la emisión de esta, con el fin de escuchar y plasmar ambas caras de la moneda.

7. FUENTES DE DOCUMENTACIÓN

7.1.1. Fuentes primarias

Se tomarán los resultados de encuestas realizadas a los distintos tipos de empresas del sector bancario y entidades de servicio, dentro del Distrito Nacional como fuente primaria de información.

7.2. Fuentes secundarias

Se realizarán investigaciones en los portales web de las instituciones principales del Distrito Nacional relacionadas al sector bancario y entidades de servicios relacionados. Así como también se emplearán el uso de libros y artículos referentes a las normas PCI DSS.

7.3. Bibliografías

- *Instrumentos de Pago*. (2020). Banco Central de la República Dominicana. https://www.bancentral.gov.do/a/d/2659-instrumentos-de-pago

- Calle, Z. A. (2015). *Análisis de la implementación del estándar PCI-DSS*. https://dspace.ups.edu.ec/bitstream/123456789/10317/1/UPS-GT001222.pdf

- BERNABÉ, M. A. (2018). *ANALISIS DE LAS NORMAS PCI DSS*. http://repositorio.ug.edu.ec/bitstream/redug/10036/1/PTG-703%20Bernab%C3%A9%20Baldano%20Manuel%20Alonso.pdf

- Calderon, S. D. (2020). *GUÍA PARA EL CUMPLIMIENTO DEL ESTÁNDAR PCI DSS V3.2.1* https://repository.unad.edu.co/bitstream/handle/10596/34365/sdcalderonr.pdf?sequence=1

- Gómez, I. P. (2016). *Norma de Seguridad PCI*. https://riunet.upv.es/bitstream/handle/10251/71379/P%C3%89REZ%20-%20Implementaci%C3%B3n%20de%20la%20norma%20de%20seguridad%20PCI-DSS%20versi%C3%B3n%203.0%20sobre%20aplicaci%C3%B3n%20web%20ASP.NET%20....pdf?sequence=2&isAllowed=y.

- Acosta, D. (2018, 2 octubre). *Vulnerabilidades*. PCI Hispano. https://www.pcihispano.com/cual-es-la-diferencia-entre-un-escaneo-de-vulnerabilidades-req-11-2-una-prueba-de-penetracion-req-11-3-y-un-analisis-de-vulnerabilidades-de-aplicacion-web-req-6-6-en-pci-dss/

- *Decreto-230-18*. (2018). https://indotel.gob.do/media/10605/decreto-230-18.pdf
- Normas de Seguridad de Datos(2018) https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf
- Guia de Normativa PCI(2020) https://stripe.com/es-us/guides/pci-compliance
- Visa - DSS de PCI(2019) https://www.visa.com.do/asociandose-con-nosotros/pci-dss-compliance-information.html
- Nuevo Estándar PCI DSS 4.0(2020) https://www.diariodigital.com.do/2020/02/13/empresas-comienzan-el-2020-preparandose-para-el-nuevo-estandar-pci-dss-4-0.html
- *Requerimientos DSS*. (2018). https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1604268991080
- Términos y Acronyms PCI. (2019). https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf?agreement=true&time=1604268991651

8. ESQUEMA PRELIMINAR DEL TRABAJO DE GRADO

Portada

Dedicatoria

Agradecimientos

Introducción

Capítulo I. Aspectos Generales del PCI DSS (Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago)

Introducción

1.1 Historia y origen de PCI DSS

1.2 Roles y responsabilidades en el cumplimiento con PCI DSS

1.3 Alcance de cumplimiento de PCI DSS

1.4 Descripción de los controles de seguridad de PCI DSS

1.5 Criterio de evaluación de PCI DSS

Resumen Capítulo I

Capítulo II. Análisis de entidades certificadas y aplicantes para certificación PCI DSS

Introducción

2.1 Levantamiento de proceso agotado por entidades certificadas PCI DSS

2.2 Levantamiento de proceso actual que están agotando entidades aplicantes para obtener certificación PCI DSS

2.3 Casos de estudios de certificaciones similares a la PCI DSS

Resumen Capítulo II

Capítulo III. Diseño Metodológico.

Introducción

3.1 Tipo de Investigación

3.2 Diseño de la Investigación

3.3 Enfoque de la Investigación