UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

SISTEMA DE PAGOS BASADO EN EL ESTÁNDAR ISO 8583 Y NORMAS PCI DSS UTILIZANDO LECTORES DE BANDA MAGNÉTICA DESAROLLADO EN JAVA.

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

AUTOR: CARLOS TEODORO SOLIS REYES

TUTOR: ING. ANTONIO RODRÍGUEZ

GUAYAQUIL – ECUADOR

2013

Presidencia de la República del Ecuador / Plan Nacional de Ciencia, Tecnología, Innovación y Saberes / SENESCYT Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación		
REPOSITORIO NACIONAL EN CIENCIAS Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS		
TÍTULO "Sistema de pagos basado en el estándar ISO 8583 y normas PCI DSS utilizando lectores de banda magnética desarrollado en java"		
	REVISORES:	
INSTITUCIÓN: **Universidad De Guayaquil**	**FACULTAD: Ciencias Matemáticas Y Físicas**	
CARRERA: Ingeniería En Sistemas Computacionales		
FECHA DE PUBLICACIÓN: **10 de Julio del 2013**	**N° DE PÁGS.: 130**	
ÁREA TEMÁTICA: Financiera		
PALABRAS CLAVES: ***Sistema de Pagos***		
RESUMEN: Sistema Alterno de Pagos que permita aumentar la disponibilidad para realizar transacciones con tarjetas de crédito en establecimientos comerciales.		
N° DE REGISTRO(en base de datos):	**N° DE CLASIFICACIÓN: Nº**	
DIRECCIÓN URL (tesis en la web):		
ADJUNTO PDF	**SI** [X]	**NO** [ ]
CONTACTO CON AUTOR: SOLIS REYES CARLOS TEODORO	**Teléfono: 0987834424**	**E-mail: c_solis2@hotmail.com**
CONTACTO DE LA INSTITUCIÓN	**Nombre:**	
	Teléfono:	

Guayaquil, 10 de Julio de 2013

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, "SISTEMA DE PAGOS BASADO EN EL ESTÁNDAR ISO 8583 Y NORMAS PCI DSS UTILIZANDO LECTORES DE BANDA MAGNÉTICA DESAROLLADO EN JAVA. "elaborado por el Sr. SOLIS REYES CARLOS TEODORO, egresado de la Carrera de Ingeniería en Sistemas Computacionales, Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Sistemas, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

Atentamente

_____

Ing. Antonio Rodríguez

TUTOR

DEDICATORIA

La culminación de mi preparación universitaria va dedicada con gran amor a mis padres Carlos Solis Flores y María Reyes Choez, a mis queridos hermanos Omar y Leonel y a mi novia Lissette.

AGRADECIMIENTO

Quiero empezar agradeciendo a Dios, por darme la sabiduría necesaria en el transcurso de mi vida, a mis padres por ser siempre una guía y fuente de inspiración, a la Facultad de Ciencias Matemáticas y Físicas la cual me abrió las puertas y me brindo todo el conocimiento necesario para desarrollarme como profesional y persona.

A mis amigos, compañeros y maestros los cuales siempre estuvieron prestos a brindarme su apoyo y conocimiento, al Ing. Antonio Rodríguez, persona de muy buena y amplia preparación académica, por su valiosa dirección en esta tesis.

TRIBUNAL DE GRADO

Ing. Fernando Abad Montero
DECANO DE LA FACULTAD
CIENCIAS MATEMÁTICAS Y FÍSICAS

Ing. Julio César Castro Rosado
DIRECTOR

Ing. Antonio Rodríguez
TUTOR

Ing. Gary Reyes
PROFESOR DEL ÁREA - TRIBUNAL

Ab. Juan Chávez Atocha
SECRETARIO

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

SISTEMA DE PAGOS BASADO EN EL ESTÁNDAR ISO 8583 Y NORMAS PCI DSS UTILIZANDO LECTORES DE BANDA MAGNÉTICA DESAROLLADO EN JAVA.

Proyecto de trabajo de grado que se presenta como requisito para optar por el título de

INGENIERO EN SISTEMAS COMPUTACIONALES.

Autor: Carlos Teodoro Solis Reyes

C.I. 0925655177

Tutor: Ing. Antonio Rodríguez

Guayaquil, Julio de 2013

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del Curso de Fin de Carrera, nombrado por el Departamento de Graduación y la Dirección de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil.

CERTIFICO:

Que he analizado el Proyecto de Grado presentado por el egresado CARLOS TEODORO SOLIS REYES, como requisito previo para optar por el título de Ingeniero cuyo problema es:

SISTEMA DE PAGOS BASADO EN EL ESTÁNDAR ISO 8583 Y NORMAS PCI DSS UTILIZANDO LECTORES DE BANDA MAGNÉTICA DESAROLLADO EN JAVA.

Considero aprobado el trabajo en su totalidad.

Presentado por:

_____ _____

Solis Reyes Carlos Teodoro Cédula de ciudadanía N°

Tutor: _____

Ing. Antonio Rodríguez

Guayaquil, Julio de 2013

ÍNDICE GENERAL

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

SISTEMA DE PAGOS BASADO EN EL ESTÁNDAR ISO 8583

Y NORMAS PCI DSS UTILIZANDO LECTORES

DE BANDA MAGNÉTICA

DESAROLLADO

EN JAVA.

RESUMEN

Sistema desarrollado en Java basado en el estándar para transacciones financieras ISO 8583 y en las normas de seguridad de datos PCI DSS, este sistema está orientado al sector comercial Y financiero proporcionando un medio seguro para realizar transacciones con tarjetas de crédito utilizando lectores de banda magnética. En este sistema podremos encontrar un módulo de parametrizacion que permitirá que la aplicación se adapte a las necesidades del lugar donde será instalada, pudiéndose configurar desde el mensaje que aparecerá impreso en el voucher hasta las tarjetas de crédito que serán aceptadas. Finalmente esta aplicación contribuirá aumentando la disponibilidad para realizar transacciones con tarjetas de crédito usando fuertes mecanismos de seguridad y algoritmos de encriptación para transmitir la información confidencial.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

SISTEMA DE PAGOS BASADO EN EL ESTÁNDAR ISO 8583

Y NORMAS PCI DSS UTILIZANDO LECTORES

DE BANDA MAGNÉTICA

DESAROLLADO

EN JAVA.

ABSTRACT

System developed in Java based on standard ISO 8583 for financial transactions and standards security data PCI DSS, this system is geared to the commercial sector and providing a safe business for credit card transactions using magnetic stripe readers. In this system we can find a parameterization module to allow the application can suit the needs of the place where it will be installed, and can be configured the message that is printed on the voucher and to credit cards will be accepted. Finally, this application will help increase the availability to perform credit card transactions using strong security mechanisms and encryption algorithms to transmit confidential information.

INTRODUCCIÓN

Décadas atrás con la aparición de las tarjetas de crédito se pretendía remplazar los cheques y el efectivo con el fin de convertirse este medio en el primer sistema de pagos global del consumidor.

Con la masificación de las tarjetas de crédito, surge la necesidad de sistemas que puedan procesar dichos requerimientos; la tendencia actual son los POS (Point of sale), estos dispositivos son capaces de leer la información de banda magnética de las tarjetas de crédito, procesarla y realizar transacciones, habiendo uno en casi cualquier establecimiento comercial que desee recibir pagos a través de este medio.

Los POS se han constituido en los principales dispositivos para procesamiento de transacciones de tarjeta presente en los establecimientos comerciales, dichos dispositivos utilizan distintos medios de comunicación ya sean LAN, GPRS, DIAL.

El presente proyecto se basa en la necesidad de contar con un sistema de pagos alterno que garanticé que los establecimientos comerciales continúen transacciónando y recibiendo pagos por medio de tarjetas de crédito en caso de que los Sistemas tradicionales de cobro o sus distintas tecnologías asociadas fallen en el momento que se está realizando la transacción.

CAPÍTULO I

EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

UBICACIÓN DEL PROBLEMA EN UN CONTEXTO

Actualmente en el Ecuador contamos con muchas facilidades para realizar compras con tarjetas de crédito en establecimientos comerciales, sin embargo, No existen sistemas alternos de pagos ante fallas que ocurran en los sistemas tradicionales, ocasionando que su actividad normal también se vea afectada, llegando a producir pérdidas económicas, malestar en los clientes e incluso afectar la imagen comercial de los establecimientos.

El presente proyecto busca proporcionar medios alternativos que garanticen la continuidad de las labores comerciales en caso de fallos de los sistemas tradicionales.

De acuerdo con las cifras de la Superintendencia de Bancos y Seguros, la cantidad de Tarjetas de Crédito durante el 2011, hasta octubre, fue de 22.13 millones; número que refleja un incremento del 12.7% en relación al mismo periodo del año inmediato anterior (2010); variación que presenta un crecimiento sostenido, ya que su tendencia ratifica que el año pasado, hasta el décimo mes, supera en promedio el 10% mensual (18)

SITUACIÓN CONFLICTO QUE DEBO SEÑALAR.

Hoy en día las redes de comercios en el Ecuador han crecido considerablemente aumentando el número de transacciones diarias que se realizan utilizando distintos medios de pagos, entre ellos, las tarjetas de créditos.

Las principales redes de pagos del Ecuador ofrecen Los POS para llevar a cabo todas están transacciones, sin embargo actualmente no se cuenta con sistemas alternos que le garanticen a los establecimientos comerciales que podrán seguir con sus actividades normales en caso de que estos dispositivos fallen.

CAUSAS Y CONSECUENCIAS

CAUSAS

- Intermitencias en el sistema telefónico
- Fallas en las redes GPRS
- Necesidad de realizar trabajos de mantenimiento en los sistemas tradicionales.
- Actualización de software en los dispositivos
- Poco interés en contar con sistemas de contingencia para pagos
- Fallas de hardware de los POS
- Desprogramación de los POS

- Problemas con la red WIFI de los equipos conectados.
- Falta de propuestas por parte de las empresas para brindar sistemas de pago a nivel Origen.
- Aumento de número de pagos que se hacen con tarjetas de crédito.
- La inseguridad que proporciona poseer dinero físico.

CONSECUENCIAS

- Incapacidad de funcionar de los POS Dial
- Incapacidad de funcionar de los POS Gprs
- Detención de las actividades comerciales
- Pérdida de clientes
- Perdidas económicas para el comercio
- Degradación de la imagen comercial del establecimiento
- Perdidas económicas para el banco y para el procesador de transacciones
- Aglomeración de personas en los establecimientos comerciales
- Malestar en los clientes
- Aumento del personal técnico necesario en caso de falla de los POS
- Aumento del tiempo necesario durante las actualizaciones de los POS

DELIMITACIÓN DEL PROBLEMA

Campo: Financiero

Área: Transacciones Financieras Electrónicas

Aspecto: Tecnológico

Tema: Sistema de pagos basado en el estándar iso 8583 y normas pci dss utilizando lectores de banda magnética desarrollado en java.

Problema: En la actualidad son pocas las empresas que brindan sistemas transaccionales a nivel origen para puntos de venta, es por esta razón que el presente proyecto busca aumentar la eficiencia de los sistemas vigentes.

Hoy en día existen pocos mecanismos para realizar cobros/pagos en los puntos de venta, el presente permitirá al usuario tener un mayor nivel de confianza, al saber que cuenta con los mecanismos necesarios para realizar sus comprar de manera segura, fácil, rápida y con una alta disponibilidad.

Delimitación Espacial: Sistema aplicado a un campo Financiero, para establecimientos que realizan transacciones con tarjetas de crédito.

Delimitación Temporal: 6 Meses (Investigación y Desarroll**o).**

FORMULACIÓN DEL PROBLEMA

El poco desarrollo e implementación de servicios orientados a aumentar la disponibilidad para realizar transacciones con tarjetas de crédito en los puntos de venta; la existencia de sistemas que no brindan una disponibilidad alta para cubrir el creciente aumento de transacciones que se realizan con tarjetas de crédito.

Con el aumento de las emisiones de tarjetas de crédito en el Ecuador y la llegada de nuevas, y el poco aumento de sistemas para procesarlas en punto de venta, sumado a la poca importancia que le dan las empresas a brindar soluciones alternas a los sistemas actuales ocasiones perdidas económicas para los comercios, procesadores de tarjetas de crédito y las instituciones financieras.

EVALUACIÓN DEL PROBLEMA

Delimitado: Sistema orientado al procesamiento de transacciones con tarjetas de crédito en establecimientos comérciales, brindándole redundancia para los sistemas actuales, ya que hoy en día son muy pocos los servicios brindados para este tipo de problemáticas. Para el desarrollo de esta herramienta se plantea un tiempo de 6 meses de desarrollo e investigación.

Claro: Se ha redactado el planteamiento del problema y se lo ha ubicado en un contexto de una manera clara y precisa tanto en delimitaciones, objetivos y alcances, teniendo como resultado el fácil entendimiento del mismo. Este sistema está basado en estándares de la industria de procesamientos de tarjetas de crédito, y normas PCI DSS, desarrollado en plataforma gratuita, orientado a procesar transacciones en los puntos de venta, convirtiéndose en una alternativa segura, fácil de usar y sencilla a los sistemas actualmente usados.

Evidente: En nuestro país es muy notorio que la mayoría de transacciones realizadas con tarjetas de crédito se realizan por medio de POS, y que cuando estos fallan es imposible continuar con la actividad comercial produciendo perdidas económicas para todas las partes afectas y degradación de la imagen comercial

Original: Actualmente las redes de comercios del Ecuador no cuentan con sistemas de contingencia para realizar cobros con tarjetas de crédito, lo que hace de este sistema una alternativa viable y fácil de usar cuando se presentan inconvenientes con los sistemas actuales.

Factible: El problema planteado claro y conciso desde un inicio, realizando las investigaciones adecuadas y extrayendo las ideas principales, hacen que se tengan los objetivos claros de lo que se desea desarrollar e implementar, la delimitación

temporal (6 meses) propuesta para la solución de este problema es totalmente acorde a los recursos disponibles, además se desarrollara bajo plataformas open source, obteniendo como resultado un bajo presupuesto.

Variables: Al estar redactado de una manera clara y teniendo un problema evidente, se puede apreciar las variables con total claridad y rapidez; como es un medio alterno para pagos, Java y la aplicación del estándar ISO 8583 y de las normas PCI DSS; en donde una vez estimada cada variable se procederá a la explicación de cada una de ellas, facilitando el desarrollo del sistema y la rápida solución del problema, obtenido como resultado un sistema de calidad y acorde a lo planteado.

OBJETIVOS

OBJETIVOS GENERALES

- Aumentar la disponibilidad de los sistemas de pagos con tarjetas de crédito en el Ecuador estableciendo de manera proactiva un sistema de pagos alterno a los tradicionales.

OBJETIVOS ESPECÍFICOS

- Proporcionar una herramienta tecnológica que se pueda usar en caso de falla de los sistemas tradicionales de pagos.
- Aumentar disponibilidad en los Establecimientos Comerciales y entidades que procesan pagos con tarjetas de crédito.
- Beneficiar a las entidades, personas y establecimientos que intervienen en el proceso de una transacción con tarjeta de crédito.
- Disminuir el costo económico que generan las fallas a nivel del origen (POS) en los sistemas de pagos.
- Brindar la confianza a los clientes y entidades, garantizando la seguridad durante el proceso de las transacciones realizadas con nuestro sistema.

ALCANCE DE LA PROPUESTA

- El presente proyecto está enfocado en una aplicación para PC que permita leer la información de banda magnética de una tarjeta de crédito y realizar transacciones financieras; Utilizando JPOS como marco de trabajo para el manejo de transacciones ISO 8583, respetando todos los protocolos de seguridad y las normas estándares de la industria.
- La plataforma de desarrollo es Java, El sistema operativo anfitrión podrá ser Microsoft Windows o Linux, además será necesario un lector de banda magnética.

Este proyecto va a abarcar las siguientes funcionalidades:

- Realizar transacciones en una PC que pertenece a la cadena que realizo acuerdos comerciales con el BANCO.
- Procesar la transacción y enviarla hacia el Autorizador de tarjetas de crédito a través de una pasarela de pago.
- Recibir la respuesta del Autorizador.
- Imprimir el voucher en caso de una transacción exitosa o mostrar el mensaje de error correspondiente de la transacción en pantalla para lo cual se requiera una impresora en el comercio, conectada a la PC (Serial, LPT o USB).
- Manejar todas las posibles excepciones y errores que se pudieran generar durante el tiempo que la transacción este vigente.

- Realizar reporte de totales.
- Cierre de lotes vigentes
- Compras corrientes y diferidos
- Anulaciones
- Manejo de Usuarios
- Encriptar la Información Utilizando el algoritmo 3DES de 128 bits.

Adicionalmente para poder demostrar el ciclo de vida de una transacción financiera se ha desarrollado un módulo servidor, el cual podrá funcionar en una maquina con sistema operativo Windows o Linux, el mismo que será parametrizado para poder responder las solicitudes realizadas por la aplicación cliente, negando o aprobando las transacciones según corresponda.

Se deberán generar las llaves que utilizara la aplicación durante el proceso de encriptación de información, para esto junto al módulo servidor se ha incluido un módulo en el cual se deberá ingresar 4 componentes de tipo hexadecimal, cada componente será de 16 caracteres, este proceso generara un archivo cifrado que la aplicación posteriormente utilizara para proteger toda la información confidencial que se va a transmitir durante la transacción financiera.

La aplicación se desarrollara aplicando varios puntos de las normas PCI DSS que ayudaran cumplir con las mismas, pero será responsabilidad de la institución o empresa que adquiera la aplicación implementar las normas que corresponden a la infraestructura, red, documentación, etc. Por lo tanto estos puntos no serán detallados.

Sin embargo la aplicación cumplirá con los Requisitos de las PCI DSS correspondientes a aplicaciones que manejan datos de titulares de tarjeta las mismas que serán detalladas en el Anexo 4.

La aplicación constará de 5 módulos, que consisten en lo siguiente:

Módulo de Transacciones: En este módulo se podrán realizar compras corrientes, compras diferidas y anulaciones.

Módulo de cierre: Este módulo permitirá cerrar todas las transacciones vigentes en el sistema y enviarlas hacia la entidad autorizadora para su respectivo pago.

Módulo de reportes: Este módulo permitirá imprimir o mostrar en pantalla todas las parametrizaciones actuales del sistema, así como las transacciones realizadas en el sistema en el lote actual.

Módulo de Parametrización: Este módulo permitirá establecer todas las configuraciones de la aplicación, el nombre del comercio, código, serie de pos, tarjetas que serán aceptadas, tipos de diferidos, tipo de cálculo del IVA, impuestos, bines, propiedades de conexión hacia la entidad autorizadora.

Módulo de Seguridad: Aquí se definirá los usuarios que tendrán acceso a las configuraciones del sistema, el sistema contara con dos tipos de usuario:

Supervisor: Tendrá acceso total al sistema, podrá cambiar la configuración y los parámetros definidos actualmente.

Vendedor: únicamente tendrá acceso al módulo de transacciones y el módulo de cierre.

JUSTIFICACIÓN E IMPORTANCIA

El creciente aumento del dinero plástico, la falta de liquidez de las personas, la inseguridad, han hecho que aumenten considerablemente las transacciones con tarjetas de crédito y que tanto las personas como los establecimientos comerciales vayan progresivamente cambiando a este medio como su principal medio de pago/cobro.

A pesar del aumento de las transacciones que se realizan con las tarjetas de crédito, esto no ha ido de la mano con el desarrollo de aplicaciones para procesarlas en los puntos de venta.

Los sistemas siguen siendo los mismos, y si estos fallan se paraliza la actividad comercial tanto del establecimiento como de los clientes.

El resultado que se desea obtener con este sistema es aumentar la disponibilidad para realizar cobros/pagos con tarjetas de crédito, disminuir las pérdidas económicas ocasionadas por los problemas que se presentan en los actuales sistemas por medio de una herramienta, multi plataforma, parametrizable y fácil de usar.

En ese vértigo por comprar y comprar, en el Ecuador se han distribuido ya 24’488.205 tarjetas con un volumen de crédito que, hasta diciembre de 2011, llego a los 6.533’197.823 dólares, pero cabe anotar que la tasa de morosidad no supera el 3%, un índice bastante aceptable que se ha mantenido durante los últimos dos años. (17)

CAPÍTULO II

MARCO TEÓRICO

ANTECEDENTES DEL ESTUDIO

Durante los últimos años, se ha registrado una tendencia a nivel mundial que indica un importante crecimiento en las transacciones que se realizan con tarjetas de crédito. El uso de dinero plástico ha aumentado significativamente en los hábitos de consumo y pago de los ecuatorianos.

Observando la necesidad de sistemas para realizar cobros con tarjetas de crédito en puntos de venta, actualmente existen los POS como principal medio para realizar esta tarea.

PCI DSS estándar desarrollado por el PCI Security Standard Council (organismo creado por VISA, MasterCard, AMEX, JCB y DISCOVER), debe ser implantado por entidades bancarias, proveedores de servicio y comercios que tratan con datos de tarjetas de pago.

Una transacción basada en una tarjeta usualmente sale desde un dispositivo de compra, tal como un POS o un cajero automático ATM, a través de una red (o redes) hacia un sistema del emisor de la tarjeta para obtener una autorización en función de la cuenta del titular de la tarjeta. La transacción contiene información que se obtiene de la tarjeta (ej. número de cuenta), la terminal (ej. nro. de comercio), la transacción

(ej. importe) en conjunto con otra información que se puede generar o agregar dinámicamente por los sistemas intervinientes. El sistema emisor de la tarjeta podrá autorizar o rechazar la transacción, y genera un mensaje de respuesta que debe ser devuelto a la terminal en un tiempo breve.

ISO 8583 define un formato de mensaje y un flujo de comunicación para que diferentes sistemas puedan intercambiar estas transacciones. La mayoría de las operaciones realizadas en ATM usan ISO 8583 en algunos puntos de la cadena de comunicación, así como también las transacciones que realiza un cliente que usa una tarjeta para hacer un pago en un local. En particular, todas las redes de tarjetas basan sus transacciones en el estándar ISO 8583.

FUNDAMENTACIÓN TEÓRICA

ESTABLECIMIENTO COMERCIAL

Se considera un establecimiento comercial al espacio físico donde se brindan bienes o servicios para la venta pública, por lo general en los establecimientos comerciales no se fabrica la materia prima de los productos que se ofrecen para la venta, exceptuando ciertas panaderías y pastelerías. También se conocen con el nombre de entidad comercial o punto de venta (1).

NORMAS DE SEGURIDAD DE DATOS PCI

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas. Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de

tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos (2).

En el presente proyecto se guiara por los estándares PCI DSS aplicables para garantizar la información que se procesa a través del sistema y mantener seguros los datos titulares de tarjetas de crédito así como su información confidencial.

ISO 8583

Por lo general las transacciones con tarjetas de crédito nacen en un punto de venta (POS) o cajero automático (ATM), y viajan hacia la red emisora de la tarjeta de crédito para obtener la autorización de dicha transacción, en el proceso de la transacción viaja información que se obtiene a partir de la banda magnética de la tarjeta de crédito, como el número de tarjeta, fecha de expiración, y otra información que es agregada dinámicamente por el sistema que procesa la transacción, como el código de terminal, o el valor de la transacción.

ISO 8583 define el formato del mensaje a ser enviado y recibido para cada transacción que se realice en el punto de venta, como son compras corrientes y diferidas, anulaciones, consultas y cierres.

En general todas las redes que procesan transacciones financieras usan ISO 8583, aunque adaptan campos específicos del ISO de acuerdo a sus necesidades.

ISO 8583 también define mensajes entre sistemas para intercambios seguros de claves, conciliación de totales y otros propósitos administrativos.

Un mensaje ISO 8583 consta de las siguientes partes:

- Message Type Indicator (MTI) - Indicador de Tipo de Mensaje
- Uno o más bitmaps, indicando qué elementos están presentes en el mensaje
- Data elements, los campos del mens (3).

CÓDIGO ABIERTO

El termino código abierto es adecuado para referirse a programas que ofrecen la libertad de leerse, modificarse y usarse, con la condición de no modificar dichas libertades en el futuro.

Al tener la facilidad de Modificarse, el código abierto proporciona muchas ventajas en relación al software cerrado, debido a que los usuarios trabajan a nivel global para desarrollarlo, mejorándolo y actualizándolo rápidamente.

EL software libre contribuye a ahorrar costos en las empresa, son una alternativa potente y viable a los productos propietarios e incluso en muchas ocasiones superan a estos últimos (4).

OPEN SOURCE UTILIZADOS EN EL PROYECTO

Para entender la importancia de Linux es significativo referenciar su origen, los sistemas UNIX.

UNIX

A finales de 1960 Uno de los programadores de los laboratorios Bell, Ken Thompson, con ayuda de Dennis Ritchie y dirigiendo a un grupo de programadores entre ellos

a Rudd Canaday, trabajaron en conjunto para desarrollar un sistema de ficheros y un sistema operativo multitarea. A lo anterior, agregaron un intérprete de órdenes (o intérprete de comandos) y un pequeño conjunto de programas. El proyecto fue bautizado UNICS, como acrónimo Uniplexed Information and Computing System, pues sólo prestaba servicios a dos usuarios. Posteriormente se cambió el nombre a UNIX, dando origen al legado que llega hasta nuestros días.

No existió apoyo económico por parte de los laboratorios Bell, hasta que el grupo de investigación en ciencias de la computación decidió utilizar UNIX en una maquina PDP-7.

Thompson y Ritchie lograron cumplir con la solicitud de agregar herramientas que permitieran el procesamiento de textos a UNIX en una máquina PDP-11/20, y como consecuencia de ello consiguieron el apoyo económico de los laboratorios Bell. Fue así como por vez primera, en 1970, se habla oficialmente del sistema operativo UNIX ejecutado en una PDP-11/20.

En 1972 se tomó la decisión de escribir nuevamente UNIX, pero esta vez en el lenguaje de programación C, este cambio permitía que UNIX sea modificado y adaptado para funcionar en otras computadoras.

Mientras tanto, AT&T creó una división comercial denominada Unix Systems Laboratories para la explotación comercial del sistema operativo.

Ya en 1978, cerca de 600 o más máquinas estaban ejecutándose con alguna de las distintas encarnaciones de UNIX.

AT&T decidió combinar varias versiones desarrolladas en distintas universidades y empresas, dando origen en 1983 al Unix System V Release 1.

Hacia 1991, un estudiante de ciencias de la computación de la Universidad de Helsinki, llamado Linus Torvalds desarrolló un núcleo para computadoras con arquitectura x86 de Intel que emulaba muchas de las funcionalidades de UNIX y lo lanzó en forma de código abierto en 1991, bajo el nombre de Linux. En 1992, el Proyecto GNU comenzó a utilizar el núcleo Linux junto a sus programas.

En 1995, Novell vendió su división UNIX comercial (es decir, la antigua Unix Systems Laboratories) a Santa Cruz Operation (SCO) reservándose, aparentemente, algunos derechos de propiedad intelectual sobre el software. SCO continúa la comercialización de System V en su producto UnixWare, que durante cierto tiempo pasó a denominarse OpenUnix, aunque ha retomado de nuevo el nombre de UnixWare (5).

UBUNTU

Ubuntu en un sistema orientado a la facilidad de Uso, el eslogan de Ubuntu “Linux para seres humanos” resume una de sus metas principales, hacer Linux un sistema más accesible y fácil de utilizar.

PRINCIPIOS DE UBUNTU

La filosofía de Ubuntu debe cumplir los siguientes principios:

- Él usuario debe poseer la libertad de cambiar y mejorar su software para cualquier propósito, sin tener que pagar derechos de licencia.
- El usuario debe ser capaz de utilizar software en su propio idioma.
- Debe ser capaz de usar el software independientemente de algún tipo de discapacidad que posea.

UBUNTU ES SOFTWARE LIBRE

Ubuntu está totalmente orientado en los principios del Software libre y motiva a sus usuarios a que lo mejoren y distribuyan.

Según la Free Software Foundation, el software es libre cuando sus usuarios gozan de las siguientes libertades:

- Libertades para usar el software con cualquier propósito.
- Libertad para Modificar el programa y mejorarlo.
- Libertad para distribuir el programa, beneficiando al resto de usuarios.
- La filosofía de software libre indica que el mismo debe estar disponible para la descarga, y debe poder usarcé de todas las maneras que se considere socialmente útiles.

UBUNTU ES CÓDIGO ABIERTO

EL código abierto permite a muchos usuarios trabajar y mejorar el software, muchos usuarios a nivel mundial ponen su esfuerzo en desarrollar y mejorar el software para posteriormente ponerlo a disposición de los demás.

A continuación varios principios básicos del código abierto:

- El software debe ser libre de distribuir, es decir, se debe incluir el código fuente.
- La licencia debe permitir a los usuarios experimentar modificaciones y luego distribuirlas.
- Todos los usuarios independientemente de cualquier tipo de discapacidad deben ser capaces de usarlos, es decir no debe existir discriminación de ningún tipo.
- Se debe permitir el uso del programa en cualquier campo, no debe existir limitantes de licencias para el uso del software en un campo específico.
- La licencia no debe ser específica de un producto ni tampoco restringir otro software.

LAS VERSIONES DE UBUNTU

Ubuntu publica una versión cada 6 meses, una en abril y otra en Octubre.

Cada dos años se publica una versión LTS con soporte extendido, 3 años para sistemas de escritorio y 5 para servidores.

La cuarta versión LTS que ha sido lanzada es la 12.04, que fue liberada en abril de 2012.

RESPALDO Y SOPORTE

Ubuntu está mantenido por una amplia comunidad a nivel mundial que no para de crecer.

Además, el proyecto está patrocinado por Canonical Ltd., una compañía creada por Mark Shuttleworth. Canonical tiene en nómina a los principales desarrolladores de Ubuntu y ofrece soporte profesional y servicios de consultoría para Ubuntu (6).

El presente proyecto se podrá ejecutar sobre el sistema operativo Ubuntu, promoviendo de esta manera el uso de software libre y disminuyendo los costos asociados a la implementación del mismo, sin embargo es multiplataforma y también se podrá ejecutar sobre sistemas Operativos Windows.

SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información son todas aquellas medidas preventivas y reactivas del hombre, de las empresas y de los sistemas informáticos para proteger la información con el fin de mantener su confidencialidad, integridad y disponibilidad.

HISTORIA DE LA SEGURIDAD DE LA INFORMACIÓN

En la antigüedad existían las bibliotecas, en dichos lugares se podía guardar la información para transmitirla y para evitar que otros las obtuvieran, considerándose las primeras muestras de protección de la información.

Sun Tzu en El arte de la guerra y Nicolás Maquiavelo en El Príncipe señalan la importancia de la información sobre los adversarios y el cabal conocimiento de sus propósitos para la toma de decisiones.

Durante la segunda guerra mundial se crean la mayoría de las redes de inteligencia del mundo, con el fin de obtener información valiosa e influyente.

También se crean mecanismos de contrainteligencia para la protección de la información, al incrementarse la tecnología en el mundo, el cuidado de la información y los medios que se usan para protegerla se han vuelto cruciales.

CONCEPCIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, se clasifica como:

- **Crítica**: La información es indispensable para las organizaciones.
- **Valiosa:** Es un activo muy valioso para las organizaciones.
- **Sensible:** Solo debe ser conocida por las personas autorizadas.

Existen dos conceptos muy importantes que son riesgo y seguridad:

- **Riesgo:** Es toda vulnerabilidad que existe, por lo tanto existe un riesgo, y la información está expuesta a amenazas que pueden ocurrir en cualquier momento y producir numerosas pérdidas para las empresas.
- **Seguridad:** Es una forma de protección contra los riesgos.

La seguridad de la información comprende varios aspectos, entre ellos la disponibilidad, comunicación, identificación, análisis de riesgo, la integridad, confidencialidad, recuperación de riesgos.

La seguridad de la información tiene como propósito la implementación de procedimientos y estrategias que ayuden a salvaguardar tanto información como los sistemas que la almacenas y administran.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, sus estados financieros caigan en manos de un competidor o manos no autorizadas, podría ser causa de pérdida de credibilidad, perdida de negocios, demandas legales o incluso la quiebra de la misma.

La confidencialidad, integridad y disponibilidad son los principios básicos de la seguridad de la información.

CONFIDENCIALIDAD

La confidencial es el acceso a determinada información, única y exclusivamente por las personas autorizadas.

Cuando personas no autorizadas logran acceder a determinada información, se produce una violación de la confidencialidad.

INTEGRIDAD

La integridad de la información consiste en mantener la información idéntica como fue creada originalmente, libre de modificaciones no autorizadas.

Cuando una persona o proceso no autorizado modifica la información, se produce la violación de la integridad y dicha información ya no es fiable.

DISPONIBILIDAD

La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que lo requieran.

Adicionalmente los sistemas informáticos usados para proteger la información, también deberán estar disponibles en todo momento.

Para garantizar las disponibilidad de la información existen varios mecanismos como replicación entre bases de datos, enlaces de comunicación redundantes, arreglos de disco, servidores espejo, generados eléctricos, etc.

AUTENTICACIÓN O AUTENTIFICACIÓN

Es la propiedad que permite identificar y garantizar que quien genera una solicitud es quien dice ser.

En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseña.

PROTOCOLOS DE SEGURIDAD DE LA INFORMACIÓN

Conjunto de reglas durante la transmisión de datos entre dispositivos para ejercer confidencialidad, integridad, autenticación y el no repudio de la información.

- **Criptografía (Cifrado de Datos):** Es el proceso que se encarga de cifrar el mensaje enviado por el emisor, consiste en transposicionar u ocultar el mensaje hasta que llega a su destino y puede ser descifrado por el receptor.
- **Lógica (Estructura y secuencia):** El orden en que se agrupa el mensaje, los datos y el significado del mismo.
- **Autenticación:** Es la comprobación de identidad entre las partes que realizan la comunicación.

NO REPUDIO

Proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, que participan en toda o parte de la comunicación.

- **No Repudio de origen:** El emisor no puede negar que envió el mensaje por que el destinatario tiene pruebas del envió, las pruebas las crea el propio emisor y la recibe el destinatario.
- **No Repudio de destino:** El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción, en este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

El "No repudio" prueba que el autor envió la comunicación y que el destinatario la recibió.

PLANIFICACIÓN DE LA SEGURIDAD

Las organizaciones deben adoptar un conjunto de controles para proteger sus sistemas e información.

El propósito del plan de seguridad es proporcionar una visión general de entorno y de los requisitos que se deben cumplir para garantizar una correcta planificación de la seguridad.

Un plan de seguridad también define los roles y el comportamiento esperado por todos los individuos que acceden a los sistemas, de tal manera que todos lo entiendan.

CREACIÓN DE UN PLAN DE RESPUESTA A INCIDENTES

Es importante elaborar un plan de respuesta a incidentes que permita solventar cualquier alteración de la seguridad que exista, un plan de respuesta a incidentes proporciona una guía de pasos a seguir en caso de presentarse un incidente, minimizando considerablemente el impacto y reduciendo los riesgos de expansión.

El plan de respuesta a incidentes consta de cuatro pasos

- Acción inmediata para detener o minimizar el incidente
- Investigación
- Restauración de recursos afectados
- Reporte del incidente a los canales apropiados

Un plan de respuesta a incidentes tiene un número de requerimientos, incluyendo:

- Un equipo de expertos locales

- Una estrategia legal revisada y aprobada
- Soporte financiero de la compañía
- Soporte ejecutivo de la gerencia superior
- Un plan de acción factible y probado
- Recursos físicos, tales como servicio de respaldo.

CONSIDERACIONES LEGALES

Es un aspecto muy importante a considerarse en un plan de respuesta a incidentes. Para la inclusión de las consideración legales se debería contar con la asesoría de un equipo jurídico, esta parte es muy importante en casos en que información confidencial se ve involucrada en el incidente o en casos donde existe acuerdos de servicios que se estarían incumpliendo.

PLANES DE ACCIÓN

Una vez desarrollado un plan de acción, este debe ser aceptado, implementado y probado previamente.

Un aspecto muy importante es medir el tiempo que tome el plan de acción así como la recolección de información que permita determinar el origen del incidente, por lo tanto la recolección de información también se deberá reflejar en el plan de acción, complementándose con las acciones a seguir.

EL MANEJO DE RIESGOS

Comprende la clasificación de las alternativas para manejar los posibles riesgos que un activo puede tener dentro de los procesos en una empresa.

Se detallan a continuación:

- **Evitar:** Se evita el riesgo cuando la organización decide no exponerse al mismo, pero tiene muchas desventajas, principalmente desaprovechar servicios fundamentales por no exponerse a riesgos.
- **Reducir**: Cuando por requerimientos el riesgo no puede evitarse, la alternativa es la reducción, la cual se consigue implementando políticas y procedimientos que reduzcan el riesgo al mínimo.
- **Retener, Asumir o Aceptar el riesgo:** Es la decisión de aceptar las consecuencias de la ocurrencia del evento, puede ser voluntaria o involuntaria, la voluntaria se produce por la falta de alternativas para mitigar el riesgo mientras que la involuntaria se da cuando el riesgo es retenido inconscientemente.
- **Transferir:** Consiste en buscar un respaldo y compartir el riesgo con otros controles o entidades. Por ejemplo una compañía aseguradora.

ACTORES QUE AMENAZAN LA SEGURIDAD

- **Hacker:** Persona con amplios conocimientos en tecnología, se mantiene permanentemente actualizado y conoce a fondo lo relacionado con programación y sistemas complejos; le interesa conocer todo lo relacionado con "información segura" y busca acceder a sistemas complejos sin ser descubiertos, también le da la posibilidad de difundir sus conocimientos y las vulnerabilidades de los sistemas que logra acceder.
- **Cracker:** Persona con comportamiento compulsivo, hábil conocedor de programación en hardware y Software, diseña programas de guerra para interferir correo, telefonía o tomar control remoto de otras computadoras.
- **Lamer:** Persona con poco conocimiento que utiliza programas desarrollados por Hackers o Crackers.
- **Bucanero:** Es un comerciante que depende exclusivamente de la red para su actividad, no poseen ningún tipo de formación en el área de sistemas pero si un amplio conocimiento en el área de negocios.
- **Phreaker**: Posee vastos conocimientos en el área de telefonía, incluso más que los propios técnicos de las compañías telefónicas.
- **Script kiddie**: Es un simple usuario de internet sin ningún conocimiento de hackeo o crackeo, pero aficionado a estos temas busca recopilar información en la web llegando en muchos casos a infectar sus equipos con virus residentes en los sitios que visita.

- **Tonto o Descuidado:** Persona descuidada que accidentalmente borra o daña información, ya sea en un mantenimiento de rutina o supervisión.

OTROS CONCEPTOS

- **Auditabilidad:** Permite la reconstrucción, revisión y análisis de eventos o sucesos.
- **Identificación:** Verificación de una persona o cosa.
- **Autenticación:** Proporciona una prueba de identidad, puede ser algo que se tiene, algo que se sabe o algo que se es.
- **Control de Acceso:** Limitar el acceso solo a las personas autorizadas.
- **Estrategia:** los pasos que se requieren para alcanzar un objetivo
- **Riesgo:** la explotación de una vulnerabilidad por parte de una amenaza.
- **Exposiciones:** Áreas que son vulnerables a un impacto por parte de una amenaza.
- **Vulnerabilidades:** deficiencias que pueden ser explotadas por amenazas
- **Riesgo residual:** El riesgo que permanece después de que se han implementado contra medidas y controles.
- **Impacto:** los resultados y consecuencias de que se materialice un riesgo.
- **Criticidad:** La importancia que tiene un recurso para el negocio
- **Sensibilidad:** el nivel de impacto que tendría una divulgación no autorizada
- **Controles:** Cualquier acción o proceso que se utiliza para mitigar el riesg**o**

- **Políticas:** declaración de alto nivel sobre la intención y la dirección de la gerencia
- **Normas:** Establecer los límites permisibles de acciones y procesos para cumplir con las políticas
- **Clasificación de datos:** El proceso de determinar la sensibilidad y Criticidad de la información (7).

JAVA

HISTORIA

Java se creó como una herramienta de programación para ser usada en un proyecto en una pequeña operación denominada the Green proyect en Sun Microsystems en el año 1991, El equipo de trabajo estuvo compuesto por trece personas y dirigido por James Gosling, se trabajó durante 18 meses en su desarrollo.

El lenguaje se denominó inicialmente Oak, luego se descubrió que ese nombre ya estaba registrado y paso a llamarse Green, posteriormente se cambió a Java.

Los objetivos de Gosling era implementar una máquina virtual y un lenguaje con una estructura y sintaxis similar a C++, en 1994 el equipo reoriento la plataforma hacia la web, uno de los miembros Naugton creo entontes un prototipo de navegador WebRunner, que más tarde sería conocido como HotJava.

En 1994, se hizo una demostración de HotJava y la plataforma Java a los ejecutivos de Sun, en 1995 durante las conferencias de Sun World Java y HotJava vieron la luz

pública, en 1996, Sun fundo el grupo empresarial llamado Java Soft para que se encargase del desarrollo tecnológico.

La filosofía inicial de Java era Escríbelo una vez, ejecútalo en cualquier lugar.
De esta manera se proporciona un lenguaje independiente de la plataforma y un entorno de desarrollo (la JVM) ligero y gratuito para las plataformas más populares.

Java ha experimentado numerosos cambios desde la primera versión, JDK 1.0, así como un enorme incremento en el número de clases y paquetes que componen la biblioteca estándar.

A continuación se detallan la historia de los lanzamientos de las versiones de Java.

- **JDK 1.0:** Primer lanzamiento (23 de enero de 1996), Comunicado de Prensa.
- **JDK 1.1:** 19 de febrero de 1997, rueda de prensa.
- **J2SE 1.2:** 8 de diciembre de 1998 — Nombre clave Playground.
- **J2SE 1.3**:8 de mayo de 2000 — Nombre clave Kestrel.
- **J2SE 1.4 :**(6 de febrero de 2002) — Nombre Clave Merlin.
- **J2SE 5.0**: (30 de septiembre de 2004) — Nombre clave: Tiger.
- **Java SE 6 :**(11 de diciembre de 2006) — Nombre clave Mustang.
- **Java SE 7:** (Julio 2011) —Nombre clave Dolphin.

FILOSOFÍA

Java fue concebido con los siguientes objetivos principales.

- Debería usar el prototipo de la programación orientada a Objetos
- Permitir la ejecución de un programa en múltiples plataformas(Sistemas Operativos)
- Debería incluir soporte para trabajo en red.
- Debería tener facilidad de uso, e incluir lo mejor de otros lenguajes orientados a objetos.

El Sistema de pagos será desarrollado en Java, de esta manera se garantiza que sea multiplataforma, basándose en una plataforma robusta como es Java (8).

TARJETA DE CRÉDITO

Es un instrumento material de identificación de usuario ante una entidad bancaria, consiste en una tarjeta plástica con una banda magnética y un número en relieve.

Es emitida por una entidad financiera o bancaria y autoriza al titular de la tarjeta a utilizarla como medio de pago en los establecimientos afiliados mediante la presentación de la tarjeta y su firma.

Entre las más conocidas del mercado están: Visa, Diners, MasterCard, JBC, Discover, entre otras.

Las grandes tiendas emiten sus propias versiones de tarjetas de crédito y las ofrecen como medio de pago y de financiamiento a sus clientes, estas son conocidas como tarjetas cerradas.

Las entidades emisoras de tarjetas de crédito asignan un cupo de acuerdo a los ingresos que posee el titular de la tarjeta y a un análisis de riesgo crediticio previamente realizado.

Un pago con tarjeta de crédito es un pago con dinero M1, (dinero crediticio) que como todo agregado monetario distinto de M0, no es creado por los bancos centrales sino por los bancos privados o las tiendas que dan créditos. Por tanto, el hacer efectivo un cobro con tarjeta de crédito depende de la solvencia de la entidad emisora de la tarjeta. Ese dinero crediticio NO es del tarjetahabiente, lo tiene que pagar.

En caso de uso fraudulento de la tarjeta se debe notificar a la entidad emisora de la tarjeta para que anule el monto y seguir el trámite respectivo de acuerdo a cada institución.

FORMA Y ORIGEN

La tarjeta de crédito consiste en una pieza de plástico, las dimensiones se han estandarizado en los últimos años, por lo general son 85,60 × 53,98 mm y cumple la norma ISO/IEC 7810 ID-1.

Cada tarjeta contiene la identidad de la institución emisora de la tarjeta así como el nombre del cliente y la fecha de vigencia de la misma, adicionalmente posee una banda magnética donde se puede encontrar el número de la tarjeta y otra información que permite al portador de la misma disponer de crédito al momento de presentarla.

Apareció en el Siglo 20 en los estados unidos bajo la modalidad de tarjeta profesional, a manos del director del Chase Manhattan Bank.

NÚMERO DE LA TARJETA

Es el número principal de cuenta (PAN) de las tarjetas de crédito y bancarias, los números de tarjeta son un caso especial de la norma ISO/IEC 7812.

Una norma ISO / IEC 7812 contiene un número de un dígito identificador principal de la Industria (MII), uno de seis dígitos Número de Identificación del Emisor (IIN), un número de cuenta, y un cheque de un solo dígito calcula utilizando el algoritmo de Luhn. El MII es considerado como parte del IIN.

El término "Emisor Número de Identificación" (IIN) sustituye a los utilizados anteriormente "Número de Identificación Bancaria" (BIN). Véase la norma ISO / IEC 7812 para más (9).

CIFRADO (CRIPTOGRAFÍA)

Es el procedimiento que utiliza un algoritmo (Algoritmo de cifrado) con cierta clave (clave de cifrado) que transforma un mensaje de tal forma que sea incomprensible, de tal manera que solo lo puedan entender las personas que posean la clave secreta (clave de descifrado) del algoritmo que se usa para poder descifrarlo (algoritmo de descifrado).

Por lo tanto se tienen dos algoritmos, cifrado y descifrado, y dos claves, clave de cifrado y clave de descifrado.

Las claves de cifrado y descifrado pueden ser iguales, a este proceso se considera criptografía simétrica o pueden ser distintas, criptografía asimétrica.

TERMINOLOGÍA

A continuación varios de los términos comúnmente utilizados en el proceso de cifrado/descifrado:

- **Texto en claro o texto plano:** El mensaje sin cifrar.
- **Criptograma o texto cifrado:** Es el mensaje resultante una vez que se ha producido el cifrado.
- **Cifrado:** Es el proceso de convertir el texto sin cifrar en texto cifrado.
- **Cifrador:** Sistema que implementa el algoritmo de cifrado
- **Algoritmo de cifrado o cifra:** Es el algoritmo que se utiliza para cifrar.

- **Clave de cifrado:** La clave que se utiliza en el algoritmo de cifrado.
- **Descifrado:** Es el proceso de convertir el texto cifrado en el texto en claro.
- **Descifrador:** Sistema que implementa el algoritmo de descifrado
- **Algoritmo de descifrado o descifra:** Es el algoritmo que se utiliza para descifrar.
- **Clave de descifrado:** La clave que se utiliza en el algoritmo de descifrado.
- **Gestión de claves:** Es el proceso de generación, certificación, distribución y cancelación de todas estas claves que son necesarios para realizar el cifrado
- **Cripto Sistema:** Conjunto estructurado de los protocolos, algoritmos de cifrado/descifrado, procesos de gestión de claves e intervención por parte del usuario.

PRE PROCESADO DEL TEXTO PLANO

Por lo general antes de cifrar un mensaje se realiza una serie de operaciones, con el fin de fortalecer el mensaje resultante del cifrado, todas las operaciones que se realicen antes de cifrar el mensaje, se deberán tomar en cuenta al momento de descifrar el mensaje, de tal manera que se pueda obtener el texto original.

Algunas técnicas que se usan para aumentar y robustecer el mensaje cifrado son por ejemplo, quitar los espacios en blanco en el mensaje original, transformarlo todo a mayúscula, o usar un alfabeto diferente al que se encuentra el texto sin cifrar.

TIPOS DE CIFRADO ATENDIENDO A SUS CLAVES

De acuerdo al tipo de claves que utilizan pueden existir sistemas simétricos y asimétricos.

Un sistema simétrico utiliza la misma clave para cifrar y descifrar la información,

Mientras que un sistema asimétrico utiliza una clave para cifrar la información y otra para descifrar, este esquema también es conocido como descomposición publica/privada.

Los métodos más conocidos con el DES, el triple DES y e AES para la criptografía simétrica, y el RSA para la criptografía asimétrica.

TIPOS DE CIFRADO ATENDIENDO A SUS ALGORITMOS

Según la forma en la que operan los algoritmos de cifrado o descifrado podemos distinguir varios tipos principales:

- **Cifrado en flujo**: El cifrado se realiza bit a bit, se utiliza la clave para cifrar y descifrar, las claves pueden ser generadas aleatoriamente o a partir de una clave de inicialización, normalmente en este tipo de algoritmo hay que mantener en secreto tanto la clave como el cifrador.

- **Cifrado por bloques**: Este tipo de algoritmo de cifrado se realiza por bloques, es decir, se descompone la cadena en bloques de la misma longitud y posteriormente se convierte en un bloque de mensaje cifrado mediante una secuencia de operaciones (10).

CRIPTOGRAFÍA SIMÉTRICA

También es conocida como criptografía de clave secreta, es un método criptográfico en el cual se utiliza la misma clave tanto para cifrar el mensaje, como para descifrarlo. Para realizar este proceso ambas partes involucradas se poner de acuerdo en la clave a utilizar, una vez que ambas partes tienen acceso a esta clave, el remitente cifra en mensaje usando la clave, lo envía al destinatario y este lo descifra con la misma clave.

SEGURIDAD

Un sistema de seguridad robusto, centra toda la seguridad en la clave y no en el algoritmo, de esta manera se garantiza que si un atacante conoce el algoritmo de cifrado, sea incapaz de descifrarlo, ya que no posee la clave.

Es muy importante la longitud de la clave que se utiliza en el algoritmo, ya que de esto dependerá la dificultad de un posible atacante de descifrarla.

En la actualidad los ordenadores pueden descifrar claves con extrema rapidez, es por esta razón que es muy importante la longitud de la misma, El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves

posibles (72.057.594.037.927.936 claves). Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como 3DES, Blowfish e IDEA usan claves de 128 bits, lo que significa que existen 2 elevado a 128 claves posibles. Esto equivale a muchísimas más claves, y aun en el caso de que todas las máquinas del planeta estuvieran cooperando, tardarían más tiempo en encontrar la clave que la edad del universo.

Algunos ejemplos de algoritmos simétricos: son

- DES
- 3DES
- AES
- Blowfish e IDEA.

INCONVENIENTES

El principal inconveniente con los sistemas de claves simétricos radica en la manera en que se realiza el intercambio de claves, ya que puede ser más fácil para un atacante interceptar las claves en lugar de adivinarlas, es por eso que se recomienda tener mecanismos adicionales para proteger las claves con la que cifra la información.

TRIPLE DES

Algoritmo desarrollado por IBM en 1998, realiza un tripe cifrado del DES, también se conoce como 3DES o TDES.

ALGORITMO

No llega a ser un cifrado múltiple, porque no son independientes todas las subclases. Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se cifra el mismo bloque dos veces con dos claves diferentes se aumenta el tamaño efectivo de la clave.

La variante más simple del Triple DES funciona de la siguiente manera:

Grafico 1

Encriptación 3DES

$$C = E_{DES}^{k_3}\left(D_{DES}^{k_2}\left(E_{DES}^{k_1}(M)\right)\right)$$

Elaboración: Carlos Solís

Fuente: Investigación

Donde M es el mensaje a cifrar y k_1, k_2 y k_3 las respectivas claves DES. En la variante 3TDES las tres claves son diferentes; en la variante 2TDES, la primera y tercera clave son iguales.

.

SEGURIDAD

Al descubrir que el algoritmo DES no era suficiente para evitar un ataque de fuerza bruta, el TDES fue elegido como una manera de agrandar el largo de la clave conservando el mismo algoritmo, a cambio de esto se triplico el número de operaciones, obteniendo un método de cifrado mucho más seguro (11).

USOS

La mayoría de instituciones que realizan pagos electrónicos, utilizan el 3DES como estándar, antes usaban el DES.

Ejemplos de estándares probados y aceptados en la industria y los algoritmos de cifrado AES incluir (128 bits y mayores), TDES (mínimo de dos llaves de longitud), RSA (1024 bits y superiores. Ver NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) para obtener más información.

Por lo tanto el tipo de Cifrado que se usara en el presente proyecto es el 3DES

BANDA MAGNÉTICA

Es toda aquella banda oscura presenta en las tarjetas de crédito, identificaciones personales o abonos de transporte público.

Está compuesta por partículas ferromagnéticas incrustadas en una matriz de resina en la cual se almacena determinada información, la banda magnética es leída o grabada por contacto físico pasándola a través de una cabeza lectora/escritora, fue inventada por IBM en 1960.

En aplicaciones estándar de tarjetas de identificación, como las usadas para las transacciones financieras, la información contenida en la banda magnética se organiza en diferentes pistas. El formato y estructura de datos de estas pistas están regulados por los estándares internacionales ISO 7813 (para las pistas 1 y 2) e ISO 4909 (para la pista 3) (12).

PASARELA DE PAGO

Es un proveedor de servicios de aplicación de comercio electrónico que autoriza pagos a negocios, en el proceso de una transacción suelen intervenir varias pasarelas de pagos, antes que el mensaje llegue a su destinatario. Las pasarelas de pago por lo general se encargan de proteger información sensible, cifrando dicha información con llaves distintas a las que originalmente reciben en el mensaje.

FUNCIONAMIENTO

Una pasarela de pago facilita la transferencia entre el origen (donde se genera la transacción) y el destino (Entidad que aprueba la transacción), la ventaja de usar pasarelas de pagos es que las entidades que aprueban las transacciones no tienen que dar acceso a cada cliente que realiza una solicitud, sino que únicamente le dan acceso a la pasarela de pago, en la cual van a estar concentradas todas las peticiones de autorización.

Por ejemplo:

- La transacción se origina en un punto de venta, con una tarjeta internacional.
- El punto de venta envía la transacción a una pasarela de pago con la cual tiene convenios comerciales.
- La pasarela de pagos envía a su vez la transacción al banco emisor de la tarjeta de crédito.
- El banco envía la respuesta a la pasarela de pagos.
- La pasarela de pagos envía la respuesta al punto de venta.
- El cliente recibe la autorización en 3 o 4 segundos de manera transparente.
- Al final del día bancario (o período de liquidación), el banco adquirente deposita el total de los fondos aprobados en la cuenta nominada del vendedor. Esta cuenta puede encontrarse en el mismo banco adquirente si el vendedor realiza sus operaciones con el mismo banco o una cuenta con otro banco (13).

ALGUNAS DEFINICIONES PARA COMPRENDER MEJOR EL FLUJO DE UNA TRANSACCIÓN

- **Autorización**: El establecimiento afiliado envía la transacción hacia su banco adquirente mediante una terminal electrónica, el cual valida en su sistema los datos recibidos, y responde con una autorización o aprobación de la transacción.

- **Pago del Tarjetahabiente:** El tarjetahabiente reembolsa al banco emisor los valores por los bienes o servicios adquiridos en el comercio afiliado.
- **Banco Emisor:** Es la entidad que emite la tarjeta de crédito a nombre del tarjetahabiente.
- **Tarjetahabiente:** Es el consumidor que posterior a un análisis de riesgo crediticio, recibe una tarjeta de crédito por parte del banco emisor.
- **Comercio Afiliado:** Cualquier compañía o entidad que desee realizar cobros con tarjetas de créditos y que cumpla con las normas establecidas por las tarjeta bancaria y su banco adquirente.

Banco Adquirente: Entidad autorizada por la tarjeta Bancaria que realiza un proceso de Evaluación y posteriormente acepta a los establecimientos afiliados en su programa de tarjetas bancarias, procesa las transacciones y realiza las liquidaciones financieras (14).

J8583

J8583 es una biblioteca Java para generar y leer mensajes ISO 8583.

j8583 ofrece una Message Factory, que una vez configurado correctamente, puede crear diferentes tipos de mensajes con algunos valores predefinidos, y también puede analizar una matriz de bytes para crear un mensaje de ISO. Los mensajes se representan mediante objetos Iso Message, que almacenan instancias iso valor para los campos de sus datos. Puede trabajar con los iso valores o utilizar los métodos de

Conveniencia de Iso Message para trabajar directamente con los valores almacenados (15).

JPOS

Marco de trabajo desarrollado en java para la implementación del estándar ISO 8583 que se utiliza para las transacciones financieras realizadas con tarjeta de crédito entre los POS (Puntos de Venta) o ATM (Cajeros Automáticos).

Un mensaje ISO

Es capaz de traducir lo siguiente en una transacción común y corriente, por ejemplo.

Los primeros cuatro dígitos pertenecen al **MTI** (0200), Requerimiento de fondos, usualmente de un ATM o Cajero Automático, la segunda parte del mensaje se llama **Mapa de Bits**(bbbbbbbb16550000), esta parte indica que campos del mensaje están presentes, puede venir en 8 bytes o 16 carácter, y luego están los **Data Elements**, que son los campos del mensaje, puede ser, el Id del Comercio, de la terminal, el monto de la transacción, el número de la tarjeta, la fecha de caducidad, depende del tipo de transacción.

Un mensaje, **no siempre tiene el mismo tamaño**, y varia para cada procesadora de tarjetas de crédito, VISA, MASTERCARD tienen sus formas de generar sus propias cadenas para comunicarse con las entidades bancarias. (16)

FUNDAMENTACIÓN LEGAL

DECRETO 1014

SOBRE EL USO DEL SOFTWARE LIBRE

Art. 1: Establecer como política pública para las entidades de administración Pública central la utilización del Software Libre en sus sistemas y equipamientos informáticos (16).

Art. 2: Se entiende por software libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan el acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas.

Estos programas de computación tienen las siguientes libertades:

a) Utilización de programa con cualquier propósito de uso común.
b) Distribución de copias sin restricción alguna.
c) Estudio y modificación de programa (Requisito: código fuente disponible)
d) Publicación del programa mejorado (Requisito: código fuente disponible

Art. 3: Las entidades de la administración pública central previa a la instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para este tipo de software.

Art. 4: Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de software libre que supla las necesidades requeridas, o cuando esté en riesgo de seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

PREGUNTAS A CONTESTARSE

Para este estudio se planea las siguientes preguntas:

¿La creación de una aplicación de pagos para puntos de ventas, segura y que cumpla con los estándares de la industria de tarjetas de pago, mejorara la disponibilidad y disminuirá los costos ocasionados por los fallos de los sistemas actuales?

¿La seguridad y normas en que se basa la aplicación, ayudara a los establecimientos comerciales a mejorar la seguridad y proteger la información del cliente cuando realiza una transacción?

VARIABLES INDEPENDIENTES

Transacciones Electrónicas Realizadas Por Instituciones Comerciales

El presente sistema está orientado a mantener y aumentar la disponibilidad para realizar transacciones electrónicas en instituciones Comerciales.

VARIABLES DEPENDIENTES

Medio Alterno De Pago

El brindar un medio alternativo de pagos es el objetivo al cual está destinada nuestra aplicación, beneficiando de todos los servicios brindados por nuestro sistema a las entidades que realizan cobros con tarjetas de crédito.

Dando como resultado alta disponibilidad en las transacciones financieras realizadas en estas entidades.

Lector De Banda Magnética

Nos permitirá leer la información de banda magnética de una tarjeta de crédito, con la cual se dará inicio al ciclo de vida de la transacción financiera.

Estándar ISO 8583 Y Normas PCI DSS

Estándares y normas en la cual será basado nuestro sistema, garantizando de esta manera la seguridad de la información durante la realización de una transacción financiera.

DEFINICIONES CONCEPTUALES

Sistema: Sistema es un conjunto de elementos que interactúan entre sí para logran un objetivo, Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia.

Pagos: El pago es uno de los modos de extinguir las obligaciones que consiste en el cumplimiento efectivo de la prestación debida.

Establecimiento Comercial: Es el lugar físico donde se brindan bienes o servicios.

ISO 8583: define un formato de mensaje y un flujo de comunicación para que diferentes sistemas puedan intercambiar transacciones que se realizan con tarjetas de crédito.

PCI DSS: Normas de seguridad de la industria de las tarjetas de crédito, las cuales proporcionan una guía para que las transacciones que se realicen con tarjetas de crédito sean efectuadas con las mayores seguridades y que la información de la tarjeta de crédito como del tarjeta habiente estén protegidas.

Banda Magnética: es toda aquella banda oscura presente en tarjetas de crédito, abonos de transporte público o carnets personales que está compuesta por partículas ferromagnéticas incrustadas en una matriz de resina.

Estándar: Según la real academia de la lengua un estándar es un modelo que sirve como norma, patrón, o referencia para realizar procesos o actividades especificas

Cifrado (criptografía): En criptografía un cifrado, es un procedimiento que utilizando un algoritmo (algoritmo de cifrado) con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal

forma que sea incomprensible o, al menos, difícil de comprender, a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo que se usa para poder descifrarlo (algoritmo de descifrado)

Open Source: Es el término con el que se conoce al software distribuido y desarrollado libremente, permitiendo la visualización de su código fuente.

Licencia: La licencia de software es el conjunto de permisos que un desarrollador da para la distribución, uso y/o modificación de la aplicación que desarrolló. Puede indicar en esta licencia también los plazos de duración, el territorio donde se aplica, etc.

Java: Java es un lenguaje de programación de alto nivel orientado a objetos, con independencia de plataforma. El diseño de Java, su robustez, el respaldo de la industria y su fácil portabilidad han hecho de Java uno de los lenguajes con un mayor crecimiento y amplitud de uso en distintos ámbitos de la industria de la informática.

Tarjeta de Crédito: La tarjeta de crédito es un instrumento material de identificación del usuario, que puede ser una tarjeta plástica con una banda magnética y un número en relieve. Es emitida por un banco o entidad financiera que autoriza a la persona a cuyo favor es emitida, utilizarla como medio de pago en los negocios adheridos al sistema, mediante su firma y la exhibición de la tarjeta

Ubuntu: Es una distribución Linux. Ofrece un sistema operativo predominantemente enfocado a ordenadores de escritorio. Basada en Debían GNU/Linux, concentra su objetivo en la facilidad de uso, la libertad en la restricción de uso, los lanzamientos regulares y la facilidad en la instalación.

CAPÍTULO III

METODOLOGÍA

DISEÑO DE LA INVESTIGACIÓN

El proyecto se ha establecido como proyecto factible, ya que es totalmente realizable dentro de los plazos establecidos y con los recursos que se cuentan, de la misma manera la plataforma de desarrollo es libre.

Un proyecto factible se define como la investigación, elaboración y desarrollo de un modelo viable, cuyo objetivo es la búsqueda de solución a problemas y la satisfacción de necesidades.

La investigación que se realizara se tratara de cómo implementar soluciones que mejoren la disponibilidad de los sistemas para realizar transacciones con tarjetas de créditos en los establecimientos comerciales, permitiendo una redundancia ante fallos, con todas las seguridades aceptadas por las industrias de tarjetas de pagos, ya que con un sistema alterno a los que existen actualmente, serán capaces de mantener las continuidad de las actividades comerciales y disminuirán los costos asociados a las fallas de los sistemas actuales.

Se llevara a cabo una encuesta, dirigida a los dependientes que laboran en los establecimientos comerciales, para obtener resultado de sus preferencias y que es lo que desean esperar de un sistema que tenga similitud al nuestro.

El estudio se basara en el proceso para realizar transacciones con tarjetas de crédito hacia una pasarela de pagos utilizando el estándar ISO 8583 y basados en las normas PCI DSS a través de una aplicación desarrollada en JAVA para establecimientos comerciales.

MODALIDAD DE LA INVESTIGACIÓN

La investigación que se realizara para la aplicación en Java, se ha establecido como proyecto factible pudiendo demostrar los diferentes beneficios que pueden tener los establecimientos comerciales, al contar con una aplicación para procesar sus requerimientos de realizar transacciones con tarjetas de crédito.

POBLACIÓN Y MUESTRA

POBLACIÓN

Según la investigación realizada basada en las estadísticas de los sitios web dos de las redes emisoras de tarjeta de crédito en el Ecuador, se determinó una población total en el Ecuador de 16000 establecimientos comerciales e instituciones que aceptan tarjetas de crédito, donde:

CUADRO NO I
ESTABLECIMIENTOS QUE ACEPTAN TARJETAS DE CRÉDITO EN ECUADOR

Ecuador	**16000**
TOTAL	**16000**

Elaboración: Carlos Solis

Fuente: http://www.creditos.com.ec/tarjeta-de-credito-visa-clasica-pacificard/

MUESTRA

Para la determinación de nuestra muestra a utilizar nos basamos en la fórmula de la universidad libertador de Venezuela cirterplan, obteniendo como resultado:

Fórmula Utilizada:

$$n = \frac{m}{e^2(m-1)+1}$$

CUADRO NO II

CÁLCULO DE LA MUESTRA PARA ESTABLECIMIENTO QUE ACEPTAN TARJETAS DE CRÉDITO

Tamaño de la población (m)	16000
Error de estimación (e)	8%
Tamaño de la muestra (n)	273

Elaboración: Carlos Solis

Fuente: Investigación

El tamaño de la muestra nos indica el número establecimientos comerciales que procesan pagos con tarjetas de crédito a encuestarse, las encuestas se realizaran a establecimientos ubicados en la ciudad de Guayaquil.

Los profesionales a entrevistarse serán seleccionados de manera práctica, eligiendo entre las personas que intervienen en el proceso de una transacción con tarjeta de crédito.

OPERACIONALIZACIÓN DE VARIABLES

CUADRO No III

MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

Variables	Dimensiones	Indicadores	Técnicas y/o Instrumentos
Variable Independiente Transacciones Electrónicas Realizadas Por Instituciones Comerciales. El presente sistema está orientado a mantener y aumentar la disponibilidad para realizar transacciones electrónicas en instituciones Comerciales.	Evaluar: Transacciones Electrónicas realizadas en establecimientos comerciales.	Comprensión de Sistema 100%	Número de transacciones electrónicas realizadas con tarjetas de crédito.

Variables	Dimensiones	Indicadores	Técnicas y/o Instrumentos
Variables dependientes **Medio Alterno para Pagos.** El contar con un medio alternativo de pagos es el objetivo al cual está destinada nuestra aplicación, beneficiando de todos los servicios brindados por nuestro sistema a las entidades que realizan cobros con tarjetas de crédito. Dando como resultado alta disponibilidad en las transacciones financieras realizadas en estas entidades.	Evaluar: Medios Tradicionales para pagos.	Comprensión de Sistema 100%	Ciclo de vida de una transacción financiera con tarjeta de crédito.

Variables	Dimensiones	Indicadores	Técnicas y/o Instrumentos
Estándar ISO y Normas PCI DSS. Estándares y normas en la cual será basado nuestro sistema, garantizando de esta manera la seguridad de la información durante la realización de una transacción financiera con tarjeta de crédito.	Seguridad: Estándares y normas con las cual se regirá nuestro sistema.	Seguridades 100%	PCI SSC (Payment Card Industry Security Standards Council) Mensajería ISO 8583

Variables	Dimensiones	Indicadores	Técnicas y/o Instrumentos
Lector de Banda Magnética. Nos permitirá leer la información de banda magnética de una tarjeta de crédito, con la cual se dará inicio al ciclo de vida de la transacción financiera.	Procesos: Obtener información de la banda magnética de la tarjeta de crédito.	Comprensión de la información 100%	Lector de banda magnética.

Elaboración: Carlos Solís

Fuente: Investigación

INSTRUMENTOS DE LA INVESTIGACIÓN

Para nuestra investigación se determinó utilizar los siguientes instrumentos:

GUIÓN DE ENTREVISTA

Se basara en obtener los inconvenientes de los establecimientos comerciales, para realizar transacciones con tarjeta de crédito con los sistemas con los que actualmente cuenta.

REGISTRO DE OBSERVACIÓN

Nos basaremos en este instrumento para poder verificar el resultado de nuestro sistema verificando si es acorde a los objetivos planteados, para así poder ir mejorando el sistema, para al final poder brindar el servicio propuesto.

INTERNET

Es una herramienta principal al momento de despejar ciertas dudas y para la obtención de información encontrada en sitios plenamente confiables, nos permite aclarar dudas con respecto a la configuración e implementación de ciertas aplicaciones utilizadas en nuestro proyecto.

PROCEDIMIENTOS DE LA INVESTIGACIÓN

Para nuestro proyecto sobre el desarrollo de un sistema de pagos para establecimientos comerciales, se siguió los siguientes puntos:

EL PROBLEMA:

Ubicación del problema.

Definición de la situación de conflicto y sus nudos críticos

Identificación de las causas y consecuencias del problema

Delimitación del problema.

Formulación del problema

Evaluación del problema

Planteamiento del problema

Identificación de objetivos generales, específicos

Justificación e importancia.

MARCO TEÓRICO:

Identificación de los antecedentes del estudio

Fundamentación teórica

Fundamentación legal

Preguntas a contestarse

Definición de las variables de la investigación

Definiciones conceptuales

METODOLOGÍA:

Diseño de Investigación

Modalidad de la Investigación

Tipo de Investigación

Población y Muestra

Operacionalización de variables, dimensiones e indicadores

Instrumentos de recolección de datos

Instrumentos de la investigación

Procedimiento de la Investigación

Criterios para la elaboración de la propuesta

RECOLECCIÓN DE LA INFORMACIÓN

Para poder obtener la información necesaria se utilizaran las siguientes técnicas:

LA ENTREVISTA

Esta técnica será utilizada para poder conseguir la información necesaria de los inconvenientes que tienen con establecimientos comerciales al momento de realizar cobros con tarjetas de créditos usando los sistemas actuales.

LA OBSERVACIÓN

Llevaremos a cabo esta técnica con la finalidad de verificar la interacción de los usuarios con nuestro sistema.

Esta técnica nos va a definir cuál es el estado actual del sistema, si está diseñado acorde a los objetivos o si falta agregar algún componente y valor agregado para así finalmente poder dar como resultado una aplicación completamente confiable y de calidad.

PROCESAMIENTO Y ANÁLISIS

Los datos obtenidos en la investigación realizada serán sometidos a pruebas de análisis con el fin de comprender y visualizar los resultados obtenidos, para así poder dar respuestas a las preguntas planteadas.

A continuación se detallan los pasos a seguir para la elaboración de nuestro análisis:

- Revisión de los instrumentos aplicados
- Tabulación de datos con relación a cada uno de los Ítems
- Diseño y elaboración de cuadros estadístico con los resultados anteriores.
- Elaboración de gráficos

El presente trabajo de Tesis de Grado, basado en la investigación que se realizó para conocer y plantear una alternativa de solución al problema planteado
"SISTEMA DE PAGOS BASADO EN EL ESTÁNDAR ISO 8583 Y NORMAS PCI DSS UTILIZANDO LECTORES DE BANDA MAGNÉTICA DESAROLLADO EN JAVA" se basó en la aplicación de una encuesta a entidades que procesan pagos con tarjetas de crédito para la recolección de datos.

El instrumento se elaboró a través de un cuestionario de preguntas en lo fundamental de tipo cerradas, para tener indicadores sencillos de tabular y de esa manera poder apoyarnos para la demostración de la hipótesis planteada.

Para el proceso de tabulación de los datos, se realizó mediante el aplicativo de office, EXCEL, mediante el cual se logró el ingreso y procesamiento de los datos recabados en la aplicación de la encuesta para manejar indicadores suficientes, que justifiquen la investigación, los mismos que se expresan en cuadros estadísticos, gráficos y analíticamente a continuación.

PREGUNTA 1

¿Tiene Usted dificultades al recibir cobros con tarjetas de crédito?

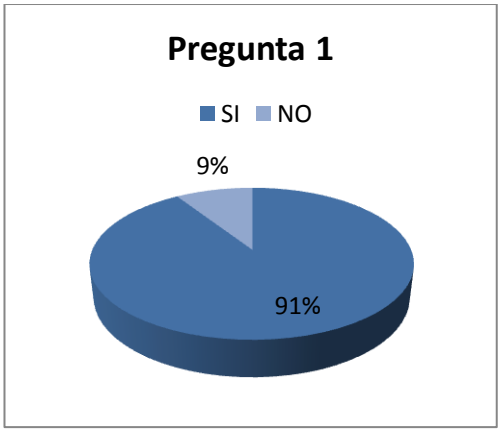
CUADRO NO IV
PREGUNTA 1

PREGUNTA	% SI	% NO
1	91%	9%

Elaboración: Carlos Solis

Fuente: Resultados de la encuesta

Gráfico 2



Elaboración: Carlos Solis

Fuente: Resultados de la encuesta

El análisis de estos datos nos indica que a 9 de cada 10 personas encuestadas se les han presentado inconvenientes al realizar cobros con tarjetas de crédito.

PREGUNTA 2

¿Conoce algún sistema alternativo para cobrar con tarjetas de crédito?

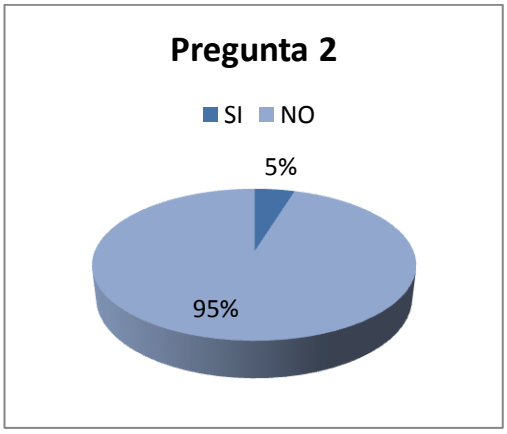
CUADRO NO V
PREGUNTA 2

PREGUNTA	% SI	% NO
1	5%	95%

Elaboración: Carlos Solis

Fuente: Resultados de la encuesta

Gráfico 3



Elaboración: Carlos Solis

Fuente: Resultados de la encuesta

Como podemos ver, tenemos más del 90% de negación por parte de las personas encuestadas con respecto a esta pregunta. El análisis de estos datos nos indica que 9 de cada 10 personas encuestadas no conocen sistemas alternativos para realizar cobros con tarjetas de crédito.

PREGUNTA 3

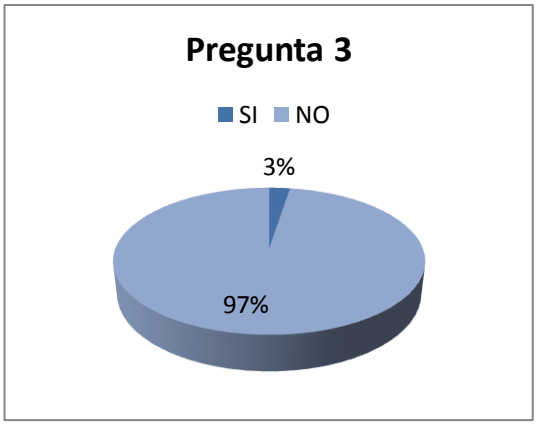
¿En caso de fallar su sistema para cobrar con tarjetas de crédito, cuenta con un medio alternativo de cobro?

CUADRO NO VI
PREGUNTA 3

PREGUNTA	% SI	% NO
1	3%	97%

Elaboración: Carlos Solis
Fuente: Resultados de la encuesta

Gráfico 4



Elaboración: Carlos Solis
Fuente: Resultados de la encuesta

Como podemos ver, tenemos más del 90% de negación por parte de las personas encuestadas con respecto a esta pregunta. El análisis de estos datos nos indica que 9 de cada 10 personas encuestadas no cuentan con un medio alterno en caso de fallas de su sistema tradicional.

PREGUNTA 4

¿Ha perdido clientes o ventas por problemas en su sistema actual?

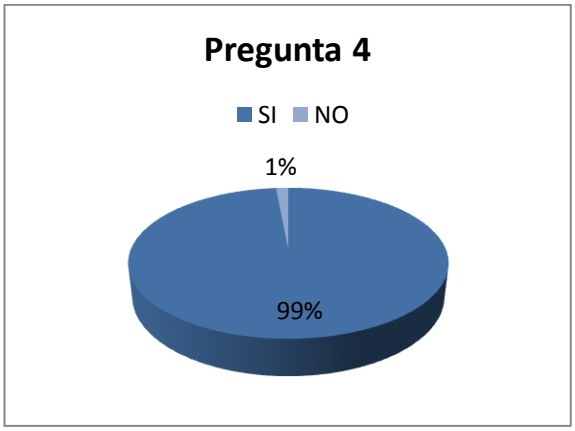
CUADRO NO VII
PREGUNTA 4

PREGUNTA	% SI	% NO
1	99%	9%

Elaboración: Carlos Solis

Fuente: Resultados de la encuesta

Gráfico 5



Elaboración: Carlos Solis

Fuente: Resultados de la encuesta

Como podemos ver, tenemos más del 90% de aceptación por parte de las personas encuestadas con respecto a esta pregunta. El análisis de estos datos nos indica que 9 de cada 10 personas encuestadas han perdido ventas o clientes por fallas con su sistema tradicional.

PREGUNTA 5

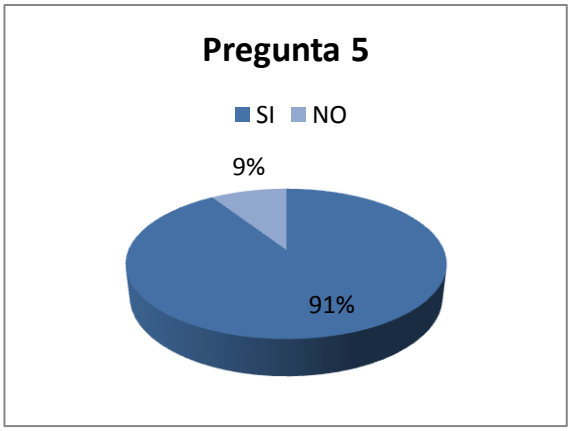
¿Le gustaría contar con un sistema alterno de cobros que le garantice mayor disponibilidad en caso de fallos del actual?

CUADRO NO VIII
PREGUNTA 5

PREGUNTA	% SI	% NO
1	84%	16%

Elaboración: Carlos Solis
Fuente: Resultados de la encuesta

Gráfico 6



Elaboración: Carlos Solis
Fuente: Resultados de la encuesta

Como podemos ver, tenemos más del 90% de aceptación por parte de las personas encuestadas con respecto a esta pregunta. El análisis de estos datos nos indica que 9 de cada 10 personas encuestadas están de acuerdo con un sistema que brinde alta disponibilidad en caso de fallas de su sistema tradicional.

CAPÍTULO IV

MARCO ADMINISTRATIVO

CRONOGRAMA

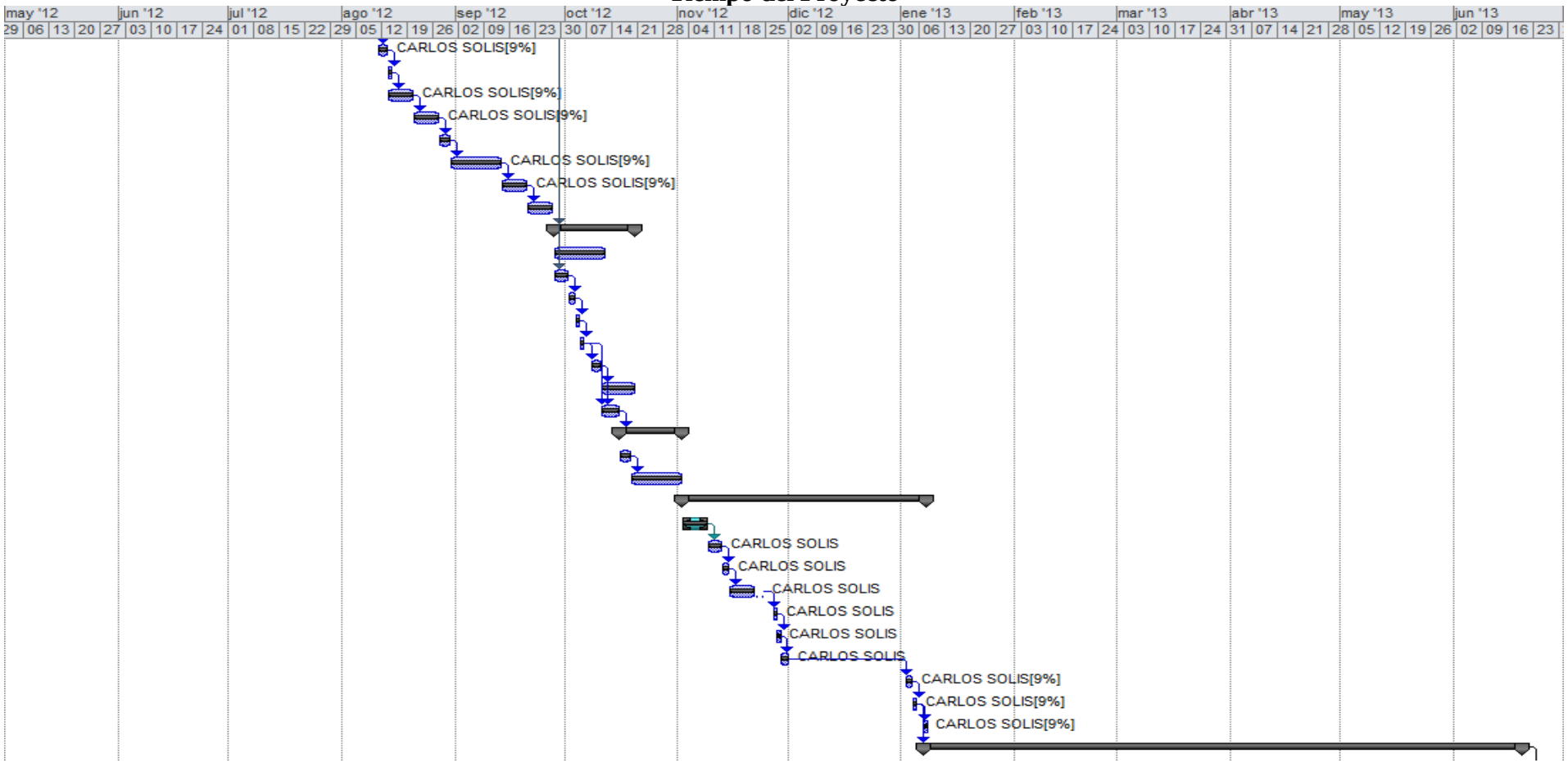
Gráfico 7
Actividades del Proyecto

Id	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	% completado
1	**INVESTIGACION**	**69 días**	**lun 25/06/12**	**jue 27/09/12**		100%
2	INSTALACION Y CONFIGURACION DE SO LINUX DISTRIBUCION UBUNTU 12.04	5 días	lun 25/06/12	vie 29/06/12		100%
3	INSTALACION Y CONFIGURACION DE SO WINDOWS 2008 SERVER	2 días	lun 02/07/12	mar 03/07/12	2	100%
4	NORMAS PCI-DSS APLICABLES	5 días	mar 03/07/12	mar 10/07/12	3	100%
5	CREACIÓN POLÍTICAS HARDENING PARA WINDOWS 2008 SERVER	10 días	mar 10/07/12	mar 24/07/12	4	100%
6	INSTALACION Y CONFIGURACION DE JAVA PARA WINDOWS	2 días	mar 24/07/12	jue 26/07/12	5	100%
7	INSTALACION Y CONFIGURACION DE JAVA PARA LINUX	3 días	jue 26/07/12	mar 31/07/12	6	100%
8	INSTALACIÓN Y CONFIGURACIÓN LECTOR DE BANDA MAGNÉTICA LINUX	2 días	mar 31/07/12	jue 02/08/12	7	100%
9	INSTALACIÓN Y CONFIGURACIÓN LECTOR DE BANDA MAGNÉTICA WINDOWS	2 días	mar 07/08/12	jue 09/08/12	8	100%
10	INSTALACION Y CONFIGURACION DE LA PLATAFORMA NETBEANS PARA WINDOWS	1 día	jue 09/08/12	vie 10/08/12	9	100%
11	INSTALACION Y CONFIGURACION DE LA PLATAFORMA NETBEANS PARA LINUX	1 día	vie 10/08/12	lun 13/08/12	10	100%
12	TIPO DE TRANSACCIONES CON TARJETAS DE CRÉDITO	1 día	lun 13/08/12	mar 14/08/12	11	100%
13	ESTABLECIMIENTOS QUE REALIZAN TRANSACCIONES CON TARJETAS DE CRÉDITO	5 días	lun 13/08/12	lun 20/08/12	12	100%
14	MANEJO DE COMPONENTES DE DISEÑO (Swing)	5 días	lun 20/08/12	lun 27/08/12	13	100%
15	CICLO DE VIDA DE UNA TRANSACCIÓN	3 días	lun 27/08/12	jue 30/08/12	14	100%
16	MANEJO DE LENGUAJE DE PROGRAMACION Y AGREGADOS (Java, Seguridad)	10 días	jue 30/08/12	jue 13/09/12	15	100%
17	CIFRADO 3DES EN JAVA	5 días	jue 13/09/12	jue 20/09/12	16	100%
18	ISO 8583 EN JAVA	5 días	jue 20/09/12	jue 27/09/12	17	100%
19	**DOCUMENTACION**	**16 días**	**vie 28/09/12**	**vie 19/10/12**	**1**	**100%**
20	DOCUMENTACIÓN EN GENERAL	10 días	vie 28/09/12	jue 11/10/12		100%
21	PREPARAR EL CUESTIONARIO	2 días	vie 28/09/12	lun 01/10/12	1	100%
22	PREPARAR EL GUION DE LA ENTREVISTA	2 días	mar 02/10/12	mié 03/10/12	21	100%
23	SEPARAR CITAS CON LOS ESPECIALISTAS	1 día	jue 04/10/12	jue 04/10/12	22	100%
24	PREPARAR EL GUION DE LA ENCUESTA	1 día	vie 05/10/12	vie 05/10/12	23	100%
25	REALIZAR ENTREVISTAS	3 días	lun 08/10/12	mié 10/10/12	24	100%
26	REALIZAR ENCUESTAS	7 días	jue 11/10/12	vie 19/10/12	25	100%
27	ANALISIS DE LOS DATOS OBTENIDOS	3 días	jue 11/10/12	lun 15/10/12	25,24	100%
28	**DISEÑO**	**13 días**	**mar 16/10/12**	**jue 01/11/12**	**27**	**100%**
29	ESTRUCTURA DEl SISTEMA DE ARCHIVOS	3 días	mar 16/10/12	jue 18/10/12		100%
30	DISEÑO DE PANTALLAS DEL SISTEMA	10 días	vie 19/10/12	jue 01/11/12	29	100%
31	**PREPARAR AMBIENTE DE DESARROLLO**	**47 días**	**vie 02/11/12**	**lun 07/01/13**		**100%**
32	ADQUISICION DE LOS SISTEMAS NECESARIOS	5 días	vie 02/11/12	jue 08/11/12		100%
33	INSTALACION Y CONFIGURACION DE SO LINUX DISTRIBUCION UBUNTU 12.04	2 días	vie 09/11/12	lun 12/11/12	32	100%
34	INSTALACION Y CONFIGURACION DE SO WINDOWS 2008 SERVER	2 días	mar 13/11/12	mié 14/11/12	33	100%
35	CREACIÓN POLÍTICAS HARDENING PARA WINDOWS 2008 SERVER	5 días	jue 15/11/12	vie 23/11/12	34	100%
36	INSTALACION Y CONFIGURACION DE JAVA PARA WINDOWS	1 día	mar 27/11/12	mar 27/11/12	35	100%
37	INSTALACION Y CONFIGURACION DE JAVA PARA LINUX	1 día	mié 28/11/12	mié 28/11/12	36	100%
38	INSTALACIÓN Y CONFIGURACIÓN LECTOR DE BANDA MAGNÉTICA LINUX	2 días	jue 29/11/12	vie 30/11/12	37	100%
39	INSTALACIÓN Y CONFIGURACIÓN LECTOR DE BANDA MAGNÉTICA WINDOWS	2 días	mié 02/01/13	jue 03/01/13	38	100%
40	INSTALACION Y CONFIGURACION DE LA PLATAFORMA NETBEANS PARA WINDOWS	1 día	vie 04/01/13	vie 04/01/13	39	100%
41	INSTALACION Y CONFIGURACION DE LA PLATAFORMA NETBEANS PARA LINUX	1 día	lun 07/01/13	lun 07/01/13	40	100%
42	**DESARROLLO DEL SISTEMA**	**118 días**	**lun 07/01/13**	**mié 19/06/13**	**40**	**100%**
43	CREAR SISTEMA DE CIFRADO	5 días	lun 07/01/13	vie 11/01/13		100%
44	CREAR SISTEMA DE ARCHIVOS	5 días	lun 14/01/13	vie 18/01/13		100%
45	CREACIÓN DE ROLES DEL SISTEMA	3 días	jue 17/01/13	lun 21/01/13		100%
46	PANTALLAS DE INICIO Y OPCIONES	15 días	mar 22/01/13	lun 11/02/13		100%
47	INICIO DE SESIÓN	5 días	mar 12/02/13	lun 18/02/13		100%
48	CREAR MÉTODO CONEXIÓN LECTOR DE BANDA MAGNÉTICA	15 días	mar 19/02/13	lun 11/03/13		100%
49	CREAR MÉTODO PARA OBTENER INFORMACIÓN DE BANDA MAGNÉTICA	8 días	mar 12/03/13	jue 21/03/13		100%
50	CREACIÓN DE MÓDULOS DEL SISTEMA	15 días	mar 26/03/13	lun 15/04/13		100%
51	MÓDULO DE PARAMETRIZACION	10 días	lun 15/04/13	vie 26/04/13		100%
52	APLICACIÓN ISO 8583	10 días	vie 26/04/13	jue 09/05/13		100%
53	PROCESAMIENTO DE TRANSACCIONES FINANCIERAS	10 días	vie 10/05/13	jue 23/05/13		100%
54	APLICACIÓN PCI-DSS	10 días	vie 24/05/13	jue 06/06/13		100%
55	MODULO SERVIDOR	10 días	jue 06/06/13	mié 19/06/13		100%
56	PRUEBAS DE CALIDAD	5 días	mié 19/06/13	mar 25/06/13	42	100%
57	DESARROLLO DE ALGUN FALTANTE	10 días	mar 25/06/13	lun 08/07/13	56	100%

Elaboración: Carlos Solis

Fuente: Análisis de actividades a desarrollar

Grafico 8
Tiempo del Proyecto



Fuente: Carlos Solis
Elaboración: Análisis de actividades a desarrollar

PRESUPUESTO

CUADRO No IV

DETALLE DE EGRESOS DEL PROYECTO

EGRESOS	**DÓLARES**
Suministros de oficina y computación	20.00
Computadora y servicios de Internet	1500.00
Transporte	25.00
Comida	350.00
Empastado, anillado de tesis de grado	30.00
Lector de Banda Magnética	30.00
TOTAL……	1955.00

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Las conclusiones y recomendaciones que se presentan a continuación, están basadas de acuerdo a un análisis elaborado a las encuestas y entrevistas, las cuales fueron realizadas a los expertos en el área y a los posibles usuarios los cuales serán los principales beneficiados con este sistema y en función del estudio realizado durante el presente trabajo.

CONCLUSIONES

El número de transacciones con tarjetas de crédito que se realizan en el país está en vías de crecimiento y con el pasar del tiempo se ha popularizado, cada día es más común poseer dinero plástico (18).

Sin embargo, este crecimiento no va de la mano con el desarrollo de sistemas alternos de pagos ante fallas que ocurran en los sistemas tradicionales, ocasionando que la actividad comercial en las entidades que no cuentan con medios alternos de pago se vea afectada, llegando a producir pérdidas económicas, malestar en los clientes e incluso afectar la imagen comercial de los establecimientos.

La aceptación por parte de las entidades de tener medios alternos, que garanticen disponibilidad para sus transacciones con tarjeta de crédito es alta, debido a que en su gran mayoría han experimentado perdidas económicas por no contar con un medio que cumpla con esta función.

RECOMENDACIONES

- Se recomiendo establecer procedimientos de actualización y mantenimiento de los sistemas tradicionales, usando nuestro sistema para mitigar el tiempo fuera de servicio, de esta manera garantizar la continuidad de las labores comerciales.
- Si recomienda seguir los puntos de la guía de cumplimiento de las PCI-DSS correspondientes a la pc donde será instalada nuestro sistema, adicionalmente se sugiere como una buena práctica tener actualizado el software antivirus, en la pc donde será instalado nuestro sistema.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS

Harvey M. Deitel, Paul J. Deitel (2004). *Como programar en Java.* México. Pearsom Educación.

O'reilly & Associates (2004). Seguridad de las redes de evaluación.

Gilles Chamillard (2011) UBUNTU - Administración de un sistema Linux.

Thierry Groussard (2012) Java 7 – Fundamentos de programación en Java.

José Dordoigne (2006) Redes informáticas - Nociones fundamentales - [3ª edición]

ACISSI (2011) Seguridad informática - Ethical Hacking.

José Dordoigne, Philippe Atelin (2006) Redes Informáticas - Conceptos Fundamentales.

Amparo Fuster Sabater (2012) - Criptografía, Protección De Datos Y Aplicaciones

VV.AA., RA-MA (2010) Criptografía - Técnicas de desarrollo para profesionales

PUBLICACIONES

JUSTIFICACIÓN E IMPORTANCIA - NORMAS PCI DSS: Nomas de seguridad de datos para la industria de tarjetas de pago

http://es.pcisecuritystandards.org/minisite/en/pa-dss-v2-0.php

(16) FUNDAMENTOS LEGALES – OPEN SOURCE: Constitución de la República del Ecuador, Sobre el Open Source. Decreto 1014.

http://www.ueb.edu.ec/uploads/Leyes/Decreto_1014_software_libre_Ecuador.pdf

(17) INCLUSIÓN DIGITAL. (23/01/2012). Tarjetas de crédito que circulan en el Ecuador

http://www.Ecuadorinmediato.com/index.php?module=Noticias&func=news_user_view&id=165772&umt=en_Ecuador_circulan_mas_24_millones_tarjetas_credito

(18) INCLUSIÓN DIGITAL. (23/01/2012). El Endeudamiento de los Tarjetahabientes se incrementó en más del 20%

http://www.elfinanciero.com/banca_especiales/tema_12_2012/banca_01_2012.pdf

DIRECCIONES WEB

(1) **ESTABLECIMIENTO COMERCIAL:** Resumen en base a información extraída del sitio web **http://es.wikipedia.org/wiki/Establecimiento_comercial**

(2) **NORMAS DE LA SEGURIDAD DE DATOS DE TARJETAS DE CRÉDITO:** Resumen en base a información extraída del sitio web:

https://www.pcisecuritystandards.org/security_standards/

(3) ISO 8583: Definición: Resumen en base a información extraída del sitio web:

http://es.wikipedia.org/wiki/ISO_8583

(4)CÓDIGO ABIERTO: Definición y origen; Resumen en base a información extraída del sitio web:

http://es.wikipedia.org/wiki/Codigo_abierto

(5) LINUX: Definiciones, estructura, versiones e historia, en base a información extraídos desde el sitio web: http://es.wikipedia.org/wiki/Unix

(6) UBUNTU: Conceptos, versiones e historia**,** en base a información extraídos desde el artículo publicado en: http://www.ubuntu-es.org

(7) Seguridad de la Información: Definiciones y funcionamiento, en base a información del artículo extraído desde el sitio web: http://es.wikipedia.org/wiki/Seguridad_de_la_informacion

(8) JAVA: Definiciones y funcionamiento, en base a información del artículo extraído desde el sitio web: http://es.wikipedia.org/wiki/Java

(9) TARJETA DE CRÉDITO: Resumen en base a información: extraída del sitio: http://es.wikipedia.org/wiki/Tarjeta_de_credito

(10) Criptografía: Definición en base a información extraída desde el sitio web: http://es.wikipedia.org/wiki/Cifrado_(criptografia)

(11) 3DES: Definición, Seguridad y usos en base a información extraídos desde: http://es.wikipedia.org/wiki/3DES

(12)BANDA MAGNÉTICA: Definición en base a información extraída desde: http://es.wikipedia.org/wiki/Banda_magnetica

(13) Pasarela de Pago: Definición y funcionamiento en base a información referenciados desde:

http://es.wikipedia.org/wiki/Pasarela_de_pago

(14) FLUJO DE UNA TRANSACCIÓN: Definiciones para entender mejor el flujo de una transacción en base a información extraída del sitio: http://www.mastercard.com

(15) J8383: Definiciones y usos:

http://j8583.sourceforge.net

(16) JPOS: Usos y librerías para transacciones ISO 8583:

http://jpos.org/

ANEXO 1

ENCUESTA

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

ENCUESTA

1. ¿Tiene Usted dificultades al recibir cobros con tarjetas de crédito?

   Si ( ) No ( )

2. ¿Conoce algún sistema alternativo para cobrar con tarjetas de crédito?

   Si ( ) No ( )

3. ¿En caso de fallar su sistema para cobrar con tarjetas de crédito, cuenta con un medio alternativo de cobro?

   Si ( ) No ( )

4. ¿Ha perdido clientes o ventas por problemas en su sistema actual?

   Si ( ) No ( )

5. ¿Le gustaría contar con un sistema alterno de cobros que le garantice mayor disponibilidad en caso de fallos del actual?

   Si ( ) No ( )

ANEXO 2

ENTREVISTA

ENTREVISTA

1. **¿Cree usted que se ha incrementado el uso de las tarjetas de crédito en el ecuador?**

   Si, muchos clientes pagan con tarjetas de crédito actualmente.

2. **¿Cuáles cree usted que son los principales problemas que tiene un establecimiento comercial que acepta tarjetas de crédito?**

   De vez en cuando el dispositivo que usamos presenta problemas, lo que nos evita seguir cobrando con tarjetas, esto nos perjudica ya que los clientes que no cuentan con dinero en efectivo en el momento, se van a otro lugar.

3. **¿Conoce algún sistema para realizar cobros con tarjetas de crédito en los establecimientos Comerciales, cuáles?**

   Si, los POS.

4. **¿Qué tan conveniente considera el costo de los sistemas actuales para poder realzar cobros con tarjetas de crédito?**

   Considero que el alquiler es un poco alto.

5. **¿Cuáles son las dificultades que existen actualmente en estos sistemas?**

   A estos equipos ocasionalmente se les daña la impresora, la batería o se suelen bloquear.

6. **¿Le gustaría contar con un sistema alternativo para cobrar con tarjetas, en caso que falle el sistema principal?**

   Por supuesto que sí, sería de gran ayuda.

Nombre: Lissette Gainza Cornejo
Trabajo: Control Salud S.A
Cargo: Asistente. Contable
Teléfono: (04)5120306 ext 115

ENTREVISTA

1. **¿Cree usted que se ha incrementado el uso de las tarjetas de crédito en el ecuador?**

   Por supuesto, muchas personas solicitan tarjetas de crédito e incluso utilizan varias.

2. **¿Cuáles cree usted que son los principales problemas que tiene un establecimiento comercial que acepta tarjetas de crédito?**

   Aglomeración de personas.

3. **¿Conoce algún sistema para realizar cobros con tarjetas de crédito en los establecimientos Comerciales, cuáles?**

   Si, los POS.

4. **¿Qué tan conveniente considera el costo de los sistemas actuales para poder realzar cobros con tarjetas de crédito?**

   Tienen un costo adecuado, aunque hay que cambiarlos cada vez que cumplen su vida útil.

5. **¿Cuáles son las dificultades que existen actualmente en estos sistemas?**

   Demoran mucho.

6. **¿Le gustaría contar con un sistema alternativo para cobrar con tarjetas, en caso que falle el sistema principal?**

   Si, esto aumentaría la disponibilidad de los sistemas actuales.

Nombre: Francisco Vega Hall
Trabajo: Dinners Club
Cargo: Asesor Comercial
Teléfono: 0980164656

ANEXO 3

GUÍA DE CUMPLIMIENTO PCI-DSS

La presente guía, muestra las políticas aplicadas a nuestro sistema, adicionalmente se incluirá aquellos requisitos que deberán aplicarse en la computadora anfitriona de nuestro sistema.

Requisito 1.4: Instale software de firewall personal en toda computadora móvil o de propiedad de los trabajadores con conectividad directa a Internet (por ejemplo, laptops que usan los trabajadores), mediante las cuales se accede a la red de la organización.

Para cumplir con este Requisito, en el sistema operativo anfitrión que se instalara la aplicación contara con un firewall personal activo.

Requisito 2.2: Desarrolle normas de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y que concuerden con las normas de alta seguridad de sistema aceptadas en la industria.

Entre las fuentes de normas de alta seguridad aceptadas en la industria, se pueden incluir, a modo de ejemplo Center for Internet Security (CIS).

Para cumplir con este requisito, la aplicación será presentada sobre un sistema Operativo Windows 2008 Server al cual previamente se le ha aplicado el Hardening CIS 1.2 para Este Sistema Operativo.

https://benchmarks.cisecurity.org/tools2/windows/CIS_Windows_Server_2008_Benchmark_v1.2.0.pdf

Requisito 3.1: Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.
La aplicación únicamente almacena el pan encriptado, estos datos permanecen almacenados hasta que se realice un cierre de lote, posterior a esto, la información es borrada.

Requisito 3.2: No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados).
La aplicación no almacena datos confidenciales de autenticación, ni cvv2, ni fecha de expiración ni el Pin de la tarjeta.

Requisito 3.2.1: No almacene contenido completo de ninguna pista de la banda magnética.
La aplicación no almacena el contenido completo de la banda magnética, una vez leído el contenido de la banda magnética, únicamente se almacena el contenido del pan encriptado, el resto de la información es eliminada una vez completada la transacción.

Requisito 3.2.2: No almacene el valor ni el código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago).
Este número solo es usado en el proceso de la transacción, pero la aplicación no lo almacena.

Requisito 3.2.3: No almacene el número de identificación personal (PIN) ni el bloqueo del PIN cifrado.

La aplicación no almacena el PIN.

Requisito 3.3: Oculte el PAN cuando aparezca (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá).

La aplicación permite enmascarar el número de tarjeta de crédito, únicamente mostrando los 6 primeros dígitos y los 6 4 últimos dígitos.

Requisito 3.4: Haga que el PAN quede ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles, en medios de copia de seguridad y en registros), se debe utilizar cifrado sólido para hacer ilegible la información la información.

La aplicación utiliza algoritmo 3DES De 128 bits, este mecanismo es uno de los mecanismos de cifrado aceptado para proteger la información.

Requisito 4.1: Utilice cifrado sólido y protocolos de seguridad (por ejemplo, SSL/TLS, IPSEC, SSH, etc.) para proteger datos confidenciales del titular de la tarjeta durante la transmisión por redes públicas abiertas.

La aplicación utiliza algoritmo 3DES De 128 bits para transmitir información Confidencial durante el proceso de la transacción.

Requisito 4.2: Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea, el chat, etc.).

La aplicación no utiliza tecnologías de mensajería de usuario final.

Requisito 5: Utilice y actualice regularmente el software o los programas antivirus

Para cumplir con este requisito, la aplicación será instalada y presentada en un sistema anfitrión el cual contara con un sistema antivirus activado y actualizado.

Requisito 6.3.1: Eliminación de las cuentas, los ID de usuario y las contraseñas personalizadas de la aplicación antes de que las aplicaciones se activen o se pongan a disposición de los clientes.

Los usuarios genéricos serán eliminados previa instalación inicial de la aplicación.

Requisito 6.4.4: Eliminación de datos y cuentas de prueba antes de que se activen los sistemas de producción.

Todos los datos generados para probar la aplicación son eliminados previo pase a producción.

Requisito 7.1.1: Restricciones a los derechos de acceso a ID de usuarios privilegiadas a la menor cantidad de privilegios necesarios para cumplir con las responsabilidades del cargo.

La aplicación cuentas con tres tipos de perfiles, los cuales permiten cumplir con este requisito, otorgando solo los permisos necesarios para cada función.

Requisito 7.1.2: La asignación de privilegios se basa en la tarea del personal individual, su clasificación y función.

Los perfiles de Cajero, supervisor y administrador permiten utilizar la aplicación de tal manera que solo se pueda acceder a los módulos necesarios para cumplir con el rol mencionado.

Requisito 8.1: Asigne a todos los usuarios una ID única antes de permitirles tener acceso a componentes del sistema o a datos de titulares de tarjetas.

La aplicación maneja acceso único para cada usuario, será responsabilidad del huésped de la aplicación generar procesos para cumplir con este requisito, es decir, asignar ID única para cada usuario de la aplicación.

Requisito 8.5.3: Configure la primera contraseña en un valor único para cada usuario y cámbiela de inmediato después del primer uso.

La aplicación solicitara cambiar la contraseña antes del primer ingreso.

Requisito 8.5.9: Cambie las contraseñas de usuario al menos cada 90 días.

La aplicación solicitara cambiar la contraseña cada 90 días.

Requisito 8.5.10: Solicite una longitud de contraseña mínima de siete caracteres.

La aplicación solicitara una longitud mínima de 7 caracteres.

Requisito 8.5.12: No permita que ninguna persona envíe una contraseña nueva igual a cualquiera de las últimas cuatro contraseñas utilizadas.

La aplicación validara que la contraseña no sea igual a las 4 últimas ingresadas.

Requisito 8.5.13: Limite los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos.

La aplicación bloqueara el ID luego de 6 intentos de acceso erróneos, hasta que un usuario con privilegio administrativo la habilite nuevamente.

ANEXO 4

MENSAJERÍA ISO UTILIZADA

Mensajería ISO 8583

Mensaje Transacción Compra (Crédito Corriente–Diferido), Anulación

Bit/ Map	Nombre del campo	Formato	Tipo	Req	Resp	Comentarios
	Longitud de la trama (No incluye estos 2 bytes)		B 16	M	M	Este campo se incluye la longitud de la trama a enviar o recibir. El formato es Hexadecimal Empaquetado. Ej: Long. Trama: 121 bytes
	Carácter Fijo		An 1	M	M	Asc: 96 " ` " o el equivalente en Hex: 0x60
	TPDU		N 4	M	M	4 bytes. Formato 0020: Origen 0030: Destino En la trama de respuesta se debe invertir el destino por el origen 0030 0020
	MESSAGE TYPE ID		N 4	0200	0210	

	BIT MAP		B 64	M	M	
	2do BIT MAP		B 64	C	C	
02	Primary account Number	LLVAR	N..19	C01		
03	Processing Code		N 6	TTA A0X	TTAA 0X	Ver tabla 2.1
04	Transaction Amount		N 12	M	O	**Requerimiento** Monto total de la transacción **Respuesta** Para MasterCard en este campo viene en la moneda del pais origen de la transacción
11	System Trace Audit Number		N 6	M	M	Echo
12	Local transaction Time		N6	M	M	HHMMSS
13	Local transaction Date		N 4	M	M	MMDD
14	Expiration Date		N 4	C01		YYMM
18	Merchant Type		N 4	C		Campo necesario en MasterCard para ISIS / VISA

22	Entry Mode		N 3	RRP	M	Ver tabla 2.2
24	Network International Id		N 3	O	O	
38	Autorization Number		An 6	C03	C03	
39	Response code		An 2		M	
41	Terminal ID		An 8	M	M	
42	Merchant ID		An 15	M		
45	TRACK I Data	LLVAR	An..99	C02		
48	Additional Data	LLLVAR	Ans..255	C04	C	Información CVC /CVV formato 9203xxx (xxx es el cvc2 o cvv2) Ver Tabla 2.3
112	Información Diferidos	LLLVAR	An..120	C09		Ver Tabla 2.10
114	Número De Lote Activo	LLLVAR	An..120	M		Ver Tabla 2.11
119	Montos Transacción	LLLVAR	An..120	M		Ver Tabla 2.14
120	Información Impuestos	LLLVAR	An..120	C10	C11	Ver Tabla 2.15
121	CVV	LLLVAR	An..120	O		Ver Tabla 2.16

122	Track 2 Data	LLLVAR	An..120	O	O	Ver Tabla 2.17
123	Mkey Data	LLLVAR	LLLVAR	O	O	Ver Tabla 2.18
127	Versión	LLLVAR	An..128	O		Ver Tabla 2.21

C01: Si la información del Track se envía encriptado; no se enviará este campo.

C02: Si la información del Track se envía encriptado; no se enviará este campo.

C03: Si la transacción es declinada este campo puede ir en ceros o ser omitido, para una anulación deberá viajar en el requerimiento

C04: Se enviará este campo cuando se envié el campo CVV y/o diferidos

C06: Este campo viajará la llave de trabajo en la trama de respuesta cuando se realice una transacción de compras de débito en la aplicación.

C09: En este campo viajará información de los tipos de diferidos

C10: En este campo viajará información de los montos adicionales (Iva, servicio…).

C11: En este campo viajará información de los rubros a ser impresos en el recibo para transacciones de diferidos viajara el valor de los intereses.

Mensaje Transacción Reversa

Bit/ Map	Nombre del campo	Formato	Tipo	Req	Resp	Comentarios
	Longitud de la trama (No incluye estos 2 bytes)		B 16	M	M	Este campo se incluye la longitud de la trama a enviar o recibir. El formato es Hexadecimal Empaquetado. Ej: Long. Trama: 121 bytes
	Carácter Fijo		An 1	M	M	Asc: 96 “ ` ” o el equivalente en Hex: 0x60
	TPDU		N 4	M	M	4 bytes. Formato 0020: Origen 0030: Destino En la trama de respuesta se debe invertir el destino por el origen 0030 0020
	MESSAGE TYPE ID		N 4	0400	0410	
	BIT MAP		B 64	M	M	
	2do BIT MAP		B 64	C	C	
02	Primary account Number	LLVAR	N..19	C		
03	Processing Code		N 6	TTAA0X	TTAA	Ver tabla 2.1

					0X	
04	Transaction Amount		N 12	M	O	**Requerimiento** Monto total de la transacción **Respuesta** Para MasterCard en este campo viene en la moneda del pais origen de la transacción
11	System Trace Audit Number		N 6	M	M	Echo
12	Local transaction Time		N6	M	M	HHMMSS
13	Local transaction Date		N 4	M	M	MMDD
14	Expiration Date		N 4	C		YYMM
18	Merchant Type		N 4	C		Campo necesario en MasterCard para ISIS / VISA
22	Entry Mode		N 3	RRP	M	Ver tabla 2.2
24	Network International Id		N 3	O	O	
38	Autorization Number		An 6	C03	C03	
39	Response code		An 2		M	

41	Terminal ID		An 8	M	M	
42	Merchant ID		An 15	M		
48	Additional Data		Ans.255	M	C04	Ver Tabla 2.3
112	Información Diferidos	LLLVAR	An..120	C09		Ver Tabla 2.10
114	Número De Lote Activo	LLLVAR	An..20	M		Ver Tabla 2.11
119	Montos	LLLVAR	An..120	M		Ver Tabla 2.14
120	Impuestos	LLLVAR	An..120	C10	C11	Ver Tabla 2.15
121	CVV	LLLVAR	An..120	O		Ver Tabla 2.16
122	Track 2 Data	LLLVAR	An..120	O	O	Ver Tabla 2.17
123	Mkey	LLLVAR	LLLVAR	O	O	Ver Tabla 2.18
127	Versión	LLLVAR	An..128	O		Ver Tabla 2.21

Mensaje Batch Upload

Bit/ Map	Nombre del campo	Formato	Tipo	Req	Resp	Comentarios
	Longitud de la trama (No incluye estos 2 bytes)		B 16	M	M	Este campo se incluye la longitud de la trama a enviar o recibir. El formato es Hexadecimal Empaquetado. Ej: Long. Trama: 121 bytes
	Carácter Fijo		An 1	M	M	Asc: 96 “ ` ” o el equivalente en Hex: 0x60
	TPDU		N 4	M	M	4 bytes. Formato 0020: Origen 0030: Destino En la trama de respuesta se debe invertir el destino por el origen 0030 0020
	MESSAGE TYPE ID		N 4	0400	0410	
	BIT MAP		B 64	M	M	

	2do BIT MAP		B 64	C	C	
03	Processing Code		N 6	*PPP PPX	*PPPP PX	De la transacción original
04	Transaction Amount		N 12	M		
07	Date & Time	N 10				MMDDHHMMSS
11	System Trace Audit Number		N 6	M	M	Echo
12	Local transaction Time		N6	M	M	HHMMSS
13	Local transaction Date		N 4	M	M	MMDD
14	Expiration Date		N 4	M		YYMM
22	Entry Mode		N 3	RRP	M	De la transacción original
24	Network International Id		N 3	O	O	
38	Autorization Number		An 6	C03	C03	
39	Response code		An 2		M	
41	Terminal ID		An 8	M	M	
42	Merchant ID		An 15	M		

62	Información UpLoad	LLLVAR	An..30	M		Ver Tabla 2.8
112	Información de Diferidos	LLLVAR	An..20	M	C01	Ver Tabla 2.10
119	Montos	LLLVAR	An..120	M		Ver Tabla 2.14
120	Impuestos	LLLVAR	An..120	C10	C11	Ver Tabla 2.15
121	CVV	LLLVAR	An..120	O		Ver Tabla 2.16
122	Track1	LLLVAR	N..40	O	O	Ver Tabla 2.17
123	Mkey	LLLVAR	N 16	O	O	Ver Tabla 2.18
127	Versión	LLLVAR	An..128	O		Versión Aplicación

Mensaje Transacción Cierre

Bit/ Map	Nombre del campo	Formato	Tipo	Req	Resp	Comentarios
	Longitud de la trama (No incluye estos 2 bytes)		B 16	M	M	Este campo se incluye la longitud de la trama a enviar o recibir. El formato es Hexadecimal Empaquetado. Ej: Long. Trama: 121 bytes
	Carácter Fijo		An 1	M	M	Asc: 96 “ ` ” o el equivalente en Hex: 0x60
	TPDU		N 4	M	M	4 bytes. Formato 0020: Origen 0030: Destino En la trama de respuesta se debe invertir el destino por el origen 0030 0020
	MESSAGE TYPE ID		N 4	0400	0410	
	BIT MAP		B 64	M	M	
	2do BIT MAP		B 64	C	C	

03	Processing Code		N 6	920000, 960000	920000, 960000	Echo
11	System Trace Audit Number		N 6	M	M	Echo
12	Local transaction Time		N6	M	M	HHMMSS
13	Local transaction Date		N4	M	M	YYMM
24	Network International Id		N 3	O	O	
39	Response code		An 2		M	
41	Terminal ID		An 8	M	M	
42	Merchant ID		An 15	M		
63	Información de Totales	LLLVAR	An..120	M		Ver Tabla 2.9
114	Número De Lote Activo	LLLVAR	An..20	M		Ver Tabla 2.11

2.1 Códigos de proceso (p-3):

TTAA0X donde TT define el tipo de transacción así:

Naturaleza Débito/Crédito

00 Compras / Consumos

20 Anulaciones

Tanto AA como 0X definen tipos de cuentas afectadas. Cuenta origen (AA) y destino (0X):

00 Default

10 Tarjeta de Débito – Cuenta de Ahorros

20 Tarjeta de Débito – Cuenta Corriente

30 Tarjeta de Crédito

2.2 Entry mode (p-22):

RRP, donde RR define el tipo de lectura del PAN así:

00 Entrada no conocida

01 Manual

03 Código de barras

04 OCR (Lector Optico)

90 Banda Magnética

Y **P** define las características de lectura de PIN así:

0 Capacidad de conocer el PIN

1 Si permite leer PIN

2 No permite leer PIN

2.8 Campo privado – Información Transacción Original Upload (p-62):

- Longitud Total del campo 2 bytes BCD n 3
- Mensaje Original tipo ID 04 bytes an 4
- Original transacción Trace Number 06 bytes an 6
- Lote de transacción original 06 bytes an 6

2.9 Campo privado – Información Totales de Cierre (p-63):

- Longitud Total del campo 2 bytes BCD n 3
- Tarjetas de Crédito y Débito
  - Número neto de consumos 03 bytes an 3
  - Monto neto de consumos 12 bytes an 12

2.10 Campo privado – Información de Diferidos (p-112):

- Longitud total en 2 bytes – BCD n 3
- Sub Tag 3 bytes – fijo 005
- Longitud 3 bytes – fijo 006
- Tipo de crédito 2 bytes – an 2
  - 01 = Diferido Cuota Fija con intereses
  - 02 = Diferido con meses de gracia con Intereses
  - 03 = Diferido Pago Mes a Mes con Intereses
  - 04 = Diferido Cuota Fija sin Intereses

- 05 =Diferido con meses de gracia sin Intereses
- 06 = Diferido Pago Mes a Mes sin Intereses
- 07 = Diferido Especial sin Intereses

- Plazo en meses 2 bytes – an 2
- Otros Plazos 2 bytes – an 2 (Ej.: Meses de Gracia), si no existen irán ceros

2.11 Campo privado – Información de Lote Activo (p-114):

- Longitud Total en 2 byte – BCD n 3
- Número de lote activo – an 6

2.14 Campo privado – Información Monto Base IVA (p-119):

- Longitud Total del campo 2 bytes BCD n 3
- Monto Base grava IVA 12 bytes an 12
- Monto Base no grava IVA

2.15 Información adicional (p-120):

Requerimiento Transacciones de Compras

Permite la descripción detallada de los valores adicionales monetarios. El formato del campo es:

- Longitud del campo 2 bytes n 3
- Número de campos adicionales enviado por la aplicación n 1. Este rango va de 1 a 9.
- Datos adicionales. (..90 bytes). Este campo tiene definido el siguiente esquema para cada campo:

1. Tipo de campo 1 byte an 1

1 = IVA

2 = Servicios

3 = Propina

4 = Intereses

5 = Monto Fijo

2. Datos (Alfanumérico 12 bytes)

Respuesta Transacciones de Compras Diferidos

En la respuesta de las transacciones de diferidos el Host enviara el valor correspondiente a los intereses. El formato del campo es:

- Longitud del campo 2 bytes n 3
- Numero de campos. Fijo 1 byte an 1
- Tipo de campo 1 byte an 1: siempre debe ir "**4**"
- Valor Interes 12 bytes an 12

2.16 Campo privado – Modo de Encripción Número de Tarjeta (p-121):

Requerimiento Transacciones de Compras, Anulaciones, Reversas, Batch Upload

- Longitud Total del campo 2 bytes BCD n 3
- Identificador de Encripción

o Flag de Encripción 01 bytes an 1

1=Viaja Información de Tarjeta encriptada

0=No viaja Información de Tarjeta encriptado

o Id Llave Master Key 03 bytes an 3

o Información CVV2 encriptada 16 bytes an 16

2.17 Información Número de Tarjeta ó Track 2 Encriptada (p-122):

- Longitud Total del campo 2 bytes BCD n 3
- Información de la Tarjeta Encriptada ó Track 2 ..80 bytes HEX ..n 40

2.18 Información Llave de trabajo – Encripción Tarjeta, Tracks 1-2, CVC2/CVV2 (p-123):

Requerimiento Transacciones de Compras, Anulaciones, Reversas, Batch Upload

Longitud Total del campo 2 bytes BCD n 3

- Llave de trabajo usada en la encripción del número de tarjeta 16 bytes HEX n8

Respuesta Transacciones de Compras, y Anulaciones

Longitud Total del campo 2 bytes BCD n 3

- Llave de trabajo nueva para la encripción del número de tarjeta 16 bytes HEX n8

2.19 Información Adicional – Campos Adicionales (p-124):

- Longitud del campo 2 bytes n 3
- Información Campo Adicional an 6

Respuesta de Transacciones Autorizadas y No Autorizadas

- Longitud del campo 2 bytes n 3
- Información Fecha y Hora a Imprimir en el Voucher an 14

Donde Formato es: AAAAMMDDHHMMSS

2.21 Información Adicional (p-127):

Requerimiento de Transacciones

- Longitud Total del campo 2 bytes BCD n 3
- Versión de Aplicación – ..20 bytes an