UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE REDES Y COMUNICACIONES

Propuesta de diseño de un sistema de inyección de llaves criptográficas de manera remota en terminales de pago, para las empresas procesadoras de medios de pagos, utilizando el estándar PCI PIN v3.1

TESIS

Para optar el título profesional de Ingeniero de Redes y Comunicaciones

AUTOR(ES)

Zelada Santiago, Frank Antony 0009-0001-7872-0791

ASESOR(ES)

Seminario García, Hernán Augusto 0000-0001-6971-355X

Lima, 16 de noviembre de 2023

DEDICATORIA

Dedico este logro a mi amada esposa, Elizabeth, quien ha sido mi fuente constante de apoyo, comprensión y amor incondicional a lo largo de este desafiante viaje. Tu paciencia y aliento han sido mi faro en las noches más oscuras de estudio.

A mis queridos hijos, Alvaro y Alberto, quienes han sido mi inspiración diaria para esforzarme y superarme. Cada paso que doy en este camino académico es para crear un futuro mejor para ustedes, lleno de oportunidades y éxitos.

Este logro no solo es mío, sino también de mi familia, quienes han compartido el sacrificio y el compromiso que conlleva la búsqueda del conocimiento. Gracias por ser mi motor y mi razón de ser. Los amo profundamente.

AGRADECIMIENTOS

Quiero dar sinceramente las gracias a todos los que me han ayudado a terminar este proyecto de tesis. Sus contribuciones han sido inestimables. Su orientación, aliento y apoyo han sido inestimables para ayudarme en mi camino hacia la consecución de mis objetivos académicos.

En primer lugar, quiero agradecer a mi tutor de tesis, Hernan Seminario, por su orientación experta y dedicación incansable. Su sabiduría y experiencia han sido guías fundamentales a lo largo de este proceso.

Finalmente, quiero mencionar a todos los profesores y expertos que compartieron sus conocimientos y experiencia conmigo. Sus enseñanzas han enriquecido mi comprensión del tema de esta tesis.

RESUMEN

Hoy en día, las transacciones con tarjeta constituyen una gran parte de los ingresos generados por empresas de procesamiento de pagos como Niubiz, Izipay, Culqui y Openpay. Estas empresas confían en este modelo de negocio para procesar los pagos y, para ampliar su red de terminales de pago por todo Perú, necesitan que los TPV estén equipados con claves criptográficas que permitan cifrar los datos sensibles de los titulares de las tarjetas.

Sin embargo, se ha evidenciado que las empresas procesadoras de pago actualmente utilizan el inyectado de llaves criptográficas de manera local para poner en producción sus terminales de pago. Este enfoque conlleva a tener un equipo inyector criptográfico donde se almacenan todas las llaves criptográficas de las empresas procesadoras de pago, lo que representa un riesgo significativo en caso de que dicho equipo caiga en manos de delincuentes. Además, los costos asociados para actualizar a nuevos algoritmos que exigen las marcas también son elevados.

En consecuencia, en un contexto marcado por la pandemia mundial a partir de 2020, que ha llevado a un proceso de transformación digital en Perú, presentamos el siguiente proyecto de tesis con el propósito de proponer un diseño de inyección de llaves criptográficas de manera remota. Esta propuesta busca reducir los riesgos y costos asociados a la implementación de un equipo local de inyección de llaves. Es fundamental demostrar que la inyección de llaves criptográficas de forma remota es completamente segura, cumpliendo con los estándares establecidos por PCI PIN 3.1.

Palabras clave**:** Criptográfico; Inyección; PCI PIN, Procesadoras de pago.

Design proposal for a remote cryptographic key injection system in payment terminals, for payment processing companies, using the PCI PIN v3.1 standard.

ABSTRACT

Nowadays, card transactions make up a large portion of the revenue generated by payment processing companies like Niubiz, Izipay, Culqui, and Openpay. These companies rely on this business model to process payments, and in order to expand their network of payment terminals throughout Peru, they need the POS to be equipped with cryptographic keys that allow sensitive cardholder data to be encrypted.

However, it has become evident that payment processing companies currently use cryptographic key injection locally to put their payment terminals into production. This approach leads to having cryptographic injector equipment where all the cryptographic keys of the payment processing companies are stored, which represents a significant risk in case such equipment falls into the hands of criminals. In addition, the costs associated with upgrading to new algorithms required by the brands are also high.

Consequently, in a context marked by the global pandemic from 2020, which has led to a process of digital transformation in Peru, we present the following thesis project with the purpose of proposing a design for remote cryptographic key injection. This proposal seeks to reduce the risks and costs associated with the implementation of a local key injection equipment. It is essential to demonstrate that the injection of cryptographic keys remotely is completely secure, complying with the standards established by PCI PIN v3.1.

Keywords: Cryptographic; Injection; PCI PIN, Payment processors.

U201200136_ ZELADA SANTIAGO, FRANK ANTONY_Propuesta de diseño de un sistema de inyección de llaves criptográficas de manera remota en terminales de pago, para las empresas procesadoras de medios

INFORME DE ORIGINALIDAD

5%	5%	0%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	upc.aws.openrepository.com Fuente de Internet	2%
2	repositorioacademico.upc.edu.pe Fuente de Internet	1%
3	www.gmsectec.com Fuente de Internet	<1%
4	www.agilescrum.cl Fuente de Internet	<1%
5	repository.unad.edu.co Fuente de Internet	<1%
6	es.mobiletransaction.org Fuente de Internet	<1%
7	hdl.handle.net Fuente de Internet	<1%
8	repository.unipiloto.edu.co Fuente de Internet	<1%

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 CAPITULO 1

1.1 Introducción

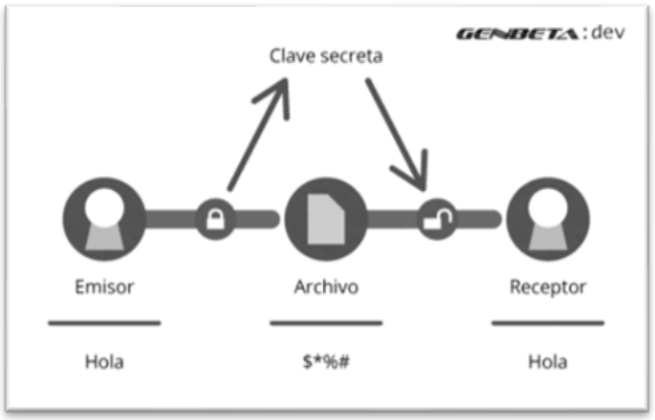
El uso de llaves criptográficas es de suma importancia para las empresas procesadoras de pago y cualquier entidad financiera que maneje, procese o transmita datos sensibles como el número de identificación personal (PIN) o el número de cuenta principal (PAN) del tarjetahabiente. Estas llaves criptográficas se basan en algoritmos actuales como 3DES o AES para llaves simétricas, o RSA para llaves asimétricas. Con el fin de proteger esta información delicada, se han implementado equipos criptográficos que garanticen el almacenamiento seguro de las llaves. Sin embargo, a lo largo de los años, estos procesos han ido mejorando debido a la constante amenaza que representan los delincuentes, quienes buscan acceder a datos sensibles y, por lo tanto, se requiere mejorar la seguridad para evitar cualquier brecha de seguridad.

Destacadas instituciones financieras se esfuerzan por garantizar la salvaguarda de la delicada información de los titulares de tarjetas mediante la aplicación de algoritmos resistentes y aparatos criptográficos acreditados para la administración de claves criptográficas. Por lo tanto, una de las cosas más importantes en las que hay que trabajar es en el desarrollo de un método más seguro de inyección de claves con el fin de reducir la vulnerabilidad y estar preparados para futuros avances en la tecnología criptográfica.

Es por esta razón que las empresas de procesamiento de pago en el Peru, que poseen el mayor número de terminales de pago desplegados en todo el país, están enfocadas en mejorar la seguridad de las llaves criptográficas. Estas llaves son esenciales para cifrar los datos sensibles de los tarjetahabientes y para asegurar la disponibilidad de nuevos algoritmos de inyección que exijan las marcas. Además, buscan reducir los costos operativos. Por lo tanto, el objetivo principal es implementar la inyección de llaves criptográficas de manera remota para brindar mayor seguridad a las empresas de procesamiento de pago y obtener mejores resultados en cuanto a seguridad en los nuevos terminales para sus comercios de medios de pago.

Figura 1

Llave Simétrico



Nota. Adaptado de "Criptografía", por Wordpress, 2023 (https://seguridadenredesgjsa.wordpress.com/criptografia/).

1.2 Organización Objetivo

La organización objetivo de este proyecto son las empresas de procesamiento de pago en Perú. Esto se debe a que todas las empresas en el país utilizan actualmente terminales de pago en sus operaciones. Este enfoque de negocio, conocido como el modelo tradicional o de tarjeta presente, ha perdurado a lo largo de los años.

El propósito principal de proponer este proyecto a las compañías es lograr una mayor eficiencia en la seguridad de las terminales de pago y reducir los costos asociados con los recursos utilizados. Las empresas de procesamiento de pago están comprometidas con el bienestar del país y buscan constantemente reinventar experiencias y la forma en que hacen negocios. Su compromiso es proporcionar servicios que, a través de la última tecnología e innovación, simplifiquen y hagan únicas las experiencias para sus clientes.

1.2.1 Campo de Acción

El diseño de un sistema de inyección remota de claves para empresas de procesamiento de pagos es la idea que debe desarrollarse. Esta estrategia se centrará en mejorar la eficacia de las operaciones de soluciones y la seguridad de la información. Cada departamento desempeña un papel distinto en el proceso; por ejemplo, el departamento de seguridad de la información se encarga de la criptografía, mientras que el departamento de operaciones de soluciones se ocupa del aprovisionamiento.

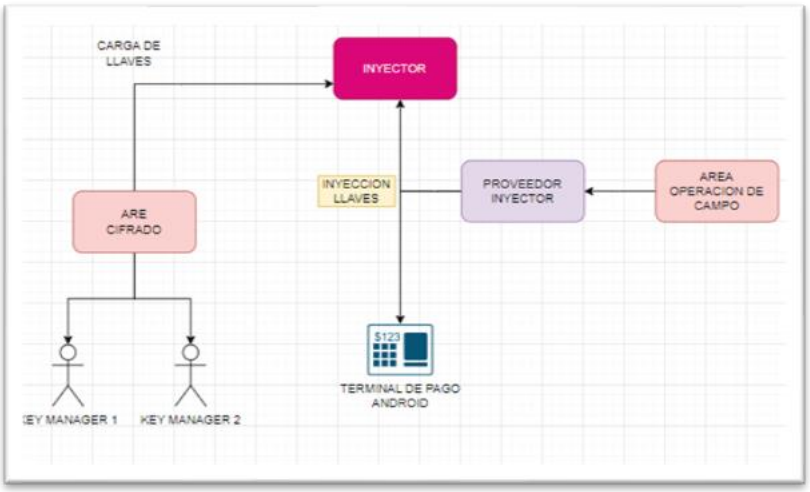
En el área de criptografía, el equipo se asegura de que las llaves criptográficas estén cargadas correctamente en los inyectores. Por otro lado, el área de abastecimiento se asegura de tener disponibles terminales de pago que ya estén inyectadas con las llaves criptográficas.

El objetivo es establecer un sistema que permita la inyección de llaves de forma remota, lo que mejorará la eficiencia en el proceso y brindará mayor seguridad a la compañía. De esta manera, el área de criptografía y el área de abastecimiento trabajarán de manera conjunta para garantizar que las llaves criptográficas estén adecuadamente gestionadas y disponibles en los terminales de pago.

Con esta propuesta, se espera optimizar los procesos internos de las empresas de procesamiento de pago y mejorar la protección de la información sensible de los tarjetahabientes, lo que redundará en una mejor experiencia para los clientes y una mayor confianza en los servicios ofrecidos por la compañía.

Figura 2

Inyección de llaves



1.3 Identificación del Problema

1.3.1 Situación Problemática

Las empresas de procesamiento de pago ofrecen soluciones tanto para transacciones en línea como para operaciones con tarjetas físicas presentes. Antes de la pandemia, una de las empresas de procesamiento de pago era el único procesador de operaciones Visa, mientras que otra empresa de procesamiento de pago se encargaba de las transacciones MasterCard. Esto llevó a la instalación de miles de terminales de pago en comercios a nivel nacional, lo que les permitió ganar reconocimiento y consolidar una posición sólida en el mercado peruano.

En el año 2020, se adoptó un modelo multimarca de TRX, lo que permitió a las empresas de procesamiento de pago, también conocidas como adquirientes, realizar transacciones con diversas marcas como Visa, MasterCard, American Express, UniónPay, entre otras. Ante este cambio, todas las empresas de procesamiento de pago tuvieron que adaptarse a las nuevas tecnologías y reducir los costos operativos sin comprometer la seguridad física y lógica de sus terminales de pago.

En el mercado peruano, existe una gran confianza en las transacciones realizadas a través de terminales de pago físicos que se encuentran en todos los comercios afiliados. Esto significa que el modelo tradicional de tarjeta presente sigue siendo relevante y se mantendrá en los próximos años. Por lo tanto, es esencial garantizar una mayor seguridad en las llaves criptográficas utilizadas en los terminales de pago y optimizar la disponibilidad de estos equipos de manera eficiente, cumpliendo con los requisitos del estándar PCI PIN v3.1.

Finalmente, los comercios en el mercado peruano siempre están buscando mejorar sus terminales de pago a corto plazo. Sin embargo, este proceso presenta desafíos, ya que implica tiempo y costos. Los nuevos terminales deben integrarse al inyector de llaves criptográficas ubicado en el cuarto seguro en modo autónomo. Posteriormente, se procede a inyectar llaves criptográficas en los terminales de manera individual, lo que prolonga el tiempo de disponibilidad de estos dispositivos.

1.3.2 Problema a Resolver

Se ha identificado un problema significativo al preparar terminales de pago en producción para los comercios que realizan transacciones con tarjeta presente. El proceso de inyección de llaves criptográficas se lleva a cabo en un cuarto seguro, lo que ralentiza el flujo operativo y prolonga la disponibilidad de terminales en producción. Además, cuando se requiere agregar nuevas marcas de terminales de pago, se incurre en costos y tiempos elevados debido a la compleja integración con el equipo inyector independiente.

1.4 Objetivo General y Objetivos Específicos

1.4.1 Objetivo General

Propuesta de diseño de un sistema de inyección de llaves criptográficas de manera remota en terminales de pago para las empresas procesadoras de medios de pago, enfocado en su modelo de negocio de pago con tarjeta presente, con el fin de proponer actividades y

controles que permitan lograr una mayor eficiencia en el aseguramiento de los terminales de pago, garantizando el cumplimiento del estándar PCI-PIN v3.1.

1.4.2 Objetivos Específicos

A. OE1- Realizar un análisis de riesgos para la actividad de inyección de llaves, la cual forma parte del área de seguridad de la información, con el objetivo de identificar las amenazas y vulnerabilidades críticas que podrían comprometer la confidencialidad de las llaves.

B. OE2- Definir los requisitos de las llaves criptográficas necesarias para los terminales de pago de las empresas procesadoras de medios de pago, mediante un proceso de "ceremonia de llaves" que garantice su absoluta imposibilidad de predicción.

C. OE3- Desarrollar un procedimiento de simulación para la inyección remota de llaves criptográficas en los terminales de pago de las empresas procesadoras de medios de pago. Este procedimiento asegurará la transmisión y carga segura de las llaves en el RKI y en los propios terminales de pago.

D. OE4- Definir los requisitos indispensables para que el equipamiento tecnológico informático utilizado en la inyección remota de llaves criptográficas cumpla con la certificación PCI PIN v3.1.

E. OE5- Proponer actividades y controles específicos para asegurar que el diseño propuesto para el sistema de inyección de llaves criptográficas remota se realice de manera eficiente y segura en los terminales de pago, minimizando riesgos potenciales.

1.4.3 Indicadores de Logro de los Objetivos

Tabla 1

Objetivos Específicos

Objetivo Específico	Indicador de Logro	Métrica
OE1- Realizar un análisis de riesgos para la actividad de inyección de llaves, la cual forma parte del área de seguridad de la información, con el objetivo de identificar las amenazas y vulnerabilidades críticas que podrían comprometer la confidencialidad de las llaves.	1) Matriz de Riesgos. 2) Informe de análisis de riesgos.	1) Numero de riesgos con criticidad Alta.
OE2- Definir los requisitos de las llaves criptográficas necesarias para los terminales de pago de las empresas procesadoras de medios de pago, mediante un proceso de "ceremonia de llaves" que garantice su absoluta imposibilidad de predicción.	1) Acta de generación de llaves criptográficas.	1) Cantidad de actas generadas para llaves criptográficas en terminales de pago.
OE3- Desarrollar un procedimiento de simulación para la inyección remota de llaves criptográficas en los terminales de pago de las empresas procesadoras de medios de pago, que permita asegurar la transmisión y carga segura de las llaves en el RKI y en los propios terminales de pago.	1) Procedimiento de simulación de inyección de llaves criptográficas.	1) Cantidad de llaves criptográficas inyectadas en el terminal de pago.
OE4- Definir los requisitos técnicos del equipamiento tecnológico informático utilizado en la inyección remota de llaves criptográficas con el fin de cumplir con la certificación PCI PIN v3.1.	1) Documentación de certificación PCI PIN de los equipos criptográficos.	1) % de equipos criptográficos Certificados.

OE5- Proponer actividades y controles específicos para asegurar que el diseño propuesto para el sistema de inyección de llaves criptográficas remota se realice de manera eficiente y segura en los terminales de pago, minimizando riesgos potenciales.	1) Propuesta del diseño	1) Versiones de propuesta

1.5 Justificación

El mercado de las empresas de procesamiento de pagos ha experimentado una competencia nivelada desde la introducción de la multimarca. Esto ha permitido a las empresas procesar transacciones con una gran variedad de tarjetas, incluidas las conocidas Visa y MasterCard. Empresas como Niubiz, Izipay, Culqui, Openpay y otras se han visto obligadas a ajustar sus planes de negocio en respuesta a esta nueva dinámica, especialmente en lo que respecta a las transacciones con tarjeta presente. Las empresas de procesamiento de pagos se enfrentan al reto de lograr una mayor eficiencia en la seguridad de los terminales para sus nuevos comercios que utilizan medios de pago, reduciendo así el tiempo y el coste asociados a la integración de nuevos terminales de pago con el inyector de claves criptográficas que actualmente funciona en modo autónomo.

Con el fin de agilizar el proceso de integración de las claves inyectadas en los terminales de pago en producción, la investigación pretende proponer un diseño de inyección remota de claves criptográficas para la actual línea de negocio de tarjetas de las empresas de procesamiento de pagos.

El diseño propuesto se implementará de conformidad con la norma PCI PIN v3.1, que estipula que todas las claves criptográficas generadas por procesos que garanticen que son imposibles de predecir o identificar probabilidades deben utilizarse en el proceso de cifrado/descifrado del PIN y cualquier otra clave relacionada. Además, se centrará en la gestión segura de estas claves criptográficas para salvaguardar la integridad de las transacciones.

La investigación representa un valioso beneficio para las empresas de procesamiento de pagos, ya que, si se revisa la propuesta de diseño y se aplica posteriormente, reducirá los costes para la empresa, al tiempo que mejorará significativamente la eficiencia de la disponibilidad de terminales de pago. Todo ello, en línea con el estándar PCI PIN v3.1, aceptado por marcas de tarjetas como Visa y MasterCard, reforzará la posición de la empresa y proporcionará mayor confianza a sus clientes y socios comerciales.

1.6 Estado del Arte

1.6.1 Antecedentes

La norma PIN de la PCI tiene su origen en el programa de seguridad PIN de VISA, al igual que la gran mayoría de las normas que actualmente gestiona el PCI Security Standards

Council (PCI SSC). Visa creó su propio conjunto de controles de seguridad en 1995, denominándolos Requisitos de seguridad del PIN de Visa (Acosta, 2023). Estos controles se esbozaron en el programa de Seguridad PIN y Gestión de Claves, junto con las categorías de entidades que debían adherirse a los requisitos del programa y la forma en que debía notificarse el cumplimiento (mediante una revisión in situ de un auditor aprobado o un cuestionario de autoevaluación, o PCI PIN SAQ).

Los requisitos de seguridad del PIN de Visa fueron adoptados por el PCI Security Standards Council (PCI SSC) en 2011 y utilizados como guía para crear la primera norma PCI PIN, conocida como PCI PIN Security Requirements (Acosta, 2023). ANSI proporcionó apoyo para este nuevo estándar. A través del grupo de trabajo X9.24, ANSI ya había adquirido una importante experiencia en la normalización de controles de seguridad para la protección de transacciones financieras, en particular con las normas ANSI X9.24-1, ANSI X9.24-2 y ANSI X9.24-3. A raíz de ello, todas las marcas de pago conectadas al PCI SSC (Visa, MasterCard, AMEX, JCB y Discovery) empezaron a utilizar esta norma para salvaguardar la información del PIN de sus tarjetas.

Figura 3

Línea de tiempo

Nota. Adaptado de "Que es PCI PIN?", por Acosta, 2023 (https://www.pcihispano.com/que-es-pci-pin/).

1.6.2 Metodología de Riesgos

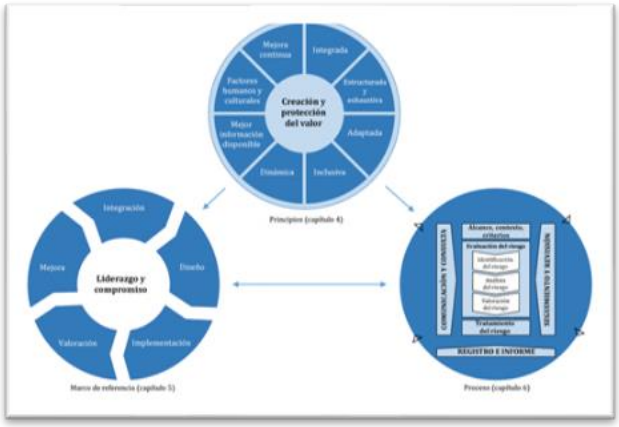
1.6.2.1 IS031000

La ISO 31000 define el proceso de gestión de riesgos como una serie de pasos que incluyen la identificación, análisis, evaluación y tratamiento de los riesgos. En el contexto de tu proyecto, la matriz de riesgos podría comenzar con la identificación de posibles amenazas,

como ataques cibernéticos, interferencias en la comunicación remota, fallos en el proceso de inyección de llaves, entre otros.

Figura 4

Principios, marco de referencia y proceso



Nota. Adaptado en "Gestión de riesgos", por ISO, 2023 (https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es).

1.6.2.2 COSO (ERM)

En Estados Unidos se creó un consorcio de organizaciones privadas conocido como Comité de Organizaciones Patrocinadoras de la Comisión Tradeway, o COSO, para ofrecer a las organizaciones un marco estándar de dirección en ámbitos importantes como la información financiera, el control del fraude, la supervisión del riesgo corporativo, la ética empresarial, la supervisión interna y la gestión ejecutiva y el gobierno.

Figura 5

Representación del Modelo COSO ERM 2017

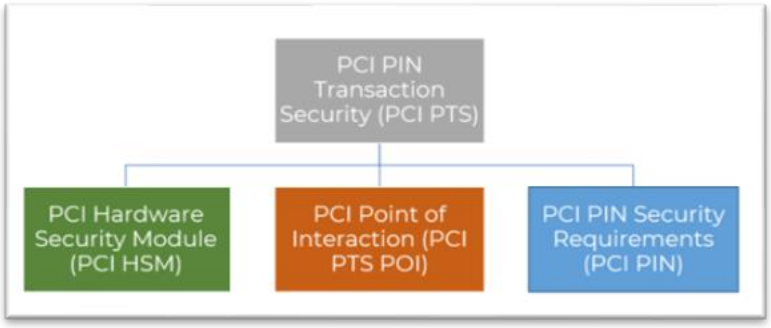
Nota. Adaptado en "Que es el modelo COSO?", por GlobalSuite, 2023 (https://www.globalsuitesolutions.com/es/que-es-modelo-coso/).

1.6.3 PCI PIN

Según Acosta (2023) los requisitos para la gestión, el procesamiento y la transmisión seguros del número de identificación personal (PIN) durante el procesamiento de operaciones de pago en línea y fuera de línea en cajeros automáticos y en terminales de punto de venta atendidos y desatendidos están establecidos por la norma de seguridad del PIN del sector de tarjetas de pago (PCI), también conocida como PCI PIN. Junto con PCI POI y PCI HSM este documento forma parte de la familia de normas PCI PIN Transaction Security (PTS).

Figura 6

Familia de estándares PCI PTS



Nota. Adaptado de "¿Que es PCI PIN?", por Acosta, 2023 (https://www.pcihispano.com/que-es-pci-pin/).

1.6.3.1 Quienes deben cumplir PCI PIN

Todos los adquirentes y agentes que procesen transacciones con PIN para tarjetas de la marca PCI SSC están obligados a utilizar la norma PCI PIN. Esto incluye las instalaciones de KIF y la distribución de claves simétricas utilizando claves asimétricas, así como las entidades que prestan servicios de operación a las autoridades de certificación. El estándar PCI PIN debe utilizarse junto con otros estándares relevantes del sector.

Todas las marcas de pago, sin embargo, se encargan de gestionar sus propios programas de cumplimiento. Por ejemplo, el programa PIN de Visa sigue vigente desde el punto de vista de la gestión de las entidades que deben cumplir la normativa, pero se basa en los controles del estándar PIN de PCI en lugar de en los requisitos de seguridad propios de Visa.

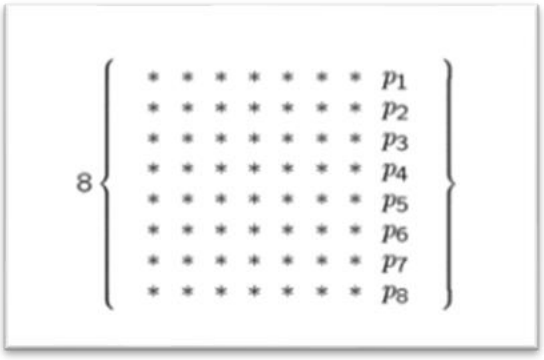
1.6.4 Llaves Key Blocks

El algoritmo DES (Data Encryption Standard), también conocido como DEA (Data Encryption Algorithm), era uno de los algoritmos de cifrado por bloques más utilizados en el sector financiero. Este algoritmo, que se seleccionó por primera vez como norma FIPS en 1976, se considera actualmente inseguro debido a la longitud extremadamente corta de su

clave (56 bits reales de clave y 8 bits de paridad), que se ve fácilmente comprometida con las técnicas computacionales existentes.

Figura 7

Estructura clave DES



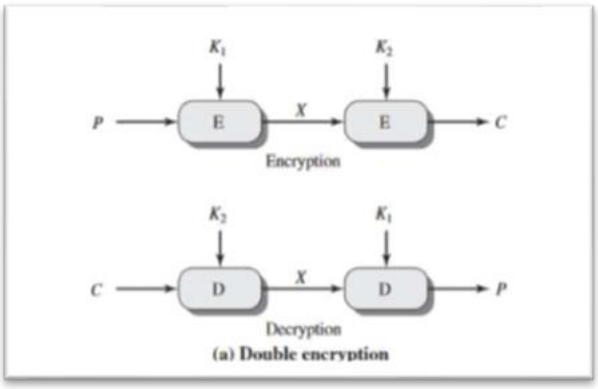
Nota. Adaptado en "la guia definitiva de Key Blocks", por Acosta, 2022 (https://www.pcihispano.com/la-guia-definitiva-de-bloques-de-claves-criptograficas-key-blocks/).

En respuesta a este problema, se implementaron dos algoritmos que utilizaban la misma base DES, pero aumentaban la complejidad del proceso mediante iteraciones y claves adicionales:

- Double-DES (2DES o 2DEA) usa dos instancias de DES en el mismo bloque de texto en claro. En cada instancia usa diferentes claves de encriptación. Actualmente, este algoritmo está obsoleto.

Figura 8

Double DES

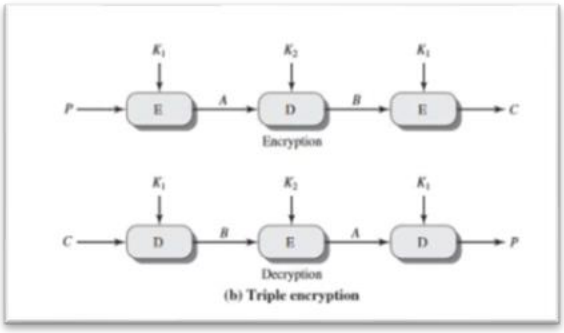


Nota. Adaptado en "la guia definitiva de Key Blocks", por Acosta, 2022 (https://www.pcihispano.com/la-guia-definitiva-de-bloques-de-claves-criptograficas-key-blocks/).

- Triple-DES (3DES o TDEA) tres instancias de DES en el mismo texto en claro, pudiendo emplear dos claves (Double-length TDEA) o tres claves diferentes de encriptación (Triple-length TDEA).

Figura 9

Doble Longitud



Nota. Adaptado en "la guia definitiva de Key Blocks", por Acosta, 2022 (https://www.pcihispano.com/la-guia-definitiva-de-bloques-de-claves-criptograficas-key-blocks/).

Una de las alternativas más usadas para gestionar este problema es mediante el uso de variantes (Key Variants). Las variantes son creadas mediante la combinación de una máscara binaria con la clave original, dependiendo del tipo de implementación. No obstante, este método no provee ninguna funcionalidad para verificación de la integridad o autenticación de la clave.

1.6.4.1 Estructura de los Key Blocks

De acuerdo con los requisitos 18-3 de PCI PIN v3.0 y de P2PE v3.0, algunos de los métodos aceptables para la implementación de key blocks son:

- Uso de una función MAC (Message Authentication Code) aplicada sobre la concatenación de los atributos en texto claro y la parte encriptada del Key Block.
- Una firma digital computada sobre todos estos datos (ejemplo: ASC X9 TR 34), o
- Una función de verificación de integridad que es una parte implícita del proceso de encriptación de claves como el que se utiliza en el proceso de key-wrapping en claves AES.

Figura 10

Estructura de Key Block usando Ansi X9.143

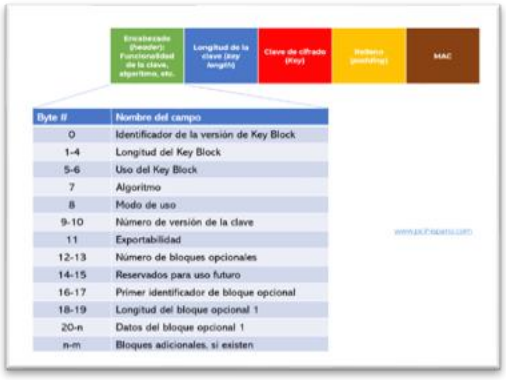
Nota. Adaptado en "la guia definitiva de Key Blocks", por Acosta, 2022 (https://www.pcihispano.com/la-guia-definitiva-de-bloques-de-claves-criptograficas-key-blocks/).

Este modelo implica la generación de una nueva clave de encriptación (Key-Block Protection Key – KBPK) de la cual se derivarán dos claves adicionales:

- Key-Block Encryption Key (KBEK), usada para encriptar la sección que contiene el criptograma de la clave y su longitud, y
- Key-Block Authentication Key (KBAK), usada para para generar un código de autenticación de mensaje (Message Authentication Code – MAC) de todo el contenido del Key Block. Esta clave también se conoce como Key-Block MAC Key (KBMK).

Figura 11

Estructura Del Encabezado (Header) De Key Block (Ansi X9.143)



Nota. Adaptado en "la guia definitiva de Key Blocks", por Acosta, 2022 (https://www.pcihispano.com/la-guia-definitiva-de-bloques-de-claves-criptograficas-key-blocks/).

1.6.5 Terminal de pago para tarjeta presente (POS)

El terminal de punto de venta (POS), también conocido como Terminal de Punto de Venta se presenta como uno de los dispositivos electrónicos más comunes en nuestra vida cotidiana, al igual que las computadoras, tabletas y teléfonos inteligentes.

Figura 12

Terminal de pago inalámbrico

Nota. Adaptado en "La historia del Datafono: nacimiento y evolución de los lectores de tarjetas.", por Sorensen, 2022 (https://es.mobiletransaction.org/historia-del-datafono)

Los lectores de tarjetas móviles para teléfonos inteligentes, más ligeros, pequeños y asequibles que los datáfonos móviles tradicionales, han vuelto a transformar las transacciones comerciales en todo el mundo.

Se trata de minúsculos artilugios que se emparejan por BT con un teléfono inteligente (o tableta) conectado a Internet, sin necesidad de tarjeta SIM. A continuación, se utiliza una aplicación móvil para controlar el terminal de pago llamado MPOS.

Figura 13

Terminal de pago MPOS

Nota. Adaptado en "La historia del Datafono: nacimiento y evolución de los lectores de tarjetas.", por Sorensen, 2022 (https://es.mobiletransaction.org/historia-del-datafono)

Al igual que la invención del microchip, el pago sin contacto, o contactless, representó un avance tecnológico significativo.

Figura 14

Pago usando un Smartphone

1.6.6 Criptografía Asimétrica

1.6.6.1 Criptografía de clave privada y publica

La base de este tipo de criptografía es una función unidireccional. Esto indica que, aunque la función puede calcularse con bastante facilidad en una dirección, se necesitaría una cantidad significativa de potencia de cálculo para invertir el cálculo en la otra dirección.

Figura 15

Llave Publica

Nota. Adaptado en "Criptografía: ¿Qué son calve pública y privada? Aprende a diferenciarlo.", por Duarte, 2018 (https://bitcoin.es/noticias/criptografia-que-son-la-clave-publica-y-la-clave-privada-aprende-a-diferenciarlas/)

1.6.6.2 Llave algoritmo RSA

Los tres inventores de RSA son Rivest, Shamir y Adleman. La base de RSA es el problema de la factorización de números extremadamente grandes, para el que actualmente no existe una solución eficaz.

1.6.7 Casos de Éxito

Empresa de Terminal de pago INGENICO, indica:

Tenemos RKI implementado a nivel Global.

En este sistema, que llamamos KeyMass usamos un HSM Payshield 10000.

Aquí te comparto algunos datos en LAR:

- RKI funciona con algunos clientes de Fiserv como Scotiabank en el Caribe.
- Tenemos 3 clientes más que están en proceso de implementación. A través de la plataforma de pago de Fiserv. Pero el sistema RKI de Ingenico
- En Centroamérica se está implementando en este momento.
- En Chile estamos en proceso de POC con un adquiriente local.

Usamos él Estate Manager como plataforma de comunicación, pero las llaves son almacenadas en nuestro Data Center en casa matriz (Francia); el cual está certificado como plataforma de gestión de llaves. (L. I. Gonzales, Comunicación personal, 04 de enero 2023).

Empresa de Terminal de pago PAX, indica:

Actualmente, paxRhinoPortal es utilizado por clientes de todo el mundo, como PayMaya en el Sudeste Asiático, Coshine en China, Disney en Estados Unidos, etc. Además, la mayoría de los clientes utilizan RKI con la entrada MAXSTORE RKI. (J. F. Garcia, Comunicación personal, 23 de febrero 2023).

1.6.8 Cronograma del Proyecto

Duración Total del Proyecto: 6 Meses

Fase 1: Análisis Preliminar y Preparación (1 Mes)

Semana 1-2: Recopilación de Información y Reunión Inicial con el directorio de la empresa.

Semana 3-4: Investigación del Estándar PCI-PIN v3.1 y Análisis de Requisitos

Fase 2: Diseño del Sistema de Inyección de Llaves Criptográficas Remotas (2 Meses)

Semana 5: Definición de Requisitos Funcionales y No Funcionales

Semana 6-7: Diseño de Arquitectura de Sistema

Semana 8-9: Definición de Procedimientos de Inyección

Fase 3: Implementación y Pruebas del Diseño Propuesto (2 Meses)

Semana 10-11: Desarrollo del Sistema

Semana 12-13: Pruebas de Seguridad y Funcionalidad

Fase 4: Propuesta de Actividades y Controles Eficientes (1 Mes)

Semana 14: Análisis de Riesgos y Vulnerabilidades

Semana 15: Propuesta de Actividades de Aseguramiento y Controles de Cumplimiento

Fase 5: Presentación y Evaluación de la Propuesta (1 Semana)

Semana 16: Elaboración del Informe de Propuesta y Presentación a directorio de la empresa.

Fase 6: Implementación y Seguimiento Continuo (3 Meses)

Semana 17-19: Implementación de la Propuesta Aprobada

Semana 20-22: Monitoreo y Evaluación Continua

Notas Adicionales:

El proyecto se llevará a cabo en un plazo de 6 meses, asegurando la dedicación de los recursos necesarios en cada fase.

Cada fase incluirá revisión y aprobación de los hitos alcanzados por parte de la empresa.

Se programarán reuniones regulares de seguimiento para garantizar la alineación con los objetivos y el cumplimiento de los plazos.

Este cronograma de proyecto establece un marco de tiempo realista para llevar a cabo la propuesta de diseño del sistema de inyección de llaves criptográficas remotas en terminales de pago para las empresas de procesamiento de pago. Cada fase se enfoca en actividades clave para lograr el objetivo general de eficiencia y seguridad en los terminales de pago, además de garantizar el cumplimiento del estándar PCI-PIN v3.1.

1.6.9 Aporte Académico

La tesis representa un aporte académico significativo al proponer un sistema novedoso de inyección remota de llaves criptográficas en terminales de pago, dirigido a las empresas procesadoras de medios de pagos y alineado con el estándar PCI PIN v3.1. Este diseño innovador no solo aborda la creciente necesidad de fortalecer la seguridad en las transacciones financieras, sino que también introduce eficiencias operativas al permitir la gestión remota de llaves. Además, al cumplir con rigurosos estándares de seguridad, como el PCI PIN v3.1, la propuesta contribuye a la integridad y conformidad de los sistemas de procesamiento de pagos, brindando una solución práctica y avanzada que puede tener un impacto significativo en la industria financiera y en la protección de la información sensible.

2 CAPITULO 2: MARCO TEORICO

2.1 Matriz de Riesgo

La matriz de riesgos, según el estándar ISO 31000, es una herramienta fundamental en la propuesta de diseño de tu sistema de inyección de llaves criptográficas para terminales de pago. En el contexto de ISO 31000, la matriz de riesgos es una representación visual que identifica y evalúa los riesgos asociados con la implementación de tu sistema.

Primero, se identificarán los riesgos potenciales, como posibles fallos en la seguridad, vulnerabilidades en la infraestructura remota, o interrupciones en la transmisión de datos. Luego, se evaluará cada riesgo en términos de su probabilidad de ocurrencia y el impacto que podría tener en la seguridad y la operación del sistema.

La matriz reflejará estos riesgos en una cuadrícula, asignando una puntuación de riesgo basada en la combinación de probabilidad e impacto. Riesgos con puntuaciones más altas serán considerados críticos y requerirán estrategias de mitigación más intensivas. La matriz de riesgos, en este contexto, proporciona una herramienta valiosa para la toma de decisiones informada, permitiendo a las empresas procesadoras de medios de pago anticiparse a posibles desafíos y garantizar la robustez y seguridad del sistema propuesto.

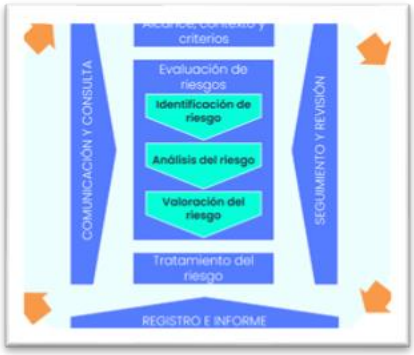
Figura 16

Marco de Gestión de Riesgos

Nota. Adaptado en "ISO 31000", por GlobalSuite, 2023 (https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-31000-y-para-que-sirve/)

Figura 17

Procesos de Gestión de Riesgos



Nota. Adaptado en "ISO 31000", por GlobalSuite, 2023 (https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-31000-y-para-que-sirve/)

2.2 Estándar PCI PIN v 3.1

Los requisitos de seguridad del PIN de la PCI lo consiguen. Esta norma PCI permite controlar de forma segura el procesamiento y la transmisión del número de identificación personal (PIN) para las transacciones de pago tanto en línea como fuera de línea en cajeros automáticos y terminales de punto de venta (TPV).

Al completar una transacción, el PIN es la principal credencial utilizada para identificar y autenticar al cliente. El PIN nunca debe revelarse durante el proceso de pago. En los

requisitos de seguridad del PIN de la PCI se describe un conjunto de directrices para la administración, el procesamiento y la transmisión seguros de los datos del PIN (número de identificación personal) durante las transacciones con tarjeta en línea y fuera de línea.

Los requisitos garantizan que el PIN de 4 dígitos del titular de la tarjeta permanezca encriptado en todos los sistemas de pago, por lo que la confidencialidad debe estar protegida en todo momento.

Si los POS son parte de la solución comercial y la puerta de alcance para las transacciones con clientes para aceptar pagos con tarjeta deben cumplir con los requisitos de seguridad PCI PIN. El propósito de una evaluación de PIN es evaluar si una organización está entregando de forma segura el cifrado de PIN en sus transacciones, como dispositivos POS, donde los clientes ingresan sus PIN.

La incorporación del estándar PCI PIN v3.1 en el proyecto de Tesis tiene como objetivo alinearnos con las prácticas que utilizan las marcas para la transferencia, carga, almacenamiento y protección de la llave criptográfica necesaria para la inyección remota de llaves.

Figura 18

PCI PIN

Nota. Adaptado en “SI el PIN”, por Information Quality, 2023 (https://iqcol.com/servicios-4/)

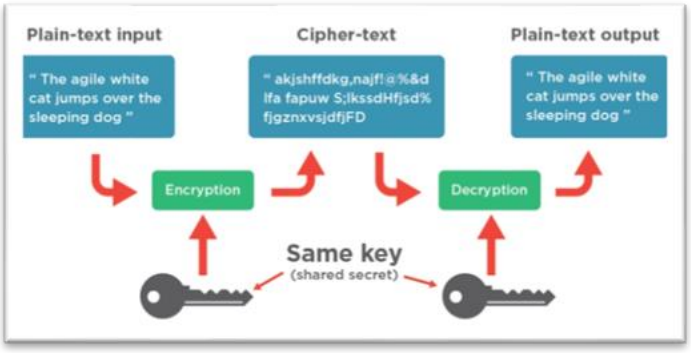
2.3 Llaves criptográficas

Las claves criptográficas simétricas, reconocidas actualmente por marcas como TRACK2 y PINBLOCK para el cifrado de datos, son importantes por la garantía de seguridad que ofrecen a los titulares de tarjetas durante las transacciones. Para garantizar la integridad y confidencialidad de las transacciones, es imprescindible utilizar algoritmos robustos, como AES, para la inyección remota de claves criptográficas en los terminales de pago. Gracias a

ello, los usuarios pueden sentirse seguros sabiendo que sus transacciones financieras se realizan en un entorno seguro.

Figura 19

Algoritmo AES



Nota. Adaptado en "Encriptación AES", por Transcend, 2023 (https://ec.transcend-info.com/embedded/technology/aes-encryption).

2.4 Certificado Asimétrico

Un algoritmo asimétrico de cifrado por bloques conocido como sistema criptográfico de clave pública RSA utiliza una clave privada que su propietario mantiene en secreto y una clave pública que se distribuye, idealmente de forma autenticada.

La utilización de certificados asimétricos tiene una finalidad esencial: autenticar la comunicación entre el host y el terminal de pago. Esto garantiza la veracidad de la identidad del equipo, asegurando que esté debidamente autorizado para llevar a cabo la inyección de llaves remotas. De esta manera, se establece un sólido nivel de confianza en la transmisión segura de información entre ambas partes.

2.5 Terminales de pago

La relevancia de los terminales de pago en esta propuesta de proyecto es crucial, ya que serán los dispositivos donde se almacenarán las llaves criptográficas previamente inyectadas de manera remota. Es fundamental que el proceso diseñado esté plenamente alineado con altos estándares de seguridad para garantizar una disponibilidad eficiente de los equipos en el despliegue en los comercios. De esta forma, se asegura la protección de la información sensible y se contribuye a una implementación exitosa en el mercado peruano.

Figura 20

Terminal de pago

Nota. Adaptado en "Terminal de pago", por Square Terminal, 2023 (https://squareup.com/us/es/hardware/terminal)

3 CAPÍTULO 3: ANALISIS DEL PROBLEMA

3.1 Alcance del problema

En los últimos años, en el contexto peruano, el negocio de las empresas de procesamiento de pago ha experimentado un crecimiento exponencial, especialmente durante y después de la pandemia. Empresas como Niubiz, Izipay, Culqui y Openpay se han posicionado fuertemente en el mercado al desplegar sus terminales de pago en todo el país, facilitando las transacciones de pago de manera masiva.

Con la llegada de la transformación digital, las empresas han buscado optimizar sus procesos para aumentar su eficiencia y reducir costos. En esta línea de mejoras, la inyección de llaves en los terminales de pago de las empresas de procesamiento de pago era un aspecto pendiente, ya que es fundamental para ofrecer a los tarjetahabientes la posibilidad de usar su medio de pago preferido y competir de manera efectiva en el mercado.

Para abordar esta necesidad, el área de seguridad de la información ha asumido la responsabilidad de velar por la protección de las llaves criptográficas de las empresas de procesamiento de pago. La propuesta de diseño de inyección de llaves remotas se presenta como una solución que permitiría realizar la inyección de llaves de manera descentralizada, garantizando un mayor aseguramiento de las llaves criptográficas y generando beneficios como una mayor eficiencia en la disponibilidad de los terminales de pago y la reducción de costos operativos. Todo esto se enmarca en el estándar PCI PIN v3.1, asegurando un proceso

seguro para poner en funcionamiento los terminales de pago en los comercios que utilizan medios de pago.

Con esta iniciativa, las empresas de procesamiento de pago se fortalecerán en el mercado, brindando un servicio seguro y eficiente, y posicionándose como una opción preferente para los usuarios y comercios que deseen realizar transacciones con confianza y comodidad.

3.2 Impacto del Problema

Las compañías actualmente cuentan con un sistema de inyección de llaves criptográficas que opera de manera standalone o local, lo que significa que el inyector de llaves se encuentra en un cuarto seguro. Aunque este proceso es aceptado por las marcas, presenta ciertas limitaciones que afectan la eficiencia y aumentan los costos cuando se busca integrar nuevas marcas de terminales.

Con el continuo avance en temas de seguridad y la migración hacia algoritmos criptográficos más robustos, surge la necesidad de actualizar el equipo inyector para adaptarse a los nuevos requisitos establecidos por las marcas. Esto genera una alerta a las empresas, debido a los costos asociados y la demora en obtener terminales de pago en producción cuando se incorporan nuevas marcas.

En este contexto, se vislumbra la importancia de implementar un sistema de inyección de llaves remotas como solución. De no contar con esta opción, se presentarían demoras y retrasos en el despliegue de terminales de pago en producción, lo que podría impactar negativamente en la competitividad y eficiencia de la compañía.

Por tanto, es crucial evaluar la implementación de un sistema de inyección de llaves criptográficas remoto, el cual permitiría agilizar los procesos de despliegue de terminales de pago y adaptarse con mayor facilidad a las nuevas exigencias de seguridad de las marcas. De esta forma, la empresa estaría preparada para afrontar los retos del mercado y ofrecer un servicio eficiente y confiable a sus clientes.

- **Impacto a Nivel de TI:** El impacto a nivel de TI de la propuesta del proyecto se enfoca en la implementación de las mejores prácticas para garantizar la seguridad de las llaves criptográficas utilizadas en los terminales de pago. Para lograrlo, se adoptará el estándar PCI PIN V3.1, el cual está vigente en la actualidad y representa una medida eficaz para fortalecer la seguridad de las transacciones.

La propuesta de diseño de inyección de llaves remota busca generar una buena aceptación en todas las áreas involucradas en el proceso. Para lograrlo, se presentará una visión más completa del proyecto, resaltando los aportes y beneficios que esta iniciativa brinda para solucionar las problemáticas actuales. Además, se destacará la incorporación de la nueva tecnología de inyección de llaves remota, la cual representa una mejora significativa en comparación con el proceso actual.

- **Impacto a nivel económico:** El impacto económico de la propuesta es significativo, ya que se abordan y resuelven los problemas asociados a la integración de nuevas marcas de terminales de pago y los costos relacionados con el proceso actual de inyección de llaves.

  En primer lugar, al implementar la inyección remota de llaves criptográficas, se eliminará la necesidad de integrar cada nueva marca de terminales en el inyector local. Esto reducirá considerablemente los costos asociados con la actualización y adaptación del equipo inyector para cada nueva marca. Además, al contar con un servicio RKI (SAAS) que maneje el estándar PCI PIN V3.1, se evitarán los gastos recurrentes de actualización y mantenimiento del inyector local, ya que el proveedor externo se encargará de mantener y asegurar la disponibilidad de las llaves criptográficas.

  En segundo lugar, al optimizar el proceso de inyección de llaves remota mediante la propuesta de diseño, se reducirán los costos operativos asociados con la colocación de terminales de pago en producción. Actualmente, el proceso de inyección en el cuarto seguro por parte de un proveedor implica gastos adicionales y tiempos de espera que impactan negativamente en la disponibilidad de los terminales. Con la inyección remota, se agilizará el proceso y se podrá disponer de los terminales de pago de manera más rápida y eficiente, lo que se traducirá en un ahorro de recursos para la compañía.

- **Impacto a nivel operativo:** El impacto operativo de la propuesta es altamente positivo, ya que se eliminarán las demoras y dependencias asociadas con el proceso actual de integración de nuevas marcas de terminales y la inyección de llaves en el cuarto seguro. Con la implementación de la inyección remota de llaves criptográficas, el proceso de integración de nuevas marcas de terminales se volverá más ágil y eficiente. Al utilizar un servicio RKI (SAAS) que maneje el estándar PCI PIN V3.1, la compañía podrá conectar rápidamente los nuevos terminales a la plataforma sin necesidad de esperar a que el inyector local esté adaptado a cada marca en particular. Esto eliminará la espera

innecesaria y reducirá significativamente el tiempo necesario para que los terminales estén en estado productivo.

Asimismo, la inyección remota de llaves permitirá que los terminales de pago estén disponibles en un plazo más corto, ya que el proceso se realizará de forma más ágil y descentralizada. Al eliminar la necesidad de inyectar las llaves en un cuarto seguro, se reducirán los tiempos de espera y se evitarán posibles cuellos de botella en el proceso operativo. Esto garantizará que los terminales de pago estén listos para su uso de manera oportuna y eficiente.

Además, la propuesta de diseño de inyección remota de llaves criptográficas también contribuirá a una mayor flexibilidad operativa. Al no depender de un cuarto seguro y un inyector local, la compañía tendrá la capacidad de realizar la inyección de llaves desde distintas ubicaciones de manera simultánea, lo que aumentará la eficiencia operativa y mejorará la disponibilidad de los terminales para su despliegue en comercios.

Al inicio del proyecto, llevamos a cabo una lluvia de ideas para comprender a fondo la situación actual de la inyección de llaves criptográficas en los terminales de pago. Nuestro objetivo era determinar el alcance necesario para proponer un diseño de inyección de llaves remota que cumpla con los más altos estándares de seguridad requeridos por la empresa, al mismo tiempo que nos permita obtener beneficios significativos en la reducción de costos operativos.

3.3 Causa del problema

Después de realizar una revisión exhaustiva del proceso de inyección de llaves criptográficas en los terminales de pago, hemos identificado dos causas principales del problema. En primer lugar, se presentan retrasos significativos al integrar una nueva marca de terminal de pago debido a la espera del desarrollo del protocolo de comunicación requerido por el proveedor para poder desplegar los terminales con la inyección adecuada.

En segundo lugar, el proceso actual de inyección de llaves en los terminales de pago es lento debido a la necesidad de utilizar un cuarto seguro para llevar a cabo la inyección de las llaves criptográficas. Esta dependencia de un inyector local está vinculada con el cumplimiento del estándar PCv.3.1 de custodiar de llaves criptográficas de producción, lo que ralentiza el tiempo de despliegue y producción de los terminales.

3.4 Stakeholders

Tabla 2

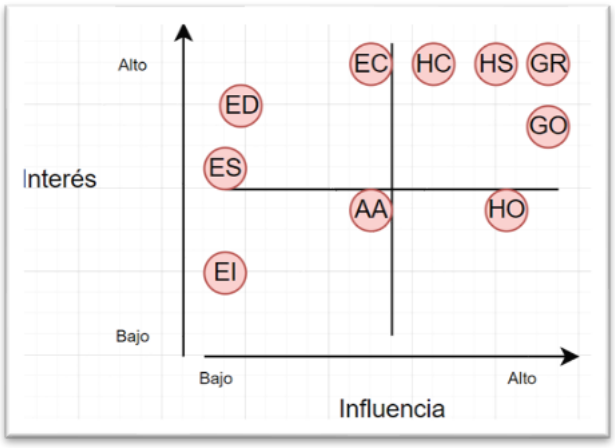
Identificación de los stakeholders

Stakeholders	Categoría del Stakeholders	Nivel de interés (B, M, A)	Nivel de Influencia (B, M, A)
Gerente de Riesgos y Cumplimiento	Patrocinador	Alto	Alto
Gerente de operaciones y Soluciones	Patrocinador	Alto	Alto
Head de Operaciones de soluciones físicas	Coordinador	Alto	Medio
Head de Seguridad de la información	Coordinador	Alto	Alto
Head de criptografía y agentes	PMO del Proyecto	Alto	Alto
Especialista de criptografía y agentes	Participa en el Proyecto	Alto	Medio
Analista de abastecimiento y laboratorio	Participa en el Proyecto	Medio	Medio
Encargado de Desarrollo	Tercero	Alto	Bajo
Encargado de Inyección	Tercero	Medio	Bajo
Encargado del Servicio Remoto	Tercero	Alto	Bajo

El cuadro de poder/interés muestra a todo el personal de la empresa involucrado e interesado en la propuesta de diseño para la inyección de llaves remotas. Este cuadro permite identificar a los actores clave y su nivel de poder e interés en el proyecto. Con esta información, podremos priorizar y asegurar una adecuada comunicación con cada uno de ellos, asegurando su participación y compromiso en el proceso.

Figura 21

Matriz Poder / Interés



3.5 Requerimientos Funcionales

3.5.1 Requerimiento de la Matriz de Riesgo

Cada proyecto que iniciamos en la empresa, incluido el proyecto de diseño de inyección remota de llaves, es objeto de un exhaustivo análisis de riesgos. Para ello utilizamos la matriz de riesgos especificada en la política de gestión de riesgos operativos de la dirección. Utilizamos la norma ISO/IEC 27005:2018, que describe las siguientes fases cruciales de la gestión de riesgos:

Tabla 3

Metodología de Riesgos

Establecimiento del contexto	¿Riesgos en qué?
Identificación de los riesgos	¿Por qué puede suceder?
Análisis de riesgos	Determinar la frecuencia y el impacto
Evaluación de riesgos	Establecer prioridades de tratamiento
Tratamiento de riesgos	Definir planes de acción
Comunicación y consulta	Comunicación y actualización de los riesgos
Monitoreo y revisión	Evaluaciones continuas

La matriz de riesgos debe utilizarse para evaluar la propuesta de diseño con el fin de identificar claramente los niveles de riesgo asociados, que se clasifican en BAJO, MEDIO, ALTO o MUY ALTO. Con la ayuda de esta evaluación, la empresa podrá decidir sabiamente

y crear planes de acción para reducir los riesgos que sean superiores a lo que la organización puede tolerar.

En la actualidad, existen diversas opciones en el mercado para el monitoreo de riesgos a través de software o servicios especializados. Sin embargo, en nuestra empresa, hemos implementado una macro que nos permite calcular la tolerancia de cada riesgo identificado mediante fórmulas específicas, facilitando el seguimiento y control de estos.

3.5.1.1 Paso 1: Definir Alcance de la Evaluación de riesgos

Conforme al primer subobjetivo del proyecto de tesis, se prescribe la necesidad de llevar a cabo una exhaustiva evaluación de riesgos. Esto permitirá adquirir una comprensión detallada del alcance del proyecto. Además, se prevé establecer con precisión los límites que regirán tanto el sistema como los procesos involucrados, así como los activos que serán sometidos a evaluación.

3.5.1.2 Paso 2: Identificación de Activos y valoración

El objetivo central es definir con precisión los activos que forman parte del ámbito de implementación del proyecto de tesis. Estos activos son los que facilitan el servicio de encriptación de datos sensibles de los titulares de tarjetas. Con este propósito, se llevarán a cabo las siguientes acciones:

- Identificar aquellos activos de información que revisten la mayor criticidad para el funcionamiento del servicio de inyección remota de claves criptográficas.
- Añada todos los elementos que se han descubierto en un inventario de activos, y enumere también los riesgos que se han descubierto en una matriz de riesgos.

Identificación de Activos:

Pasaremos a la fase de reconocimiento de todos los activos implicados en la propuesta de diseño para la inyección remota de claves una vez identificados los activos de información y finalizado el proceso de delimitación del alcance. Como resultado de este proceso se elaborará un inventario exhaustivo de estos activos. A continuación, se llevará a cabo una evaluación y verificación de cada uno de ellos.

En la etapa final, se logrará una identificación exhaustiva del impacto. Se clasificarán los activos de información del proyecto de diseño de inyección remota de llaves, asignándoles propietarios y documentando información pertinente. Además, se establecerán niveles de

estimación para los activos: "Bajo", "Medio", "Alto". Se otorgará prioridad a los activos categorizados como "Alto" a fin de brindarles la atención adecuada, dado que son esenciales para el funcionamiento óptimo del proyecto de diseño.

Tabla 4

Inventario AI

Código Activo	Categoría del Activo	Descripción del Activo
AI-001	Activo Físico	Terminal de pago
AI-002	Activos de Información	Llaves criptográficas
AI-003	Activos de Software	Aplicativo de inyección de llaves
AI-004	Activos de Servicios	Sistema de inyección de llaves (RKI)

Descripción de los activos de información

Figura 22

Descripción del Activo

- **Numero**: Se asigna un código que empieza con la numeración 1.
- **ID Activo**: Es un ID que empieza con AI-001 que es la nomenclatura inicial.
- **Nombre del activo**: Nombre de AI
- **Descripción del activo**: Describir la función del AI.
- **Categoría del activo**: Elegir la categoría del AI, en nuestro caso se escoge el tipo: Activo físico, Información, Software o Servicios.
- **Ubicación del activo**: Tipo de ubicación del activo, en nuestro caso se escoge del tipo: Virtual o Física.
- **Propietario**: Cargo del dueño del proceso.
- **Tipo de Operador**: Esta operado por un proveedor Externo o colaborador Interno.
- **Total**: Suma de los totales fundamentales de su categoría, disponibilidad, confidencialidad e integridad. La media de las tres categorías es la suma.
- **Valor criticidad**: Es el resultado final del valor del activo.

Valoración de activos

Evalúa el valor de cada activo en términos de su impacto en el proyecto y la organización en caso de una amenaza.

Asigna niveles de importancia y prioridad a los activos.

Tabla 5

Valor AI

Valor de Activo	**Descripción**	**Confidencialidad**
1	Bajo	La información es confidencial pero su divulgación tendría un impacto mínimo en la organización. Aunque se prefiere mantenerla protegida, su exposición no causaría daños graves.
2	Medio	La información es confidencial y su divulgación podría tener un impacto moderado en la organización. La pérdida de confidencialidad podría causar inconvenientes y posibles pérdidas.
3	Alto	La información es altamente confidencial y su divulgación tendría un impacto significativo en la organización. La pérdida de confidencialidad podría resultar en daños financieros o dañar la reputación.
Valor de Activo	**Descripción**	**Integridad**
1	Bajo	La información es importante pero su alteración tendría un impacto mínimo. Su integridad es deseable, pero su corrupción no causaría daños graves.
2	Medio	La información es relevante para las operaciones de la organización. Su alteración podría causar inconvenientes y posibles pérdidas.
3	Alto	La información es esencial para las operaciones y su alteración tendría un impacto significativo. La pérdida de integridad podría resultar en daños financieros o pérdida de confianza.
Valor de Activo	**Descripción**	**Disponibilidad**

1	Bajo	La información es importante pero su falta de disponibilidad tendría un impacto mínimo. Su acceso es deseable, pero su interrupción no causaría daños graves.
2	Medio	La información es relevante para las operaciones de la organización. Su falta de disponibilidad podría causar inconvenientes y posibles pérdidas.
3	Alto	La información es esencial para las operaciones y su falta de disponibilidad tendría un impacto significativo. La interrupción podría resultar en daños financieros o pérdida de productividad.

Ahora, basándonos en los tres parámetros anteriormente mencionados, mostraremos la tabla de Nivel de Evaluación o el total de las estimaciones para los Activos de Información.

Tabla 6

Valor Críticos de AI

Nivel	**Valor del Activo**
Bajo	1-3
Medio	3-6
Alto	6-9

A continuación, procederemos a brindarte una concisa explicación sobre los intervalos obtenidos en la Tabla anterior, los cuales serán utilizados para generar el análisis de riesgos pertinente:

- **Bajo:** Los AI en este nivel tienen una importancia limitada en el logro de los objetivos de negocio y la continuidad operativa. Si bien su compromiso o pérdida podría causar cierta molestia o inconveniencia, no representarían una amenaza significativa para la organización ni para sus partes interesadas. Estos activos suelen tener un valor financiero y operativo moderado. Por lo tanto, las medidas de seguridad para estos activos pueden ser menos intensivas y más enfocadas en salvaguardar los aspectos básicos de la información.

- **Medio:** Los AI en este nivel poseen un nivel intermedio de importancia. Su compromiso o pérdida podría tener un impacto moderado en la operación de la organización y podría resultar en daños económicos y pérdida de confianza en algunos casos. Estos activos generalmente contienen información valiosa que, si se ve comprometida, podría causar inconvenientes y dificultades en las operaciones. Las medidas de seguridad para los activos de nivel medio son más robustas que las del nivel bajo y buscan garantizar su protección y disponibilidad adecuadas.
- **Alto:** Los activos de información en este nivel son críticos para la operación y los objetivos de negocio de la organización. Su compromiso o pérdida tendría un impacto significativo y, en algunos casos, catastrófico. Esto podría resultar en pérdidas financieras sustanciales, daño a la reputación, sanciones legales graves o interrupción severa de operaciones. Los activos de nivel alto contienen información altamente sensible y valiosa que debe ser protegida con las medidas de seguridad más rigurosas. Se destinan recursos significativos para asegurar su confidencialidad, estar disponible e integridad.

3.5.1.3 Paso 3: Identificación de Amenazas y Vulnerabilidades

Se identificará cada activo y luego se evaluará para ver cuáles se incluirán en el análisis de riesgos. Después, los activos que se hayan considerado más importantes y hayan recibido una calificación "ALTA" se utilizarán para identificar amenazas y vulnerabilidades.

Es crucial tener en cuenta que las amenazas son situaciones que podrían poner en peligro o afectar significativamente a los AI. Sin embargo, primero hay que encontrar las vulnerabilidades porque, aunque no causan daño por sí solas, podrían convertirse en peligrosas si se aprovechan o se utilizan de forma inadecuada.

A continuación, se presenta una matriz de amenazas que se conectará a los activos de información que se determinaron como los más pertinentes. Este es un paso crucial para garantizar que la información valiosa esté adecuadamente protegida y para comprender y evaluar los riesgos a los que puede enfrentarse.

Tabla 7

Distribución de Amenazas

ID	Tipo	Amenazas

1	Amenazas Naturales	Incluyen eventos naturales como terremotos, inundaciones, incendios forestales, tormentas y otros fenómenos climáticos que pueden dañar la infraestructura física y los sistemas de información.
2	Amenazas Humanas	Comprenden acciones maliciosas, negligencia o errores humanos que pueden causar daños. Esto abarca desde ataques cibernéticos hasta divulgación no intencionada de información confidencial.
3	Amenazas Ambientales	Se refieren a elementos externos que pueden repercutir en la seguridad y funcionalidad de los activos de información, como el polvo, la humedad y los cambios de temperatura.
4	Amenazas Tecnológicas	Involucran problemas técnicos, fallas de hardware o software, interrupciones en la red y otras cuestiones tecnológicas que pueden comprometer la disponibilidad o integridad de la información.
5	Amenazas Deliberadas	Incluyen ataques dirigidos y planificados, como intrusiones cibernéticas, malware, phishing y otros intentos de comprometer la seguridad de la información.
6	Amenazas Accidentales	Son incidentes no intencionados que pueden resultar en pérdida o corrupción de información, como el derrame de líquidos sobre equipos o la eliminación accidental de datos.
7	Amenazas de Fraude y Robo	Abordan actividades fraudulentas, robo de identidad y otras formas de engaño que pueden afectar la confidencialidad y la integridad de la información.
8	Amenazas de Espionaje y Vigilancia	Implican la obtención no autorizada de información valiosa por parte de terceros, ya sea a través de escuchas, vigilancia electrónica u otras técnicas de espionaje.
9	Amenazas Regulatorias y Legales	Se refieren a sanciones, multas o medidas legales que podrían ser impuestas debido a incumplimientos normativos en relación con la seguridad de la información.
10	Amenazas Sociales y Culturales	Involucran factores sociales y culturales que pueden influir en la seguridad de la información, como el robo de identidad, la manipulación de la opinión pública o la ingeniería social.

Tabla 8

Distribución de Vulnerabilidades

Numero	Tipo	Vulnerabilidades
1	Vulnerabilidades Tecnológicas	Comprenden fallas en sistemas operativos, software, hardware, aplicaciones y dispositivos, que pueden ser aprovechadas para comprometer la seguridad de la información.
2	Vulnerabilidades de Red	Incluyen debilidades en la infraestructura de red que pueden ser explotadas para realizar ataques, como la falta de encriptación, configuraciones inseguras y puntos de acceso no protegidos.
3	Vulnerabilidades de Configuración	Se refieren a configuraciones incorrectas o inseguras en sistemas, aplicaciones y dispositivos que podrían permitir el acceso no autorizado.
4	Vulnerabilidades de Autenticación y Autorización	Abordan problemas en los mecanismos de autenticación y autorización que podrían permitir que usuarios no autorizados obtengan acceso a información confidencial.
5	Vulnerabilidades de Ingeniería Social	Implican debilidades que permiten a los atacantes manipular a individuos para que divulguen información confidencial o realicen acciones no autorizadas.
6	Vulnerabilidades de Interfaz	Se relacionan con debilidades en las interfaces de sistemas y aplicaciones que podrían ser explotadas para acceder a funciones no autorizadas o información sensible.
7	Vulnerabilidades Físicas	Incluyen debilidades en la seguridad física de los activos de información, como acceso no autorizado a instalaciones o equipos.
8	Vulnerabilidades de Procesos y Procedimientos	Comprenden fallas en los procedimientos operativos y procesos internos que podrían permitir la pérdida o corrupción de información.
9	Vulnerabilidades de Cumplimiento	Implican debilidades en el cumplimiento de regulaciones y políticas de seguridad, lo que podría exponer a la organización a riesgos legales y sanciones.

10	Vulnerabilidades de Gobernanza y Cultura Organizacional	Abordan la gestión de los riesgos para la seguridad de la información y los fallos de la cultura organizativa que podrían fomentar comportamientos de riesgo.

3.5.1.4 Paso 4: Análisis de Riesgo

Se han identificado las amenazas a las que se enfrentan los activos de información y se han clasificado con un nivel de estimación "Alto". Esto indica que se ha aplicado una escala de amenazas de tres puntos. A partir de esta clasificación, determinaremos la probabilidad de ocurrencia del riesgo. La calcularemos promediando los valores asignados a los niveles de amenaza y vulnerabilidad. Esto nos permitirá calcular la probabilidad de que el riesgo se materialice.

Los parámetros de evaluación de la probabilidad, tanto para las vulnerabilidades como para las amenazas, figuran en el cuadro siguiente. A continuación, se examinarán estos elementos con mayor detalle:

Tabla 9

Referencia de Análisis Riesgos

N°	ID Activo	Nombre del activo	Descripcion del activo	Producto	Criticidad del AI	Amenaza	Vulnerabilidad	Evento	Consecuencia

- **Numero**: Numeración de los activos
- **ID Código**: Se asigna un código que empieza con la nomenclatura AI, que hace referencia al activo de información.
- **Nombre del activo**: Se indica nombre del AI.
- **Descripción del activo**: Se indica una descripción de uso del AI.
- **Producto**: Se coloca el producto o proyecto donde se identificó el riesgo
- **Criticidad del AI**: Se coloca la criticidad del activo de información identificado en el Inventario de AI.
- **Amenaza**: Se coloca la amenaza del riesgo.
- **Vulnerabilidad**: Se coloca la vulnerabilidad del Riesgo
- **Evento**: Se coloca el evento del riesgo.
- **Consecuencias**: Se coloca el evento del riesgo.

Esta evaluación considera aspectos cruciales para comprender y cuantificar la probabilidad de que los riesgos se materialicen. La meticulosa consideración de estas dimensiones permitirá tomar decisiones informadas para la gestión de riesgos.

3.5.1.5 Paso 5: Evaluación de Riesgo

Una vez que hayamos completado el análisis de riesgos, avanzaremos hacia la etapa de evaluación. Para ello, utilizaremos como base los riesgos con sus respectivas probabilidades identificadas. En otras palabras, en esta fase de evaluación de riesgos, nos centraremos en valorar el impacto que podrían tener las amenazas identificadas durante el análisis.

Este enfoque nos permitirá comprender cómo la probabilidad de que ocurra un evento y el alcance del impacto que conlleva pueden traducirse en niveles de riesgo que varían de bajo a alto. Esto será particularmente relevante para la propuesta de diseño de inyección de llaves remotas de las empresas de procesamiento de pago.

Al final, esta evaluación nos permitirá determinar de manera precisa cómo la interacción entre la probabilidad de ocurrencia y la magnitud del impacto se traduce en distintos niveles de riesgo: bajo, medio o alto. Este enfoque estratégico nos ayudará a tomar decisiones fundamentadas y a priorizar acciones para salvaguardar adecuadamente la propuesta de diseño de inyección de llaves remotas en el ámbito de procesamiento de medios de pago.

Nivel Probabilidad: Estos niveles de probabilidad ayudan a la organización a comprender su exposición al riesgo y le permiten tomar decisiones bien informadas sobre la gestión del riesgo de la SI, ya que ayudan a determinar la probabilidad de que se produzca un evento de riesgo concreto.

Tabla 10

Jerarquía de Probabilidad que ocurra el riesgo

Nivel de Probabilidad	Descripción
Muy Baja	En promedio 0.5 veces al año como máximo.
Baja	En promedio 1 vez al año como máximo.
Moderada	En promedio 4 veces al año como máximo.
Alta	En promedio 12 veces al año como máximo.
Muy Alta	En promedio más de 12 veces al año como máximo.

Nivel de Impacto: Para evaluar cómo un evento de riesgo podría afectar a los recursos y operaciones de la organización, estos niveles de impacto son esenciales. Facilitan la toma de decisiones informadas en la gestión de la seguridad de la información al ayudar a definir la posible gravedad del riesgo.

Tabla 11

Nivel Impacto

Impacto	Descripción
Critico	Puede repercutir en todos los procedimientos, bienes producidos y gestión sobre el terreno. pérdida financiera extrema.
Mayor	Puede tener un impacto en muchos de los procedimientos, bienes y procesos creados o supervisados sobre el terreno. pérdida financiera significativa.
Moderado	Puede tener un impacto en algunos de los productos o procesos creados o gestionados sobre el terreno. pérdida financiera sustancial.
Menor	puede tener un impacto en un porcentaje minúsculo de los productos o procesos creados o supervisados en la región. pérdida financiera leve.
Inferior	impacto extremadamente pequeño en un proceso o producto creado o supervisado en la región. Ningún daño, poca pérdida financiera.

Matriz de Evaluación: Con ayuda de esta matriz, las organizaciones pueden determinar el nivel de riesgo total vinculado a un conjunto concreto de combinaciones de impacto y probabilidad. En la gestión de riesgos de seguridad de la información, ofrece una base para establecer prioridades en la distribución de recursos y la toma de decisiones.

Tabla 12

Matriz de Evaluación de los niveles de riesgo

	Impacto						
Probabilidad			**Inferior**	**Menor**	**Moderado**	**Mayor**	**Critico**
			1	**2**	**3**	**4**	**5**
	Muy Alta	**5**	Medio	Alto	Muy Alto	Muy Alto	Muy Alto
	Alta	**4**	Medio	Alto	Muy Alto	Muy Alto	Muy Alto
	Media	**3**	Bajo	Medio	Alto	Alto	Muy Alto

	Baja	**2**	Bajo	Bajo	Medio	Medio	Alto
	Muy Baja	**1**	Bajo	Bajo	Bajo	Medio	Medio

Matriz de criterios: Esta matriz se utiliza para clasificar los niveles de riesgo en función de cómo interactúan el impacto, la probabilidad y la posibilidad. Mediante esta matriz, las organizaciones pueden determinar el mejor curso de acción para abordar un riesgo en función de su gravedad.

Tabla 13

Matriz de Normas de valoración de riesgos

Nivel del Riesgo	Descripción del riesgo
Muy Alto	Los riesgos clasificados como "Muy alto" representan una amenaza grave y crítica para la organización. La probabilidad de ocurrencia de eventos adversos es extremadamente alta y el impacto resultante podría tener consecuencias catastróficas para los activos de información y para la organización en su conjunto. Se requiere una acción inmediata y significativa para reducir la probabilidad de ocurrencia y minimizar el impacto potencial.
Alto	Los riesgos categorizados como "Alto" indican una amenaza sustancial para la organización. Si bien la probabilidad de ocurrencia es significativa, el impacto puede variar desde graves a críticos. Estos riesgos requieren una atención urgente y medidas efectivas de mitigación para reducir tanto la probabilidad de ocurrencia como el impacto en caso de que ocurran.
Medio	Los riesgos clasificados como "Medio" representan una amenaza moderada para la organización. La probabilidad de ocurrencia es plausible y el impacto podría variar desde moderado hasta grave. Si bien estos riesgos no son tan críticos como los niveles superiores, aún requieren atención y medidas de mitigación para garantizar que los impactos potenciales sean manejables y controlables.
Bajo	Las clasificaciones de riesgo "bajo" denotan un bajo nivel de amenaza para la organización. Hay pocas posibilidades de que esto ocurra, y el impacto que se produzca será mínimo. Aunque estos riesgos no sean tan graves, sigue siendo

	necesario gestionarlos para proteger los activos de información y mantener la integridad operativa.

3.5.1.6 Paso 6: Tratamiento del Riesgo

Discutiremos el proceso de tratamiento tras identificar los riesgos y ocurrencias potenciales que podrían tener un impacto en los activos de información en el contexto del diseño sugerido de inyección remota de claves para empresas de procesamiento de pagos. Es imperativo reconocer que las ocurrencias iniciales plausibles pueden transformarse en peligros plausibles y eventualmente culminar en incidentes o problemas recurrentes dentro del servicio.

La elección de los controles que nos permitirán reducir, mantener, evitar o compartir los riesgos identificados es el paso más importante de este proceso. Estos controles serán necesarios para proteger los recursos y mantener la integridad del servicio. Este procedimiento se guiará por un plan de tratamiento de riesgos claramente definido, que ofrecerá un plan paso a paso para establecer los controles necesarios y garantizar una gestión de riesgos satisfactoria a largo plazo.

Para reducir la probabilidad de que los riesgos se conviertan en problemas graves, es importante asegurarse de que se gestionan de forma eficaz y proactiva. Como resultado, se cumplirán las normas de seguridad, se satisfarán las necesidades de los usuarios y de la organización, y el servicio de inyección remota de claves para empresas de procesamiento de pagos funcionará de forma segura y fiable.

Enumerará las opciones de tratamiento de riesgos disponibles:

- **Modificación del riesgo:** La modificación de la probabilidad de que un riesgo se materialice o tenga un impacto implica la aplicación de determinadas políticas. Esto se consigue estableciendo las medidas de seguridad adecuadas para disminuir el impacto en caso de que se materialice una amenaza o para reducir la probabilidad de que se materialice. Al alterar la correlación entre probabilidad e impacto, la modificación del riesgo pretende reducir el riesgo a niveles más aceptables y manejables.
- **Retención del riesgo:** La retención del riesgo es la decisión consciente de la organización de aceptar un riesgo sin implementar medidas de tratamiento específicas. Esto ocurre cuando el costo de aplicar controles supera los beneficios que proporcionaría

la reducción del riesgo. Sin embargo, la retención del riesgo no significa ignorar el riesgo por completo; implica un seguimiento y monitoreo constante para asegurarse de que el riesgo siga siendo aceptable en el tiempo y que no evolucione a niveles inaceptables.

- **Evitar el riesgo:** Evitar el riesgo implica la identificación y la eliminación de las condiciones que podrían llevar a la materialización de un riesgo. Esto puede lograrse eliminando actividades, procesos, sistemas o componentes que presenten una amenaza significativa para los activos de información. En otras palabras, se trata de tomar medidas para asegurarse de que el riesgo no pueda manifestarse en primer lugar. Esta opción es especialmente útil cuando los riesgos son inaceptablemente altos o cuando no es factible aplicar medidas de mitigación.
- **Distribución del riesgo:** La distribución del riesgo implica transferir una parte o la totalidad del riesgo a terceros, como aseguradoras o proveedores. Esto se logra mediante acuerdos contractuales que establecen cómo se manejarían los riesgos en caso de que ocurran. Si bien el riesgo sigue existiendo, su impacto financiero u operativo se comparte con otras partes. La distribución del riesgo puede ser particularmente útil para riesgos específicos que están fuera del control directo de la organización o cuando se desea mitigar la exposición financiera.

En la toma de decisiones sobre cómo tratar los riesgos, es fundamental evaluar cada opción en función de su eficacia, viabilidad y alineación con los objetivos y recursos de la organización. Estas opciones permiten a las organizaciones adaptar su enfoque de tratamiento según la naturaleza y la gravedad de los riesgos identificados.

Es imperativo tener en cuenta el proceso de Aceptación del Riesgo, que consiste en reconocer la posibilidad de que un riesgo se manifieste sin necesidad de tomar medidas inmediatas. Esta opción se elige cuando el impacto potencial de la reducción del riesgo -especialmente si el riesgo es pequeño- es mayor que el de la aplicación de controles adicionales, la asignación de recursos o la asunción de tareas adicionales.

Además, existen enfoques adicionales para el tratamiento de riesgos que vale la pena destacar. Por ejemplo:

- **Riesgo Aceptado:** El riesgo aceptado es aquel que la organización decide conscientemente asumir sin aplicar medidas de tratamiento específicas. Esta decisión se toma después de una evaluación exhaustiva de los riesgos, considerando factores como

la probabilidad de ocurrencia y el impacto potencial. Aceptar un riesgo implica reconocer que existe la posibilidad de que ocurra, pero que se ha considerado aceptable dentro de los límites y los objetivos de la organización. Esta opción es adecuada cuando el costo de mitigación supera los beneficios potenciales o cuando las medidas de tratamiento no son factibles.

- **Riesgo Apreciable:** El riesgo apreciable es aquel que, aunque se ha aceptado, aún requiere una supervisión y un seguimiento cercanos. Aunque la organización puede haber decidido no aplicar medidas de tratamiento adicionales, reconoce que el riesgo sigue siendo significativo y podría tener impactos negativos en sus operaciones, activos o reputación. El monitoreo constante permite a la organización estar preparada para tomar medidas adicionales si el riesgo evoluciona y se convierte en un problema más grave.
- **Riesgo critico:** El riesgo crítico es aquel que está más allá de los niveles aceptables para la organización y representa una amenaza grave y significativa para sus objetivos, activos u operaciones. Este nivel de riesgo implica una atención inmediata y la implementación de medidas de tratamiento para reducir la probabilidad de ocurrencia y el impacto. Los riesgos críticos deben abordarse de manera prioritaria y eficaz, ya que su materialización podría tener consecuencias catastróficas. En muchos casos, los riesgos críticos no se aceptan y se implementan acciones agresivas para mitigarlos.

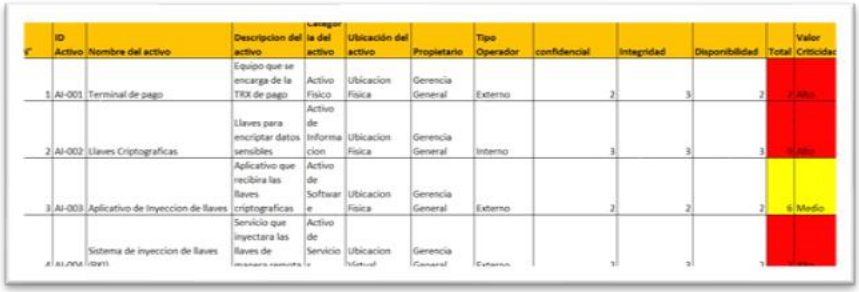
3.5.1.7 Paso 7: Aplicar la metodología de Riesgo

Para proceder aplicar la metodología de riesgo tomamos como ejemplo una plantilla que está adaptada al estándar ISO/IEC 27005:2018 para recopilar toda la información relevante sobre el riesgo y realizar un análisis inmediato del riesgo.

Primero, realizamos el inventario de AI para conocer la criticidad del activo.

Figura 23

Inventario de Activo de información



Nº	ID Activo	Nombre del activo	Descripcion del activo	Categoria del activo	Ubicación del activo	Propietario	Tipo Operador	confidencial	Integridad	Disponibilidad	Total	Valor Criticidad
1	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Activo Fisico	Ubicacion Fisica	Gerencia General	Externo	2	3	2	7	Alto
2	AI-002	Llaves Criptograficas	Llaves para encriptar datos sensibles	Activo de Informacion	Ubicacion Fisica	Gerencia General	Interno	3	3	3	9	Alto
3	AI-003	Aplicativo de Inyeccion de llaves	Aplicativo que recibira las llaves criptograficas	Activo de Software	Ubicacion Fisica	Gerencia General	Externo	2	2	2	6	Medio
4	AI-004	Sistema de inyeccion de llaves	Servicio que inyectara las llaves de manera remota	Activo de Servicio	Ubicacion Virtual	Gerencia General	Externo	3	3	3	9	Alto

Segundo, realizamos la identificación de amenazas y vulnerabilidades de los activos de información.

Figura 24

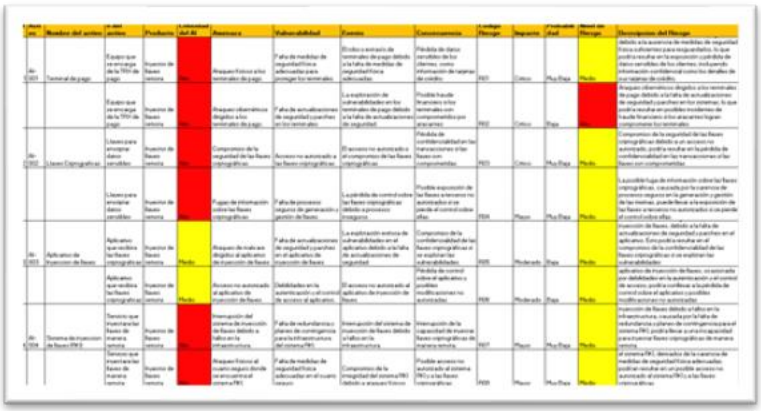
Identificación de amenazas y vulnerabilidades

N°	ID Activo	Nombre del activo	Descripcion del activo	Producto	Criticidad del AI	Amenazas	Descripcion de la amenaza	Descripción de la vulnerabilidad
1	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Inyector de llaves remota	Alto	Humanas	Ataques físicos a los terminales (por ejemplo, intentos de robo o manipulación de terminales).	Falta de medidas de seguridad física adecuadas para proteger los terminales.
			Equipo que se encarga de la TRX de pago	Inyector de llaves remota	Alto	Tecnologicas	Ataques cibernéticos dirigidos a los terminales (por ejemplo, malware o ataques de skimming).	Falta de actualizaciones de seguridad y parches en los terminales.
2	AI-002	Llaves Criptograficas	Llaves para encriptar datos sensibles	Inyector de llaves remota	Alto	Tecnologicas	Compromiso de la seguridad de las llaves criptográficas.	Acceso no autorizado a las llaves criptográficas.
			Llaves para encriptar datos sensibles	Inyector de llaves remota	Alto	Humanas	Fugas de información sobre las llaves criptográficas.	Falta de procesos seguros de generación y gestión de llaves.
3	AI-003	Aplicativo de Inyeccion de llaves	Aplicativo que recibira las llaves criptograficas	Inyector de llaves remota	Medio	Tecnologicas	Ataques de malware dirigidos al aplicativo de inyección de llaves.	Falta de actualizaciones de seguridad y parches en el aplicativo de inyección de llaves.
			Aplicativo que recibira las llaves criptograficas	Inyector de llaves remota	Medio	Tecnologicas	Acceso no autorizado al aplicativo de inyección de llaves.	Debilidades en la autenticación y el control de acceso al aplicativo.
4	AI-004	Sistema de inyeccion de llaves (RKI)	inyectara las llaves de manera remota	Inyector de llaves remota	Alto	Tecnologicas	Interrupción del sistema de inyección de llaves debido a fallos en la infraestructura.	Falta de redundancia y planes de contingencia para la infraestructura del sistema RKI.
			inyectara las llaves de manera remota	Inyector de llaves remota	Alto	Tecnologicas	Ataques físicos al cuarto seguro donde se encuentra el sistema RKI.	Falta de medidas de seguridad física adecuadas en el cuarto seguro.

Luego identificamos y analizamos los riesgos, con una encuesta a personas del rubro, se encuentra el impacto y la probabilidad de acuerdo con la matriz de la metodología, y con esos valores no muestra el nivel de riesgo P * I.

Figura 25

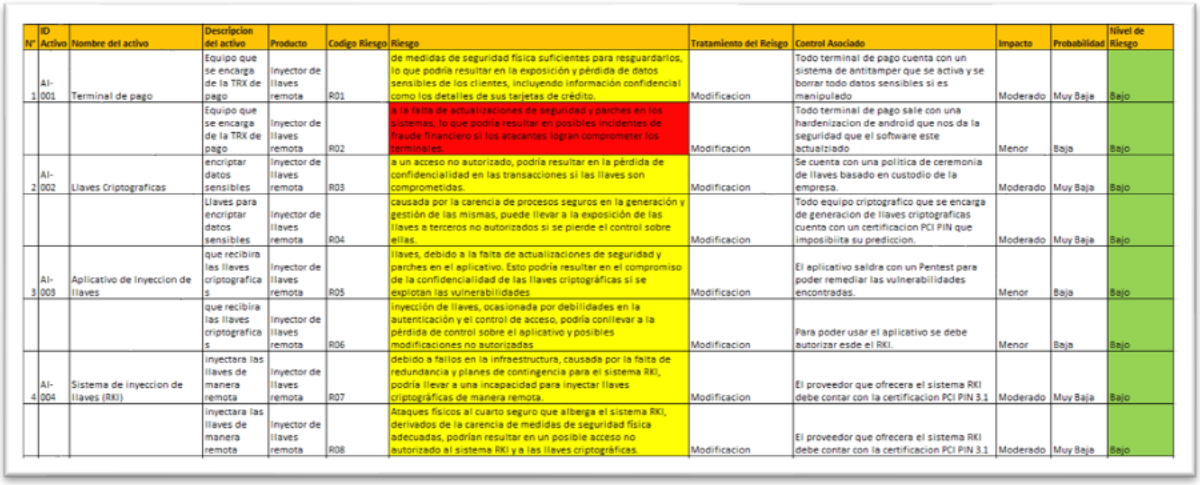
Análisis de Riesgo



Una vez que conocemos el riesgo resultante, realizamos el tratamiento del riesgo para reducir el nivel del riesgo.

Figura 26

Evaluación del control



Nº	ID Activo	Nombre del activo	Descripcion del activo	Producto	Codigo Riesgo	Riesgo	Tratamiento del Reigo	Control Asociado	Impacto	Probabilidad	Nivel de Riesgo
1	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Inyector de llaves remota	R01	de medidas de seguridad física suficientes para resguardarlos, lo que podría resultar en la exposición y pérdida de datos sensibles de los clientes, incluyendo información confidencial como los detalles de sus tarjetas de crédito.	Modificacion	Todo terminal de pago cuenta con un sistema de antitamper que se activa y se borrar todo datos sensibles si es manipulado	Moderado	Muy Baja	Bajo
			Equipo que se encarga de la TRX de pago	Inyector de llaves remota	R02	a la falta de actualizaciones de seguridad y parches en los sistemas, lo que podría resultar en posibles incidentes de fraude financiero si los atacantes logran comprometer los terminales.	Modificacion	Todo terminal de pago sale con una hardenizacion de android que nos da la seguridad que el software este actualizado	Menor	Baja	Bajo
2	AI-002	Llaves Criptograficas	encriptar datos sensibles	Inyector de llaves remota	R03	a un acceso no autorizado, podría resultar en la pérdida de confidencialidad en las transacciones si las llaves son comprometidas.	Modificacion	Se cuenta con una política de ceremonia de llaves basado en custodio de la empresa.	Moderado	Muy Baja	Bajo
			Llaves para encriptar datos sensibles	Inyector de llaves remota	R04	causada por la carencia de procesos seguros en la generación y gestión de las mismas, puede llevar a la exposición de las llaves a terceros no autorizados si se pierde el control sobre ellas.	Modificacion	Todo equipo criptografico que se encarga de generacion de llaves criptograficas cuenta con un certificacion PCI PIN que imposibilita su prediccion.	Moderado	Muy Baja	Bajo
3	AI-003	Aplicativo de Inyeccion de llaves	que recibira las llaves criptograficas	Inyector de llaves remota	R05	llaves, debido a la falta de actualizaciones de seguridad y parches en el aplicativo. Esto podría resultar en el compromiso de la confidencialidad de las llaves criptográficas si se explotan las vulnerabilidades	Modificacion	El aplicativo saldra con un Pentest para poder remediar las vulnerabilidades encontradas.	Menor	Baja	Bajo
			que recibira las llaves criptograficas	Inyector de llaves remota	R06	inyección de llaves, ocasionada por debilidades en la autenticación y el control de acceso, podría conllevar a la pérdida de control sobre el aplicativo y posibles modificaciones no autorizadas	Modificacion	Para poder usar el aplicativo se debe autorizar esde el RKI.	Menor	Baja	Bajo
4	AI-004	Sistema de inyeccion de llaves (RKI)	inyectara las llaves de manera remota	Inyector de llaves remota	R07	debido a fallos en la infraestructura, causada por la falta de redundancia y planes de contingencia para el sistema RKI, podría llevar a una incapacidad para inyectar llaves criptográficas de manera remota.	Modificacion	El proveedor que ofrecera el sistema RKI debe contar con la certificacion PCI PIN 3.1	Moderado	Muy Baja	Bajo
			inyectara las llaves de manera remota	Inyector de llaves remota	R08	Ataques físicos al cuarto seguro que alberga el sistema RKI, derivados de la carencia de medidas de seguridad física adecuadas, podrían resultar en un posible acceso no autorizado al sistema RKI y a las llaves criptográficas.	Modificacion	El proveedor que ofrecera el sistema RKI debe contar con la certificacion PCI PIN 3.1	Moderado	Muy Baja	Bajo

3.5.2 Definir requisitos de las llaves criptográficas

Este procedimiento asegura que la "ceremonia de llaves" se realice de manera segura, transparente y en cumplimiento con el estándar PCI PIN v3.1, garantizando la imposibilidad de predicción de las llaves criptográficas necesarias para los terminales de pago de empresas de procesamiento de pagos.

Pasos para la Ceremonia de Llaves según PCI PIN V3.1

3.5.2.1 Paso 1: Preparación y Planificación

- Designa a un equipo responsable de la ceremonia, incluyendo roles como "custodios", "Testigo" y "Key Manager".

Tabla 14

Tabla de custodios

Custodios	Descripción
Custodio 1	Se selecciona a un colaborador de la empresa que ostente al menos el cargo de jefe y que cuente con un historial de 3 años de servicio ininterrumpido en la organización. Es importante que esta persona pertenezca a una gerencia diferente a la de los otros custodios designados.
Custodio 2	Se selecciona a un colaborador de la empresa que ostente al menos el cargo de jefe y que cuente con un historial de 3 años de servicio

	ininterrumpido en la organización. Es importante que esta persona pertenezca a una gerencia diferente a la de los otros custodios designados.
Custodio 3	Se selecciona a un colaborador de la empresa que ostente al menos el cargo de jefe y que cuente con un historial de 3 años de servicio ininterrumpido en la organización. Es importante que esta persona pertenezca a una gerencia diferente a la de los otros custodios designados.

- Define el lugar y la fecha de la ceremonia.
- Asegúrate de que todos los componentes necesarios estén listos, como generadores aleatorios criptográficamente seguros y módulos de seguridad aprobados (HSM)

3.5.2.2 Paso 2: Generación de llaves Criptográficas

- Utiliza generadores aleatorios criptográficamente seguros para generar las llaves requeridas.
- Verifica que los generadores no sean predecibles y cumplan con los estándares de seguridad.

3.5.2.3 Paso 3: Configuración de ambiente

- Verifica que el ambiente donde se realizará la ceremonia esté físicamente seguro y libre de dispositivos no autorizados.
- Asegúrate de que los equipos y los sistemas estén configurados correctamente.

3.5.2.4 Paso 4: Roles y autenticación

- Asigna roles claros a los participantes, como el Key Manager y Custodios.

Tabla 15

Tabla de Key Manager

Key Manager	Descripción
Key Manager 1	Se elige para el puesto a una persona con tres años de servicio ininterrumpido en la división de seguridad de la información de la empresa.

Key Manager 2	Se elige para el puesto a una persona con tres años de servicio ininterrumpido en la división de seguridad de la información de la empresa.

- Verifica la identidad de los participantes y su autorización para participar en la ceremonia.

3.5.2.5 Paso 5: Inicio de la ceremonia de llaves

- El Key Manager inicia la ceremonia con un acta formal.
- Se procede a generar las llaves criptográficas de acuerdo con las especificaciones y requisitos establecidos.

3.5.2.6 Paso 6: Verificación y autenticación

- Los custodios y Key Manager participan en la validación y autenticación del proceso de generación.
- Verifican que las llaves generadas cumplan con los parámetros establecidos.

3.5.2.7 Paso 7: División de llaves

- En la política de empresas de procesamiento de pagos, se solicita que la llave se divide en mínimo 3 componentes para asegurar la seguridad de esta.

3.5.2.8 Paso 8: Cierre de ceremonia de llaves

- El Key Manager finaliza la ceremonia con un acta formal de cierre.
- Los participantes firman un acta que documenta los detalles de la ceremonia.

3.5.2.9 Paso 9: Registro y Documentación

- Documenta cada paso de la ceremonia, incluyendo la fecha, los participantes, los roles y las acciones realizadas.
- Guarda los registros y la documentación en un lugar seguro y accesible solo para personas autorizadas.

3.5.2.10 Paso 10: Seguimiento y auditoria.

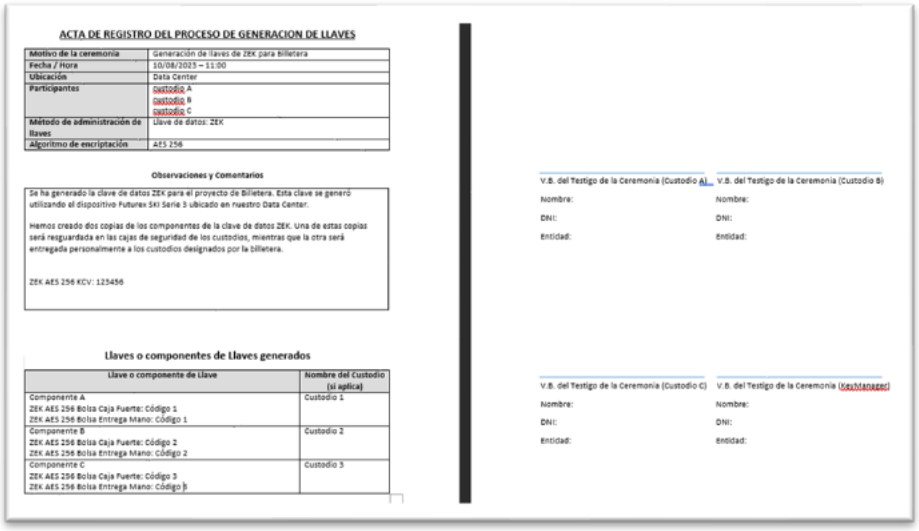
- Programa auditorías regulares para revisar el procedimiento de la ceremonia y verificar su cumplimiento continuo con los estándares.
- Actualiza los procedimientos según sea necesario en función de los hallazgos de auditoría y los cambios en los requisitos.

3.5.2.11 Paso 11: Resultado de aplicar los requisitos de generación de llaves criptográficas.

Cuando se concluye una ceremonia de generación de llaves criptográficas, es necesario elaborar un acta de finalización de la ceremonia. Esta acta es un requisito del estándar de certificación PCI PIN v3.1 y debe incluir la justificación de la ceremonia, así como la firma de todos los custodios y del key manager.

Figura 27

Formato de Ceremonia de llaves



ACTA DE REGISTRO DEL PROCESO DE GENERACION DE LLAVES

Motivo de la ceremonia	Generación de llaves de ZEK para Billetera
Fecha / Hora	10/08/2023 – 11:00
Ubicación	Data Center
Participantes	custodio A custodio B custodio C
Método de administración de llaves	Llave de datos: ZEK
Algoritmo de encriptación	AES 256

Observaciones y Comentarios

Se ha generado la clave de datos ZEK para el proyecto de Billetera. Esta clave se generó utilizando el dispositivo Futurex SKI Serie 3 ubicado en nuestro Data Center.

Hemos creado dos copias de los componentes de la clave de datos ZEK. Una de estas copias será resguardada en las cajas de seguridad de los custodios, mientras que la otra será entregada personalmente a los custodios designados por la billetera.

ZEK AES 256 KCV: 123456

Llaves o componentes de Llaves generados

Llave o componente de Llave	Nombre del Custodio (si aplica)
Componente A ZEK AES 256 Bolsa Caja Fuerte: Código 1 ZEK AES 256 Bolsa Entrega Mano: Código 1	Custodio 1
Componente B ZEK AES 256 Bolsa Caja Fuerte: Código 2 ZEK AES 256 Bolsa Entrega Mano: Código 2	Custodio 2
Componente C ZEK AES 256 Bolsa Caja Fuerte: Código 3 ZEK AES 256 Bolsa Entrega Mano: Código 3	Custodio 3

V.B. del Testigo de la Ceremonia (Custodio A) — Nombre: — DNI: — Entidad:

V.B. del Testigo de la Ceremonia (Custodio B) — Nombre: — DNI: — Entidad:

V.B. del Testigo de la Ceremonia (Custodio C) — Nombre: — DNI: — Entidad:

V.B. del Testigo de la Ceremonia (KeyManager) — Nombre: — DNI: — Entidad:

3.5.3 Llave Criptográficas

En lo referente a las llaves criptográficas, es importante destacar que constituyen la información más delicada para una empresa adquiriente. Estas llaves son utilizadas para cifrar datos sensibles del tarjetahabiente, como su número de tarjeta (PAN) y su identificación personal (PIN). Por tanto, es esencial que la generación y transferencia de estas llaves siempre cumplan con el estándar vigente exigido por las marcas, tal como ocurre en el caso de empresas de procesamiento de pagos, que se esfuerza constantemente por obtener la Certificación PCI PIN v3.1.

Es relevante mencionar que existen diferentes tipos de llaves criptográficas, los cuales se detallan a continuación:

Tabla 16

Sistemas de llaves

Tipo de Llave	Algoritmos	Uso de llave

LMK	3DES y AES	Están llaves son las llaves raíz que se encargan de cifrar las otras llaves, se tiene actualmente como VARIANT y KEYBLOCK
ZMK	3DES y AES	Esta llave se utiliza como transporte de otras llaves, se comparte entre entidades, y solo está en el host.
TMK	3DES y AES	Esta llave se utiliza para encriptar una llave de trabajo, y se encuentra tanto en el terminal de pago como en el host.
TWK	3DES y AES	Esta llave se utiliza para encriptar el numero PAN del tarjetahabiente, y se encuentra en el terminal de pago y el host
ZPK	3DES y AES	Esta llave se utiliza para cifrar el identificar del tarjetahabiente (PIN), es uso solo entre entidades para transferir el PIN.
ZEK	3DES y AES	Esta llave se utiliza para cifrar el número de tarjeta (PAN), es uso solo entre entidades para transferir el PAN.
DEK	3DES y AES	Esta llave se utiliza en las procesadoras o en una aplicación para poder almacenar el numero PAN.
PEK	3DES y AES	Esta llave se utiliza en las procesadoras para poder realizar una traslación del número PIN.

Utilizaremos estos diversos tipos de claves en nuestro proyecto de tesis, asegurándonos de que siempre nos atenemos a las mejores prácticas de seguridad y a la norma PCI PIN v3.1. Esta estrategia garantizará que las claves criptográficas se gestionen de forma fiable y segura, respetando las directrices de la marca y protegiendo la confidencialidad de los titulares de las tarjetas. Al adherirnos al estándar y utilizar estas prácticas de seguridad, podremos crear una propuesta de diseño de inyección remota de claves que cumpla con los requisitos más estrictos de seguridad y calidad en el manejo de claves criptográficas.

3.5.4 Requerimiento de inyección de llaves

En esta etapa, se requiere del sistema de inyección remota más conocido como RKI (Remote Key Injection), que puede ser alojado en una nube propietaria del proveedor o en alguna otra nube pública como AWS, Azure o Google. El sistema criptográfico del proveedor debe cumplir con el estándar PCI PIN v3.1 para asegurar que las llaves criptográficas transferidas cuenten con todos los controles de seguridad necesarios.

Por otro lado, el proveedor debe contar con una página web o un BackOffice que liste todos los terminales de pago seriados y permita verificar qué terminales están autorizados para la inyección de llaves. Este BackOffice debe cumplir con los más altos requerimientos de seguridad para garantizar una inyección de llaves criptográficas segura.

En relación con los terminales de pago, es necesario generar un certificado asimétrico que facilite la autenticación con el host. Este certificado debe utilizar un algoritmo que brinde seguridad en la comunicación entre el host y el terminal de pago. La generación del certificado debe realizarse en un ambiente seguro, asegurando que solo la llave pública esté disponible en los terminales de pago de la empresa y que esté integrada en el firmware para evitar desinstalaciones o cambios no autorizados.

Una vez que todos los requerimientos anteriores hayan pasado exitosamente los procesos de seguridad según el estándar PCI PIN v3.1 y las llaves estén cargadas en el host y los terminales tengan el certificado asimétrico para la autenticación, se podrá iniciar la etapa final de la propuesta de diseño.

En esta etapa, una aplicación desarrollada a medida permitirá realizar la inyección remota en los diferentes sistemas operativos de los terminales de pago. Gracias a esto, los terminales de pago podrán encontrarse en cualquier ubicación, ya sea en comercios de utilizan medios de pago u otros lugares, y recibirán la inyección de llaves criptográficas de manera remota y segura. Con todo este proceso establecido, se garantiza una gestión eficiente y confiable de las llaves criptográficas para los terminales de pago de la empresa.

3.5.5 Requerimiento de Equipo criptográficos

En este requerimiento, se solicita que todos los equipos criptográficos que forman parte de la propuesta de diseño de inyección de llaves remotas cuenten con la certificación PCI PIN v3.1. Esta certificación es obligatoria por parte de las marcas de pago y garantiza que los equipos han sido sometidos a rigurosas pruebas de vulnerabilidad en diversos laboratorios.

Gracias a esta certificación, podemos tener plena confianza en que las llaves criptográficas transferidas y almacenadas podrán ser inyectadas en los terminales de pago de manera segura. Además, nos asegura que los equipos cumplen con los estándares de seguridad más exigentes establecidos por las marcas de pago, brindando así una protección sólida y confiable para los datos cifrados de los tarjetahabientes.

3.6 Matriz de especificación del requerimiento del modelo

Los requisitos enumerados a continuación son los que se mencionaron en los capítulos anteriores y son necesarios para completar el diseño de inyección remota de llave sugerido. Estos requisitos satisfacen las necesidades de las partes interesadas en el proyecto.

A continuación, se muestra una tabla que relaciona los objetivos específicos con los requerimientos:

Tabla 17

Relación de objetivos con norma

N°	Objetivo	Descripción del objetivo	Normas o Estándar
OE1	Realizar un análisis de riesgos para la actividad de inyección de llaves, la cual forma parte del área de seguridad de la información, con el objetivo de identificar las amenazas y vulnerabilidades críticas que podrían comprometer la confidencialidad de las llaves.	Un paso importante en el ámbito de la seguridad de la información es realizar un análisis de riesgos exhaustivo para la actividad de inyección de claves criptográficas. Para garantizar la confidencialidad e integridad de las transacciones en los terminales de pago, la inyección de claves es un procedimiento esencial. Encontrar y evaluar los principales riesgos y puntos débiles que podrían poner en peligro la confidencialidad de las claves utilizadas en este procedimiento es el objetivo del análisis de riesgos.	ISO/EIC 27005:2018 “metodología para la gestión de riesgos”
OE2	Definir los requisitos de las llaves criptográficas necesarias para los terminales de pago de las empresas procesadoras de medios de pago,	El propósito de este subobjetivo es establecer un conjunto de requisitos esenciales para las llaves criptográficas que serán utilizadas en los terminales de pago de las empresas procesadoras de medios de pago. Estos requisitos serán definidos a través de una meticulosa "ceremonia de llaves", un proceso	Estándar PCI PIN v3.1 – Objetivo 1 y 2 NIST SP 800-133 "Recommendation for Cryptographic Key Generation"

	mediante un proceso de "ceremonia de llaves" que garantice su absoluta imposibilidad de predicción.	altamente seguro y controlado diseñado para garantizar que las llaves sean generadas, distribuidas y almacenadas de manera que su predicción sea absolutamente imposible.	
OE3	Desarrollar un procedimiento de simulación para la inyección remota de llaves criptográficas en los terminales de pago de las empresas procesadoras de medios de pago, que permita asegurar la transmisión y carga segura de las llaves en el RKI y en los propios terminales de pago.	Diseñar y desarrollar un procedimiento de simulación que permita la inyección remota de llaves criptográficas en los terminales de pago las empresas de procesamiento de pagos. Este procedimiento, que simulará el proceso real de inyección, garantizará que la transmisión y carga de las llaves se realicen de manera segura y eficiente, tanto en el host central ("Master") como en los terminales de pago distribuidos.	Estándar PCI PIN v3.1 – Objetivo 3 ISO/IEC
OE4	Definir los requisitos técnicos del equipamiento tecnológico informático utilizado en la inyección remota de llaves criptográficas con el fin de cumplir con la certificación PCI PIN v3.1.	Identificar los requisitos necesarios que deben cumplir los equipos informáticos para que sean conformes con las normas de seguridad recogidas en la certificación PCI PIN v3.1 en lo que se refiere al proceso de inyección remota de claves criptográficas. Es imprescindible que estos equipos cumplan los requisitos de seguridad más estrictos, ya que son esenciales para la salvaguarda de las claves criptográficas.	Estándar PCI PIN v3.1 – Objetivo 7
OE5	Proponer actividades y controles específicos para asegurar que el diseño propuesto para	Desarrollar un conjunto detallado de actividades y controles diseñados para garantizar que el diseño del sistema de inyección de llaves criptográficas remota	Estándar PCI PIN v3.1 – Objetivo 6 ISO/IEC 27001:2013

	el sistema de inyección de llaves criptográficas remota se realice de manera eficiente y segura en los terminales de pago, minimizando riesgos potenciales.	se implemente de manera óptima en los terminales de pago, mientras se minimizan los riesgos potenciales. Estas actividades y controles estarán enfocados en asegurar la eficiencia operativa y la seguridad integral del sistema, tanto en la transmisión y carga de llaves como en la administración general del proceso.	"Enfoque integral para la seguridad de la información.

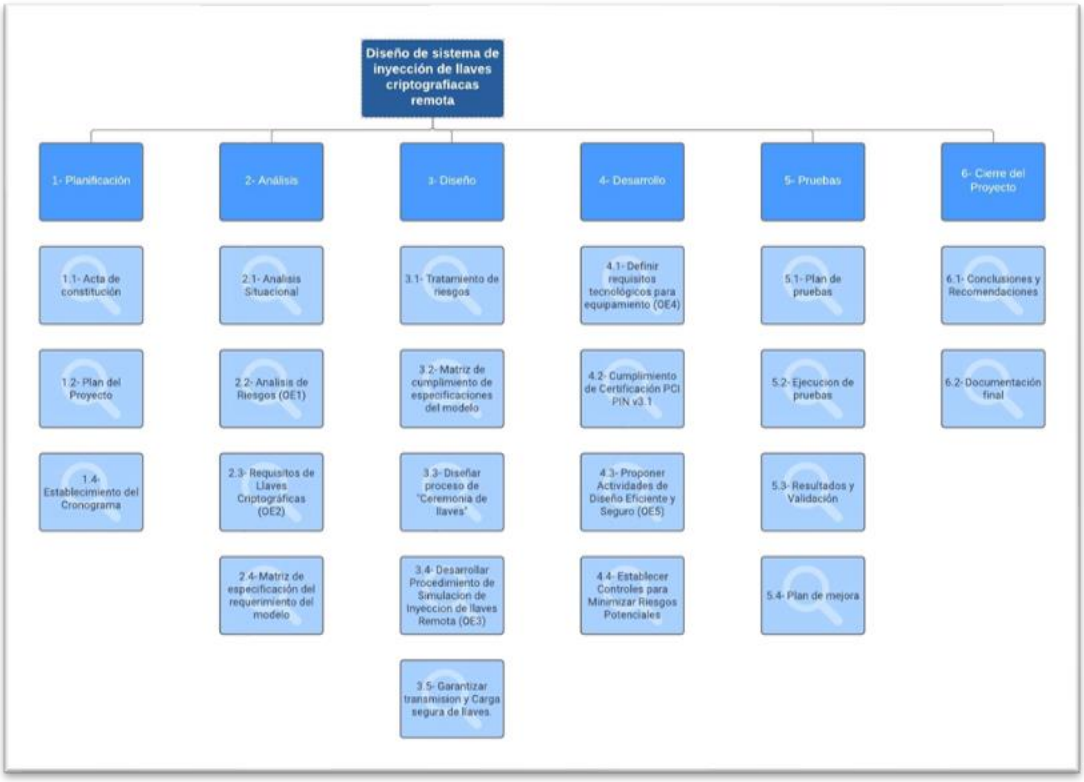
Estos requerimientos son fundamentales para garantizar la seguridad y eficiencia en la inyección de llaves remotas en los terminales de pago, y permitirán cumplir con los estándares establecidos por las marcas de pago y las necesidades de las compañías.

3.7 EDT del proyecto

Se va a mostrar el siguiente EDT que nos organiza visualmente las fases del proyecto en sus diferentes niveles.

Figura 28

EDT



4 CAPÍTULO 4: DISEÑO DE LA SOLUCION

4.1 Diseño de Modelo de la inyección remota de llaves

4.1.1 Alcance

El presente capítulo se enfocará en el diseño y desarrollo de la inyección remota de llaves criptográficas para los terminales de pago utilizados en las TRX de las empresas de procesamiento de pago. Esta propuesta tiene como objetivo principal lograr una mayor eficiencia en el aseguramiento y disponibilidad de los terminales de pago en producción, a la vez que garantiza la confidencialidad y seguridad de las llaves criptográficas.

El alcance del proyecto abarca el área de seguridad de la información, ya que se busca migrar hacia un entorno remoto para la inyección de llaves, lo que permitirá descentralizar este proceso, eliminando la necesidad de un cuarto seguro como lo exigen las marcas para la inyección local de llaves criptográficas.

La propuesta de tesis propone un diseño que ofrece beneficios significativos a las empresas de procesamiento de pagos, incluyendo la reducción de costos al eliminar la dependencia de nuevas versiones de equipos criptográficos para la inyección de llaves. En su lugar, se plantea el desarrollo de un servicio que se ajuste a los cambios de nuevos algoritmos, lo que brindará mayor flexibilidad y agilidad a la empresa ante futuras actualizaciones de seguridad.

El diseño contempla la generación de llaves criptográficas seguras y únicas, la transmisión segura entre el host y los terminales de pago, y un procedimiento de simulación para garantizar la efectividad y robustez del proceso de inyección remota.

En resumen, la implementación de la inyección remota de llaves criptográficas permitirá a las empresas procesadoras de medios de pago mejorar sus operaciones, aumentar la eficiencia en la disponibilidad de terminales de pago y fortalecer la seguridad en el procesamiento de transacciones, todo ello con un enfoque en reducir costos y brindar una solución sostenible y adaptable a futuras exigencias del mercado.

4.1.2 Limitaciones

Es importante destacar que el alcance de esta propuesta de diseño de inyección remota de llaves está enfocado en migrar hacia un modelo de inyección como servicio, reemplazando así la inyección local que presenta ciertos problemas y ofrece grandes beneficios. Sin embargo, es relevante mencionar que este proyecto no abarca la selección del proveedor o

marca específica con la que la empresa procesadora de medios de pago debe trabajar para implementar la solución.

El principal inconveniente del proyecto es la falta de una recomendación clara sobre la marca o el proveedor que se debe utilizar para implantar con éxito la inyección remota de claves. Como resultado, la empresa debe llevar a cabo un proceso independiente de evaluación y selección de proveedores que satisfagan sus necesidades y se adhieran a las directrices de seguridad establecidas por la norma PCI PIN v3.1.

Además, es fundamental considerar que este proyecto se enfoca en proporcionar pautas y lineamientos para el diseño de la solución de manera segura y eficiente, pero no define la estrategia de implementación o las posibles limitaciones técnicas que puedan surgir al adoptar la inyección remota de llaves. Estas limitaciones serán específicas para cada empresa y requerirán un análisis detallado por parte del equipo técnico.

En resumen, la propuesta de diseño ofrece una guía valiosa para la implementación exitosa de la inyección remota de llaves criptográficas, pero la elección del proveedor y las consideraciones técnicas serán responsabilidad de la empresa de procesamiento de pagos al adaptar la solución a sus necesidades y requerimientos específicos.

4.2 Matriz de Cumplimento de especificaciones del modelo

Tabla 18

Matriz de Cumplimento de especificaciones del modelo

N°	Objetivo	Descripción del objetivo	Normas o Estándar	Cumplimiento
OE1	Realizar un análisis de riesgos para la actividad de inyección de llaves, la cual forma parte del área de seguridad de la información, con el objetivo de identificar las amenazas y	Un paso importante en el ámbito de la seguridad de la información es realizar un análisis de riesgos exhaustivo para la actividad de inyección de claves criptográficas. Para garantizar la	ISO 31000:2018 ISO/EIC 27005:2018 “metodología para la gestión de riesgos”	Utilizaremos la información proporcionada en las normas ISO 31000:2018 e ISO/EIC 27005:2018 para lograr el objetivo. En primer lugar, debemos crear un marco de gestión

	vulnerabilidades críticas que podrían comprometer la confidencialidad de las llaves.	confidencialidad e integridad de las transacciones en los terminales de pago, la inyección de claves es un procedimiento esencial. Encontrar y evaluar los principales riesgos y puntos débiles que podrían poner en peligro la confidencialidad de las claves utilizadas en este procedimiento es el objetivo del análisis de riesgos.		de riesgos. A continuación, debemos identificar los activos de información, los riesgos potenciales y los propios riesgos. Por último, debemos evaluar los riesgos y tratarlos para reducir su probabilidad de ocurrencia. Por último, debemos supervisar y revisar las medidas de mitigación para determinar su eficacia e introducir los ajustes necesarios.
OE2	Definir los requisitos de las llaves criptográficas necesarias para los terminales de pago de las empresas procesadoras de medios de pago, mediante un proceso de "ceremonia de llaves" que garantice su absoluta	El propósito de este subobjetivo es establecer un conjunto de requisitos esenciales para las llaves criptográficas que serán utilizadas en los terminales de pago de las empresas procesadoras de medios de pago. Estos requisitos serán	Estándar PCI PIN v3.1 – Objetivo 1 y 2 NIST SP 800-133 "Recommendation for Cryptographic Key Generation"	Para cumplir el objetivo deben cumplirse los requisitos descritos en NIST SP 800-133 y Standard PCI PIN v3.1 - Objetivos 1-2. En concreto, debemos declarar que las claves criptográficas se están utilizando de acuerdo con prácticas

	imposibilidad de predicción.	definidos a través de una meticulosa "ceremonia de llaves", un proceso altamente seguro y controlado diseñado para garantizar que las llaves sean generadas, distribuidas y almacenadas de manera que su predicción sea absolutamente imposible.		seguras y que el proceso de generación de claves se está llevando a cabo de acuerdo con su predicción exacta. También respetaremos las directrices para la creación de claves criptográficas.
OE3	Desarrollar un procedimiento de simulación para la inyección remota de llaves criptográficas en los terminales de pago de las empresas procesadoras de medios de pago, que permita asegurar la transmisión y carga segura de las llaves en el RKI y en los propios terminales de pago.	Diseñar y desarrollar un procedimiento de simulación que permita la inyección remota de llaves criptográficas en los terminales de pago las empresas de procesamiento de pagos. Este procedimiento, que simulará el proceso real de inyección, garantizará que la transmisión y carga de las llaves se realicen de manera segura y eficiente,	Estándar PCI PIN v3.1 – Objetivo 3 - 4	Para lograr el objetivo, utilizaremos la información proporcionada en la norma ISO/IEC 24745:2011 y la norma PCI PIN v3.1 - Objetivos 3-4. Utilizando las claves generadas previamente, crearemos una simulación de inyección de clave. Para ello, debemos cargar la clave en el RKI para inyectar la

		tanto en el host central ("Master") como en los terminales de pago distribuidos.		clave criptográfica en el terminal.
OE4	Definir los requisitos técnicos del equipamiento tecnológico informático utilizado en la inyección remota de llaves criptográficas con el fin de cumplir con la certificación PCI PIN v3.1.	Identificar los requisitos necesarios que deben cumplir los equipos informáticos para que sean conformes con las normas de seguridad recogidas en la certificación PCI PIN v3.1 en lo que se refiere al proceso de inyección remota de claves criptográficas. Es imprescindible que estos equipos cumplan los requisitos de seguridad más estrictos, ya que son esenciales para la salvaguarda de las claves criptográficas.	Estándar PCI PIN v3.1 – Objetivo 7	Para lograr el objetivo, seguiremos las directrices indicadas en la norma PCI PIN v3.1 - Objetivo 7, lo que significa que dependeremos de la marca y el modelo del equipo. A continuación, confirmaremos que el equipo cumple la certificación PIN utilizando el sitio web oficial del CONSEJO.
OE5	Proponer actividades y controles específicos para asegurar que el diseño propuesto para	Desarrollar un conjunto detallado de actividades y controles diseñados para garantizar que el	Estándar PCI PIN v3.1 – Objetivo 6	Utilizaremos la norma ISO/IEC 27001:2013 y la norma PCI PIN v3.1 - Objetivo 6 para

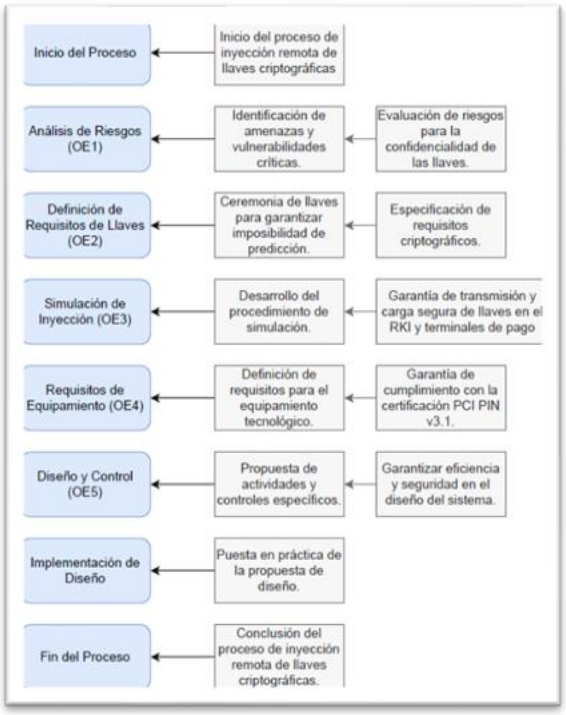
	el sistema de inyección de llaves criptográficas remota se realice de manera eficiente y segura en los terminales de pago, minimizando riesgos potenciales.	diseño del sistema de inyección de llaves criptográficas remota se implemente de manera óptima en los terminales de pago, mientras se minimizan los riesgos potenciales. Estas actividades y controles estarán enfocados en asegurar la eficiencia operativa y la seguridad integral del sistema, tanto en la transmisión y carga de llaves como en la administración general del proceso.		ayudarnos a establecer requisitos generales para la inyección segura de claves criptográficas con el fin de cumplir el objetivo.

4.3 Diagrama de bloques de la inyección remotas de llaves

En este capítulo, presentaremos un diagrama de bloques del proyecto de tesis, que permitirá obtener una comprensión clara y sencilla del proceso que abarca desde la carga o transferencia de llaves criptográficas hasta la inyección remota en los terminales de pago.

Figura 29

Diagrama de Bloques



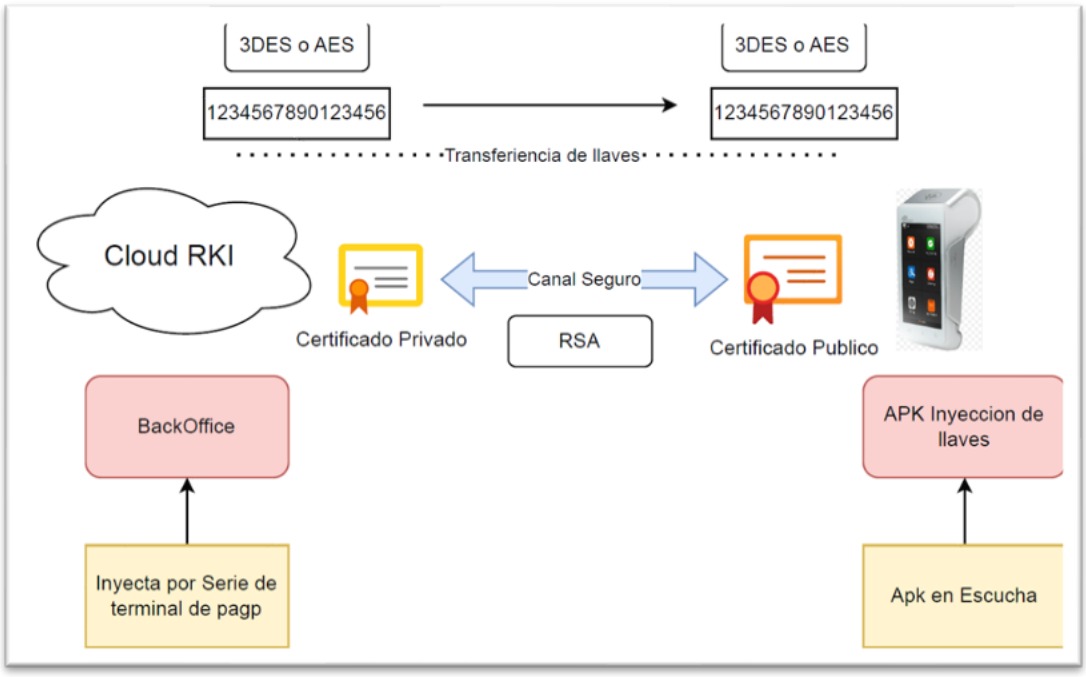
4.3.1 Arquitectura del diseño propuesto

En la propuesta de la tesis de diseño de inyección remota de llaves criptográficas en los terminales de pago, es fundamental presentar una arquitectura de ejemplo que permita una identificación más técnica de todas las partes involucradas. Esto facilitará la comprensión de lo que el diseño debe cubrir para su correcta implementación.

Además, en la presentación se incluirán algoritmos y diseños estándar, lo que resultará de gran ayuda para buscar información relevante y favorecer el proceso de implementación.

Figura 30

Arquitectura de inyección de llaves remotos



4.3.2 Matriz de Riesgo

Comenzar con una evaluación de riesgos es crucial para el diseño propuesto de inyección remota de claves en terminales de pago, porque nos proporciona una comprensión más completa de los riesgos relacionados con el procedimiento actual. De este modo podremos reconocer los riesgos superiores a lo que la empresa puede tolerar.

Actualmente, la empresa de procesamiento de pagos dispone de una macro propia que facilita la identificación y selección de varias opciones para evaluar el riesgo inherente por parte del personal de riesgos. Es imperativo recordar que los controles de seguridad que la empresa de procesamiento de pagos tiene en vigor también deben incluirse en esta evaluación de riesgos. Mientras que el área de cumplimiento se asegura de que todos los procesos del proyecto estén debidamente alineados, el área de ciberseguridad es crucial para llevar a cabo el Pentesting requerido. Para que el diseño propuesto tenga éxito y sea seguro, ambos elementos son esenciales.

Figura 31

Matriz de Riesgo

N°	ID Activo	Nombre del activo	Descripción del activo	Producto	Criticidad del Al	Amenaza	Vulnerabilidad	Evento	Consecuencia	Codigo Riesgo	Riesgo	Impacto	Probabilidad	Nivel de Riesgo
1	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Inyector de llaves remota	Alto	Ataques físicos a los terminales (por ejemplo, intentos de robo o manipulación de terminales).	Falta de medidas de seguridad física adecuadas para proteger los terminales.	El robo o extravío de terminales de pago debido a la falta de medidas de seguridad física adecuadas.	Pérdida de datos sensibles de los clientes, como información de tarjetas de crédito.	R01	Riesgo de robo o extravío de terminales de pago debido a la falta de medidas de seguridad física	Critico	Muy Baja	Medio
			Equipo que se encarga de la TRX de pago	Inyector de llaves remota	Alto	Ataques cibernéticos dirigidos a los terminales (por ejemplo, malvware o ataques de skimming).	Falta de actualizaciones de seguridad y parches en los terminales.	La explotación de vulnerabilidades en los terminales de pago debido a la falta de actualizaciones de seguridad.	Posible fraude financiero si los terminales son comprometidos por atacantes.	R02	Riesgo de explotación de vulnerabilidades en terminales de pago debido a la falta de actualizaciones de seguridad.	Critico	Baja	Alto
2	AI-002	Llaves Criptograficas	Llaves para encriptar datos sensibles	Inyector de llaves remota	Alto	Compromiso de la seguridad de las llaves criptográficas.	Acceso no autorizado a las llaves criptográficas.	El acceso no autorizado o el compromiso de las llaves criptográficas.	confidencialidad en las transacciones si las llaves son comprometidas.	R03	Riesgo de acceso no autorizado o compromiso de las llaves criptográficas.	Critico	Muy Baja	Medio
			Llaves para encriptar datos	Inyector de llaves		Fugas de información sobre las llaves	Falta de procesos seguros de generación y gestión de	La pérdida de control sobre las llaves criptográficas	Posible exposición de las llaves a terceros no autorizados si se pierde		Riesgo de pérdida de control sobre las llaves criptográficas debido a			

4.3.2.1 Inventario de activos de información

Es importante tener en cuenta que, para llevar a cabo una evaluación de riesgos en cualquier tipo de proyecto, incluyendo la tesis sobre la propuesta de diseño de inyección remota de llaves criptográficas en terminales de pago, es necesario realizar un inventario exhaustivo de activos de información. Este proceso ayudará a identificar todos los activos involucrados en la propuesta de diseño. A través de esta identificación, podremos evaluar qué activos son críticos para la empresa y brindarles un tratamiento diferenciado.

Para facilitar este proceso, las empresas procesadoras de medio de pago han desarrollado una macro propia que permite listar todos los activos informáticos con sus respectivos detalles. Mediante una serie de preguntas diseñadas para identificar el impacto y clasificación de cada activo, podremos determinar su criticidad de manera efectiva. Esta herramienta resulta fundamental para asegurar un análisis completo y preciso de los riesgos involucrados en el proyecto.

Figura 32

Plantilla de Activos de información

N°	ID Activo	Nombre del activo	Descripcion del activo	Categoria del activo	Ubicación del activo	Propietario	Tipo Operador	confidencial	Integridad	Disponibilidad	Total	Valor Criticidad
1	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Activo Fisico	Ubicacion Fisica	Gerencia General	Externo	2	3	2	7	Alto
2	AI-002	Llaves Criptograficas	Llaves para encriptar datos sensibles	Activo de Informacion	Ubicacion Fisica	Gerencia General	Interno	3	3	3	9	Alto
			Aplicativo que	Activo								

4.3.2.2 Dueño de la información

En el proyecto de diseño de inyección remota de claves criptográficas, el papel del propietario de la información es crucial. La persona u organización encargada de gestionar,

mantener a salvo y salvaguardar los datos y la información relacionados con el proyecto se conoce como propietario de la información.

Su principal deber es garantizar que los activos de información del proceso estén adecuadamente protegidos y que se sigan las normas de seguridad y privacidad establecidas. Además, el propietario de la información es responsable de asegurarse de que se toman todas las precauciones necesarias para evitar y atenuar cualquier riesgo y vulnerabilidad que pueda comprometer la confidencialidad e integridad de los datos.

Aparte de sus responsabilidades en materia de seguridad de la información, los propietarios de la información son esenciales en la toma de decisiones y el establecimiento de políticas y procedimientos específicos del proyecto. Es imprescindible que colaboren estrechamente con otros miembros del equipo, incluidos los responsables de ciberseguridad, cumplimiento y tecnología, para garantizar una alineación adecuada de los objetivos y una ejecución eficaz del diseño sugerido.

En resumen, el dueño de la información es el guardián y defensor de la integridad y seguridad de los datos en el proyecto de diseño de inyección remota de llaves criptográficas, desempeñando un papel clave para el éxito y la protección de la información sensible involucrada.

4.3.3 Sistema de RKI

En este capítulo, revisaremos el sistema RKI (Remote Key Injection) o cualquier otro sistema preparado para realizar la inyección remota de llaves criptográficas. Para garantizar la seguridad de dicho sistema, es fundamental que cuente con diversas certificaciones, entre ellas, la del estándar PCI PIN v3.1. Esta certificación asegura que el sistema proporciona una sólida protección de las llaves criptográficas.

El sistema RKI debe ser compatible con diferentes activos, y es especialmente importante que incorpore un equipo HSM (Hardware Security Module). El HSM es una herramienta diseñada específicamente para administrar las llaves criptográficas, y su uso nos permite mantener la seguridad de estas al estar actualizado con las últimas medidas de protección de las marcas, como la llave KEY BLOCK.

Para asegurar una óptima seguridad, el sistema debe utilizar algoritmos confiables, como 3DES con doble longitud y AES 256. Todo esto deberá llevarse a cabo bajo el estándar TR-31, garantizando la máxima eficacia en la gestión de las llaves criptográficas.

En el proyecto de diseño de inyección remota de llaves criptográficas, el Sistema RKI (Remote Key Injection) cumple un papel fundamental y estratégico. Este sistema es responsable de la gestión y distribución segura de las llaves criptográficas utilizadas en los terminales de pago.

Garantizar la generación, almacenamiento y transmisión segura de claves criptográficas a los terminales de pago es responsabilidad del Sistema RKI. Esto implica una meticulosa preparación y ejecución de los procedimientos de seguridad, garantizando en todo momento la autenticidad, confidencialidad e integridad de las claves.

Entre sus funciones principales, el Sistema RKI debe llevar a cabo una gestión adecuada de los roles y permisos de los usuarios autorizados para acceder a las llaves criptográficas. Además, debe mantener un registro detallado de las operaciones realizadas, lo que facilita la auditoría y el monitoreo constante del sistema.

Para garantizar una renovación regular y reforzar la seguridad del proceso de inyección, el sistema debe ser capaz de realizar actualizaciones periódicas de las claves. Además, debe ser capaz de reaccionar con rapidez y eficacia ante posibles incidentes o amenazas a la seguridad.

En resumen, el Sistema RKI es el componente clave para asegurar la seguridad y protección de las llaves criptográficas en el proyecto de diseño de inyección remota. Su correcto funcionamiento es esencial para garantizar la confianza en el proceso de transacciones electrónicas y proteger la integridad de la información en el ámbito de los pagos digitales.

Figura 33

Sistema RHINO

Nota. Adaptado en “Portal paxRhino”, por PAX, 2023 (https://www.paxtechnology.com/)

4.3.3.1 Ejecución de Pentest

El rol del Pentest (Prueba de Penetración) en el sistema RKI (Remote Key Injection) es de suma importancia para garantizar la seguridad y robustez del sistema. El Pentest es una

evaluación exhaustiva y controlada de la seguridad del sistema, que se realiza mediante simulaciones de ataques con el objetivo de identificar vulnerabilidades potenciales.

En el contexto del sistema RKI, el Pentest despliega su función clave al analizar minuciosamente todos los aspectos relacionados con la gestión, distribución y almacenamiento de las llaves criptográficas. Durante este proceso, se simulan ataques cibernéticos para detectar posibles puntos débiles, brechas de seguridad o errores en la configuración que puedan ser explotados por actores maliciosos.

El Pentest permite a los responsables del sistema RKI conocer en profundidad las fortalezas y debilidades del sistema, ofreciendo una visión integral de su resistencia a potenciales amenazas. Esto permite la identificación temprana de riesgos de seguridad y la implementación de medidas correctivas para fortalecer la protección del sistema.

Además, el Pentest también desempeña un papel relevante en la obtención de certificaciones de seguridad, como el estándar PCI PIN v3.1 mencionado anteriormente. Al someter el sistema RKI a rigurosas pruebas de penetración, se puede demostrar que cumple con los requisitos de seguridad establecidos y brinda la confianza necesaria a las partes interesadas.

En resumen, el Pentest en el sistema RKI es una actividad esencial para asegurar la confiabilidad y protección de las llaves criptográficas. Al simular ataques y evaluar la seguridad de manera controlada, se identifican vulnerabilidades y se implementan acciones preventivas para fortalecer la resistencia del sistema ante posibles amenazas cibernéticas.

4.3.3.2 Controles de Ciberseguridad

Para garantizar la integridad y la protección de las claves criptográficas y, por extensión, la seguridad de todo el proceso de inyección remota, los controles de ciberseguridad desempeñan un papel fundamental en el sistema RKI (Remote Key Injection).

Los controles de ciberseguridad son medidas y procedimientos diseñados para prevenir, detectar y responder a posibles amenazas y vulnerabilidades en el sistema RKI. Estos controles abarcan diversos aspectos, entre los cuales se incluyen:

- **Autenticación y autorización robustas:** Implementación de mecanismos sólidos para verificar la identidad de los usuarios y garantizar que solo aquellos autorizados tengan acceso a las operaciones críticas del sistema.

- **Monitoreo y registro de actividades:** Establecimiento de sistemas de monitoreo continuo para detectar actividades inusuales o sospechosas. El registro detallado de todas las operaciones realizadas permite un análisis posterior en caso de incidentes de seguridad.
- **Protección de datos y cifrado:** Utilización de técnicas de cifrado avanzadas para proteger tanto las llaves criptográficas como la información confidencial almacenada en el sistema.
- **Actualizaciones y parches:** Mantenimiento constante del sistema RKI mediante la aplicación oportuna de actualizaciones de seguridad y parches para corregir vulnerabilidades conocidas.
- **Respaldo y recuperación de datos:** Implementación de procedimientos de respaldo regulares y la capacidad de recuperar rápidamente los datos en caso de pérdida o corrupción.
- **Evaluaciones periódicas de seguridad:** Realización de auditorías y pruebas de seguridad periódicas, incluyendo pruebas de penetración (Pentest), para identificar posibles brechas y asegurar la efectividad de los controles implementados.

El conjunto de estos controles de ciberseguridad garantiza que el sistema RKI opere de manera segura y confiable, protegiendo las llaves criptográficas de accesos no autorizados o acciones maliciosas. Esto es esencial para asegurar la confianza en el proceso de inyección remota de llaves criptográficas y salvaguardar la integridad de las transacciones y datos sensibles involucrados en los terminales de pago.

4.3.4 Generación de llaves criptográficos simétricos

Una parte crucial del proyecto de diseño de la inyección remota de claves es la creación de claves criptográficas simétricas. Para garantizar la confidencialidad y la seguridad de las comunicaciones, estas claves simétricas se utilizan para cifrar y descifrar los datos entre los terminales de pago y los sistemas de gestión.

El proceso de generación de llaves criptográficas simétricas se inicia con la utilización de algoritmos de generación que producen una secuencia de bits aleatorios. Estos bits constituyen la llave simétrica única y compartida entre las partes que necesitan comunicarse de manera segura.

La generación de llaves simétricas requiere de un entorno seguro y confiable para evitar cualquier tipo de compromiso o filtración. Por tanto, se siguen rigurosos protocolos de seguridad durante todo el proceso, incluyendo la protección adecuada de las llaves generadas.

Es importante señalar que se utiliza la misma clave para cifrar y descifrar los datos debido a la naturaleza simétrica de estas claves. Esto garantiza una comunicación bidireccional eficaz y segura entre los sistemas de gestión y los terminales.

Adicionalmente, se establecen procedimientos para la renovación periódica de las llaves, lo que contribuye a reforzar la seguridad del sistema y mantener la confidencialidad a lo largo del tiempo.

En resumen, la generación de llaves criptográficas simétricas es un proceso crítico dentro del proyecto de diseño de inyección remota de llaves. A través de un proceso seguro y confiable, se garantiza la confidencialidad de las comunicaciones y la protección de la información sensible, brindando una base sólida para una implementación exitosa del sistema de inyección remota.

4.3.4.1 Flujo operativo

En este flujo, vamos a visualizar cómo se generan las llaves criptográficas simétricas utilizando algoritmos 3DES o AES, las cuales serán empleadas para la inyección remota en los terminales de pago. Es importante tener en cuenta que estas llaves o claves, una vez procesadas mediante cifrado, serán responsables de proteger la información sensible de los tarjetahabientes.

Para garantizar la seguridad de las llaves criptográficas, las empresas de procesamiento de pago siempre se basan en el estándar PCI PIN v3.1, que proporciona objetivos clave para salvaguardar dichas llaves. A continuación, se presenta el flujo de generación de llaves criptográficas:

- **Paso 1: Coordinación de los custodios de llaves criptográficas:** Se establece un equipo de custodios encargados de garantizar la seguridad y confidencialidad de las llaves criptográficas durante todo el proceso. Estos custodios colaboran para asegurar la integridad y control adecuado de las llaves.
- **Paso 2: Generación de las llaves criptográficas en un equipo HSM:** Las llaves criptográficas simétricas se generan mediante un equipo HSM (Hardware Security

Module). Este dispositivo especializado ofrece un ambiente seguro para la generación de llaves, asegurando su aleatoriedad y fortaleza.

- **Paso 3: Firma del acta de la generación de las llaves criptográficas:** Una vez que las llaves han sido generadas exitosamente, se procede a firmar un acta que certifica el proceso de generación y asegura la trazabilidad y responsabilidad en la gestión de las llaves.

Este flujo operativo garantiza la ejecución fiable y eficiente de los procedimientos de cifrado y protección de datos, así como la generación de claves criptográficas con los más altos estándares de seguridad. La puesta en marcha de estos protocolos permite lograr una inyección remota segura en los terminales de pago, al tiempo que se mantiene la privacidad de los titulares de las tarjetas y se protegen los datos sensibles.

4.3.4.2 Esquema de administración de llaves

Después de entender el flujo de la llave criptográfica, que es un componente fundamental en la propuesta de diseño de inyección remota de llaves criptográficas en terminales de pago, es importante conocer que por ejemplo una de las empresas de procesamiento de pago utiliza un equipo criptográfico certificado PCI PIN v3.1 para la generación, transporte y almacenamiento seguro de las llaves criptográficas. Este equipo es un HSM de la marca FUTUREX, que brinda altos niveles de seguridad al generar llaves de manera aleatoria con los algoritmos DES y AES.

En este equipo criptográfico, la administración de llaves se rige por el siguiente esquema:

•**Paso 1: Creación de grupos de llaves criptográficas:** Se establecen grupos de llaves criptográficas para organizar y gestionar de manera eficiente las llaves generadas.

• **Paso 2: Selección del tipo de llave criptográfica:** Dependiendo de las necesidades específicas, se elige el tipo de llave criptográfica más adecuado para cada caso, asegurando una gestión personalizada y segura.

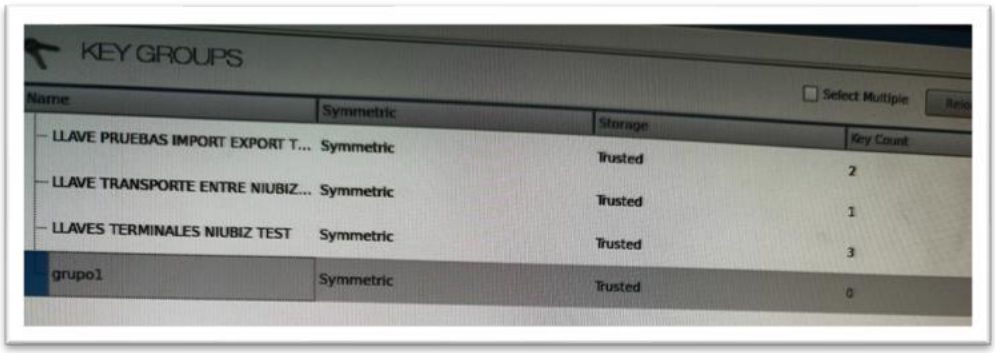
• **Paso 3: Selección del algoritmo de la llave criptográfica:** Se opta por el algoritmo más apropiado, ya sea DES o AES, según los requisitos de seguridad y complejidad requeridos.

• **Paso 4: Creación de la llave criptográfica:** Con los parámetros establecidos, se procede a generar de forma aleatoria la llave criptográfica, garantizando su fortaleza y seguridad.

El esquema de gestión de claves del equipo criptográfico FUTUREX apoya la seguridad y protección de las transacciones en los terminales de pago garantizando la disponibilidad, confidencialidad e integridad de las claves utilizadas en el diseño de inyección remota sugerido.

Figura 34

Administración de llaves FUTUREX



4.3.4.3 Monitoreo de la generación de llaves

El rol de monitoreo en la generación de llaves criptográficas es esencial dentro del proyecto de diseño de inyección remota de llaves. Esta función tiene como objetivo supervisar y garantizar la integridad, seguridad y eficacia del proceso de generación de llaves criptográficas utilizadas en los terminales de pago.

El monitoreo de la generación de llaves criptográficas involucra diversas actividades y responsabilidades clave:

- **Paso 1: Supervisión en tiempo real:** El equipo de monitoreo realiza un seguimiento constante del proceso de generación de llaves en tiempo real. Esto permite detectar de manera temprana cualquier anomalía o comportamiento inusual que pueda indicar un riesgo de seguridad o un error en la generación de llaves.
- **Paso 2: Análisis de registros:** Se analizan y revisan minuciosamente los registros y registros de actividad relacionados con la generación de llaves. Esta revisión exhaustiva ayuda a identificar patrones, tendencias o desviaciones que puedan requerir acciones correctivas.
- **Paso 3: Detección de intentos no autorizados:** El monitoreo constante permite identificar intentos de acceso no autorizado al proceso de generación de llaves o cualquier actividad sospechosa que pueda comprometer la seguridad del sistema.

- **Paso 4: Auditorías y evaluaciones periódicas:** Se realizan auditorías y evaluaciones periódicas para asegurar que el proceso de generación de llaves cumpla con las mejores prácticas de seguridad y esté en conformidad con los estándares establecidos, como el PCI PIN v3.1.
- **Paso 5: Respuesta a incidentes de seguridad:** En caso de detectar un incidente de seguridad o una posible vulnerabilidad, el equipo de monitoreo debe responder de manera oportuna y efectiva, aplicando medidas correctivas para mitigar los riesgos.
- **Paso 6: Informe y comunicación:** El equipo de monitoreo debe generar informes periódicos para comunicar los hallazgos, resultados y acciones tomadas en relación con la generación de llaves. Esta comunicación es fundamental para mantener informadas a las partes interesadas y asegurar la transparencia del proceso.

El rol de monitoreo en la generación de llaves criptográficas garantiza que el sistema de inyección remota opere de manera segura y confiable. La supervisión constante y proactiva contribuye a la prevención de incidentes de seguridad y al cumplimiento de los estándares de seguridad, brindando confianza y tranquilidad en el manejo de las llaves criptográficas y protegiendo la integridad de las transacciones en los terminales de pago.

4.3.5 Transferencia de llaves criptográficas

En este capítulo de la propuesta de diseño de inyección remota de llaves criptográficas en terminales de pago, se definirá el procedimiento de envío de llaves criptográficas a otros entornos o servicios. Todo este proceso se fundamenta en los objetivos del estándar PCI PIN v3.1, que busca salvaguardar la protección de las llaves criptográficas.

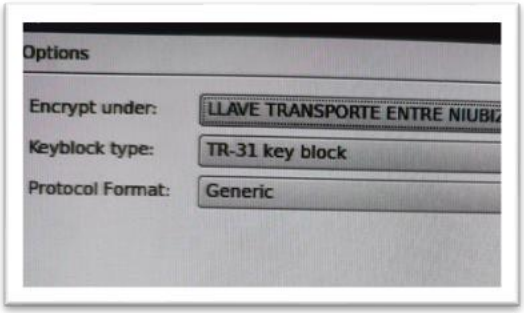
La transferencia de las llaves criptográficas se realiza entre equipos de criptografía certificados bajo PCI PIN v3.1. Esto asegura que ambos equipos empleen el mismo idioma de traslación de algoritmos, lo que resulta crucial para una comunicación eficiente y segura. Por ejemplo, una de las empresas de procesamiento de pago cuenta con el equipo criptográfico FUTUREX y otra empresa utiliza un equipo de diferente marca, ambas deben asegurarse de enviar las llaves en modo de criptograma, permitiendo que únicamente el equipo receptor pueda entender y almacenar las llaves de manera adecuada.

La transferencia de llaves es una etapa de gran importancia, ya que implica enviar las llaves que se utilizarán en la inyección remota de llaves en los terminales de pago. La seguridad y confidencialidad en este proceso son fundamentales para garantizar la integridad de las

transacciones y la protección de la información sensible en el ecosistema de pagos digitales. Por ende, el cumplimiento de los estándares PCI PIN v3.1 y la utilización de equipos criptográficos certificados son elementos cruciales para el éxito y la confianza en el sistema de inyección remota de llaves.

Figura 35

Modulo de transferencia de llaves criptográficas



4.3.5.1 Requisitos de envió de llaves

Existen requisitos específicos para el envío o transferencia de llaves criptográficas, los cuales se basan en buenas prácticas y en el estándar PCI PIN v3.1. A continuación, se detallan los pasos involucrados:

- **Paso 1: Reunión inicial con los Key manager de la otra entidad:** En esta reunión se identifican los responsables de la gestión de llaves en la otra entidad, así como la dirección de envío de las llaves.
- **Paso 2: Acceso al correo seguro de la empresa:** Se genera un acceso seguro al correo de la empresa de procesamiento de pago, permitiendo que la entidad receptora pueda recibir el criptograma de la llave final de manera protegida.
- **Paso 3: Generación y transferencia de la llave de transporte:** Se crea una llave de transporte que será enviada por medio de un servicio de Courier. La cantidad de componentes se define siguiendo las políticas de seguridad de la empresa de procesamiento de pago. La entidad receptora confirma la carga de la llave utilizando el Valor de Control de Clave (KCV).
- **Paso 4: Generación de la llave de datos o PIN:** Se genera la llave de datos o PIN que será transportada y protegida durante el proceso de transferencia.

- **Paso 5: Envío del criptograma de la llave bajo llave de transporte por correo seguro:** Se genera el archivo del criptograma utilizando el módulo de transferencia de llaves y se envía de forma segura mediante correo protegido.
- **Paso 6: Confirmación de importación de la otra entidad:** La entidad receptora importa la llave entregada a través del correo seguro y confirma su recepción utilizando el Valor de Control de Clave (KCV).

El cumplimiento de estos requisitos y pasos asegura que el proceso de envío o transferencia de las llaves criptográficas se realice de manera segura y confiable, garantizando la protección de la información sensible y la integridad de las transacciones en el sistema de inyección remota de llaves.

4.3.6 BackOffice de la inyección de llaves

El módulo de BackOffice de la inyección remota de llaves criptográficas es una parte fundamental del proyecto de diseño de inyección remota de llaves. Este módulo juega un papel crucial en la gestión y administración centralizada de las llaves criptográficas utilizadas en los terminales de pago. A continuación, se describe el módulo de BackOffice y sus principales funciones:

Descripción del módulo de BackOffice:

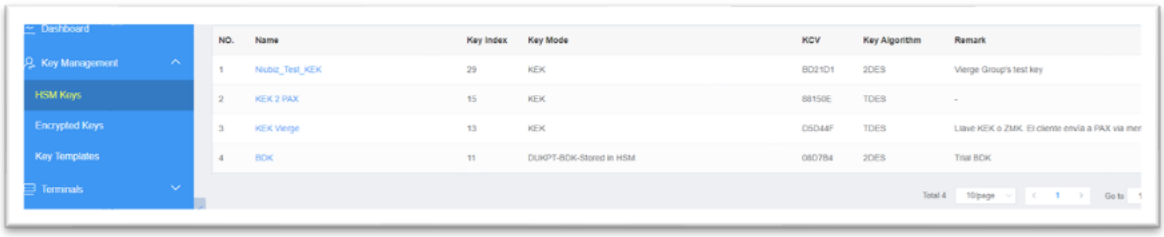
El módulo de BackOffice es una interfaz de administración basada en una plataforma segura y accesible, diseñada para gestionar de manera eficiente todas las operaciones relacionadas con las llaves criptográficas del sistema de inyección remota de llaves. Este módulo permite a los administradores y custodios de llaves supervisar y controlar de forma centralizada la generación, distribución, actualización y revocación de las llaves criptográficas.

Funciones principales:

- **Paso 1: Carga e importación de llaves de transporte:** Este módulo ofrece una interfaz sencilla y segura para llevar a cabo la carga e importación de las llaves de transporte enviadas vía Courier a los custodios de llaves. De esta manera, los custodios pueden utilizar esta funcionalidad para importar de manera eficiente las nuevas llaves que sean necesarias para el sistema.

Figura 36

Llave de transporte

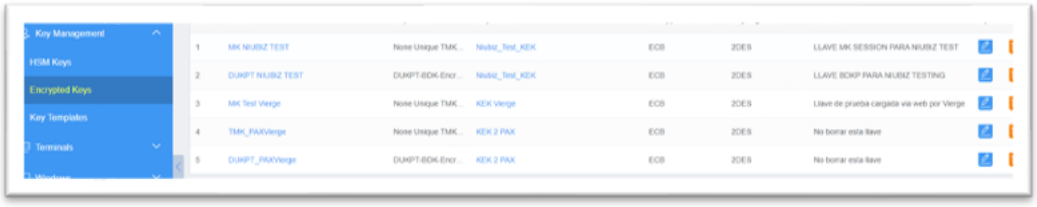


Nota. Adaptado en "Portal paxRhino", por PAX, 2023 (https://www.paxtechnology.com/)

- **Paso 2: Importación y gestión de llaves criptográficas:** El módulo de BackOffice permite importar llaves criptográficas simétricas utilizando algoritmos como 3DES o AES. Los administradores tienen la capacidad de definir parámetros de importación, para asegurar la fortaleza y seguridad de las llaves generadas.

Figura 37

Llaves importadas

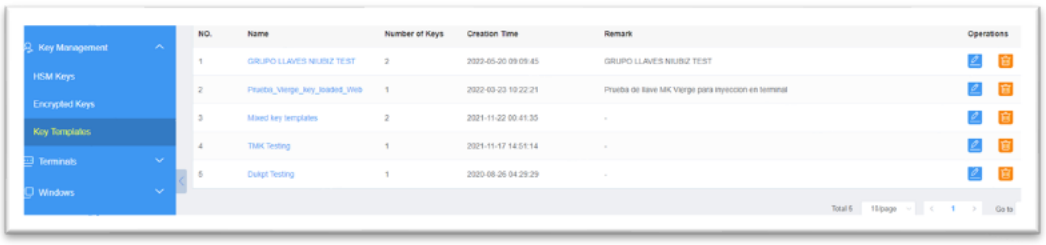


Nota. Adaptado en "Portal paxRhino", por PAX, 2023 (https://www.paxtechnology.com/)

- **Paso 3: Creación de plantilla para las llaves criptográficas:** Este módulo se emplea para la creación de grupos o plantillas de inyección, lo que nos permite agrupar las llaves criptográficas y realizar la inyección remota de todas ellas en un solo paquete.

Figura 38

Key Template



Nota.

Adaptado en "Portal paxRhino", por PAX, 2023 (https://www.paxtechnology.com/)

- **Paso 4: Distribución e inyección remota segura:** El módulo facilita la distribución segura de las llaves criptográficas a los terminales de pago a través del Sistema RKI o sistemas preparados para la inyección remota. Además, permite programar y realizar inyecciones de llaves por medio de serie de los terminales de pago.
- **Paso 5: Control de acceso y roles:** Se implementan mecanismos de control de acceso y roles que permiten asignar niveles de autorización y responsabilidad a los usuarios del BackOffice. Esto garantiza que solo personal autorizado pueda llevar a cabo operaciones críticas relacionadas con las llaves criptográficas.
- **Paso 6: Auditoría y trazabilidad:** El módulo registra y almacena de manera segura las acciones realizadas en relación con las llaves criptográficas. Esto incluye registros de generación, distribución, actualización y revocación de llaves, asegurando la trazabilidad y facilitando auditorías periódicas.
- **Paso 7: Monitoreo y alertas:** Se integra un sistema de supervisión en tiempo real para identificar cualquier evento potencial o actividad inusual relacionados con la gestión de claves. Las alertas permiten reaccionar con rapidez y eficacia ante posibles amenazas.
- **Paso 8: Generación de informes**: El módulo de BackOffice proporciona la generación de informes detallados y personalizados sobre el estado de las llaves criptográficas, actividades realizadas y estadísticas relevantes. Estos informes son valiosos para la toma de decisiones y la evaluación del rendimiento del sistema.

En resumen, el módulo de BackOffice es un componente crítico del proyecto de diseño de inyección remota de llaves criptográficas, ya que brinda una interfaz de administración segura y centralizada para gestionar las llaves criptográficas de manera eficiente y proteger la integridad de las transacciones en los terminales de pago, todo bajo el estándar PCI PIN v3.1

4.3.7 Generación y carga de certificación de autenticación

La Generación y Carga de Certificación de Autenticación en el proyecto de diseño de inyección remota de llaves criptográficas tiene como objetivo establecer un proceso seguro y confiable para la generación de certificados de autenticación utilizados en el sistema.

Descripción de la función:

- **Paso 1: Generación de certificados de autenticación:** El módulo de Generación y Carga de Certificación es responsable de la creación de certificados de autenticación

utilizando algoritmos criptográficos robustos. Estos certificados son utilizados para garantizar la identidad y autenticidad de los participantes autorizados en el proceso de inyección remota de llaves.

- **Paso 2: Asignación de claves públicas y privadas:** Durante la generación de los certificados de autenticación, se generan pares de claves públicas y privadas para cada entidad o participante autorizado. Estas claves forman parte del mecanismo criptográfico utilizado para el intercambio seguro de información y aseguran la confidencialidad de los datos transmitidos.
- **Paso 3: Firma digital y verificación:** Los certificados de autenticación son firmados digitalmente utilizando la clave privada del emisor. Esta firma digital garantiza la integridad de los certificados y su procedencia legítima. Al recibir un certificado, el sistema puede verificar la firma digital utilizando la clave pública del emisor para asegurar su autenticidad.
- **Paso 4: Carga y validación de certificados:** Una vez generados y firmados los certificados de autenticación, el módulo se encarga de cargarlos de manera segura en el sistema. Durante este proceso, se lleva a cabo una verificación de la validez de los certificados para asegurar que sean confiables y estén en vigencia. Lo mismo se realiza en el terminal de pago en cargar la clave publica ah nivel de Firmware para que no puedan cambiarlo o modificarlo
- **Paso 5: Gestión y actualización de certificados:** El módulo también se encarga de gestionar y mantener actualizados los certificados de autenticación a lo largo del tiempo. Esto incluye la renovación periódica de certificados vencidos y la revocación de certificados en caso de que se requiera por motivos de seguridad.

Importancia de la función:

La Generación y Carga de Certificación de Autenticación es esencial para garantizar la seguridad en el proceso de inyección remota de llaves criptográficas. Al emplear certificados digitales, se establece un sólido sistema de autenticación y validación de identidades, protegiendo así las comunicaciones y asegurando que solo los terminales de pago autorizados puedan participar en la inyección remota de llaves criptográficas. Esta función contribuye a salvaguardar la confidencialidad, integridad y autenticidad de las transacciones en el entorno de pagos digitales.

4.3.8 Inyección de llaves por medio de APP

La función de inyección de llaves a través de la aplicación en el proyecto de diseño de inyección remota de llaves tiene como objetivo principal permitir a los usuarios autorizados realizar de manera segura y efectiva la transferencia de llaves criptográficas desde el módulo de BackOffice hacia los terminales de pago. A continuación, se detallan los aspectos clave de esta función:

4.3.8.1 Paso 1: Interfaz de Usuario Intuitiva y Segura:

La aplicación cuenta con una interfaz de usuario intuitiva y fácil de usar, diseñada para brindar una experiencia fluida y eficiente a los usuarios. Se implementan medidas de seguridad sólidas, como la autenticación multifactor y cifrado de datos, para garantizar la protección de la información confidencial.

4.3.8.2 Paso 2: Autenticación y Autorización de Usuarios:

Antes de acceder a la función de inyección de llaves, los usuarios deben autenticarse utilizando credenciales seguras y autorizadas. Dependiendo de los roles y permisos asignados, los usuarios tendrán acceso a diferentes niveles de funcionalidad y operaciones relacionadas con la inyección de llaves.

4.3.8.3 Paso 3: Inyección de Llaves Criptográficas:

Una vez autenticado, el usuario puede activar la opción de escucha para que puedan inyectar las llaves criptográficas en los terminales de pago. La aplicación realiza verificaciones y validaciones para asegurar que las llaves estén en el slot correspondiente.

4.3.8.4 Paso 4: Transferencia Segura de Llaves:

La aplicación utiliza protocolos de comunicación seguros para transmitir las llaves seleccionadas desde el módulo de BackOffice hacia los terminales de pago habilitados para la inyección remota de llaves criptográficas. Durante el proceso de transferencia, se garantiza que las llaves viajen por un canal seguro y protegidas contra posibles ataques.

4.3.8.5 Paso 5: Registro y Auditoría de Operaciones:

Cada operación de inyección de llaves se registra detalladamente en un registro de auditoría. Estos registros proporcionan un historial completo de las acciones realizadas, lo que permite una supervisión constante y una trazabilidad precisa de las operaciones llevadas a cabo.

4.3.8.6 Paso 6: Monitoreo en Tiempo Real:

Un sistema de supervisión en tiempo real está integrado en la aplicación para identificar cualquier problema potencial o actividad inusual que pueda surgir durante el procedimiento de inyección de claves. Se activarán alertas en caso de que se detecte cualquier anomalía para permitir una actuación rápida y la reducción de riesgos.

4.3.8.7 Paso 7: Actualizaciones y Mantenimiento:

La aplicación se mantiene actualizada con las últimas medidas de seguridad y mejoras funcionales para asegurar un entorno seguro y confiable de inyección de llaves. Se realizan periódicamente actualizaciones y parches para mantener la aplicación libre de vulnerabilidades conocidas.

En conclusión, la función de inyección de llaves a través de la aplicación es esencial en el proyecto de diseño de inyección remota de llaves, ya que proporciona una forma segura y eficiente de inyectar las llaves criptográficas a los terminales de pago, garantizando la confidencialidad e integridad de las transacciones en el entorno de pagos digitales.

4.4 Procedimiento de Simulación de inyección Remota de llaves Según PCI PIN v3.1

Este procedimiento de simulación garantiza que la inyección remota de llaves criptográficas en los terminales de pago se realice de manera segura y eficiente, asegurando que los requisitos del estándar PCI PIN v3.1 se cumplan satisfactoriamente.

4.4.1 Titulo

Simulación de inyección remota de llaves criptográficas en terminales de pago

4.4.2 Objetivo del documento

Desarrollar un procedimiento de simulación para la inyección remota de llaves criptográficas en los terminales de pago de las empresas de procesamiento de pago, que permita asegurar la transmisión y carga segura de las llaves en el RKI y en los propios terminales de pago.

4.4.3 Maro normativo

Se basa en el estándar PCI PIN v3.1

4.4.4 Revisión y responsables

Seguridad de la información: Especialista en Criptografía.

4.4.5 Descripción de Procesos

En este apartado se encuentra el núcleo del documento, que presenta una secuencia lógica y ordenada de pasos a seguir, culminando en el resultado final esperado.

4.4.5.1 Paso 1: Definición de Roles y Responsabilidades

- Designa un equipo responsable de desarrollar y ejecutar el procedimiento de simulación.
- Asigna roles específicos, como el "Coordinador de Simulación", "Participantes del RKI" y "Participantes de Terminales de Pago".

Tabla 19

Roles del equipo de inyección remota

Roles	Responsable
Coordinador de simulación	Especialista de Seguridad de la información
Participantes del RKI	Proveedor que ofrecerá el servicio
Participante de Terminal de Pago	Proveedor encargado de realizar la inyección de llaves de manera remoto.

4.4.5.2 Paso 2: Configuración del Entorno de Simulación

- Prepara un entorno de prueba que simule de manera realista el proceso de inyección remota de llaves.
- Configura los equipos y sistemas necesarios, incluyendo el RKI y los terminales de pago. Por ejemplo, vamos a utilizar un entorno de prueba de PAX Rhino:

Figura 39

paxRhino

Nota. Adaptado en “Portal paxRhino”, por PAX, 2023 (https://www.paxtechnology.com/)

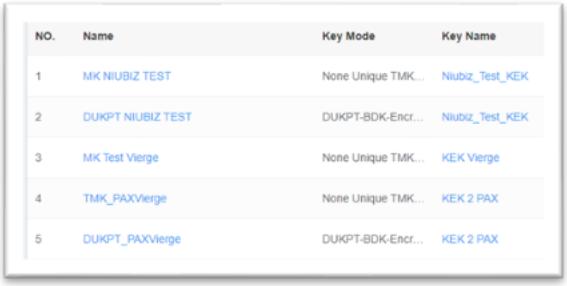
4.4.5.3 Paso 3: Generación de Llaves Criptográficas de Prueba

- Utiliza generadores aleatorios criptográficamente seguros para generar llaves criptográficas de prueba, se va a realizar la ceremonia de llaves ya visto en el capítulo anterior.
- Estas llaves se utilizarán para simular la transmisión y carga segura en el RKI y en los terminales de pago.

  Por ejemplo, se muestra llaves cargadas en el RKI:

Figura 40

Llaves Cargadas



Nota. Adaptado en "Portal paxRhino", por PAX, 2023 (https://www.paxtechnology.com/)

4.4.5.4 Paso 4: Habilitar las series de los terminales de pago para la inyección remota de llaves criptográficas

- Identificar la serie de los terminales de pago

Figura 41

Serie de terminales de pago agregados

Nota. Adaptado en "Portal paxRhino", por PAX, 2023 (https://www.paxtechnology.com/)

4.4.5.5 Paso 4: Simulación de Transmisión y Carga Segura

- Inicia el procedimiento de simulación siguiendo los pasos establecidos en el proceso real de inyección remota.

- Simula la transmisión de llaves desde el RKI a los terminales de pago, asegurando la autenticidad y confidencialidad.

4.4.5.6 Paso 5: Validación y Autenticación

- Verifica que las llaves de prueba se transmitan y carguen de manera segura y exitosa en el RKI y en los terminales de pago.
- Asegúrate de que todos los controles y medidas de seguridad se apliquen correctamente.

4.4.5.7 Paso 6: Pruebas de Integración

- Realiza pruebas de integración para confirmar que las llaves criptográficas de prueba se utilizan adecuadamente en los terminales de pago, en esta prueba se utiliza el KCV de cada llave.

4.4.5.8 Paso 7: Evaluación de Resultados y Ajustes

- Evalúa los resultados de la simulación y compara con los objetivos establecidos.
- Realiza ajustes y mejoras en el procedimiento según los hallazgos y las recomendaciones.

4.4.5.9 Paso 8: Aplicar los resultados de la inyección remota de llaves

- Documenta todos los detalles de la simulación, incluyendo los pasos, los resultados, las observaciones y las mejoras realizadas, por ejemplo, vamos a demostrar cómo se inyecto de manera exitosa la llave en un terminal Android de la marca PAX.

Figura 42

Keys en Terminal Info

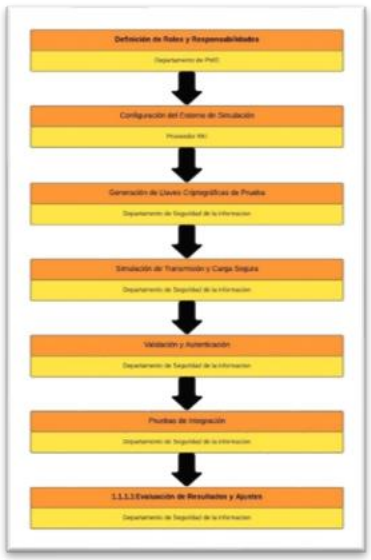
Figura 43

Listado de llaves vía aplicación

4.4.6 Diagrama de flujo y responsables

Figura 44

Diagrama de Flujo y responsables



4.5 Definir requisitos tecnológicos para el equipamiento criptográfica

Este enfoque garantiza que el equipamiento tecnológico informático utilizado en la inyección remota de llaves cumpla con los requisitos de certificación PCI PIN v3.1, garantizando la seguridad y cumplimiento de los estándares en todo momento.

4.5.1 Paso 1: Revisión del Estándar PCI PIN V3.1

Eche un vistazo a la norma PCI PIN v3.1 para conocer las especificaciones precisas de la tecnología utilizada en la inyección remota de claves criptográficas. Hay que prestar especial atención al objetivo 7, que dice que "Los equipos utilizados para procesar PIN y claves deben manejarse de forma segura."

Figura 45

Estándar PCI PIN

4.5.2 Paso 2: Identificación de Requisitos Técnicos:

Identifica los requisitos técnicos establecidos en el estándar que se relacionan con el equipamiento tecnológico informático utilizado en la inyección remota de llaves, se debe descargar el Datasheet de cada modelo.

Figura 46

Datasheet de PAX A910

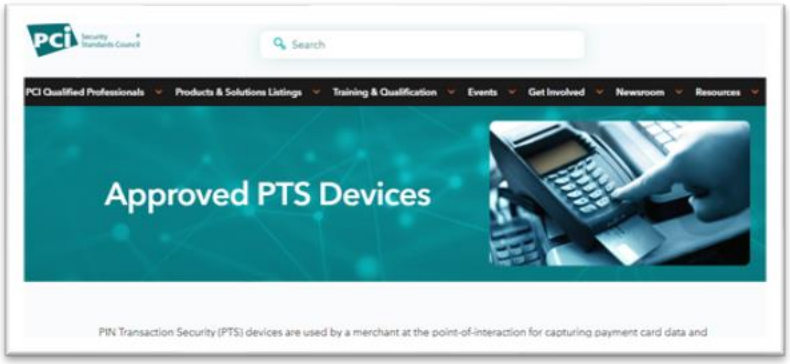
Nota. Adaptado en "A910 Android", por PAX, 2023 (https://www.paxtechnology.com/a910)

4.5.3 Paso 3: Evaluación del Equipamiento Existente

Realiza una evaluación exhaustiva del equipamiento tecnológico informático actual utilizado en la inyección remota de llaves criptográficas, y se debe verificar en la página de COUNCIL que el equipo criptográfico utilizado en el diseño de inyección de llaves remota debe contar con PCI PTS, ya que eso nos asegura que el equipo paso por diferentes laboratorios de pruebas.

Figura 47

Certificación PTS



Nota. Adaptado en "PTS Device", por Council, 2023 (https://listings.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true)

4.5.4 Paso 4: Verificación y Pruebas

Realiza pruebas exhaustivas para asegurarte de que el equipamiento cumple con los estándares, podemos verificar en el número de probación la información que cumple el equipo criptográfico.

Figura 48

Approbal Number

Nota. Adaptado en "PTS Device", por Council, 2023 https://listings.pcisecuritystandards.org/popups/pts_device.php?appnum=4-70047

4.5.5 Paso 5: Auditoría y Validación

Sujeta el equipamiento actualizado a una auditoría externa para validar su cumplimiento con los requisitos del estándar PCI PIN v3.1, la empresa procesadora de medio de pago por el tema de negocio tiene que pasar la certificación de manera obligatoria cada 2 años.

Figura 49

Certificación PCI PIN

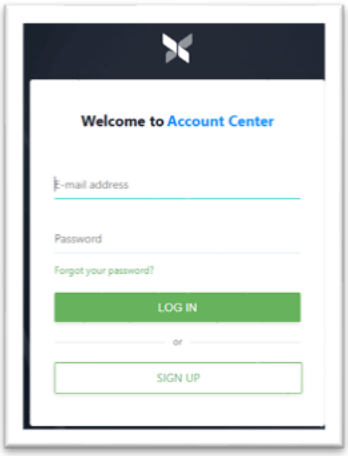
Nota. Adaptado en "Centro de ayuda", por Niubiz, 2023 (https://www.niubiz.com.pe/centro-de-ayuda/niubiz-en-linea/)

4.5.6 Paso 6: Mantenimiento Continuo

Establece un plan de mantenimiento continuo para asegurarte de que el equipamiento mantenga su cumplimiento a lo largo del tiempo, en este parte nos apoyamos con la fábrica de la misma marca para que nos brinde soporte u algunas actualizaciones de los equipos hasta su fin de vida. Por ejemplo, el TMS de la marca PAX donde hay nuevas actualizaciones:

Figura 50

TMS de fabrica PAX



Nota. Adaptado en "whatspos", por PAX, 2023 (https://auth.whatspos.com/passport/login?client_id=account&market=www)

4.6 Proponer actividades de Diseño eficiente y seguro

Al seguir estos pasos, podrás proponer actividades y controles efectivos que aseguren que el diseño del sistema de inyección de llaves criptográficas remota se realice de manera eficiente y segura en los terminales de pago, minimizando los riesgos potenciales y cumpliendo con los requisitos del estándar PCI PIN v3.1.

4.6.1 Paso 1: Estudio del Estándar PCI PIN V3.1

Familiarízate con los requisitos y recomendaciones establecidos en el estándar PCI PIN v3.1 para garantizar la seguridad en la inyección remota de llaves.

4.6.2 Paso 2: Análisis de Riesgos (OE1)

Realizar un análisis detallado de los riesgos asociados a la actividad de inyección remota de llaves, identificando amenazas y vulnerabilidades críticas que puedan comprometer la confidencialidad de las llaves.

4.6.3 Paso 3: Definición de Requisitos de Llaves Criptográficas (OE2)

Establecer los requisitos precisos para las llaves criptográficas necesarias en los terminales de pago, a través de un proceso de "ceremonia de llaves" que garantice su completa imposibilidad de predicción.

4.6.4 Paso 4: Desarrollo de Procedimiento de Simulación (OE3)

Crear un procedimiento de simulación para la inyección remota de llaves criptográficas en terminales de pago. Asegurar la transmisión y carga segura de las llaves en el RKI y en los propios terminales de pago.

4.6.5 Paso 5: Certificación de Equipamiento Tecnológico (OE4):

Definir los requisitos esenciales para que el equipamiento tecnológico informático utilizado en la inyección remota de llaves cumpla con la certificación PCI PIN v3.1.

4.6.6 Paso 6: Documentación Detallada

Documenta todas las actividades y controles propuestos en detalle.

Incluye instrucciones claras sobre cómo implementar y mantener cada control.

4.6.7 Paso 7: Mejora Continua

Utiliza los resultados de las auditorías y la simulación para mejorar las actividades y controles propuestos.

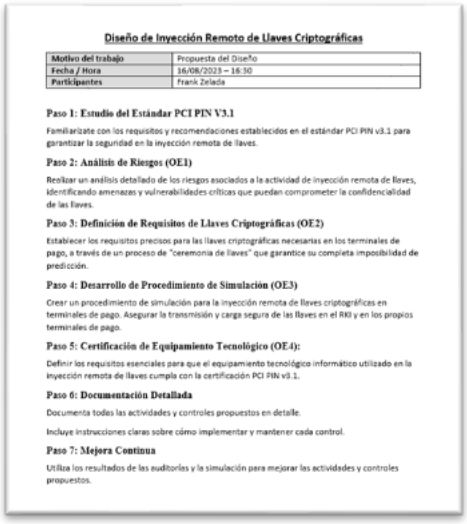
Mantén una mentalidad de mejora continua para adaptarte a nuevos riesgos y tecnologías

4.6.8 Aplicando la eficiencia de inyección remota de llaves

Asegúrate de que comprendan su importancia y cómo aplicarlos correctamente.

Figura 51

Inyección remota de llaves



Diseño de Inyección Remoto de Llaves Criptográficas

Motivo del trabajo	Propuesta del Diseño
Fecha / Hora	16/08/2023 – 16:30
Participantes	Frank Zelada

Paso 1: Estudio del Estándar PCI PIN V3.1

Familiarizate con los requisitos y recomendaciones establecidos en el estándar PCI PIN v3.1 para garantizar la seguridad en la inyección remota de llaves.

Paso 2: Análisis de Riesgos (OE1)

Realizar un análisis detallado de los riesgos asociados a la actividad de inyección remota de lloves, identificando amenazas y vulnerabilidades críticas que puedan comprometer la confidencialidad de las llaves.

Paso 3: Definición de Requisitos de Llaves Criptográficas (OE2)

Establecer los requisitos precisos para las llaves criptográficas necesarias en los terminales de pago, a través de un proceso de "ceremonia de llaves" que garantice su completa imposibilidad de predicción.

Paso 4: Desarrollo de Procedimiento de Simulación (OE3)

Crear un procedimiento de simulación para la inyección remota de lleves criptográficas en terminales de pago. Asegurar la transmisión y carga segura de las lleves en el RKI y en los propios terminales de pago.

Paso 5: Certificación de Equipamiento Tecnológico (OE4):

Definir los requisitos esenciales para que el equipamiento tecnológico informático utilizado en la inyección remota de llaves cumpla con la certificación PCI PIN v3.1.

Paso 6: Documentación Detallada

Documenta todas las actividades y controles propuestos en detalle.

Incluye instrucciones claras sobre cómo implementar y mantener cada control.

Paso 7: Mejora Continua

Utiliza los resultados de las auditorías y la simulación para mejorar las actividades y controles propuestos.

5 CAPÍTULO 5: RESULTADO Y VALIDACIONES

5.1 Alcance

En este capítulo, llevaremos a cabo la elaboración de un plan de pruebas para cada objetivo específico que se estableció al inicio del proyecto. A continuación, se verificarán los resultados obtenidos para demostrar que las métricas propuestas son coherentes con los objetivos planteados.

Se definirán planes de pruebas detallados para cada objetivo identificado en la fase inicial del proyecto. Estos planes se enfocarán en evaluar la funcionalidad, seguridad, rendimiento y usabilidad del sistema, asegurando que cada objetivo se cumpla de manera efectiva y confiable.

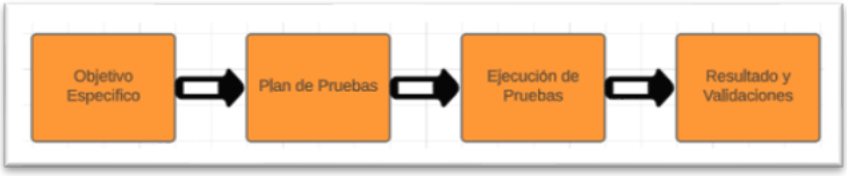
En resumen, el plan de pruebas y la verificación de resultados son etapas cruciales en el proceso de desarrollo del proyecto de diseño de inyección remota de llaves criptográficas en terminales de pago. Mediante una evaluación exhaustiva, demostraremos que los objetivos planteados se han alcanzado exitosamente, proporcionando una sólida base para el éxito del proyecto en su conjunto.

5.2 Fases para las pruebas y validaciones de la propuesta de diseño

Se ha elaborado un minucioso flujo de tareas para cada uno de los objetivos específicos del proyecto con el fin de cumplir esas metas y evaluar las métricas y los indicadores de logro que se han sugerido.

Figura 52

Flujos de pruebas



Para confirmar y validar que se llevan a cabo las actividades desarrolladas en el proyecto, como se muestra en la figura anterior, se tendrán en cuenta los procesos enumerados en cada objetivo específico.

5.3 Esquematización del Proceso para los Objetivos Específicos definidos

Este proceso tiene como finalidad validar y demostrar los objetivos específicos propuestos. Para lograrlo, se emplearon varios métodos de validación, tales como la aplicación de una metodología de riesgo, la presentación de actas de resultados, la realización de pruebas de simulación, la verificación de páginas certificadas y la integración del proceso de diseño.

5.3.1 Verificación de OE 1

La siguiente tabla enumera el OE 1 junto con su métrica asociada y el indicador de logro:

Tabla 20

OE 1

OE1	Indicador del Logro	Métrica
Realizar un análisis de riesgos para la actividad de inyección de llaves, la cual forma parte del área de seguridad de la información, con el objetivo de identificar las amenazas y vulnerabilidades críticas que podrían comprometer la confidencialidad de las llaves.	-Matriz de Riesgos. -Informe de análisis de riesgos.	-Número de riesgos con criticidad Alta.

5.3.1.1 Plan de Pruebas

Como se ha tratado en el Capítulo 3, es crucial tener en cuenta el análisis y la evaluación de los riesgos de los activos de información en relación con el diseño de la inyección remota de claves criptográficas durante esta fase.

Para garantizar la ejecución eficaz del plan anteriormente delineado, se ha elaborado una matriz de pruebas para el objetivo actual y otra que identifica los riesgos primordiales susceptibles de evolucionar en incidencias durante la utilización del servicio de inyección remota de llaves criptográficas en los terminales de pago.

En el contexto de este proyecto de investigación, utilizaremos la siguiente matriz como herramienta de validación para el objetivo específico que estamos estudiando:

Tabla 21

Matriz de Pruebas OE1

Objetivo especifico	Realizar un análisis de riesgos para la actividad de inyección de llaves, la cual forma parte del área de seguridad de la información, con el objetivo de identificar las amenazas y vulnerabilidades críticas que podrían comprometer la confidencialidad de las llaves.
Método de validación	Método de validación serán las encuestas de modo online.
Recursos Humanos	• Head de Criptografía • Especialista de Criptografía • Especialista de riesgos tecnológicos.
Actividades para Desarrollar	1. Recopilación para finalizar encuestas de valoración de activos de información. 2. Recopilar la información del análisis de riesgos realizado y utilizarla para valorar los activos de información teniendo en cuenta la disponibilidad, la confidencialidad y la integridad. 3. Para determinar el riesgo, enumere los eventos, las vulnerabilidades, las amenazas y las consecuencias correspondientes. 4. Elaborar cuestionarios de evaluación de riesgos que se agruparán en función de un umbral predeterminado.

Herramientas utilizadas	Ofimática Forms
Fecha de Prueba	01/05/2023
Tiempo de Prueba	30 días

5.3.1.2 Ejecución

Las siguientes personas se mencionan específicamente en el Plan de Pruebas actual:

- 1 especialista de criptografía
- 1 head de criptografía
- 1 especialista de riesgos tecnológicos

Actividad 1. Recopilación para finalizar encuestas de valoración de activos de información

Se realiza encuestas con la herramienta forms de manera online a las personas que esta involucradas en el mundo de tecnología de información.

Figura 53

Encuestas

Actividad 2. Recopilar la información del análisis de riesgos realizado y utilizarla para valorar los activos de información teniendo en cuenta la disponibilidad, la confidencialidad y la integridad.

En esta fase, se incorpora lo abordado la actividad 1, que comprende la evaluación de los activos de información en relación con la propuesta de diseño de inyección remota de llaves

criptográficas. Es importante tener en cuenta que estos elementos están susceptibles a riesgos que podrían desencadenar incidencias.

Figura 54

Activo de información

N°	ID Activo	Nombre del activo	Descripcion del activo	Categoria del activo	Ubicación del activo	Propietario	Tipo Operador	Confidencialidad	Integridad	Disponibilidad	Total	Valor Criticidad
1	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Activo Fisico	Ubicacion Fisica	Gerencia General	Externo	3	2	3	8	Alto
2	AI-002	Llaves Criptograficas	Llaves para encriptar datos sensibles	Activo de Informacion	Ubicacion Fisica	Gerencia General	Interno	2	3	3	8	Alto
3	AI-003	Aplicativo de Inyeccion de llaves	Aplicativo que recibira las llaves criptograficas	Activo de Software	Ubicacion Fisica	Gerencia General	Externo	1	2	1	4	Medio
4	AI-004	Sistema de inyeccion de llaves (RKI)	inyectara las llaves de manera remota	Activo de Servicios	Ubicacion Virtual	Gerencia General	Externo	3	2	3	8	Alto

Actividad 3. Para determinar el riesgo, enumere los eventos, las vulnerabilidades, las amenazas y las consecuencias correspondientes.

En esta etapa, el riesgo ha sido identificado las amenazas y vulnerabilidades de los activos de información declarados en el capítulo 3.

Figura 55

Identificar el riesgo

Amenaza	Vulnerabilidad	Evento	Consecuencia
Ataques cibernéticos dirigidos a los terminales de pago.	Falta de actualizaciones de seguridad y parches en los terminales.	La explotación de vulnerabilidades en los terminales de pago debido a la falta de actualizaciones de seguridad.	Posible fraude financiero si los terminales son comprometidos por atacantes.

Actividad 4. Elaborar cuestionarios de evaluación de riesgos que se agruparán en función de un umbral predeterminado.

Fue posible determinar el valor de riesgo global y, posteriormente, el nivel de riesgo de los activos de información conectados al diseño de inyección remota de claves sugerido, asignando un nivel de riesgo alto basado en la encuesta y la identificación en la actividad 3.

Figura 56

Encuestas de Evaluación de riesgo

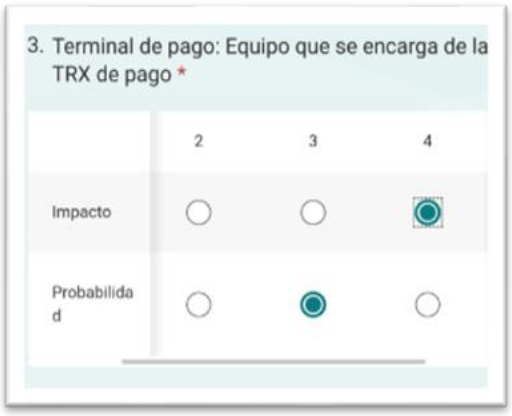


Figura 57

Evaluación del riesgo

Codigo Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Desrcipcion del Riesgo
R20	4	3	Alto	Ataques cibernéticos dirigidos a los terminales de pago debido a la falta de actualizaciones de seguridad y parches en los sistemas, lo que podría resultar en posibles incidentes de fraude financiero si los atacantes logran comprometer los terminales.

5.3.1.3 Resultados y validaciones

Como resultado, de la cantidad de riesgos identificados según el **Anexo V**, se observa un total de 8 riesgos, de los cuales 7 se han clasificado como "Medio" y solo 1 se cataloga como "Alto". Esto nos da un porcentaje del **13%,** lo que sugiere la necesidad de llevar a cabo un tratamiento de riesgo.

Tabla 22

Porcentaje de Riesgos

Numeración	Nivel de Riesgo	Porcentaje
7	Medio	87%
1	Alto	13%

5.3.1.4 Plan de Mejora

En este proyecto de tesis, no se contempla la implementación de un sistema de inyección de llaves remoto, ya que se centra exclusivamente en la propuesta de diseño. Sin embargo, se recomienda considerar luego de la implementación utilizar la metodología propuesta y llevar

a cabo un tratamiento de riesgo para reducir los riesgos a los niveles aceptables para las empresas procesadoras de medios de pagos.

5.3.2 Verificación de OE 2

La siguiente tabla enumera el OE 2 junto con su métrica asociada y el indicador de logro:

Tabla 23

OE 2

OE2	Indicador del Logro	Métrica
Definir los requisitos de las llaves criptográficas necesarias para los terminales de pago de las empresas procesadoras de medios de pago, mediante un proceso de "ceremonia de llaves" que garantice su absoluta imposibilidad de predicción.	-Acta de generación de llaves criptográficas.	-Cantidad de actas generadas para llaves criptográficas en terminales de pago.

5.3.2.1 Plan de Pruebas

En esta fase, es esencial tener en cuenta los requisitos de la ceremonia de llaves relacionados con el diseño de la inyección remota de llaves criptográficas, tal como se detalla en el capítulo 3. Este capítulo proporciona todas las directrices necesarias, conforme al estándar PCI PIN v3.1.

Cuando surge la necesidad de generar una nueva llave criptográfica para la inyección remota en un terminal de pago, es crucial que este proceso se realice de manera eficiente y con la máxima seguridad, dado que se trata de información altamente sensible.

Para garantizar que se sigue el plan establecido, se creará una matriz de objetivos y un registro de la ceremonia clave, que se describen en el Apéndice X. Los custodios de la empresa de procesamiento de pago respaldan plenamente esta documentación.

La siguiente matriz se utilizará en el contexto de este proyecto de investigación como herramienta de validación para el objetivo concreto que nos ocupa:

Tabla 24

Matriz de Pruebas OE2

Objetivo especifico	Definir los requisitos de las llaves criptográficas necesarias para los terminales de pago de las empresas procesadoras de medios de pago, mediante un proceso de "ceremonia de llaves" que garantice su absoluta imposibilidad de predicción.
Método de validación	El método de validación a utilizar es checklist online.
Recursos Humanos	• Head de Criptografía • Especialista de Criptografía • Custodios de llaves criptográficas
Actividades para Desarrollar	1. Verificar los requisitos de la generación de llaves en la ceremonia de llaves. 2. Validar el acta de conformidad 3. Reunión para el completado del checklist de las tareas realizadas.
Herramientas utilizadas	Ofimática Inyector Futurex
Fecha de Prueba	01/06/2023
Tiempo de Prueba	7 días

5.3.2.2 Ejecución

Las siguientes personas se mencionan específicamente en el Plan de Pruebas actual:

- 1 especialista de criptografía
- 1 head de criptografía
- 3 custodios de llaves de tres gerencias distintas

Actividad 1. Verificar los requisitos de la generación de llaves en la ceremonia de llaves.

En esta actividad se tendrá una revisión de los pasos necesarios para la generación de una llave criptográfica, la ceremonia de llaves inicia de la siguiente forma:

Paso 1: Coordinación con custodios

En esta etapa, procederemos a seleccionar a tres custodios que participarán en la ceremonia de llaves, dado que la llave se dividirá en tres componentes. El maestro de ceremonias

indicará la fecha y el motivo de su participación. Puede consultar el **Anexo VII** para conocer el formato del correo de invitación.

A continuación, se presentará una tabla que ilustra la composición de los custodios de la ceremonia de llaves.

Tabla 25

Custodios

Custodio	Nombre	Gerencia
Custodio A Principal	María Rodríguez	Gerencia de Recursos Humanos
Custodio A Backup	Carlos Martínez	Gerencia de Marketing
Custodio A Backup	Laura Gómez	Gerencia de Finanzas
Custodio B Principal	Javier López	Gerencia de Operaciones
Custodio B Backup	Ana Herrera	Gerencia de Desarrollo de Producto
Custodio B Backup	Alberto Sánchez	Gerencia de Ventas
Custodio C Principal	Claudia Vargas	Gerencia de Riesgos
Custodio C Backup	Juan Pérez	Gerencia de Tecnología de la Información
Custodio C Backup	Elena Ramírez	Gerencia de Desarrollo de Negocios

Paso 2. Generación de llaves criptográficas

En esta fase, el maestro de ceremonias procede a preparar el equipo criptográfico, el cual debe contar con la certificación PCI PIN para garantizar su imposibilidad de predicción. Posteriormente, se encarga de generar de manera aleatoria la llave 3DES de doble longitud, asignándole el nombre de "LLAVE DATOS REMOTA" y solo nos muestra el KCV Final que es el siguiente **2EF697**.

Se ingresa con doble factor de autenticación:

Figura 58

Login futurex

Se crea un grupo donde se almacenara la llave:

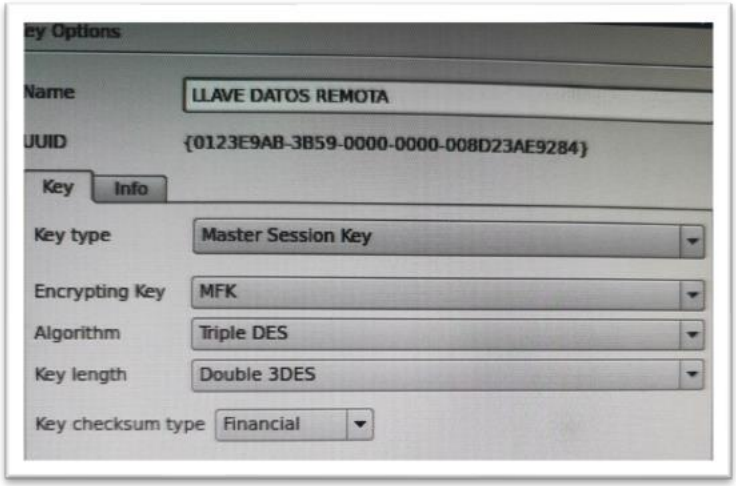
Figura 59

Creación grupo FUTUREX

Se crea la llave de datos:

Figura 60

Llave creada de manera aleatoria



Paso 3. Registro de las llaves criptográficas

Después de generar la llave en la actividad 2, el maestro de ceremonias procede a exportarla en tres componentes. A continuación, los custodios copian los valores correspondientes de la llave 3DES de doble longitud en un formato de registro que será resguardado en la caja fuerte de la empresa. Este formato requiere la inclusión de los 32 valores hexadecimales, junto con el KCV del componente. Puede consultar la estructura de la llave en la tabla que se presenta a continuación.

Se exporta las llaves en 3 componentes:

Figura 61

Exportación de componentes FUTUREX

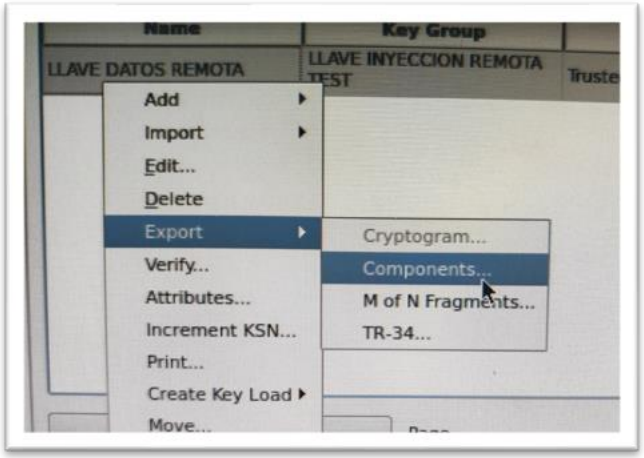


Tabla 26

Llave criptográfica

Llave Componente 1	**KCV Componente**
D0E05ACA4A4B6FD91579B8DA9098C7E6	7746EE
Llave Componente 2	**KCV Componente**
C681E4FF55AF995BB5D94FC57734B3ED	6CD1E7
Llave Componente 3	**KCV Componente**
BB9C226D4B24CE6B9FA743F16E146A6F	081E92

Paso 4. Verificación de las llaves criptográficas

Después, los custodios deben verificar que el componente copiado en el formato, al ser combinado, resulte en la llave final o combinada. Esta verificación se lleva a cabo ingresando las llaves en un equipo criptográfico o módulo especializado para la generación de llaves. Cada llave se introduce en el módulo y, al final del proceso, debe generarse la llave combinada. Este procedimiento garantiza que la llave copiada en el formato sea la correcta. Para una visualización detallada del proceso de generación de la llave, se proporciona información en el **Anexo IX**.

Actividad 2. Validar el acta de conformidad

Al concluir la actividad 1, se observa que el KCV Final es 2EF697, lo cual coincide con el valor obtenido durante la generación de llaves. Con esta validación, se procede a documentar la ceremonia de llaves en una bitácora específica, así como a elaborar un acta de generación de llaves que llevará la firma de cada custodio. El acta correspondiente se encuentra detallada en el **Anexo X** para su referencia.

Actividad 3. Reunión para el completado del checklist delas tareas a realizarse.

Se realiza una reunión con el head de criptografía para que realice un checklist de los puntos realizados para que se verifique que todo está conforme.

Figura 62

Checklist de generación de llaves criptográficas

5.3.2.3 Resultados y validaciones

Después de llevar a cabo las actividades de generación de las llaves criptográficas y la validación que todo está conforme en el checklist, se evidencia el éxito a través de la firma

del acta correspondiente. Esta firma valida que los custodios están satisfechos con el proceso y la validación de la llave, el cual se ha llevado a cabo de acuerdo con las buenas prácticas de seguridad de la información, siguiendo el estándar PCI PIN.

Además, se ha confirmado que el proceso de ceremonia de llaves garantiza su absoluta imposibilidad de predicción, gracias al uso de equipos criptográficos certificados y a la división de la llave en tres componentes.

Tabla 27

Cantidad Actas Generadas

Acta Generada	Cantidad de Acta
Acta de Generación de llaves	1

5.3.2.4 Plan de Mejora

En este proyecto de tesis, no se contempla la implementación de un sistema de inyección de llaves remoto, ya que se centra exclusivamente en la propuesta de diseño. Sin embargo, se recomienda considerar luego de la implementación realizar los pasos de los requisitos de la generación de llaves para que validen que se cumple con los controles indicados en el estándar PCI PIN v3.1

5.3.3 Verificación de OE 3

La siguiente tabla enumera el OE 3 junto con su métrica asociada y el indicador de logro:

Tabla 28

OE 3

OE3	Indicador del Logro	Métrica
Desarrollar un procedimiento de simulación para la inyección remota de llaves criptográficas en los terminales de pago de las empresas procesadoras de medios de pago, que permita asegurar la transmisión y carga segura de las llaves en el RKI y en los propios terminales de pago.	-Procedimiento de simulación de inyección de llaves criptográficas.	-Cantidad de llaves criptográficas inyectadas en el terminal de pago.

5.3.3.1 Plan de Pruebas

A continuación, analizaremos el proceso de simulación creado en el capítulo 4 para la inyección remota de claves criptográficas en terminales de pago.

Se generará una matriz de prueba y una muestra de las claves inyectadas en el terminal de pago para garantizar el cumplimiento del plan predeterminado. Esto permitirá a las empresas de procesamiento de pagos confirmar que la clave inyectada es legítima.

En el contexto de este proyecto de investigación se utilizará la siguiente matriz como herramienta de validación para el objetivo concreto que nos ocupa:

Tabla 29

Matriz de pruebas OE3

Objetivo especifico	Desarrollar un procedimiento de simulación para la inyección remota de llaves criptográficas en los terminales de pago de las empresas procesadoras de medios de pago, que permita asegurar la transmisión y carga segura de las llaves en el RKI y en los propios terminales de pago.
Método de validación	El método de validación a utilizar es checklist online.
Recursos Humanos	• Head de Criptografía • Especialista de Criptografía
Actividades para Desarrollar	1. Verificar el procedimiento de simulación. 2. Validar las llaves inyectadas en el terminal de pago 3. Reunión para el completado del checklist de las tareas realizadas.
Herramientas utilizadas	-Terminal de pago -Herramientas Office -PoC RKI
Fecha de Prueba	09/06/23
Tiempo de Prueba	15 días

5.3.3.2 Ejecución

Las siguientes personas se mencionan específicamente en el Plan de Pruebas actual:

- 1 especialista de criptografía

- 1 head de criptografía

Actividad 1. Verificar el procedimiento de simulación.

En esta actividad, disponemos del procedimiento detallado en el capítulo 4, el cual presenta paso a paso cómo se realiza la inyección remota de una llave en un terminal de pago con sistema operativo Android utilizando un sistema RKI. A partir de esta información, se procederá a confirmar que las llaves serán inyectadas de manera remota. Para obtener una representación visual de la Prueba de Concepto (PoC), se puede consultar la imagen en el **Anexo XI.**

Actividad 2. Validar las llaves inyectadas en el terminal de pago

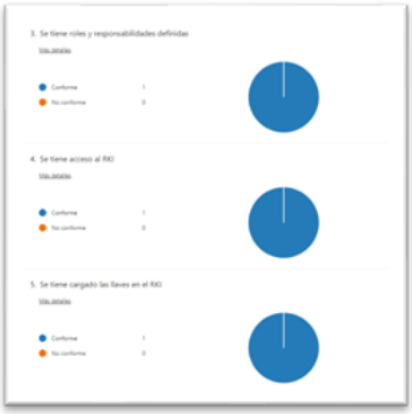
En esta actividad de validación de las llaves criptográficas inyectadas de manera remota, procederemos a validar únicamente dos llaves destinadas al cifrado del PAN y PIN de un tarjetahabiente. Utilizando estos datos, verificaremos con el KCV que han sido inyectadas correctamente en un terminal de pago. Los resultados de esta validación se encuentran ilustrados en una imagen del **Anexo XII.**

Actividad 3. Reunión para el completado del checklist de las tareas realizadas.

Se realiza una reunión con el head de criptografía para que realice un checklist de los puntos realizados para que se verifique que todo está conforme.

Figura 63

Checklist de simulación RKI



5.3.3.3 Resultados y validaciones

Como resultado de la validación del checklist, se confirma que dos llaves con algoritmo 3DES, una con esquema para PIN en BDK y la otra para PAN en MK, fueron transmitidas

y cargadas de manera segura en el terminal de pago. Esta validación respalda la seguridad de la vía de transmisión, la cual se ampara en el uso de certificados de autenticación, así como en el almacenamiento de las llaves en Slots dentro de la memoria segura.

Tabla 30

Llaves inyectadas

Tipos de llaves	Uso	Cantidad de llaves
BDK	PIN	1
MK	PAN	1

5.3.3.4 Pan de mejora

En este proyecto de tesis, no se contempla la implementación de un sistema de inyección de llaves remoto, ya que se centra exclusivamente en la propuesta de diseño. Sin embargo, se recomienda considerar luego de la implementación realizar el procedimiento de simulación de inyección remota de llaves en terminales de pago para que validen que se cumple con los controles indicados en el estándar PCI PIN v3.1.

5.3.4 Verificación de OE 4

La siguiente tabla enumera el OE 4 junto con su métrica asociada y el indicador de logro:

Tabla 31

OE 4

OE4	Indicador del Logro	Métrica
Definir los requisitos técnicos del equipamiento tecnológico informático utilizado en la inyección remota de llaves criptográficas con el fin de cumplir con la certificación PCI PIN v3.1.	-Documentación de certificación PCI PIN de los equipos criptográficos.	-% de equipos criptográficos Certificados.

5.3.4.1 Plan de Pruebas

A continuación, se considerarán los requisitos detallados en el capítulo 4 de esta tesis, el cual aborda los aspectos técnicos que un equipo debe cumplir para obtener la certificación PCI PIN v3.1. Esto permitirá que, en el caso de necesitar un nuevo equipo para formar parte de la propuesta de diseño de inyección remota de llaves, se pueda utilizar estos requisitos como guía para asegurar una integración eficiente.

Para lograr este propósito, se generará una matriz de pruebas específica para este objetivo, junto con una muestra de certificaciones del Council que indican cuando un equipo criptográfico cumple con los requisitos técnicos necesarios.

Tabla 32

Matriz de pruebas OE4

Objetivo especifico	Definir los requisitos técnicos del equipamiento tecnológico informático utilizado en la inyección remota de llaves criptográficas con el fin de cumplir con la certificación PCI PIN v3.1.
Método de validación	El método de validación a utilizar es checklist presencial.
Recursos Humanos	• Head de Criptografía • Especialista de Criptografía • Head de soluciones físicas • Analista e soluciones físicas
Actividades para Desarrollar	1. Verificar los requisitos técnicos de los equipos criptográficos. 2. Validar la certificación de los equipos criptográficos. 3. Reunión para el completado del checklist de las tareas realizadas.
Herramientas utilizadas	-Página Web -Datasheet -TMS
Fecha de Prueba	01/07/23
Tiempo de Prueba	7 días

5.3.4.2 Ejecución

Las siguientes personas se mencionan específicamente en el Plan de Pruebas actual:

- 1 especialista de criptografía
- 1 head de criptografía
- 1 especialista de soluciones físicas
- 1 analista de soluciones físicas

Actividad 1. Verificar los requisitos técnicos de los equipos criptográficos.

En esta actividad, disponemos de todos los requisitos necesarios para verificar que un equipo cuenta con la certificación PCI PIN. Estos requisitos están detallados en el capítulo 4. A continuación, se procederá a seleccionar un equipo de la marca PAX y se verificará posteriormente su inscripción en la página del Council, puede ver el detalle de la página en el **Anexo XIII.**

Actividad 2. Validar la certificación de los equipos criptográficos.

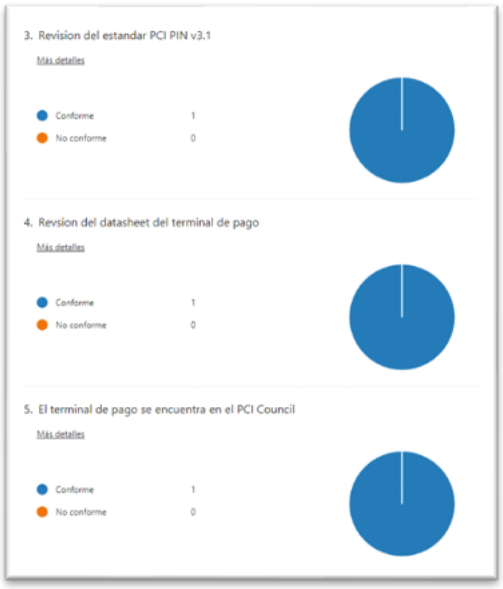
Después de verificar los requisitos en la actividad 1, se selecciona el terminal de pago A910 y se confirma en la página que su certificación está vigente hasta el año 2030. Con esta verificación, se determina que puede estar en el mercado para las empresas de procesamiento de pago y ser utilizado en la inyección remota de llaves, puede verificar el equipo en cumplimiento en el **Anexo XIV**.

Actividad 3. Reunión para el completado del checklist de las tareas realizadas.

Se realiza una reunión con el head de criptografía para que realice un checklist de los puntos realizados para que se verifique que todo está conforme.

Figura 64

Checklist de requisitos de terminal de pago



5.3.4.3 Resultados y validaciones

Con esta validación y el checklist realizado, podemos concluir que el porcentaje de los equipos criptográficos utilizados en la propuesta de diseño de inyección de llaves, en nuestro

caso el inyector y el terminal de pago, alcanza el 100%. Esto se debe a que a nivel de todas las marcas de medios de pago es imperativo utilizar equipos que cumplan con los requisitos necesarios para llevar a cabo la inyección de llaves, ya sea de forma remota o presencial.

Tabla 33

Equipos PCI PTS

Equipos Criptográficos	Certificación	validación
Futurex SKI	PCI PTS v 3.x	100%
PAX A910	PCI PTS v 6.x	100%

5.3.4.4 Plan de mejora

En este proyecto de tesis, no se contempla la implementación de un sistema de inyección de llaves remoto, ya que se centra exclusivamente en la propuesta de diseño. Sin embargo, se recomienda considerar luego de la implementación realizar la definición de los requisitos e técnicos de un equipo criptográfico para que validen que se cumple con los controles indicados en el estándar PCI PIN v3.1.

5.3.5 Verificación de OE 5

La siguiente tabla enumera el OE 5 junto con su métrica asociada y el indicador de logro:

Tabla 34

OE 5

OE5	Indicador del Logro	Métrica
Proponer actividades y controles específicos para asegurar que el diseño propuesto para el sistema de inyección de llaves criptográficas remota se realice de manera eficiente y segura en los terminales de pago, minimizando riesgos potenciales.	-Propuesta del diseño	-Versiones de propuesta

5.3.5.1 Plan de Pruebas

Posteriormente, la propuesta de diseño esbozada en el capítulo 4 recopila todos los objetivos particulares necesarios para completar la inyección remota de llaves. Esto asegura que todas

las actividades y controles necesarios para llevar a cabo la propuesta estén representados en una lista única y fácil de entender para el diseño.

Para lograr este objetivo, se creará una matriz de pruebas particular para este objetivo:

Tabla 35

Matriz de pruebas OE5

Objetivo especifico	Proponer actividades y controles específicos para asegurar que el diseño propuesto para el sistema de inyección de llaves criptográficas remota se realice de manera eficiente y segura en los terminales de pago, minimizando riesgos potenciales.
Método de validación	El método de validación a utilizar es checklist presencial
Recursos Humanos	• Head de Criptografía • Especialista de Criptografía
Actividades para Desarrollar	1. Verificar la propuesta de diseño. 2. Reunión para el completado del checklist de las tareas realizadas.
Herramientas utilizadas	Ofimática
Fecha de Prueba	15/07/23
Tiempo de Prueba	15 días

5.3.5.2 Ejecución

Las siguientes personas se mencionan específicamente en el Plan de Pruebas actual:

- 1 especialista de criptografía
- 1 head de criptografía

Actividad 1. Verificar la propuesta de diseño.

En esta actividad, se llevará a cabo la verificación de la propuesta presentada en el capítulo 4. Esta propuesta consiste en un listado ordenado de todos los objetivos específicos indicados en el diseño. Este proceso nos permitirá obtener una visión general de todos los puntos necesarios. Si alguno de estos puntos estuviera ausente o no se cumpliera según lo

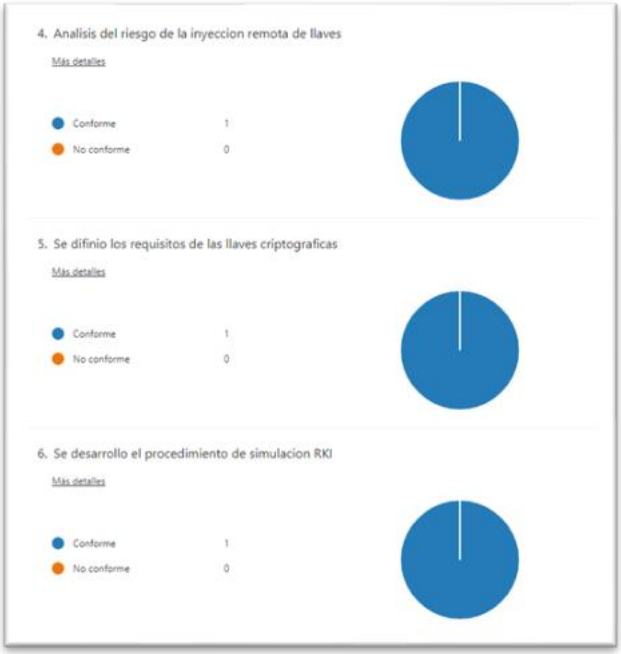
establecido, la futura implementación podría no satisfacer los requisitos de certificación PCI PIN v3.1, se puede ver el listado en el **Anexo XV.**

Actividad 2. Reunión para el completado del checklist de las tareas realizadas.

Se realiza una reunión con el head de criptografía para que realice un checklist de los puntos realizados para que se verifique que todo está conforme.

Figura 65

Checklist de actividades y controles de la inyección remota de llaves



5.3.5.3 Resultados y validaciones

Con este objetivo, con el completado del checklist llegamos a la conclusión de que todos los procesos, requisitos o simulaciones de implementación detallados en el presente proyecto deben ser registrados y documentados. Estos registros deben formar parte de la política interna de la empresa de procesamiento de pago. Esto permitirá llevar a cabo el mantenimiento adecuado y actualizar los documentos según sea necesario. En este caso, estamos ante la versión inicial del documento, designada como "Versión 1".

5.3.5.4 Plan de mejora

En este proyecto de tesis, no se contempla la implementación de un sistema de inyección de llaves remoto, ya que se centra exclusivamente en la propuesta de diseño.

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

El proyecto de tesis plantea la posibilidad de inyectar claves a distancia en terminales de pago. Se garantiza una inyección segura en estos dispositivos implementando correctamente el estándar PCI PIN v3.1.

Se destaca la importancia de llevar a cabo un análisis de riesgos para identificar posibles amenazas a los activos de información que componen la propuesta de diseño. Esta medida proactiva permite abordar los riesgos antes de que se conviertan en incidencias potenciales.

La adherencia a los requisitos de la ceremonia de llaves se revela como un factor crucial para la generación segura de las llaves criptográficas. Esto garantiza que las llaves sean producidas de manera segura y que su predicción sea imposible.

La simulación de la inyección remota de llaves proporciona un detallado análisis de cada etapa del proceso, incluyendo la utilización del Remote Key Injection (RKI) y todas sus implicaciones. Es importante destacar que todas las transmisiones son seguras gracias a la utilización de certificados de autenticación, cuya integridad es respaldada por el proveedor RKI, que debe cumplir con todas las certificaciones exigidas por las marcas.

Además, se enfatiza en que todo equipo criptográfico que participe en la propuesta de diseño debe contar con la certificación PCI PIN. Esto asegura que el equipo ha superado rigurosas pruebas de vulnerabilidad y está apto para la carga de las llaves criptográficas. Es esencial garantizar que estos equipos cumplan con las versiones de hardware y software especificadas por el Council.

Por último, se subraya la necesidad de alinear todos los puntos planteados en los objetivos específicos dentro de una política interna. Esto permitirá que cada empresa procesadora de medios de pago realice el mantenimiento correspondiente después de cada implementación, asegurando así que la inyección remota de llaves se mantenga en conformidad con la certificación PCI PIN v3.1.

6.2 Recomendaciones

Se sugiere implementar la propuesta de diseño en todas las empresas de procesamiento de pago. Esto facilitaría el aseguramiento y la distribución de llaves criptográficas de manera remota, sin necesidad de depender de un proveedor especializado. En lugar de ello, se podría llevar a cabo en el mismo lugar de operación del comercio. Esta práctica sería sumamente

beneficiosa en caso de una eventual vulneración de la llave, al permitir su despliegue de manera rápida y eficaz en múltiples ubicaciones.

Además, contribuiría significativamente a la eficiencia en la puesta en producción de terminales de pago. La inyección remota de llaves podría llevarse a cabo de forma masiva en el sitio de almacenamiento, evitando la necesidad de depender de un cuarto seguro. Este enfoque también reduciría los costos asociados al servicio de inyección, al centralizar las operaciones a través de un RKI.

La implementación generalizada de esta propuesta representa una mejora sustancial en la seguridad y la operatividad de los sistemas de inyección de llaves criptográficas en el ámbito de los pagos electrónicos.

Se recomienda llevar a cabo un análisis de riesgos exhaustivo, identificando y evaluando todas las posibles amenazas y vulnerabilidades que podrían comprometer la confidencialidad de las llaves criptográficas. Es importante involucrar a expertos en seguridad de la información y utilizar metodologías reconocidas para este tipo de evaluación. Además, se sugiere mantener un registro actualizado de los riesgos identificados y las medidas de mitigación propuestas.

Se aconseja establecer un proceso de "ceremonia de llaves" riguroso y bien documentado. Esto garantizará que las llaves criptográficas generadas sean completamente impredecibles y seguras. Es esencial involucrar a personal capacitado en criptografía y seguridad para llevar a cabo este proceso. Se sugiere mantener registros detallados de cada ceremonia de llaves realizada.

Se recomienda crear un procedimiento de simulación detallado que abarque cada paso de la inyección remota de llaves. Este procedimiento debe incluir pruebas de transmisión y carga segura de las llaves en el RKI y en los terminales de pago. Es importante realizar pruebas exhaustivas en un entorno controlado antes de la implementación en producción. Se sugiere documentar los resultados de las pruebas y realizar ajustes según sea necesario.

Es esencial establecer requisitos claros para el equipamiento tecnológico que se utilizará en la inyección remota de llaves. Esto incluye hardware y software específicos que deben cumplir con la certificación PCI PIN v3.1. Se recomienda mantener una lista actualizada de los equipos certificados y verificar regularmente su estado de certificación.

Se aconseja proporcionar una lista detallada de actividades y controles específicos para garantizar la eficiencia y seguridad del diseño propuesto. Esto puede incluir procedimientos operativos estándar, listas de verificación y medidas de seguridad adicionales. Es importante involucrar a los operadores y personal de seguridad en la revisión y ejecución de estos controles.

Al seguir estas recomendaciones específicas para cada objetivo, se fortalecerá la propuesta de diseño y se asegurará una implementación exitosa y segura del sistema de inyección de llaves criptográficas remota en terminales de pago.

7 GLOSARIO Y SIGLARIO

PCI: Payment Card Industry

PIN: NÚMERO DE IDENTIFICACIÓN PERSONAL

POS: Terminal de pago

RKI: Sistema de inyección remota

CEREMONIA DE LLAVES: Proceso de generación de llaves

PTS: Seguridad de las transacciones con PIN

3DES: Algoritmo de encriptación de Triple Data Encryption Standard

AES: Algoritmo de encriptación de Advanced Encryption Standard

SSC: Security Standards Council

8 REFERENCIAS

Acosta, D. (2023, 25 de enero). *¿Qué es PCI PIN?*. PCI Hispano. Recuperado el 1 de agosto de 2023, de https://www.pcihispano.com/que-es-pci-pin/

Acosta, D. (2022, 14 de diciembre). *La guía definitiva de bloques de claves criptográficas (Key Blocks)*. PCI Hispano. Recuperado el 15 de septiembre de 2023, de https://www.pcihispano.com/la-guia-definitiva-de-bloques-de-claves-criptograficas-key-blocks/

Council (2023, 17 de agosto). *Approved PTS Devices*. Pci security standards. Recuperado el 17 de agosto de 2023, de https://listings.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true

Departamento consultoría (2023, 28 de setiembre). *¿Qué es el modelo COSO?*. GlobalSuite. Recuperado el 15 de octubre de 2023, de https://www.globalsuitesolutions.com/es/que-es-modelo-coso

Duarte, B. (2018, 31 de marzo). *Criptografía: ¿Qué son calve pública y privada? Aprende a diferenciarlo*. Bitcoin. Recuperado el 20 de julio de 2023, de https://bitcoin.es/noticias/criptografia-que-son-la-clave-publica-y-la-clave-privada-aprende-a-diferenciarlas/

GlobalSuite Solutions (2023, 19 de octubre). *ISO 31000: La norma que te ayuda a gestionar los riesgos*. GlobalSuite. Recuperado el 20 de octubre de 2023, de https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-31000-y-para-que-sirve

Information Quality (2023, 25 de setiembre). *SI el PIN*. IQCOL. Recuperado el 25 de setiembre de 2023, de https://iqcol.com/servicios-4/

ISO (2023, 27 de octubre). *Gestión del riesgo*. ISO 31000:2018. Recuperado el 27 de octubre de 2023, de https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Niubiz (2023, 11 de agosto). *Materiales de descarga*. Niubiz en línea. Recuperado el 11 de agosto de 2023, de https://www.niubiz.com.pe/centro-de-ayuda/niubiz-en-linea/

PAX (2023, 10 de octubre). *ALL PAX Terminals*. Paxtechnology. Recuperado el 10 de octubre de 2023, de https://www.paxtechnology.com/

Transcend (2023, 17 de agosto). *Encriptación AES.* Transcend-info. Recuperado el 17 de agosto de 2023, de https://ec.transcend-info.com/embedded/technology/aes-encryption

Sorensen, E. (2022, 11 de agosto). *La historia del datáfono: nacimiento y evolución de los lectores de tarjetas.* Mobile Transaction. Recuperado el 18 de setiembre de 2023, de https://es.mobiletransaction.org/historia-del-datafono/#:~:text=Las%20primeras%20terminales%20de%20pago,utiliz%C3%B3%20esta%20medida%20de%20seguridad.

Square Terminal (2023, 25 de setiembre). *Olvídate de tu anticuado y costoso lector de tarjetas de crédito.* Squareup. Recuperado el 25 de setiembre de 2023, de https://squareup.com/us/es/hardware/terminal

WordPress (2023, 26 de agosto). *Criptografía*. SEGURIDADENREDESGJA. Recuperado el 26 de agosto de 2023, de https://seguridadenredesgjsa.wordpress.com/criptografia/

9 ANEXOS

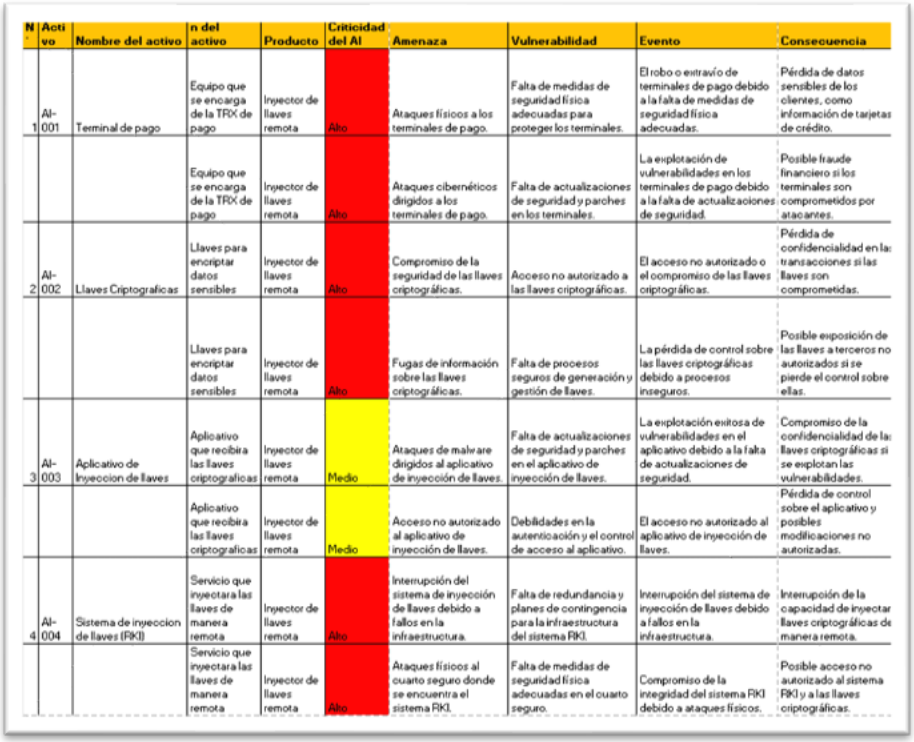
Anexo I: Inventario de activo de información

N°	ID Activo	Nombre del activo	Descripcion del activo	Categoria del activo	Ubicación del activo	Propietario	Tipo Operador	Confidencialidad	Integridad	Disponibilidad	Total	Valor Criticidad
1	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Activo Fisico	Ubicacion Fisica	Gerencia General	Externo	2	3	2	7	Alto
2	AI-002	Llaves Criptograficas	Llaves para encriptar datos sensibles	Activo de Informacion	Ubicacion Fisica	Gerencia General	Interno	3	3	3	9	Alto
3	AI-003	Aplicativo de Inyeccion de llaves	Aplicativo que recibira las llaves criptograficas	Activo de Software	Ubicacion Fisica	Gerencia General	Externo	2	2	2	6	Medio
4	AI-004	Sistema de inyeccion de llaves (RKI)	Servicio que inyectara las llaves de manera remota	Activo de Servicios	Ubicacion Virtual	Gerencia General	Externo	2	3	2	7	Alto

Anexo II: Identificación de amenazas y vulnerabilidades

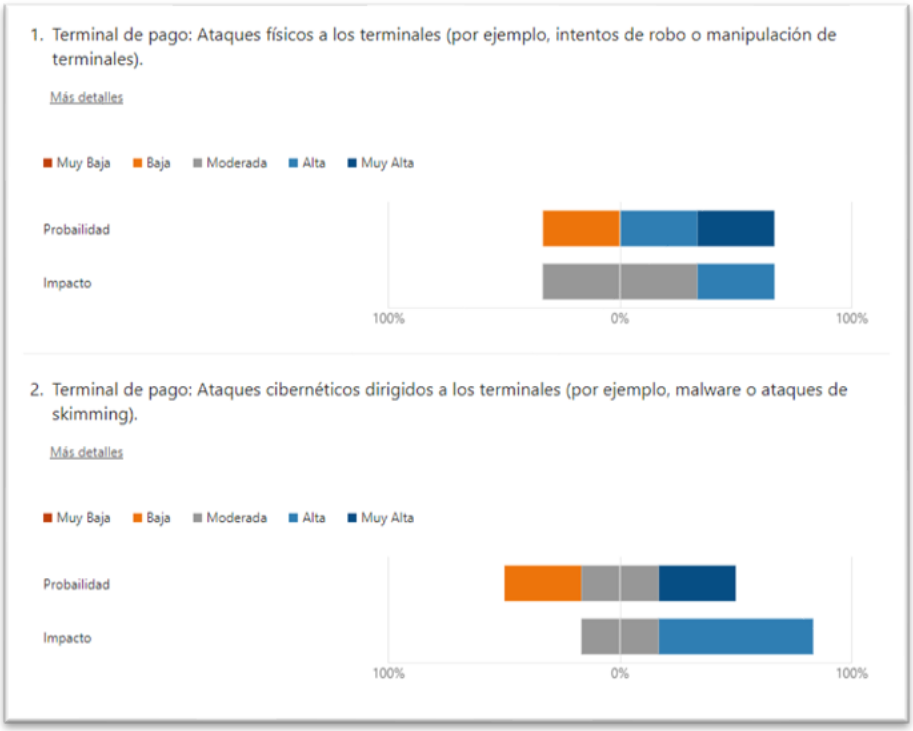
N°	ID Activo	Nombre del activo	Descripcion del activo	Producto	Criticidad del AI	Amenazas	Descripcion de la amenaza	Descripción de la vulnerabilidad
1	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Inyector de llaves remota	Alto	Humanas	Ataques físicos a los terminales (por ejemplo, intentos de robo o manipulación de terminales).	Falta de medidas de seguridad física adecuadas para proteger los terminales.
			Equipo que se encarga de la TRX de pago	Inyector de llaves remota	Alto	Tecnologicas	Ataques cibernéticos dirigidos a los terminales (por ejemplo, malware o ataques de skimming).	Falta de actualizaciones de seguridad y parches en los terminales.
2	AI-002	Llaves Criptograficas	Llaves para encriptar datos sensibles	Inyector de llaves remota	Alto	Tecnologicas	Compromiso de la seguridad de las llaves criptográficas.	Acceso no autorizado a las llaves criptográficas.
			Llaves para encriptar datos sensibles	Inyector de llaves remota	Alto	Humanas	Fugas de información sobre las llaves criptográficas.	Falta de procesos seguros de generación y gestión de llaves.
3	AI-003	Aplicativo de Inyeccion de llaves	Aplicativo que recibira las llaves criptograficas	Inyector de llaves remota	Medio	Tecnologicas	Ataques de malware dirigidos al aplicativo de inyección de llaves.	Falta de actualizaciones de seguridad y parches en el aplicativo de inyección de llaves.
			Aplicativo que recibira las llaves criptograficas	Inyector de llaves remota	Medio	Tecnologicas	Acceso no autorizado al aplicativo de inyección de llaves.	Debilidades en la autenticación y el control de acceso al aplicativo.
4	AI-004	Sistema de inyeccion de llaves (RKI)	inyectara las llaves de manera remota	Inyector de llaves remota	Alto	Tecnologicas	Interrupción del sistema de inyección de llaves debido a fallos en la infraestructura.	Falta de redundancia y planes de contingencia para la infraestructura del sistema RKI.
			inyectara las llaves de manera remota	Inyector de llaves remota	Alto	Tecnologicas	Ataques físicos al cuarto seguro donde se encuentra el sistema RKI.	Falta de medidas de seguridad física adecuadas en el cuarto seguro.

Anexo III: Análisis de Riesgo



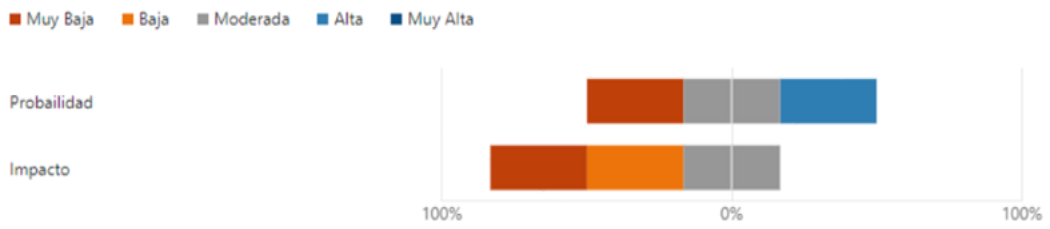
N°	Activo	Nombre del activo	n del activo	Producto	Criticidad del Al	Amenaza	Vulnerabilidad	Evento	Consecuencia
1	Al-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Inyector de llaves remota	Alto	Ataques físicos a los terminales de pago.	Falta de medidas de seguridad física adecuadas para proteger los terminales.	El robo o extravío de terminales de pago debido a la falta de medidas de seguridad física adecuadas.	Pérdida de datos sensibles de los clientes, como información de tarjetas de crédito.
			Equipo que se encarga de la TRX de pago	Inyector de llaves remota	Alto	Ataques cibernéticos dirigidos a los terminales de pago.	Falta de actualizaciones de seguridad y parches en los terminales.	La explotación de vulnerabilidades en los terminales de pago debido a la falta de actualizaciones de seguridad.	Posible fraude financiero si los terminales son comprometidos por atacantes.
2	Al-002	Llaves Criptograficas	Llaves para encriptar datos sensibles	Inyector de llaves remota	Alto	Compromiso de la seguridad de las llaves criptográficas.	Acceso no autorizado a las llaves criptográficas.	El acceso no autorizado o el compromiso de las llaves criptográficas.	Pérdida de confidencialidad en las transacciones si las llaves son comprometidas.
			Llaves para encriptar datos sensibles	Inyector de llaves remota	Alto	Fugas de información sobre las llaves criptográficas.	Falta de procesos seguros de generación y gestión de llaves.	La pérdida de control sobre las llaves criptográficas debido a procesos inseguros.	Posible exposición de las llaves a terceros no autorizados si se pierde el control sobre ellas.
3	Al-003	Aplicativo de Inyeccion de llaves	Aplicativo que recibira las llaves criptograficas	Inyector de llaves remota	Medio	Ataques de malware dirigidos al aplicativo de inyección de llaves.	Falta de actualizaciones de seguridad y parches en el aplicativo de inyección de llaves.	La explotación exitosa de vulnerabilidades en el aplicativo debido a la falta de actualizaciones de seguridad.	Compromiso de la confidencialidad de las llaves criptográficas si se explotan las vulnerabilidades.
			Aplicativo que recibira las llaves criptograficas	Inyector de llaves remota	Medio	Acceso no autorizado al aplicativo de inyección de llaves.	Debilidades en la autenticación y el control de acceso al aplicativo.	El acceso no autorizado al aplicativo de inyección de llaves.	Pérdida de control sobre el aplicativo y posibles modificaciones no autorizadas.
4	Al-004	Sistema de inyeccion de llaves (RKI)	Servicio que inyectara las llaves de manera remota	Inyector de llaves remota	Alto	Interrupción del sistema de inyección de llaves debido a fallos en la infraestructura.	Falta de redundancia y planes de contingencia para la infraestructura del sistema RKI.	Interrupción del sistema de inyección de llaves debido a fallos en la infraestructura.	Interrupción de la capacidad de inyectar llaves criptográficas de manera remota.
			Servicio que inyectara las llaves de manera remota	Inyector de llaves remota	Alto	Ataques físicos al cuarto seguro donde se encuentra el sistema RKI.	Falta de medidas de seguridad física adecuadas en el cuarto seguro.	Compromiso de la integridad del sistema RKI debido a ataques físicos.	Posible acceso no autorizado al sistema RKI y a las llaves criptográficas.

Anexo IV: Encuestas realizada para evaluación de riesgo



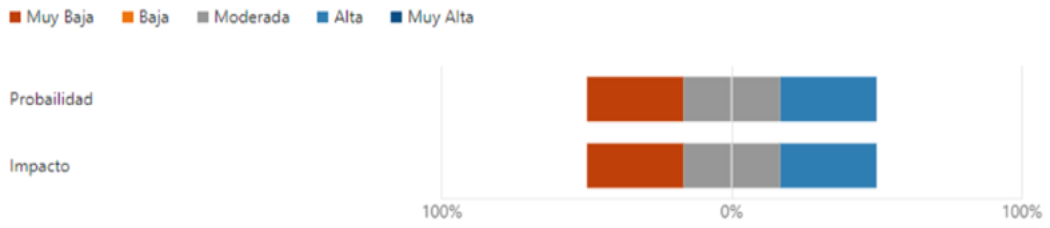
3. Llaves Criptograficas: Compromiso de la seguridad de las llaves criptográficas.

Más detalles



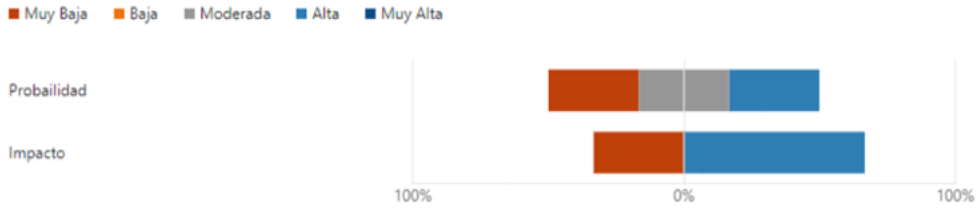
4. Llaves Criptograficas: Fugas de información sobre las llaves criptográficas.

Más detalles



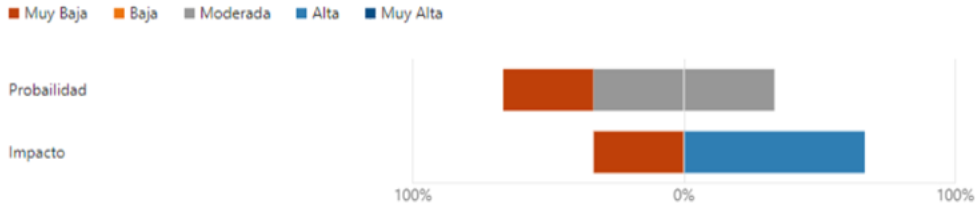
5. Aplicativo de inyeccion de llaves: Ataques de malware dirigidos al aplicativo de inyección de llaves.

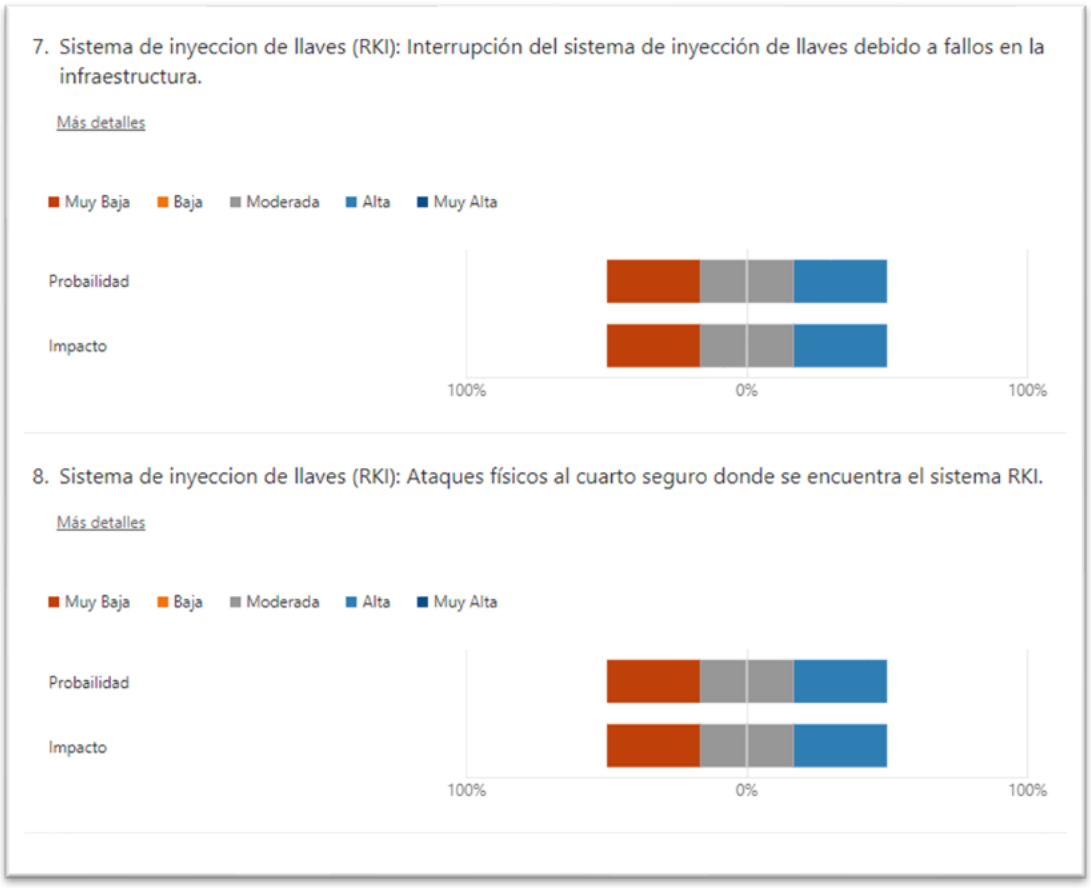
Más detalles



6. Aplicativo de inyeccion de llaves: Acceso no autorizado al aplicativo de inyección de llaves.

Más detalles





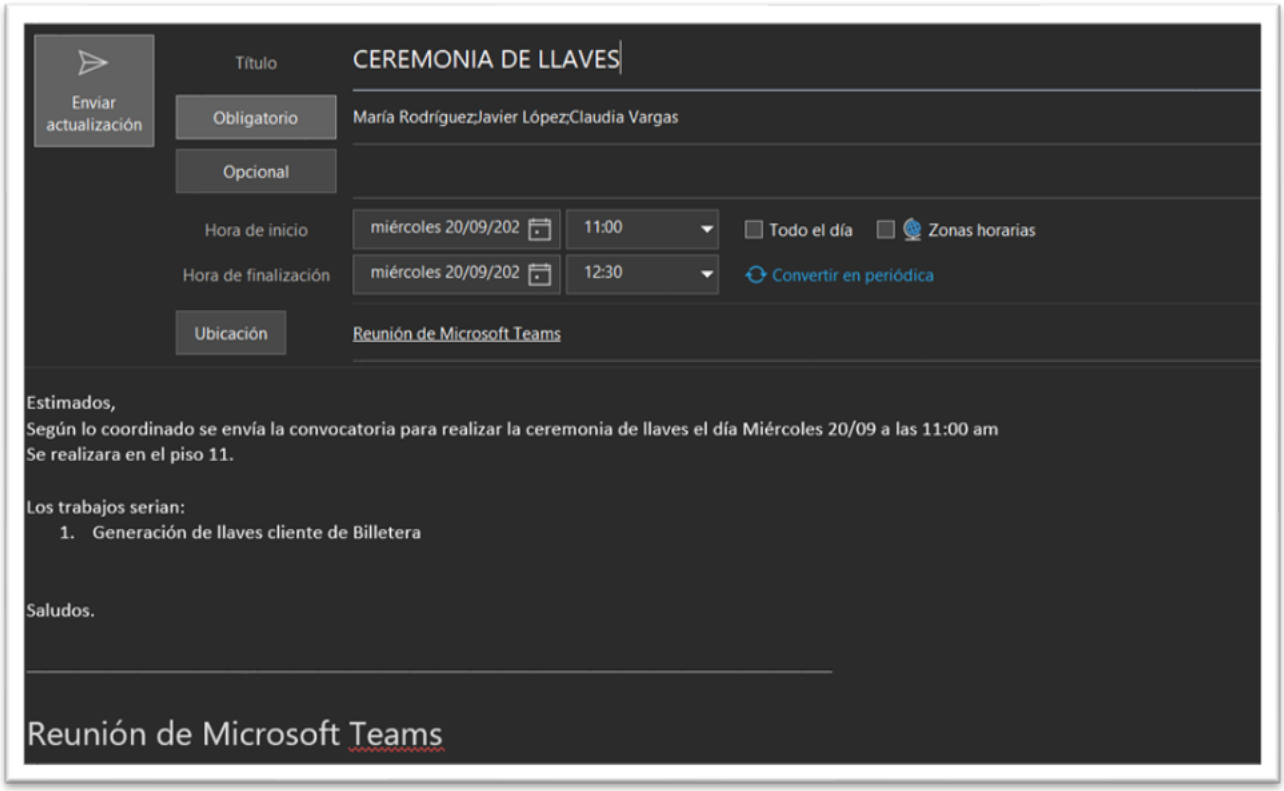
Anexo V: Evaluación de Riesgo

N°	Activo	Nombre del activo	n del activo	Producto	Criticidad del AI	Amenaza	Vulnerabilidad	Evento	Consecuencia	Codigo Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Descripcion del Riesgo
1	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Inyector de llaves remota	Alto	Ataques físicos a los terminales de pago.	Falta de medidas de seguridad física adecuadas para proteger los terminales.	El robo o extravío de terminales de pago debido a la falta de medidas de seguridad física adecuadas.	Pérdida de datos sensibles de los clientes, como información de tarjetas de crédito.	R19	2	3	Medio	debido a la ausencia de medidas de seguridad física suficientes para resguardarlos, lo que podría resultar en la exposición y pérdida de datos sensibles de los clientes, incluyendo información confidencial como los detalles de sus tarjetas de crédito.
2	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Inyector de llaves remota	Alto	Ataques cibernéticos dirigidos a los terminales de pago.	Falta de actualizaciones de seguridad y parches en los terminales.	La explotación de vulnerabilidades en los terminales de pago debido a la falta de actualizaciones de seguridad.	Posible fraude financiero si los terminales son comprometidos por atacantes.	R20	4	3	Alto	Ataques cibernéticos dirigidos a los terminales de pago debido a la falta de actualizaciones de seguridad y parches en los sistemas, lo que podría resultar en posibles incidentes de fraude financiero si los atacantes logran comprometer los terminales.
3	AI-002	Llaves Criptograficas	Llaves para encriptar datos sensibles	Inyector de llaves remota	Alto	Compromiso de la seguridad de las llaves criptográficas.	Acceso no autorizado a las llaves criptográficas.	El acceso no autorizado o el compromiso de las llaves criptográficas.	Pérdida de confidencialidad en las transacciones si las llaves son comprometidas.	R21	4	2	Medio	Compromiso de la seguridad de las llaves criptográficas debido a un acceso no autorizado, podría resultar en la pérdida de confidencialidad en las transacciones si las llaves son comprometidas.
4			Llaves para encriptar datos sensibles	Inyector de llaves remota	Alto	Fugas de información sobre las llaves criptográficas.	Falta de procesos seguros de generación y gestión de llaves.	La pérdida de control sobre las llaves criptográficas debido a procesos inseguros.	Posible exposición de las llaves a terceros no autorizados si se pierde el control sobre ellas.	R22	4	1	Medio	La posible fuga de información sobre las llaves criptográficas, causada por la carencia de procesos seguros en la generación y gestión de las mismas, puede llevar a la exposición de las llaves a terceros no autorizados si se pierde el control sobre ellas.
5	AI-003	Aplicativo de Inyeccion de llaves	Aplicativo que recibira las llaves criptograficas	Inyector de llaves remota	Medio	Ataques de malware dirigidos al aplicativo de inyección de llaves.	Falta de actualizaciones de seguridad y parches en el aplicativo de inyección de llaves.	La explotación exitosa de vulnerabilidades en el aplicativo debido a la falta de actualizaciones de seguridad.	Compromiso de la confidencialidad de las llaves criptográficas si se explotan las vulnerabilidades.	R23	4	2	Medio	inyección de llaves, debido a la falta de actualizaciones de seguridad y parches en el aplicativo. Esto podría resultar en el compromiso de la confidencialidad de las llaves criptográficas si se explotan las vulnerabilidades
6			Aplicativo que recibira las llaves criptograficas	Inyector de llaves remota	Medio	Acceso no autorizado al aplicativo de inyección de llaves.	Debilidades en la autenticación y el control de acceso al aplicativo.	El acceso no autorizado al aplicativo de inyección de llaves.	Pérdida de control sobre el aplicativo y posibles modificaciones no autorizadas.	R24	2	3	Medio	aplicativo de inyección de llaves, ocasionada por debilidades en la autenticación y el control de acceso, podría conllevar a la pérdida de control sobre el aplicativo y posibles modificaciones no autorizadas
7	AI-004	Sistema de inyeccion de llaves (RKI)	Servicio que inyectara las llaves de manera remota	Inyector de llaves remota	Alto	Interrupción del sistema de inyección de llaves debido a fallos en la infraestructura.	Falta de redundancia y planes de contingencia para la infraestructura del sistema RKI.	Interrupción del sistema de inyección de llaves debido a fallos en la infraestructura.	Interrupción de la capacidad de inyectar llaves criptográficas de manera remota.	R25	1	4	Medio	inyección de llaves debido a fallos en la infraestructura, causada por la falta de redundancia y planes de contingencia para el sistema RKI, podría llevar a una incapacidad para inyectar llaves criptográficas de manera remota.
8			Servicio que inyectara las llaves de manera remota	Inyector de llaves remota	Alto	Ataques físicos al cuarto seguro donde se encuentra el sistema RKI.	Falta de medidas de seguridad física adecuadas en el cuarto seguro.	Compromiso de la integridad del sistema RKI debido a ataques físicos.	Posible acceso no autorizado al sistema RKI y a las llaves criptográficas.	R26	3	2	Medio	el sistema RKI, derivados de la carencia de medidas de seguridad física adecuadas, podrían resultar en un posible acceso no autorizado al sistema RKI y a las llaves criptográficas.

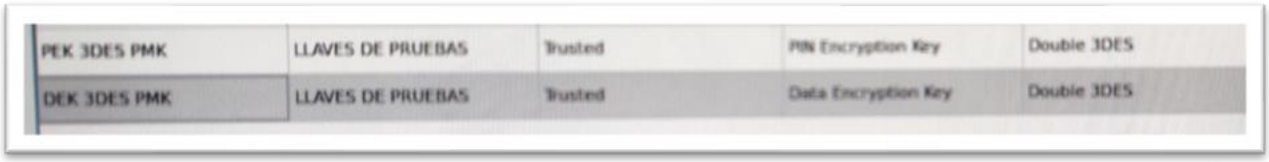
Anexo VI: Tratamiento de riesgo

N°	ID Activo	Nombre del activo	Descripcion del activo	Producto	Codigo Riesgo	Riesgo	Tratamiento del Reisgo	Control Asociado	Impacto	Probabilidad	Nivel de Riesgo
1	AI-001	Terminal de pago	Equipo que se encarga de la TRX de pago	Inyector de llaves remota	R01	de medidas de seguridad fisica suficientes para resguardarlos, lo que podria resultar en la exposición y pérdida de datos sensibles de los clientes, incluyendo información confidencial como los detalles de sus tarjetas de crédito.	Modificacion	Todo terminal de pago cuenta con un sistema de antitamper que se activa y se borrar todo datos sensibles si es manipulado	Moderado	Muy Baja	Bajo
			Equipo que se encarga de la TRX de pago	Inyector de llaves remota	R02	a la falta de actualizaciones de seguridad y parches en los sistemas, lo que podría resultar en posibles incidentes de fraude financiero si los atacantes logran comprometer los terminales.	Modificacion	Todo terminal de pago sale con una hardenizacion de android que nos da la seguridad que el software este actualizado	Menor	Baja	Bajo
2	AI-002	Llaves Criptograficas	encriptar datos sensibles	Inyector de llaves remota	R03	a un acceso no autorizado, podría resultar en la pérdida de confidencialidad en las transacciones si las llaves son comprometidas.	Modificacion	Se cuenta con una politica de ceremonia de llaves basado en custodio de la empresa.	Moderado	Muy Baja	Bajo
			Llaves para encriptar datos sensibles	Inyector de llaves remota	R04	causada por la carencia de procesos seguros en la generación y gestión de las mismas, puede llevar a la exposición de las llaves a terceros no autorizados si se pierde el control sobre ellas.	Modificacion	Todo equipo criptografico que se encarga de generacion de llaves criptograficas cuenta con un certificacion PCI PIN que imposibilita su prediccion.	Moderado	Muy Baja	Bajo
3	AI-003	Aplicativo de inyeccion de llaves	que recibira las llaves criptograficas	Inyector de llaves remota	R05	llaves, debido a la falta de actualizaciones de seguridad y parches en el aplicativo. Esto podría resultar en el compromiso de la confidencialidad de las llaves criptográficas si se explotan las vulnerabilidades	Modificacion	El aplicativo saldra con un Pentest para poder remediar las vulnerabilidades encontradas.	Menor	Baja	Bajo
			que recibira las llaves criptograficas	Inyector de llaves remota	R06	inyección de llaves, ocasionada por debilidades en la autenticación y el control de acceso, podría conllevar a la pérdida de control sobre el aplicativo y posibles modificaciones no autorizadas	Modificacion	Para poder usar el aplicativo se debe autorizar esde el RKI.	Menor	Baja	Bajo
4	AI-004	Sistema de inyeccion de llaves (RKI)	inyectara las llaves de manera remota	Inyector de llaves remota	R07	debido a fallos en la infraestructura, causada por la falta de redundancia y planes de contingencia para el sistema RKI, podría llevar a una incapacidad para inyectar llaves criptográficas de manera remota.	Modificacion	El proveedor que ofrecera el sistema RKI debe contar con la certificacion PCI PIN 3.1	Moderado	Muy Baja	Bajo
			inyectara las llaves de manera remota	Inyector de llaves remota	R08	Ataques físicos al cuarto seguro que alberga el sistema RKI, derivados de la carencia de medidas de seguridad física adecuadas, podrían resultar en un posible acceso no autorizado al sistema RKI y a las llaves criptográficas.	Modificacion	El proveedor que ofrecera el sistema RKI debe contar con la certificacion PCI PIN 3.1	Moderado	Muy Baja	Bajo

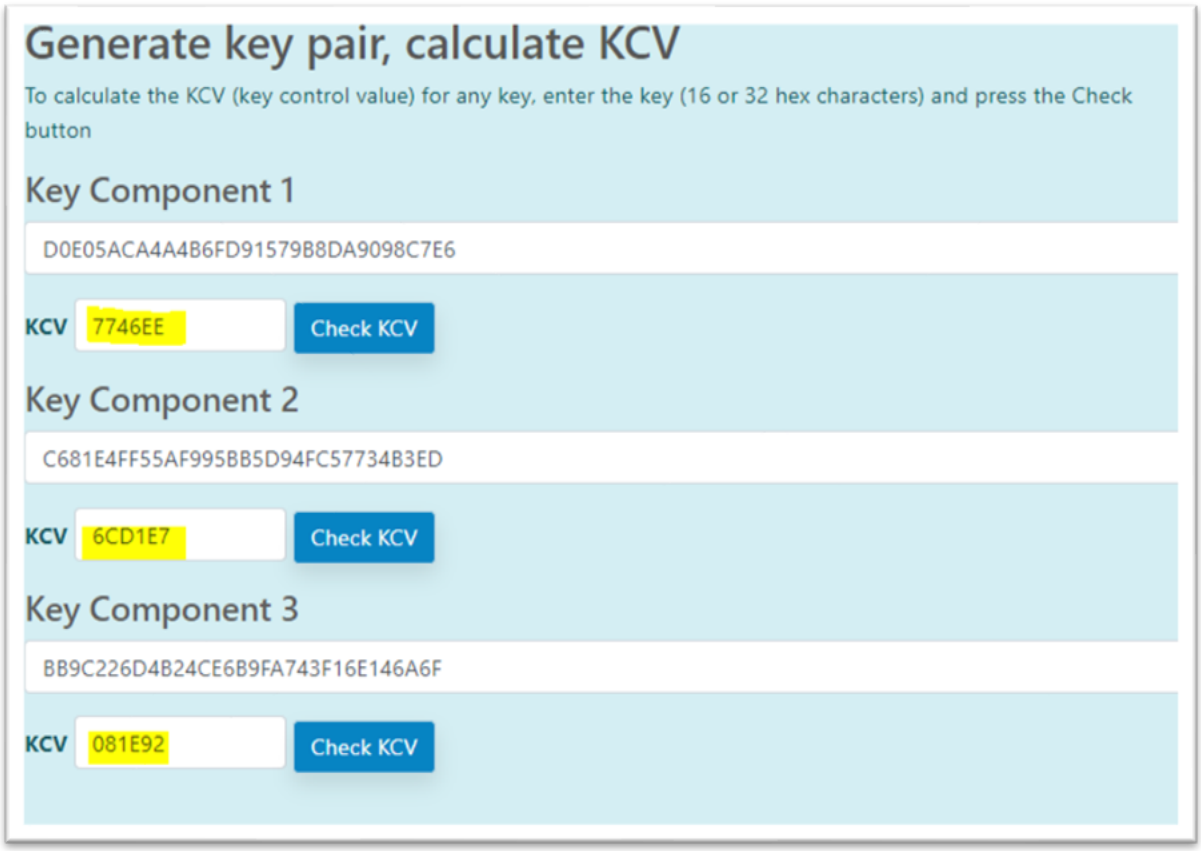
Anexo VII: Coordinación de Ceremonia de llaves

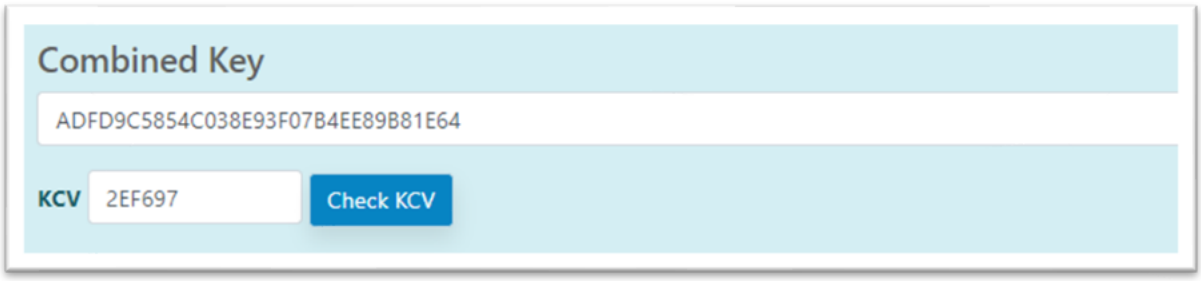


Anexo VIII: Equipo Criptográfico

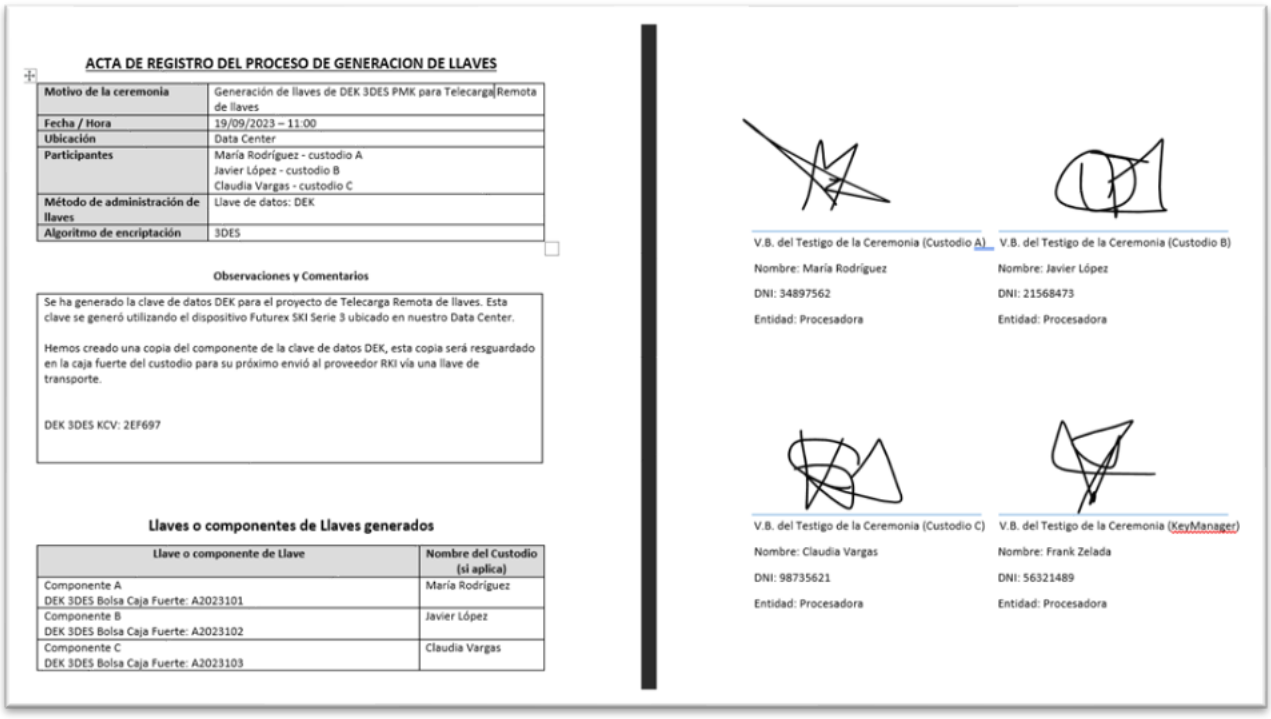


Anexo IX: Generación de llave





Anexo X: Acta de Generación de llaves



ACTA DE REGISTRO DEL PROCESO DE GENERACION DE LLAVES

Motivo de la ceremonia	Generación de llaves de DEK 3DES PMK para Telecarga Remota de llaves
Fecha / Hora	19/09/2023 – 11:00
Ubicación	Data Center
Participantes	María Rodríguez - custodio A Javier López - custodio B Claudia Vargas - custodio C
Método de administración de llaves	Llave de datos: DEK
Algoritmo de encriptación	3DES

Observaciones y Comentarios

Se ha generado la clave de datos DEK para el proyecto de Telecarga Remota de llaves. Esta clave se generó utilizando el dispositivo Futurex SKI Serie 3 ubicado en nuestro Data Center.

Hemos creado una copia del componente de la clave de datos DEK, esta copia será resguardado en la caja fuerte del custodio para su próximo envió al proveedor RKI vía una llave de transporte.

DEK 3DES KCV: 2EF697

Llaves o componentes de Llaves generados

Llave o componente de Llave	Nombre del Custodio (si aplica)
Componente A DEK 3DES Bolsa Caja Fuerte: A2023101	María Rodríguez
Componente B DEK 3DES Bolsa Caja Fuerte: A2023102	Javier López
Componente C DEK 3DES Bolsa Caja Fuerte: A2023103	Claudia Vargas

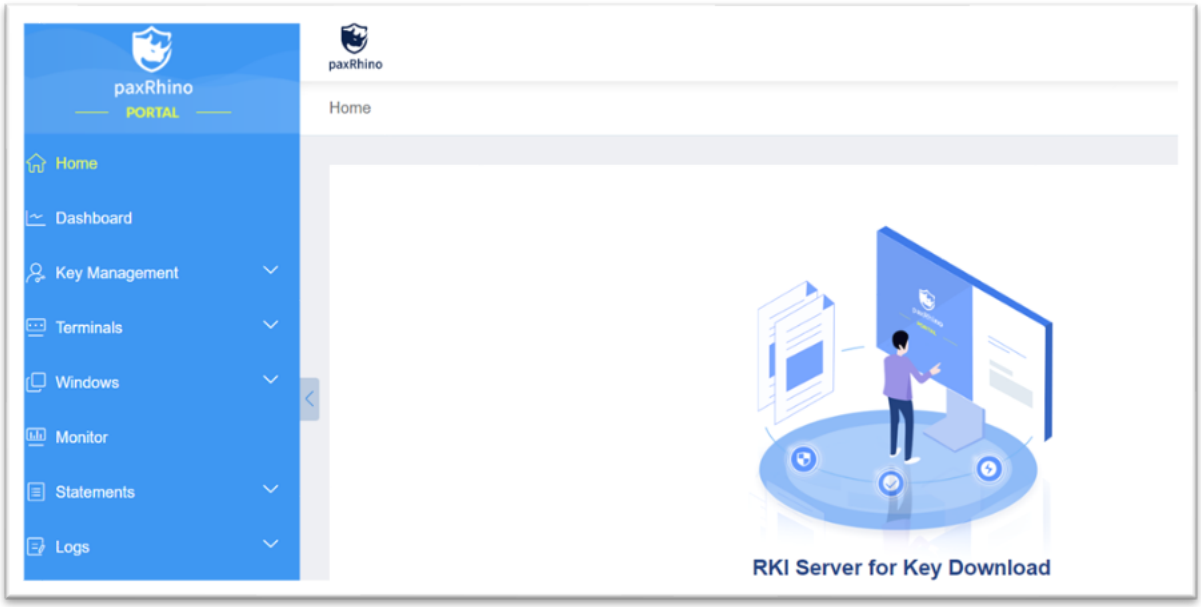
V.B. del Testigo de la Ceremonia (Custodio A)
Nombre: María Rodríguez
DNI: 34897562
Entidad: Procesadora

V.B. del Testigo de la Ceremonia (Custodio B)
Nombre: Javier López
DNI: 21568473
Entidad: Procesadora

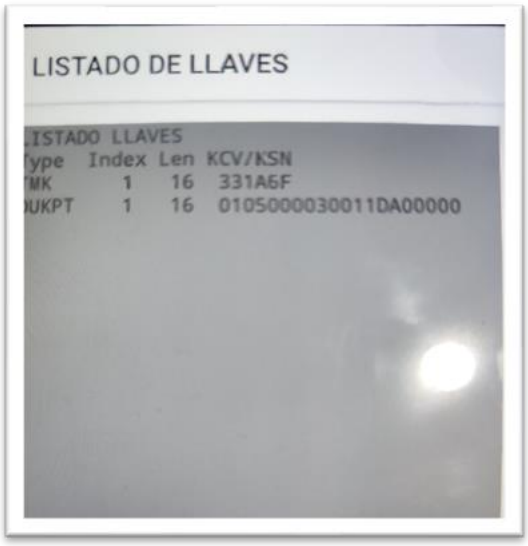
V.B. del Testigo de la Ceremonia (Custodio C)
Nombre: Claudia Vargas
DNI: 98735621
Entidad: Procesadora

V.B. del Testigo de la Ceremonia (KeyManager)
Nombre: Frank Zelada
DNI: 56321489
Entidad: Procesadora

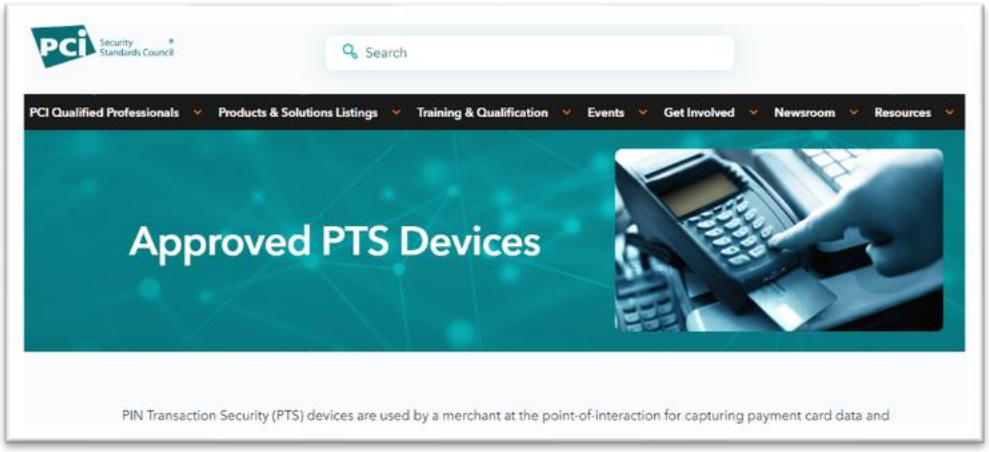
Anexo XI: PoC RKI



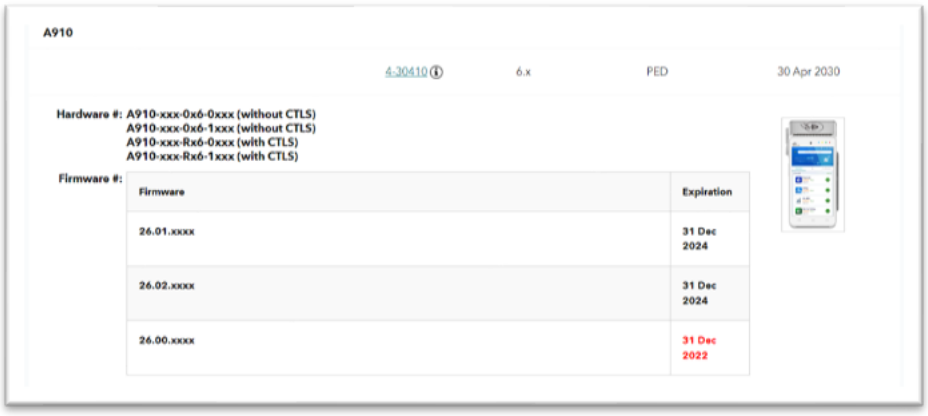
Anexo XII: Terminal de pago con llave inyectada



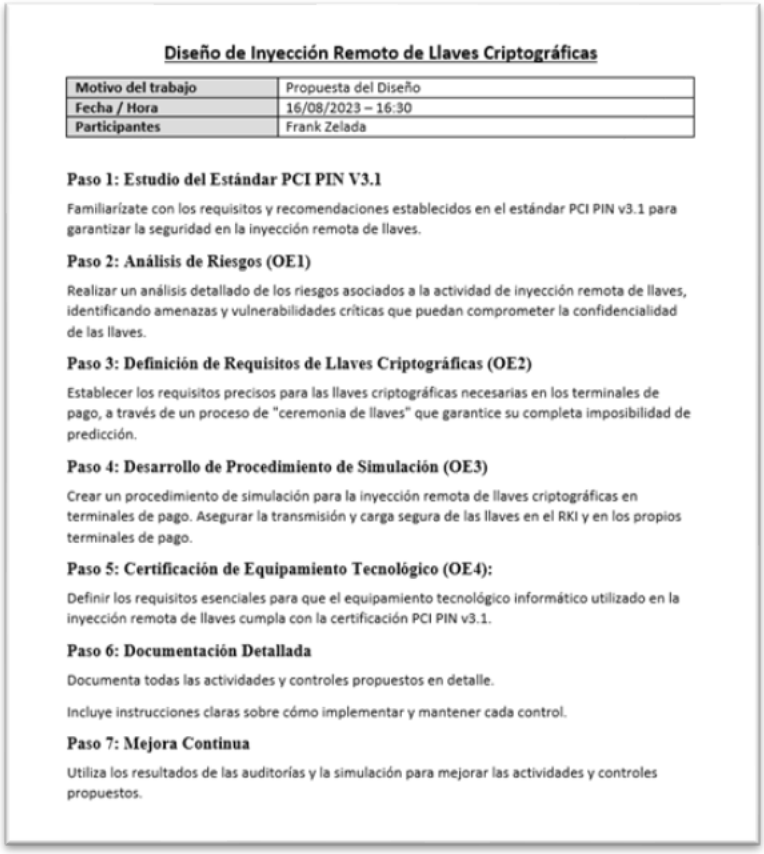
Anexo XIII: Pagina Council



Anexo XIV: Terminal de pago en cumplimiento



Anexo XV: Propuesta de diseño.



Diseño de Inyección Remoto de Llaves Criptográficas

Motivo del trabajo	Propuesta del Diseño
Fecha / Hora	16/08/2023 – 16:30
Participantes	Frank Zelada

Paso 1: Estudio del Estándar PCI PIN V3.1

Familiarízate con los requisitos y recomendaciones establecidos en el estándar PCI PIN v3.1 para garantizar la seguridad en la inyección remota de llaves.

Paso 2: Análisis de Riesgos (OE1)

Realizar un análisis detallado de los riesgos asociados a la actividad de inyección remota de llaves, identificando amenazas y vulnerabilidades críticas que puedan comprometer la confidencialidad de las llaves.

Paso 3: Definición de Requisitos de Llaves Criptográficas (OE2)

Establecer los requisitos precisos para las llaves criptográficas necesarias en los terminales de pago, a través de un proceso de "ceremonia de llaves" que garantice su completa imposibilidad de predicción.

Paso 4: Desarrollo de Procedimiento de Simulación (OE3)

Crear un procedimiento de simulación para la inyección remota de llaves criptográficas en terminales de pago. Asegurar la transmisión y carga segura de las llaves en el RKI y en los propios terminales de pago.

Paso 5: Certificación de Equipamiento Tecnológico (OE4):

Definir los requisitos esenciales para que el equipamiento tecnológico informático utilizado en la inyección remota de llaves cumpla con la certificación PCI PIN v3.1.

Paso 6: Documentación Detallada

Documenta todas las actividades y controles propuestos en detalle.

Incluye instrucciones claras sobre cómo implementar y mantener cada control.

Paso 7: Mejora Continua

Utiliza los resultados de las auditorías y la simulación para mejorar las actividades y controles propuestos.