UNIVERSIDAD NACIONAL DE LOJA

Facultad de Energía, las Industrias y los Recursos Naturales No Renovables

Carrera de Ingeniería en Sistemas

"Implementación de seguridad en las transacciones de pago realizadas a través de dispositivos móviles utilizando la tecnología NFC"

TESIS DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

Autor:

- Nixon Camilo Briceño Merino

Director:

- Ing. Hernán Leonardo Torres Carrión, Mg. Sc.

LOJA –ECUADOR
2021

Certificación del director

Ing. Hernán Leonardo Torres Carrión, Mg. Sc.

DIRECTOR DE TESIS

CERTIFICA:

Que he dirigido, revisado y corregido en todas sus partes el desarrollo del trabajo de titulación denominado “IMPLEMENTACIÓN DE SEGURIDAD EN LAS TRANSACCIONES DE PAGO REALIZADAS A TRAVÉS DE DISPOSITIVOS MÓVILES UTILIZANDO LA TECNOLOGÍA NFC” desarrollado por el egresado Nixon Camilo Briceño Merino con número de cédula 1105670366, una vez terminada la misma y luego de que reúne satisfactoriamente los requisitos exigidos, certifico que ha cumplido con el 100% del trabajo de titulación considerando pertinente la presentación, sustentación y defensa del trabajo ante el tribunal que se designe para el efecto.

Loja, 31 de marzo del 2020

Autoría

Yo, **NIXON CAMILO BRICEÑO MERINO** declaro ser autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de la tesis en el Repositorio Institucional – Biblioteca Virtual.

Firma: NIXON CAMILO BRICENO MERINO

Firmado digitalmente por NIXON CAMILO BRICENO MERINO
DN: C=EC, O=BANCO CENTRAL DEL ECUADOR, OU=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, L=QUITO, SERIALNUMBER=0000577637 + CN=NIXON CAMILO BRICENO MERINO
Razón: Soy el autor de este documento
Ubicación: la ubicación de su firma aquí
Fecha: 2021-02-04 14:48:55
Foxit Reader Versión: 9.7.0

Cédula: 1105670366

Fecha: 4 de febrero. del 2021

Carta de autorización de la tesis parte del Autor, para la consulta, reproducción parcial o total y publicación electrónica del texto completo

Yo, **Nixon Camilo Briceño Merino**, declaro ser autor de la tesis titulada: **"Implementación de seguridad en las transacciones de pago realizadas a través de dispositivos móviles utilizando la tecnología NFC"**, como requisito para optar al grado de: **INGENIERO EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la universidad. La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 4 días del mes de febrero del 2021.

Firma: NIXON CAMILO BRICENO MERINO

Firmado digitalmente por NIXON CAMILO BRICENO MERINO
DN: C=EC, O=BANCO CENTRAL DEL ECUADOR, OU=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, L=QUITO, SERIALNUMBER=0000577637 + CN=NIXON CAMILO BRICENO MERINO
Razón: Soy el autor de este documento
Ubicación: Coloque aquí la firma aquí
Fecha: 2021-02-04 14:49:18
Foxit Reader Versión: 9.7.0

Autor: Nixon Camilo Briceño Merino

Cédula: 1105670366

Dirección: Loja, Avenida Pio Jaramillo entre Cuba y Malvinas

Correo electrónico: ncbricenom@unl.edu.ec

Celular: 0998289720

DATOS COMPLEMENTARIOS

Director de Trabajo de Titulación: Ing. Hernán Leonardo Torres Carrión

Tribunal de grado: Ing. Mario Enrique Cueva Hurtado
Ing. Roberth Gustavo Figueroa Díaz
Ing. Cristian Ramiro Narváez Guillen

Dedicatoria

El presente trabajo lo dedico principalmente a Dios, a mis padres y hermanos puesto que por ellos me lleno de fuerza y dedicación para poder cumplir metas como esta de poder culminar la Carrera, ellos están en los momentos difíciles con palabras de aliento.

Agradecimiento

Agradezco a la Universidad Nacional de Loja y sobre todo a la Carrera de Ingeniería en Sistemas en sus aulas obtuve los conocimientos necesarios para afrontar los obstáculos que la vida día a día trae consigo. Al mismo tiempo agradecer a todos los docentes por brindarme sus conocimientos y enseñanzas con lo que logré crecer tanto intelectualmente como profesionalmente.

Índice General

Índice de Figuras

Índice de Tablas

1. Título

“Implementación de seguridad en las transacciones de pago realizadas a través de dispositivos móviles utilizando tecnología NFC”

2. Resumen

El presente Trabajo de Titulación (TT) consiste en asegurar la transmisión de datos a través de la tecnología NFC implementando el algoritmo criptográfico denominado Curvas Elípticas (ECC), para seleccionar este algoritmo se realizó una Revisión Sistemática de Literatura siguiendo la metodología propuesta por Barbara Kitchenham [1].

Una vez determinado el algoritmo de encriptación, se desarrolló una aplicación móvil utilizando la metodología ágil Programación Extrema (XP), para el desarrollo de dicha aplicación se tomó en cuenta el uso de la tecnología NFC la misma que permite realizar una comunicación simple y segura entre dispositivos que se encuentran a una distancia de hasta diez centímetros. El algoritmo utilizado fue ECC con la curva 25519.

Para la fase de pruebas se estableció un sistema utilizando componentes de hardware y software, se utilizó un Arduino Mega 2560 al cual se le añadió un módulo PN532 para la comunicación NFC y un módulo SIM900 para enviar los datos al servidor. Se planteó dos escenarios: uno denominado “inseguro” en donde no se utilizó el algoritmo criptográfico y otro denominado “seguro" en donde se implementó ECC, los resultados se presentan de acuerdo a los objetivos planteados para el presente TT. Finalmente, en la sección de discusión se presentó el desarrollo de una propuesta alternativa y la valoración técnica económica ambiental.

Palabras clave: NFC, Near Field Communication, algoritmos criptográficos, criptografía y pagos móviles.

Summary

This Degree Project consists of securing data transmission through NFC technology by implementing the cryptographic algorithm called Elliptic Curves (ECC). To select this algorithm, a Systematic Literature Review was carried out following the methodology proposed by Barbara Kitchenham [1].

When the encryption algorithm was determined, a mobile application was developed using the agile methodology Extreme Programming (XP), for the development of this application the use of NFC technology was considered, which allows a simple and secure communication between devices that are in a distance up to ten centimeters. The algorithm used was ECC with curve 25519.

For the testing phase, a system was set up using hardware and software components, an Arduino Mega 2560 was used, to which a PN532 module was added for NFC communication and a SIM900 module to send data to the server. Two scenarios were proposed: one called “insecure”; where the cryptographic algorithm was not used and another called “secure”; where ECC was implemented, the results are presented according to the objectives set for the present Degree Project. Finally, in the discussion section, the development of an alternative proposal and the technical and economic environmental evaluation were presented.

Keywords: NFC, Near Field Communication, cryptographic algoritms, cryptography and mobile payment.

3. Introducción

Los dispositivos móviles en la actualidad se han convertido en una herramienta de uso diario de las personas, a estos se orientan muchas aplicaciones y tecnologías con el fin de tener acceso a múltiples funcionalidades, una de ellas y que tiene mucho auge hoy en día son las transacciones de pago, con lo cual las personas para no llevar dinero físico o evitar el robo de sus tarjetas de crédito utilizan sus dispositivos móviles para realizar los pagos en establecimientos bancarios, en medios de transporte, en locales comerciales. Estas transacciones requieren asegurar los datos mediante mecanismos de seguridad para ello existen varios algoritmos criptográficos que pueden realizar esta tarea.

El desarrollo del presente Trabajo de Titulación tuvo como principal objetivo la implementación de un algoritmo criptográfico para garantizar la seguridad en las transacciones de pago realizadas a través de dispositivos móviles utilizando la tecnología NFC. Para el cumplimiento del objetivo principal se establecieron tres fases divididas de la siguiente manera: en la fase 1 se planteó analizar algoritmos criptográficos que garanticen la seguridad en la transmisión de datos en NFC, para esto se desarrolló una revisión sistemática de literatura (RSL) siguiendo la metodología propuesta por Barbara Kitchenham en donde se obtuvo como resultado que la mejor opción a utilizar es la criptografía basada en curvas elípticas por su ahorro de memoria y puesto que es asimétrica en donde se utilizan dos llaves de cifrado esto combinado con el algoritmo de intercambio de llaves Diffie-Hellman proporciona un nivel de seguridad más alto; en la fase 2 se desarrolló la aplicación utilizando el algoritmo criptográfico seleccionado, que simule las transacciones de pago seguras realizadas a través de dispositivos móviles con tecnología NFC, para lo cual se utilizó la metodología de desarrollo ágil XP adaptándola a las necesidades del TT, para la implementación del algoritmo seleccionado se utilizó una comparación de las distintas curvas utilizadas actualmente planteadas en el portal web safecurves, en donde se pudo evidenciar que la mejor opción es la curva 25519 puesto que existen las librerías necesarias tanto para Android como para Arduino y en la fase 3 se realizó las pruebas de funcionamiento en un entorno simulado, para esto se implementó un escenario que consta de hardware y software necesarios para esta fase, una vez montado el escenario se procedió a realizar dos casos de prueba con el fin de obtener los resultados del TT, se planteó un caso “inseguro” y un caso “seguro” donde en el primero no se utilizó el algoritmo de encriptación y en el segundo se realizó las pruebas utilizando el algoritmo de ECC.

El Trabajo de Titulación está conformado de la siguiente manera, una revisión de literatura, en esta sección se da a conocer al lector los conceptos necesarios involucrados en el desarrollo del presente TT, se abarcan temas como: dispositivos móviles, transacciones de pago, la tecnología NFC, la criptografía NFC y se añaden algunos trabajos relacionados. La siguiente sección es la de materiales y métodos, en donde se detallan los métodos y técnicas utilizadas para la determinación y selecciones del algoritmo que se utilizaría, así mismo como la metodología utilizada para el desarrollo de la aplicación móvil segura y la implementación del algoritmo. En la sección de resultados, se describe cada fase realizada con el fin de cumplir el desarrollo del presente TT. Seguidamente se presenta la fase de discusión, en donde se presenta una breve explicación acerca de los resultados obtenidos y como aportaron al cumplimiento de las fases planteadas. En la sección de conclusiones se presentan las deducciones obtenidas a partir de la experiencia durante el proceso de elaboración de los resultados. Finalmente se encuentra la sección de recomendaciones en donde se brindan sugerencias para una mejor realización de trabajos similares al presente.

4. Revisión de literatura

Esta sección introducirá al lector en los conceptos básicos necesarios para comprender el contexto y la solución que se plantea en el presente Trabajo de Titulación (TT). Se presenta un enfoque de las transacciones de pago a través de Near Field Communication (NFC). Luego se presentan las características relevantes sobre la seguridad en NFC.

Para que el lector tenga conocimiento sobre que es la criptografía y que tipos existen se presenta un apartado relacionado a estos conceptos, apoyado principalmente en la realización de una Revisión Sistemática de Literatura (RSL) (Ver Sección 6.1).

4.1. Dispositivos móviles

Los dispositivos móviles son llamados así por su facilidad de transportarlos de un lugar a otro y poder usarlos al mismo tiempo, a su vez poseen funcionalidades avanzadas que los diferencian de teléfonos normales [2].

4.1.1. Características de los dispositivos móviles inteligentes

Las principales características de estos dispositivos son:

- Aparatos electrónicos pequeños, que pueden ser transportados en el bolsillo o bolsos pequeños.
- Poseen mayor capacidad de procesamiento con respecto a los teléfonos celulares convencionales.
- Capacidad de memoria interna (RAM, ROM, flash), en algunos casos con capacidad para tarjetas de memoria externas (Micro SD).
- La interacción es mayormente a través de la pantalla o del teclado.

4.1.2. Android

El sistema operativo Android hasta hace algunos años estuvo presente sólo en Smartphones. Luego fue expandiéndose, por ejemplo, en televisores que poseen conexión a internet. Actualmente, es el sistema operativo más utilizado entre los Smartphones en el mundo.

Esta plataforma fue integrada por primera vez en un dispositivo móvil en España, en Marzo de 2009. Android ha ido conquistando rápidamente numerosos equipos, ya sean móviles o notebooks, tabletas, televisores con conexión a internet, convirtiéndose en el sistema operativo más utilizado hoy en día a nivel mundial [3].

4.1.3. NFC en Android

Principalmente se debe tomar en cuenta que no todos los dispositivos móviles tienen la tecnología NFC incorporada, el número aún es reducido en comparación con el número de dispositivos en el mercado. Por lo general se debe acceder a las configuraciones en el apartado de conectividad y habilitar NFC, con esto ya se podrá hacer uso de las bondades que la misma provee [3].

4.2. Transacciones de pago

Los medios de pago se utilizan cuando se desea realizar alguna transacción financiera o adquirir un bien o servicio, estos medios de pago se utilizan como herramienta para transferir valor monetario en una transacción económica con el fin de pagar un bien o servicio [4]. Para que cualquier sistema de pagos opere eficazmente se debe garantizar que las transacciones realizadas por algún medio sean seguras y rápidas [5].

4.2.1. Pagos Móviles con Tecnología NFC

Actualmente la tecnología NFC se encuentra integrada en tarjetas de viajero, tarjetas inteligentes, boletos de autobús, entre otros. Los teléfonos inteligentes también incorporan un chip NFC, con esta tecnología dos dispositivos colocados a pocos centímetros el uno del otro, permite el envío y recepción de datos a una alta velocidad, por lo que esto es adecuado para la realización de transacción y pagos.

Para el proceso de un pago móvil basado en NFC, se requiere al menos 1 dispositivo móvil emisor y un receptor de los datos el segundo, por lo generar es el terminal de punto de venta de algún comercio [2].

En [4] se afirma que para cualquier economía es necesario contar con un sistema de pago eficiente y seguro. En búsqueda de esa eficiencia la mayoría de los gobiernos del mundo han dado mayor esfuerzo hacia los pagos electrónicos.

4.3. Tecnología NFC

NFC significa, por sus siglas en inglés, Near Field Communication, es una tecnología de radiofrecuencia que permite una comunicación bidireccional inalámbrica entre dispositivos móviles cuando estos se encuentran muy cerca (inferior a 10 centímetros) [6, 7]. NFC se deriva de la tecnología RFID (Radio Frequency IDentification), la cual es una tecnología similar, pero con menos prestaciones. La lectura del contenido presente en NFC se realiza mediante la inducción de un campo magnético desde el dispositivo de lectura al chip contenedor de la información [8].

Los dispositivos con NFC pueden trabajar en dos modos diferentes de comunicación: el activo y el pasivo. La diferencia es que en el modo activo el dispositivo crea su propio campo de radiofrecuencia para la comunicación, mientras que en el modo pasivo el dispositivo aprovecha el campo generado por el activo para comunicarse [8, 9, 10] (Ver TABLA I).

TABLA I: MÉTODOS DE COMUNICACIÓN ENTRE DOS DISPOSITIVOS NFC

Dispositivo A	Dispositivo B	Descripción
Activo	Activo	Los capos de radiofrecuencia son generados de manera alternativa entre el dispositivo A y el dispositivo B.
Activo	Pasivo	El campo de radiofrecuencia es generado únicamente por el dispositivo A.
Pasivo	Activo	El campo de radiofrecuencia es generado únicamente por el dispositivo B.

4.3.1. Modos de operación de NFC

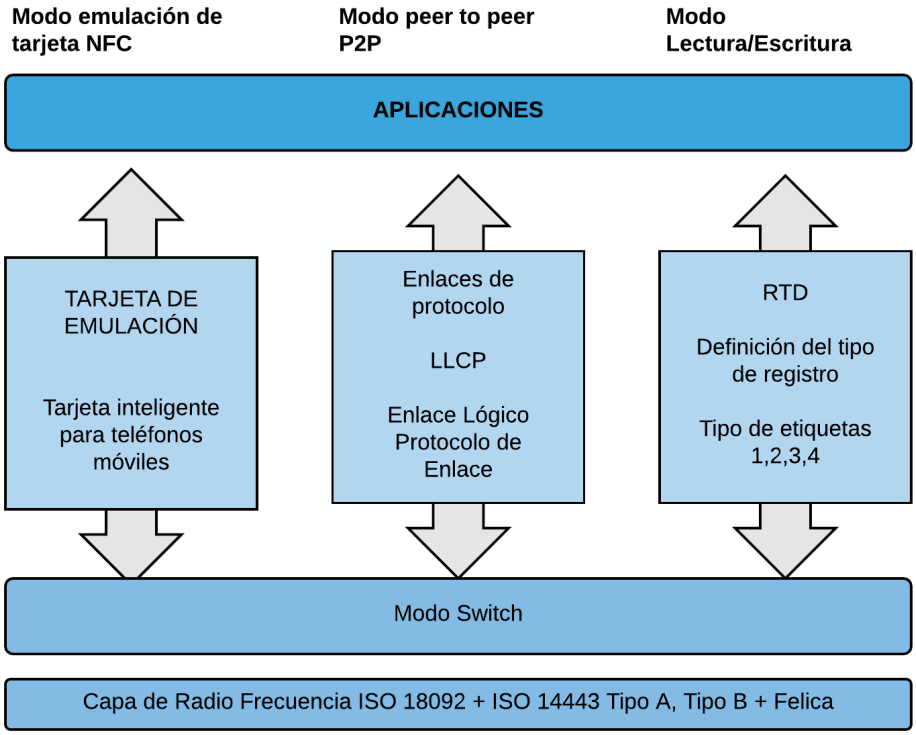

Figura 1: Modos de funcionamiento NFC

Como se describe en la Figura 1, los 3 modos de operación de NFC pueden ser [7, 10, 11]:

- Modo emulación de tarjeta NFC.
- Modo Peer-to-Peer.
- Modo Lectura / Escritura.

4.3.1.1. Modo emulación de tarjeta NFC

Con este modo los dispositivos que poseen NFC pueden emular el comportamiento y propiedades de una tarjeta con estándar ISO/EC 14443 Tipo A y Tipo B, y Felica (Ver TABLA II).

En este caso el dispositivo con NFC no genera su propio campo de radiofrecuencia ya que el lector NFC es el encargado de crearlo, por lo que el dispositivo NFC se comporta como una tarjeta normal [11]. La arquitectura de comunicación del modo de operación emulación de etiquetas se puede observar en la Figura 2.

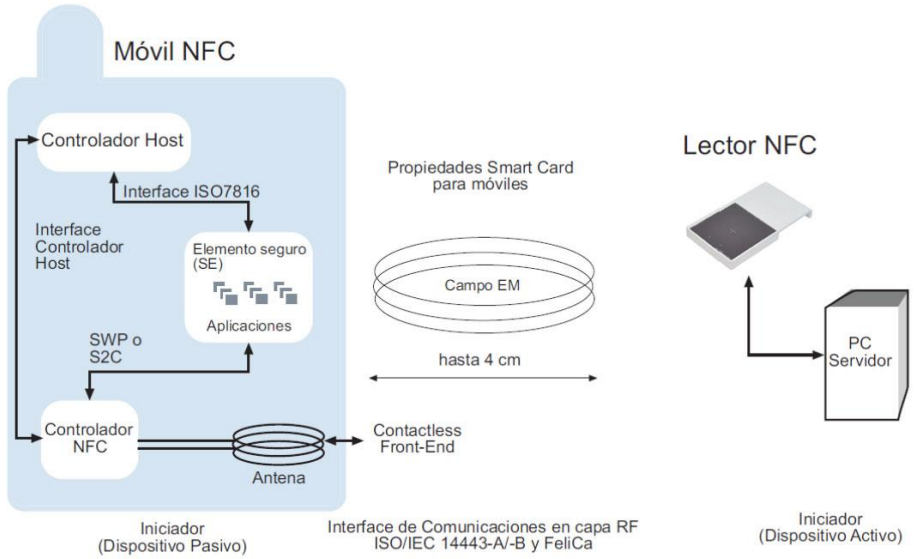

Figura 2: Arquitectura de comunicación en la emulación de tarjetas NFC [11]

4.3.1.2. Modo Peer-to-Peer

Este modo permite a los dispositivos con NFC una comunicación bidireccional de los datos [10]. Las propiedades de electromagnetismo y el protocolo usado en este modo de operación se encuentran estandarizados en la ISO/IEC 18092 como NFCIP-1 y ECMA 320/340 [11]. En la Figura 3 se puede observar la arquitectura de comunicación del modo Peer-to-Peer.

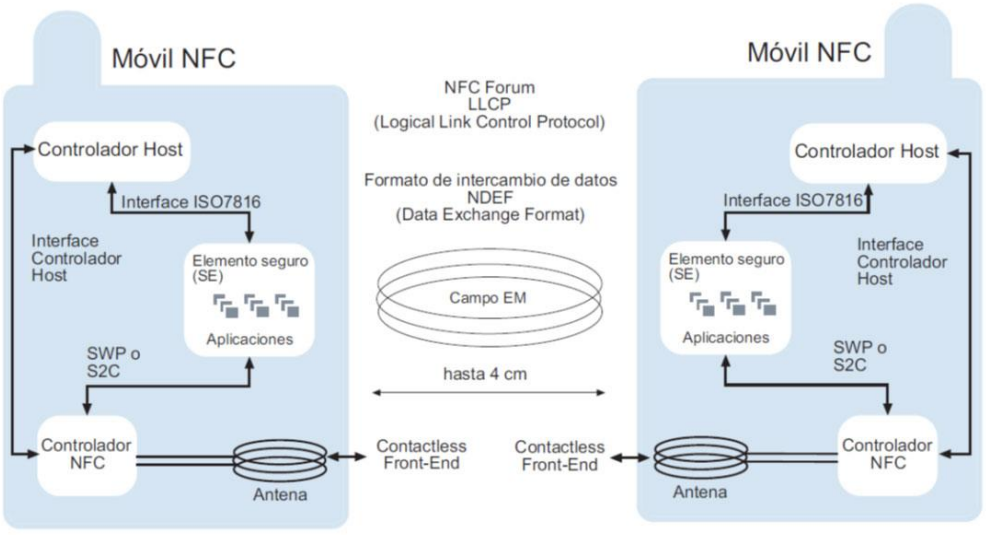

Figura 3: Arquitectura de comunicación en modo Peer-to-Peer [11]

4.3.1.3. Modo Lectura / Escritura

El dispositivo NFC en este modo puede leer y escribir información en cualquier otro terminal con el que se conecte [4]. En este modo la velocidad aproximada en la transmisión de los datos se aproxima a los 106 Kbit/seg. El modo de operación escritura / lectura está basado en la ISO/IEC 14443 Tipo A, Tipo B y el esquema FeliCa [6]. En la Figura 4 se puede observar la arquitectura de comunicación del modo de operación lectura / escritura.

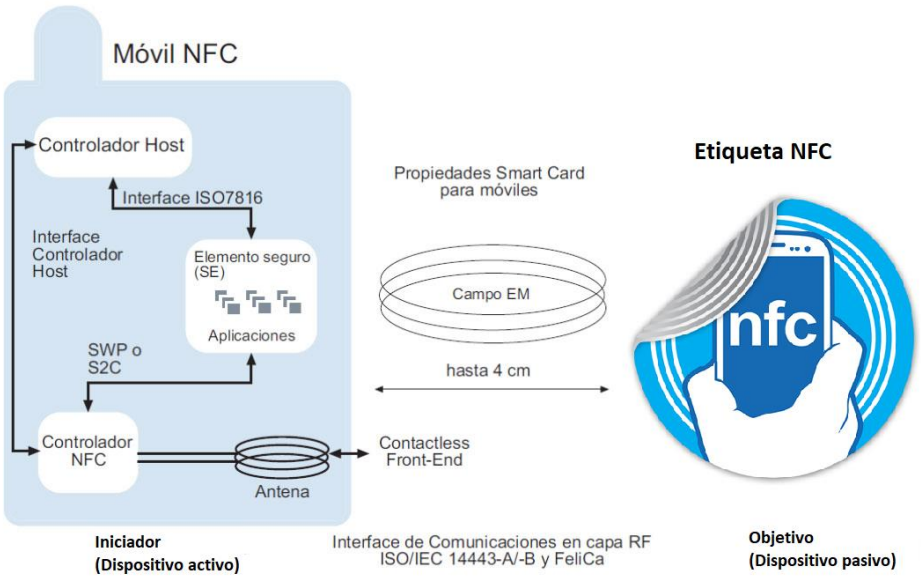

Figura 4: Arquitectura de comunicación del modo Lectura/Escritura [11]

4.3.2. Etiquetas NFC

Las etiquetas NFC son dispositivos conformados por 3 elementos: circuito integrado, antena y contenedor de energía. Existen 4 tipos de etiquetas NFC [2]:

- **Tipo 1:** tiene capacidad de lectura y escritura, aunque es posible configurarla solo para lectura.
- **Tipo 2:** tiene capacidad de lectura y escritura, o solo para lectura.
- **Tipo 3:** vienen pre configuradas para lectura/escritura o sólo de lectura.
- **Tipo 4:** son configuradas para lectura/escritura o sólo de lectura.

TABLA II: COMPARACIÓN ENTRE ETIQUETAS NFC

	Tipo 1	tipo 2	Tipo 3	Tipo 4
Estándar	ISO-14443 A	ISO-14443 B	FeliCa	ISO-14443 A/B
Identificador de usuario	Si	Si	No	Si
Velocidad de transmisión	106 kbps	106 kbps	212 kbps	424 kbps
Soporte anticolisión	No	Si	Si	Si
Lectura / Escritura	Si	Si	Si	Si
Modo activo	No	No	No	Si

4.3.3. Formato de intercambio de datos NDEF

Es el formato para el encapsulamiento de los mensajes que se van a transferir en la comunicación NFC. Con este formato se puede transmitir información como [7]:

- Documentos o fragmentos XML, imágenes de diversos formatos y datos encriptados.
- Cadenas de información encapsulada.
- Documentos múltiples que guardan alguna relación lógica.

NDEF intercambia los mensajes que son una secuencia de registros en donde cada registro lleva una carga útil y una cabecera [4].

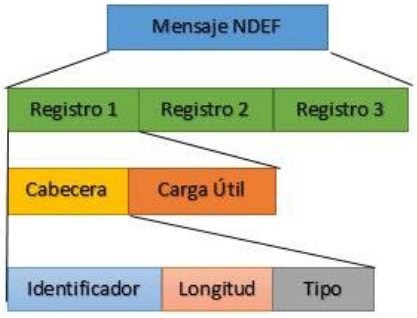

Figura 5: Estructura de un mensaje NDEF

4.3.3.1. Formato del registro NDEF

Los mensajes en NDEF se organizan en registros, en la Figura 6 se describe el formato que tienen estos registros [7, 2].

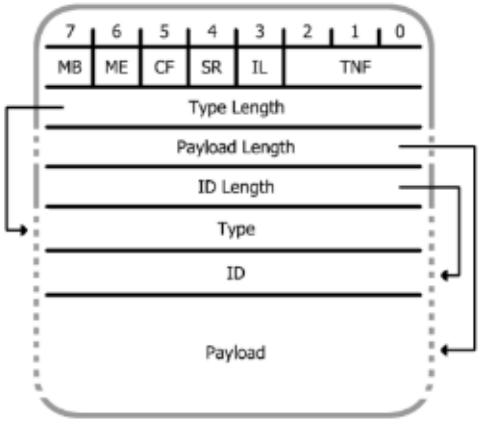

Figura 6: Formato de un registro NDEF

La unidad que se utiliza para el almacenamiento de los registros NDEF es el byte, los datos son transmitido de izquierda a derecha y también de arriba hacia abajo, el bit más significativo es el del lado izquierdo [7, 2].

A continuación, se describen los campos que conforman el formato de registro NDEF:

- **MB (Message Begin):** cuando su valor está en 1 indica que es el inicio del registro.
- **ME (Message End):** con esta bandera se indica el fin del registro.
- **CF (Chunk Flag):** cuando existen registros anidados, con CF se indica el primer segmento de este.
- **SR (Short Record):** con este valor se indica el tamaño de longitud de datos, si está activo quiere decir que se enviará un registro.
- **IL (ID Length):** es un flag que indica si el campo 'ID Length' debe estar presente en la cabecera.
- **TNF (Type Name Formar):** cuenta con un tamaño de 3 bits y permite indicar el nombre del tipo de dato que se enviara por NDEF. En la TABLA III se pueden ver los valores aceptados.

TABLA III: ESTRUCTURA TNF

Type Name	Format
Valor vacío	0x00
Tipo NFC Forum (NFC RTD)	0x01
Tipo de medios	0x02
URI absoluto	0x03
Tipo NFC Forum extremo	0x04
Tipo desconocido	0x05
Sin cambio	0x06
Reservado	0x07

- **Type Length:** se almacena el tamaño del campo TYPE, su valor varía de acuerdo al tamaño de TYPE.
- **ID Length:** indica el tamaño del campo ID.
- **Payload Length:** su valor es un numero entero y variable que indica el tamaño en bytes del campo PAYLOAD.
- **Type:** se indica que tipo de dato va a ser transmitido en el mensaje NDEF. El valor será cualquiera de los descritos en la TABLA III.
- **TNF:** la longitud máxima de este campo es de 255 octetos.
- **ID:** está representado por un Identificador de Recurso Uniforme (URI). Este URI ayuda a NDEF a identificar a cada registro que será transmitido.
- **Payload:** aquí es en donde se guarda la información que se va a transmitir, la estructura utilizada es indiferente para el formato NDEF.

4.3.4. Aplicaciones de NFC

Actualmente existe una amplia variedad de campos en los que la tecnología NFC ha destacado y ha simplificado la realización de tareas cotidianas. A continuación, se mencionan algunas de las aplicaciones actuales de esta tecnología [7]:

- Sistema de cobro de transporte público y privado.
- Pagos móviles.
- Control de acceso físico.
- Control de acceso lógico a sistemas informáticos.
- Cupones de descuentos.

- Fichas médicas digitales.
- Seguros para apertura de autos.
- Poster virtual, tarjetas de presentación y similares.

4.4. Seguridad en NFC

A pesar de que la tecnología NFC se limita a un rango de comunicación de tan solo 10 cm, existen algunas amenazas de seguridad y privacidad sobre los dispositivos pasivos como pueden ser la tarjeta con esta tecnología. Por su parte, en los dispositivos que trabajan en modo lectura/escritura, se puede vulnerar la seguridad, insertando etiquetas manipuladas en sustitución de las etiquetas originales [2].

Según lo define la Unión Internacional de las Telecomunicaciones el término de seguridad abarca cuatro grandes rasgos, los cuales son [4]:

- **Autenticación:** garantizar la identidad de los que se comunican en la red.
- **Integridad:** garantizar que la información que se transmite no ha sido alterada y que llega íntegra al receptor tal y como ha sido enviada.
- **Confidencialidad:** asegurar que la comunicación sea confidencial, es decir, que nadie distinto del emisor y receptor tienen acceso a la información.
- **No repudio:** que las partes intervinientes en una transacción o en una comunicación no puedan negar haberlo hecho.

Existen diferentes tipos de ataques, la mayoría buscan por una parte alterar los datos que están siendo transferidos de forma que la comunicación fracase sin que ni siquiera las partes interesadas se den cuenta, y por otra obtener información de los datos transferidos. Ambos casos se consideran serias amenazas que pueden provocar verdaderos desastres [10]. En este TT estamos hablando de información delicada como son las transacciones de pago.

4.4.1. Vulnerabilidades en NFC

Algunas de las amenazas que se pueden dar al momento de realizar intercambio de información entre dispositivos que utilizan tecnología NFC son:

4.4.1.1. Interceptación de comunicaciones (Eavesdropping / sniffing):

En este tipo de amenaza, un atacante puede ser capaz de interceptar y leer la información transmitida entre los dispositivos [2, 10].

4.4.1.2. Modificación de datos (Data Modification):

Un atacante, en lugar de únicamente escuchar, intentará modificar los datos que se transmiten entre los dispositivos NFC [2, 10].

4.4.1.3. Ataque Man-in-the-Middle:

Es un ataque en el que el intruso tiene la capacidad de leer, insertar y modificar a voluntad. En la Figura 7 se puede observar este escenario independientemente de la tecnología que se esté usando para la comunicación [2, 10].

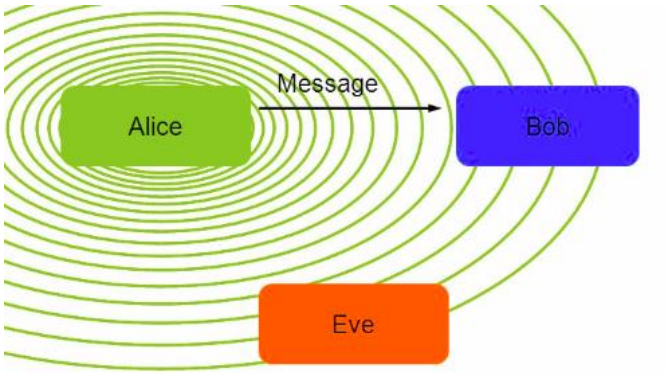

Figura 7: Esquema de ataque Man-in-the-middle

También se puede observar en la TABLA IV los tipos de ataque de acuerdo al modo de operación NFC.

TABLA IV: TIPO DE ATAQUES EN LOS MODOS DE OPERACIÓN NFC

Modo de operación	**Tipo de ataque**
NFC Card Emulation	Denegación de servicios (DoS)
	Interceptación de comunicaciones (Eavesdropping)
	Ataque relay
NFC Reader/Writer	Autenticación
	Estafa (Phishing)
	Clonación de tickets

4.5. Criptografía

El concepto de la criptografía es el de ocultar la información, disfrazándola de tal forma que no sea compresible a simple vista, para luego almacenarla en un disco duro o intercambiar dicha información con otro individuo de forma segura [11]. En la criptografía existen dos procesos básicos que son:

Encriptación: es un proceso mediante en donde el mensaje se transforma a otro que está cifrado mediante una función compleja y una llave de codificación especial.

Desencriptación: es el proceso inverso, en el cual el texto cifrado se convierte nuevamente en el texto original mediante una función compleja y una llave de desencriptación.

Un criptosistema se define como una quitupla (M, C, K, E, D), lo que significa [8]:

- M es el mensaje sin cifrar.
- C es el mensaje cifrado.
- K es el conjunto de claves que emplea el criptosistema.
- E es la función que utilizando K transforma el mensaje M en C.
- D análogo a E es el conjunto de transformaciones de descifrado.

Se conocen dos tipos de criptografía: simétricos y asimétricos [11, 4, 8]. La criptografía simétrica debe cumplir que con un mensaje cifrado C se desencripta utilizando la misma clave k empleada a la hora de encriptar el mensaje original M [8].

Y la criptografía asimétrica o de llave pública utiliza una clave pública p y otra privada k para encriptar y desencriptar respectivamente [11].

4.5.1. Protocolos simétricos y asimétricos

4.5.1.1. Protocolo simétrico

En este tipo de protocolo se utiliza la misma llave para encriptar y desencriptar el mensaje. Entre los algoritmos de llaves simétricas más comunes se encuentran [4]:

- DES (Estándar de Encriptación de Datos).
- TripleDES (Estándar de Encriptación de Datos Triple).
- AES (Advanced Encryption Standard).

Para entender mejor el protocolo simétrico, se describe el ejemplo de que si Alice quisiera enviarle un mensaje a Bob [8]:

1. Alice y Bob se ponen de acuerdo en un criptosistema simétrico.
2. Alice y Bob se ponen de acuerdo en una clave de cifrado k.
3. Alice encripta el mensaje usando el algoritmo de encriptación del criptosistema y la clave acordada. Se genera un mensaje cifrado.
4. Alice envía el mensaje cifrado a Bob.

5. Bob desencripta el mensaje cifrado con el algoritmo de desencriptación y la clave y obtiene el mensaje original

Existiendo un tercer personaje en este ejemplo, Eve, podría intentar entrometerse en la comunicación. Si Eve escuchara el paso 4 del protocolo obtendría el mensaje cifrado. Con ello podría intentar efectuar criptoanálisis y obtener el texto original. Sin embargo, existen implementaciones bastante seguras para evitar exponer la información a ataques de este tipo.

No obstante, Eve sabe que el objetivo en este protocolo sería interponerse en la comunicación para escuchar los puntos 1 y 2. Así, cuando se alcanzara el paso 4 solo tendría que realizar la misma operación que haría Bob para recuperar el mensaje original. Un buen criptosistema debería relegar la seguridad del criptosistema al conocimiento de la clave y no al del algoritmo que se emplea. Por ello, realizar el paso 1 en público no debería ser un problema, sin embargo, el paso 2 para elegir la clave debería ser secreto entre Alice y Bob. Con ello se reutiliza la clave para encriptar y desencriptar [8].

4.5.1.2. Protocolo asimétrico

Los protocolos asimétricos o conocido como protocolos de clave pública son los que utilizan una llave para encriptar el mensaje y otra para desencriptarlo [8, 4].

Entre los más comunes se encuentran [8, 4].

- RSA. (Rivest Shamir Adleman)
- EL GAMAL.
- DSS. (Digital Signature Estándar)
- ECC (Criptografía de curvas elípticas)

Para entender mejor este protocolo se describe un ejemplo similar al descrito para el protocolo simétrico. En este, Alice posee una clave pública que es conocida por Bob y otra clave privada que no es conocida por nadie más que Alice y viceversa. Por lo que el protocolo quedaría de la siguiente forma [8]:

1. Alice y Bob se ponen de acuerdo en un criptosistema de clave pública.
2. Alice consulta la clave pública de Bob k.
3. Alice encripta el mensaje usando el algoritmo de encriptación del criptosistema y la clave privada de Bob. Se genera un mensaje cifrado.

4. Alice envía el mensaje cifrado a Bob.
5. Bob desencripta el mensaje cifrado con el algoritmo de desencriptación y la clave privada y obtiene el mensaje original.

Ahora Eve no es capaz de desencriptar el mensaje ya que para ello necesita la clave privada de Bob. Las claves públicas de cada usuario se pueden disponer en cualquier lugar de acceso público. Lo único que puede hacer es encriptar un mensaje con la clave pública de un usuario y éste será el único que pueda desencriptarlo. El problema que tiene este tipo de sistemas es la distribución de claves, que ha de ser privado [8].

4.5.2. AES

AES usa un cifrado simétrico por bloques, lo que quiere decir que cifra y descifra los datos en bloques de 128 bits cada uno. Para ello, utiliza una clave criptográfica específica, que es efectivamente un conjunto de protocolos para manipular información. Esta clave puede ser de 128, 192 o 256 bits de tamaño [2].

La ventaja radica en que resulta casi imposible de descifrar si no se conoce la clave, lo que brinda un alto nivel de seguridad [12].

4.5.3. Criptografía de curva elíptica (ECC)

ECC proporciona la utilización más eficiente de la memoria para entornos de comunicación NFC restringidos por un amplio margen sobre las soluciones equivalentes basadas en RSA [12].

Una curva elíptica sobre los números reales R es el conjunto de puntos del plano (x, y) que cumplen la siguiente ecuación:

$$y^2 = x^3 + ax + b$$

El uso de criptosistemas con curvas elípticas emplea claves de un tamaño reducido respecto a otros sistemas de encriptación asimétricos considerados seguros.

La metodología de criptografía basada en curvas elípticas reduce considerablemente la cantidad de almacenamiento necesaria respecto a otros algoritmos [8].

4.6. Trabajos relacionados

Conforme la realización de la RSL (Ver Sección 6.1), se seleccionó los trabajos que tengan mayor relación con el presente TT (Ver TABLA V).

TABLA V: RESUMEN DE ESTUDIOS RELACIONADOS

Título	**Hallazgo**
Seguridad utilizando dispositivos NFC	este trabajo se propone una solución para desarrollar sistemas seguros para dispositivos de bajos recursos y criptología avanzada, de este modo, para optimizar los recursos este trabajo sugiere el uso de la metodología basada en curvas elípticas la cual reduce la cantidad de almacenamiento necesaria respecto a otros algoritmos
Application of Elliptic Curve Cryptography in Pretty Good Privacy (PGP)	Se sugiere el uso de Curvas Elípticas que no solo es adecuado para dispositivos móviles que funcionan con poca potencia, ya que puede proporcionar una seguridad equivalente a tamaños de clave más bajos, sino que también es difícil de romper, debido a una mejor función de trampilla y matemáticas difíciles, siempre que se implemente correctamente
A Secure and Efficient Key Authentication using Bilinear Pairing for NFC Mobile Payment Service.	Se propone un esquema de autenticación de clave segura para ayudar a la comunicación de pago móvil en dispositivos habilitados para NFC utilizando el emparejamiento bilineal. El esquema propuesto proporciona el uso de la criptografía de curva elíptica (ECC), de igual manera el trabajo presenta las ventajas de utilizar ECC como método de encriptación

5. Materiales y métodos

De acuerdo con el Reglamento de Régimen Académico que rige a las Instituciones de Educación Superior de Ecuador, en el artículo 21, numeral 3, se estipula que un Trabajo de Titulación (TT) se basará en procesos de investigación e intervención [13]. Por otro lado, todo TT deberá consistir en una propuesta innovadora que contenga como mínimo una investigación exploratoria y diagnóstica, además, de acuerdo con el artículo 72 del mismo reglamento, la investigación a nivel de grado es de carácter exploratorio y descriptivo [14]. La investigación exploratoria permitió planear cual era el problema de investigación, buscar sobre la tecnología NFC y como se puede asegurar la trasmisión de datos a través de la misma. La investigación descriptiva en cambio, permitió analizar el objeto de estudio, por describir su funcionamiento y las limitantes que se tienen al tratar de resolver el problema encontrado.

5.1. Contexto

El presente Trabajo de Titulación (TT) se desarrolló en el cantón Loja, en la Facultad de Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja, Carrera de Ingeniería en Sistemas.

5.2. Proceso

Para alcanzar el objetivo general del presente proyecto de investigación se usó el siguiente proceso para cada uno de los objetivos específicos:

1. **Análisis de algoritmos criptográficos (Ver Sección 246.1 de Resultados):** se realizó con el fin de seleccionar el algoritmo criptográfico para asegurar la transmisión de datos en las transacciones de pago a través de dispositivos móviles.

- **Planificación de la RSL (Ver Sección 6.1.1 de Resultados):** para llevar a cabo la RSL, se siguió el esquema planteado por Kitchenham [15], seleccionando las siguientes partes fundamentales: justificación de la revisión, formulación de las preguntas de investigación y diseño de protocolo de búsqueda.
- **Ejecución de la RSL (Ver Sección 6.1.3 de Resultados):** proceso aplicado para la ejecución de la RSL, con el fin de obtener los estudios primarios para su respectivo análisis.
- **Reporte de resultados de la RSL (Ver Sección 6.1.4 de Resultados):** se presenta los estudios primarios, resultado de la aplicación de los criterios de inclusión y exclusión.

- **Selección y descripción de algoritmos a analizar (Ver Sección 6.1.5 de Resultados):** análisis de los estudios primarios relevantes para el cumplimiento de la RSL.
- **Determinación del algoritmo a utilizar (Ver Sección 6.1.6 de Resultados):** esta fase permitió obtener objetivamente el algoritmo criptográfico a utilizar para asegurar los datos que viajan en la comunicación a través de NFC.

2. **Desarrollo de la aplicación móvil segura (ver Sección 6.2 de Resultados):** en esta fase se procedió a desarrollar la aplicación móvil segura y la arquitectura necesaria para los recursos API REST.

- **Análisis de los requisitos necesarios para desarrollar la aplicación. (ver Sección 6.2.1 de Resultados):** para esta fase se elaboró un documento correspondiente a la Especificación de Requisitos según el formato que provee el estándar IEEE 830.
- **Diseño de la aplicación. (Ver Sección 6.2.2 de Resultados):** en esta fase se presenta la arquitectura del sistema, las clases de acceso a datos y el prototipo de la aplicación como base para que el desarrollador codifique la misma.
- **Desarrollo de la aplicación. (Ver Sección 6.2.3 de Resultados):** esta fase se procede a codificar la aplicación móvil y los recursos REST.
- **Implementación del algoritmo seleccionado. (Ver Sección 6.2.4 de Resultados):** una vez seleccionado el algoritmo criptográfico se procede a la implementación del mismo.

3. **Realización de pruebas. (Ver Sección 6.3 de Resultados):** se realiza las pruebas necesarias para demostrar la seguridad del algoritmo criptográfico y las pruebas de rendimiento de los recursos REST y la aplicación móvil.

- **Análisis de los requisitos de prueba. (Ver Sección 6.3.1 de Resultados):** se identifica los datos y las funcionalidades existentes en la transacción de pago, que pueden ser vulneradas. Adicional, se selecciona las pruebas a realizar.
- **Generar un plan de pruebas. (Ver Sección 6.3.2 de Resultados):** se plantean las fases para el análisis de las vulnerabilidades presentes en la transacción de pago a través de la tecnología NFC.
- **Desarrollar escenario de prueba. (Ver Sección 6.3.3 de Resultados):** se realizar el planteamiento y descripción del escenario de pruebas.
- **Ejecución de las pruebas. (Ver Sección 6.3.4 de Resultados):** se ejecuta el plan de pruebas planteado.

- **Presentación de resultados. (Ver Sección 6.3.5 de Resultados):** en esta actividad final, se analizaron los resultados, y se validó la seguridad en las transacciones de pago utilizando el algoritmo seleccionado en la primera fase.

5.3. Recursos

Para dar respuesta a la pregunta de investigación y cumplir con los objetivos planteados en este TT de usaron los siguientes recursos:

5.3.1. Científicos

5.3.1.1. Método para RSL

Gracias a este método propuesto por Barbara Kitchenham [1] se pudo obtener una base sólida de literatura científica que fue pertinente para la realización del primer objetivo del presente TT (Ver Sección 6.1 de Resultados).

5.3.1.2. Observación directa

A través de esta técnica se pudo observar la realidad que se vive en la ciudad al no hacer uso de la tecnología NFC como medio de transmisión de datos, los problemas que genera utilizar otros medios y la manera en cómo este método de pago facilitaría la realización en las transacciones de pago.

5.3.1.3. Método Científico:

Este método sirvió para poder trazar el camino que se iba a seguir para cumplir la realización del TT; además, con el fin de solventar el problema encontrado y ver si lo que se pensaba hacer en un inicio es lo esperado, es decir cuando se presentó la propuesta de trabajo de titulación, el proceso de este método es el siguiente:

- Definición del problema: se hizo una investigación previa sobre los pagos tradicionales, en donde luego de haber identificado los problemas y validado la existencia del problema se planteó la siguiente interrogante: ¿Cómo hacer que las transacciones de pago a través de tecnología NFC sean confiables?
- Hipótesis: como respuesta a la interrogante antes descrita se planteó la implementación de un algoritmo criptográfico para asegurar las transacciones de pago a través de dispositivos móviles utilizando la tecnología NFC.

- Experimentación: esta fase se pudo evidenciar en la realización del tercer objetivo del presente TT, en donde luego de hacer las pruebas pertinentes se evidencia si la hipótesis planteada era la correcta.
- Conclusiones: una vez culminado el presente TT se presentan las conclusiones que se obtendrán (Ver Sección 8).

5.3.2. Técnicos

5.3.3. Metodología XP

Es el proceso ágil más destacado, el cual permitió seguir una serie de pasos ordenados y conocer los avances realizados [16], fue útil para la realización de la aplicación móvil (Ver Sección 6.2 de Resultados).

5.3.4. Estándar IEEE 830

Este documento ayudó a especificar de mejor manera los requisitos, y así poder determinar las funciones con las que cumplirá la aplicación (ver Anexo 1, de la Sección 11).

5.4. Participantes

El presente TT fue ejecutado por Nixon Camilo Briceño Merino, estudiante de la Carrera de Ingeniería en Sistemas, con la dirección del Ingeniero Hernán Leonardo Torres Carrión, docente de la Universidad Nacional de Loja.

6. Resultados

En esta sección, se describe los resultados obtenidos de la realización de cada objetivo propuesto para el presente TT. Como el resultado del primer objetivo, se seleccionó el algoritmo criptográfico para asegurar la transmisión de datos a través de la tecnología NFC, para ello se realizó un revisión sistemática de literatura (RSL) con la metodología propuesta por Kitchenham [1]; en el segundo objetivo se desarrolló un aplicación móvil utilizando la metodología de desarrollo ágil XP, en la que se implementó el algoritmo seleccionado; finalmente para el tercer objetivo, se planteó dos casos de prueba denominados “inseguro” y “seguro” respectivamente, por lo que, se implementó un escenario compuesto por el dispositivo móvil con la aplicación desarrollada y un lector realizado con un Arduino Mega 2560 conjuntamente con el módulo PN532 para la comunicación a través de NFC y el módulo SIM900 para la conexión con el servidor, una vez listo se procedió a realizar las pruebas necesarias con el fin de obtener una conclusión sobre el uso de un algoritmo criptográfico para asegurar la transmisión de datos a través de NFC.

6.1. Fase 1: Análisis de algoritmos criptográficos

Para el cumplimiento de esta fase, se realizó una revisión sistemática de literatura (RSL) con el fin de determinar los algoritmos de encriptación que garanticen la seguridad en la transmisión de datos a través de la tecnología Near Field Communication (NFC).

A continuación, se presentará de forma detallada como se realizó la RSL. Este proceso se desarrolló considerando las guías de desarrollo de RSL [17, 18, 19, 20] que a su vez están basadas en la metodología propuesta por Barbara Kitchenham [15].

El proceso de RSL seguido para el presente trabajo de titulación (TT) es señalado gráficamente en la Figura 8, donde se indica las fases en las que estará dividida la misma.

6.1.1. Planificación de la RSL.

Este proceso se basa en la presentación descrita por Kitchenham [15], donde se consideraron los siguientes puntos: Justificación de la revisión, formulación de las preguntas de investigación y diseño de protocolo de búsqueda [4].

6.1.1.1. Justificación de la revisión:

En este apartado se presenta el objetivo por el cual se realiza la RSL el cual es conocer sobre los algoritmos criptográficos que garantizan la seguridad en la transmisión de datos a través de la tecnología NFC en dispositivos móviles como medio de pago.

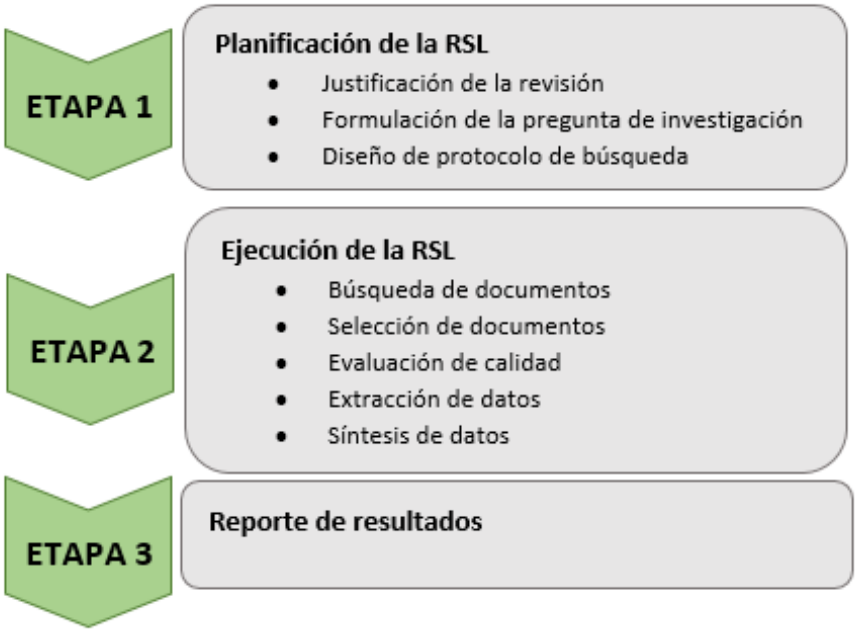

Figura 8: Proceso revisión sistemática de literatura

6.1.1.2. Formulación de las preguntas de la investigación.

Para la formulación de la pregunta de investigación se aplicó el método PICOC, que consiste en definir las variables: Población, Intervención, Comparación, Resultado, Contexto [21], en la TABLA VI se describen las variables utilizadas para el planteamiento de la pregunta.

TABLA VI: CRITERIOS PICOC UTILIZADOS EN LA INVESTIGACIÓN

Criterio	**Descripción**
Población	Algoritmos criptográficos
Intervención	Tecnología Near Field Communication (NFC)
Comparación	Algoritmos utilizados para asegurar los datos
Resultado	Algoritmos crptigraficos para asegurar los pagos móviles a través de NFC
Contexto	Pagos móviles a través de la tecnología NFC

La pregunta de investigación que se plantea es: ¿Cuáles son los algoritmos de encriptación que garantizan la seguridad en la transmisión de datos a través de la tecnología NFC?

6.1.1.3. Diseño del protocolo de búsqueda:

De acuerdo a la guía [20] en donde se indica que es requerido que se documente el proceso de búsqueda, en este apartado se encuentra descrito cómo se realizó la búsqueda de los estudios primarios que se escogieron como resultado para la RSL.

1. Selección de las fuentes de búsqueda

Luego de analizar preliminarmente documentos en diferentes bases de datos sugeridas en [20] entre ellas IEEE Xplorer, ScienceDirect, Scopus, ACM, Kluwer, Google Scholar, entre otras. Para las estrategias de búsqueda de la RSL se tomaron en cuenta las presentes en la TABLA VII.

TABLA VII: FUENTES DE BÚSQUEDA

Fuente	**Dirección web**
IEEE	https://ieeexplore.ieee.org/Xplore/home.jsp
ACM	https://dl.acm.org/
Scopus	https://www.scopus.com

2. Palabras claves y cadenas de búsqueda

Para cada motor de búsqueda, dada su particular forma de operación, se utilizó la opción avanzada con el fin de formular las cadenas (Ver TABLA VIII), probando combinaciones de las palabras clave que se derivaron de la pregunta de investigación, las mismas que son: NFC, Near Field Communication, cryptographic algoritms, cryptography, y mobile payment.

TABLA VIII: PARÁMETROS PARA EL PROCESO DE BÚSQUEDA

Fuente bibliográfica	Cadena de búsqueda
IEEE	(((“All Metadata”:NFC) OR (“All Metadata”:Neard Field Communication)) AND (“All Metadata”:cryptographic algorithmsOR“All Metadata”:cryptography) AND (“All Metadata”:mobile payment))
ACM	((“NFC” OR “Near Field Communication”) AND (“cryptographic algorithms” OR “cryptography”) AND (“mobile payment))
Scopus	((TITLE-ABS-KEY (nfc) OR TITLE-ABS-KEY(near AND field AND communication)) AND (TITLE-ABS-KEY (cryptographic AND algorithms) OR TITLE-ABS-KEY (cryptography)) AND TITLE-ABS-KEY (mobile AND payment)) AND PUBYEAR ¿2012

3. Criterios de inclusión y exclusión

Como sostiene Gonzalez et al. [22] al definir los criterios de selección que se utilizan para obtener los estudios primarios, se reduce la posibilidad de sesgo. Estos criterios de inclusión y exclusión se basan en la pregunta de investigación (Ver TABLA IX).

TABLA IX: CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Criterios de Inclusión	Criterios de Exclusión
• Artículos científicos publicados en revistas o congresos • Estudios publicados a partir de año 2013 • Tipo de documentos: artículos, libros, tesis o trabajos relacionados • Trabajos publicados en español o en ingles • Estudios que el título o resumen contengan las palabras claves • Estudios cuyo título tenga relación con el tema de investigación	• Criterios que no contribuyan a la pregunta de investigación • Trabajos poco claros • Estudios duplicados • Todos los que no cumplen con los criterios de inclusión

4. Selección de estudios primarios

Tomando en cuenta los criterios de inclusión y exclusión (Ver TABLA IX), para seleccionar los estudios primarios se escogió en base al título, resumen y palabras claves de los documentos obtenidos.

En la TABLA X se puede observar un resumen de los estudios primarios que se seleccionó, una vez aplicados los criterios de inclusión se obtuvo un total de 82 estudios, luego se procedió a aplicar los criterios de exclusión lo que sirvió para poder obtener los estudios primarios.

TABLA X: RESULTADOS DEL PROCESO DE SELECCIÓN DE ESTUDIOS PRIMARIOS

Fuente de búsqueda	Estudios incluidos	Estudios excluidos	Estudios primarios
IEEE	33	30	3
ACM	12	10	2
Scopus	37	31	6
Total	82	71	11

5. Evaluación de calidad

Se revisó los criterios utilizado para la evaluación de calidad descritos en el estudio realizado por Kitchenham [15], de los cuales se consideraron los expuestos en la TABLA XI, en donde se describe la pregunta y los parámetros utilizados para los siguientes puntajes: Y=1, P=0.5, N=0.

TABLA XI: CRITERIOS DE CALIDAD PARA LOS ESTUDIOS PRIMARIOS

#	Pregunta	Evaluación
QA1	¿El documento cumple con los criterios de inclusión y exclusión?	Y= si, N= no, P= parcialmente
QA2	¿El autor o autores sustentan el problema de investigación?	Y= en su totalidad, N= no se sustenta, P=se sustenta parcialmente
QA3	¿El autor o autores sustentan el uso de un algoritmo criptográfico en el problema de investigación?	Y= si, N= no, P= parcialmente
QA4	¿Los hallazgos abordan la pregunta de investigación original?	Y= si, N= no, P= parcialmente

TABLA XII: RESULTADOS DE EVALUACIÓN DE CALIDAD

Doc	QA1	QA2	QA3	QA4	Puntaje
ES01	Y	Y	Y	Y	4
ES02	Y	Y	Y	Y	4
ES03	Y	Y	Y	Y	4
ES04	Y	Y	Y	Y	4
ES05	Y	Y	Y	Y	4
ES06	Y	Y	Y	Y	4
ES07	Y	Y	Y	Y	4
ES08	Y	Y	Y	Y	4
ES09	Y	Y	Y	Y	4
ES10	Y	Y	Y	Y	4
ES11	Y	Y	Y	Y	4

6.1.2. Extracción de Datos

Una vez ejecutado el protocolo de RSL, se obtuvo un total de diez estudios primarios. La TABLA XIII es una adaptación a las necesidades del actual TT tomando como modelo la tabla de extracción de datos elaborada en [23], se presenta el modelo de las tablas que se utilizó para mostrar la información relevante extraída de cada estudio seleccionados. Los resultados de muestran a continuación:

TABLA XIII: MODELO DE TABLA PARA LA EXTRACCIÓN DE DATOS

#	Descripción	Detalle	
1	Información bibliográfica	Título	Nombre del estudio
		Autor	Nombre de autor o autores
		Referencia	Numero referencia correspondiente a la bibliografía
		Año	En el que fue publicado
2	Aplicación	Objetivo principal del documento seleccionado	
3	Algoritmo criptográfico	Algoritmo(s) criptográficos utilizados	
4	Conclusiones relevantes	Perspectiva personal del documento	

TABLA XIV: RESULTADOS DEL ARTÍCULO ES01

#	Descripción	Detalle	
1	Información bibliográfica	Título	A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems
		Autor	Norbert Druml, Manuel Menghin, Adnan Kuleta, Christian Steger, Reinhold Weiss Holger Bock, Josef Haid
		Referencia	[24]
		Año	2014
2	Aplicación	**Seguridad:** se presenta una solución de autenticación flexible y ligera basada en CCE, tomando en cuenta los sistemas con recursos limitado	
3	Algoritmo criptográfico	Curvas elípticas	
4	Conclusiones relevantes	La utilización de ECC se basa en la limitación de recursos. Se evalúa el comportamiento en la transmisión de datos seguro entre un dispositivo lector basado en Android y un sistema servidor de fondo. Las curvas elípticas con intercambio Diffie-Hellman (ECDHE) se utiliza para el mecanismo de intercambio de llaves. La encriptación simétrica de los mensajes se realiza con AES de 256 bits en modo de Encadenamiento de Bloques Cifrados (CBC) con Algoritmo Hash Seguro (SHA) para la autenticación de los mensajes. Se utilizan bibliotecas criptográficas de código abierto, como Spongy Castle, para llevar a cabo ECC.	

TABLA XV: RESULTADOS DEL ARTÍCULO ES02

#	Descripción	Detalle	
1	Información bibliográfica	Título	A Secure and Efficient Key Authentication using Bilinear Pairing for NFC Mobile Payment Service
		Autor	Xinyi Chen, Kyung Choi, Kijoon Cha
		Referencia	[12]
		Año	2017
2	Aplicación	**Seguridad:** se propone un esquema que utiliza un método de criptografía ECC basado en propiedades del emparejamiento bilineal	
3	Algoritmo criptográfico	Curvas elípticas	
4	Conclusiones relevantes	Se propone un esquema de autenticación de clave segura para ayudar a la comunicación de pago móvil en dispositivos habilitados para NFC utilizando el emparejamiento bilineal. El esquema propuesto proporciona el uso de la criptografía de curva elíptica (ECC), de igual manera el trabajo presenta las ventajas de utilizar ECC como método de encriptación. De acuerdo a la seguridad que se encuentra inherente en NFC contra los ataques como hombre en el medio, es bastante seguro establecer un canal seguro. ECC ahora espacio de memoria, ya que proporciona fuerza de cifrado equivalente con tamaño de clave más pequeños (en bits) en comparación con otros algoritmos como RSA. Se recomienda utilizar un emparejamiento bilineal de llave para generar un “secreto emparejado” y algún algoritmo simétrico para encriptar la información.	

TABLA XVI: RESULTADOS DEL ARTÍCULO ES03

#	Descripción	Detalle	
1	Información bibliográfica	Título	A secure end-to-end proximity NFC-based mobile payment protocol
		Autor	Sriramulu Bojjagani, V.N. Sastry
		Referencia	[25]
		Año	2019
2	Aplicación	**Seguridad:** se presenta un modelo de pagos seguro a través de NFC para P2P y P2	
3	Algoritmo criptográfico	Curvas elípticas	
4	Conclusiones relevantes	El protocolo propuesto proporciona una comunicación segura de extremo a extremo entre el cliente y el comerciante a través del banco mediante una aplicación de lectura y escritura. El modelo de pago utiliza la criptografía de curva elíptica (ECC) para cifrar los datos de los clientes. Para el cifrado y descifrado se ha utilizado la ECIES y para la generación y velicación de la firma se ha utilizado el algoritmo ECDSA. La ventaja de ECC es que es más eficiente (tanto en tiempo como en el espacio), por lo que es preferible en entornos con recursos limitados. En ECC se necesitan menos bits para el mismo nivel de seguridad en comparación con RSA. Se utilizó un tamaño de clave de 224bits de ECC, equivalente al tamaño de clave de 2048bits de RSA. El tiempo de generación de la clave también es menor en comparación con RSA.	

TABLA XVII: RESULTADOS DEL ARTÍCULO ES04

#	Descripción	Detalle	
1	Información bibliográfica	Título	Authentication Systems Using ID Cards over NFC Links: the Spanish Experience using DNIe
		Autor	León Coca J. M., Reina D. G., Toral S. L., Barrero F., Bessis N.
		Referencia	[26]
		Año	2013
2	Aplicación	**Seguridad:** se propone un sistema de autenticación basado en el DNI español y en la tecnología inalámbrica NFC. En donde se utiliza técnicas de criptografía y certificados de autenticación para establecer comunicaciones seguras entre dos interlocutores	
3	Algoritmo criptográfico	RSA	
4	Conclusiones relevantes	Se utiliza técnicas criptográficas para establecer un enlace de comunicación seguro y utilizar el DNi español para obtener la autenticación personal. Se propone el intercambio seguro de claves para resolver los problemas que surgen al utilizar algoritmos de claves simétricas	

TABLA XVIII: RESULTADOS DEL ARTÍCULO ES05

#	Descripción	Detalle	
1	Información bibliográfica	Título	NFC-Based Payment System Using Smartphones for Public Transport Service
		Autor	Diego Veloz-Cherrez, Jaime Suarez
		Referencia	[27]
		Año	2019
2	Aplicación	Seguridad: implementación de software y una infraestructura para pagos con teléfonos inteligentes Android con NFC	
3	Algoritmo criptográfico	3DES	
4	Conclusiones relevantes	Se presenta una implementación de aplicaciones de software y una infraestructura para pagos con teléfonos inteligentes Android compatibles con NFC, se describe una metodología para implementar este sistema de manera eficiente, cubriendo todos los requisitos de seguridad a través de la comunicación entre los usuarios y la plataforma para garantizar la protección de datos y brinda los resultados de las vulnerabilidades de prueba que demuestran la resistencia del sistema. Para cifrar los datos de los usuarios se utiliza el algoritmo 3DES y las contraseñas se cifran utilizando SHA-1	

TABLA XIX: RESULTADOS DEL ARTÍCULO ES06

#	Descripción	Detalle	
1	Información bibliográfica	Título	The Secure Transaction Protocol in NFC Card Emulation mode
		Autor	Yi-Lun Chi, Iuon-Chang Lin, Cheng-Hao Chen, Min-Shiang Hwang
		Referencia	[28]
		Año	2015
2	Aplicación	**Seguridad:** se propone un protocolo de transacción seguro para el modo Emulación de tarjeta NFC	
3	Algoritmo criptográfico	Curvas elípticas	
4	Conclusiones relevantes	La investigación proporciona un protocolo para las transacciones seguras en la emulación de tarjetas NFC. Aplica el protocolo Diffie-Hellman Key Exchange y el Criptosistema de curva elíptica. La investigación se basa en cumplir los cinco requisitos de seguridad que son Confidencialidad de datos, Integridad de datos, Inobservabilidad, Desvinculación y Trazabilidad, también presenta que este método tiene el menor tamaño de cálculo y cantidad de transferencia que otro propuesto lo cual es más adecuado para dispositivos móviles que tienen una capacidad limitada de cálculo y espacio de almacenamiento. Se establece la criptografía basada en Curvas elípticas e intercambios de claves Diffie-Hellman para que los dos lados de la transacción obtengan una misma clave que servirá para utilizar la encriptación simétrica AES	

TABLA XX: RESULTADOS DEL ARTÍCULO ES07

#	Descripción	Detalle	
1	Información bibliográfica	Título	Conditional Privacy Preserving Security Protocol for NFC Applications
		Autor	Hasoo Eun, Hoonjung Lee, Heekuck Oh, Member
		Referencia	[29]
		Año	2013
2	Aplicación	**Seguridad:** se propone métodos de protección de la privacidad basada en seudónimos con el fin de proteger la privacidad de los usuarios	
3	Algoritmo criptográfico	Curvas elípticas	
4	Conclusiones relevantes	El método propuesto consigue reducir al mínimo el costo de actualización y los gastos de computación aprovechando las características físicas de NFC. La NFC-SEC define los procedimientos de acuerdo de clave utilizando ECDHE entre terminales NFC	

TABLA XXI: RESULTADOS DEL ARTÍCULO ES08

#	Descripción	Detalle	
1	Información bibliográfica	Título	Development of Integrated Mobile Money System Using Near Field Communication (NFC
		Autor	Adrian Ariono Emir Husni
		Referencia	[30]
		Año	2014
2	Aplicación	**Desarrollo:** desarrollo de un sistema de pago electrónico basado en teléfonos inteligentes con NFC	
3	Algoritmo criptográfico	AES	
4	Conclusiones relevantes	Se sugiere utilizar varios algoritmos criptográficos, como la función de derivación de clave basada en contraseña y el algoritmo de ajuste de clave para mantener la seguridad del sistema, para la desarrollar el diseño de seguridad en este trabajo el algoritmo de cifrado simétrico que se utiliza es AES, debido a que es considerado el algoritmo de cifrado más seguro y práctico en la actualidad	

TABLA XXII: RESULTADOS DEL ARTÍCULO ES09

#	Descripción	Detalle	
1	Información bibliográfica	Título	Providing Security for NFC-Based Payment Systems Using a Management Authentication Server (AES)
		Autor	Ali Al-Haj, Mayyadah Adnan Al-Tameemi
		Referencia	[31]
		Año	2018
2	Aplicación	**Seguridad:** se propone un protocolo para mejorar la seguridad de los mensajes intercambiados en el protocolo EMV	
3	Algoritmo criptográfico	Cifrado utilizando clave de sesión	
4	Conclusiones relevantes	Se propone un nuevo protocolo para proporcionar seguridad para las transacciones de pago en línea entre dispositivos habilitados por NFC. El protocolo propuesto agrega una nueva capa de seguridad llamada Servidor de autenticación de administración (MAS) al tiempo que toma en cuenta los recursos restringidos de NFC	

TABLA XXIII: RESULTADOS DEL ARTÍCULO ES10

#	Descripción	Detalle	
1	Información bibliográfica	Título	Secure Physical Access with NFC-enabled Smartphones
		Autor	Chrstof Arnosti, Dominik Gruntz, Marco Hauri
		Referencia	[32]
		Año	2015
2	Aplicación	**Seguridad:** se propone un proceso de autenticaci´on que evita los ataques de proxy de software en dispositivos con NFC	
3	Algoritmo criptográfico	RSA	
4	Conclusiones relevantes	Se presenta un Sistema de Control de Acceso Físico (PACS) que es independiente de los proveedores externos. La tarjeta inteligente es reemplazada por el teléfono inteligente que está conectado al servidor de acceso. De igual manera en este documento se describe y analiza la seguridad de las diferentes soluciones de autenticación desarrolladas en el contexto de un PACS concreto. Por lo que, presentan un proceso de autenticación novedoso que evita los ataques de proxy de software	

TABLA XXIV: RESULTADOS DEL ARTÍCULO ES11

#	Descripción	Detalle	
1	Información bibliográfica	Título	OpenKeychain: An Architecture for Cryptography with Smart Cards and NFC Rings on Android
		Autor	Dominik Schurmann, Sergej Dechand, Lars Wolf
		Referencia	[33]
		Año	2017
2	Aplicación	**Seguridad:** diseño, implementación y evaluación de una arquitectura para criptografía basada en NFC	
3	Algoritmo criptográfico	AES, RSA	
4	Conclusiones relevantes	Se diseña, implementa y evalúa una arquitectura para criptografía basada en NFC en dispositivos Android denominada OpenKeyChain que es una API que proporciona operaciones criptografía sin requerir conocimiento de criptografía de clave publica	

6.1.3. Ejecución de la RSL

Luego de haber establecido como serán los lineamientos para realizar la RSL, en este apartado se procede a aplicar la revisión sistemática de estudios realizados sobre algoritmos criptográficos que garanticen la seguridad en la transmisión de datos a través de la tecnología NFC.

El procedimiento que se siguió para la realización de la RSL se detalla a continuación:

- En base a los parámetros señalados en la TABLA VIII, se encontró documentos se almacenó en el repositorio Mendeley, haciendo uso de su herramienta de escritorio.
- Se procedió a realizar una depuración de los documentos duplicados, encontrados anteriormente, a través del programa Mendeley.
- Se realizó una depuración al aplicar los criterios de inclusión y exclusión.
- Se hizo una depuración de los documentos obtenidos en el punto anterior, cuyo título, palabras claves o resumen, no tengan una relación directa con la pregunta de investigación.
- Los resultados obtenidos al realizar estos pasos se pueden observar en la Figura 9.

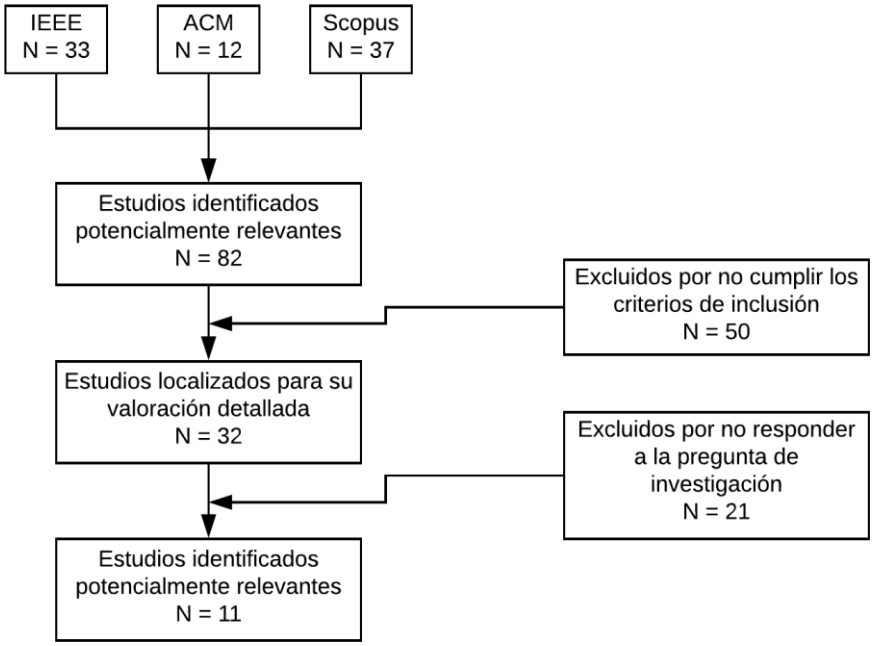

Figura 9: Proceso de selección

6.1.4. Reporte de resultados de la RSL

Una vez que se aplicó los criterios de inclusión y exclusión se obtuvo un total de 11 trabajos relacionados que responden la pregunta de investigación (Ver TABLA XXV), y partir de la información extraída de los documentos reunidos se realizó un análisis para poder determinar el algoritmo criptográfico que se utilizaría en el desarrollo del presente TT.

TABLA XXV: RESUMEN DE ESTUDIOS SELECCIONADOS

Código	Titulo	Año de publicación	Buscador
ES01	A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems	2014	Scopus
ES02	A Secure and Efficient Key Authentication using Bilinear Pairing for NFC Mobile Payment Service	2017	Scopus
ES03	A secure end-to-end proximity NFC based mobile payment protocol	2019	Scopus
ES04	Authentication Systems Using ID Cards over NFC Links: the Spanish Experience using DNIe	2013	Scopus
ES05	NFC-Based Payment System Using Smartphones for Public Transport Service	2019	Scopus
ES06	The Secure Transaction Protocol in NFC Card Emulation Mode	2015	Scopus
ES07	Conditional Privacy Preserving Security Protocol for NFC Applications	2013	IEEE
ES08	NFC-Based Payment System Using Smartphones for Public Transport Service	2014	IEEE
ES09	Providing Security for NFC-Based Payment Systems Using a Management Authentication Server	2018	IEEE
ES10	Secure Physical Access with NFC-enabled Smartphones	2015	ACM
ES11	OpenKeychain: An Architecture for Cryptography with Smart Cards and NFC Rings on Android	2017	ACM

6.1.5. Selección y descripción de algoritmos a analizar.

En base a la RSL realizada se pudo obtener los datos necesarios que serán relevantes para el cumplimiento de esta fase. En todos los estudios se pudo encontrar que:

- Para garantizar la seguridad en la transmisión de datos a través de la tecnología NFC se utiliza los algoritmos AES, ECC, RSA, 3DES y basado en clave de sesión (otros) (Ver TABLA XXVI).
- En todos los estudios la utilización de un protocolo de seguridad es fundamental en los sistemas de pagos.

TABLA XXVI: ALGORITMOS UTILIZADOS EN CADA ESTUDIO

Estudio	AES	ECC	3DES	RSA	Otros
ES01		X			
ES02		X			
ES03		X			
ES04				X	
ES05			X		
ES06		X			
ES07		X			
ES08	X				
ES09					X
ES10			X		
ES11				X	

- En la Figura 10 se aprecia que el algoritmo criptográfico usado con más frecuencia para la encriptación de datos en las transacciones de pago a través de la tecnología NFC es la criptografía basada en Curvas Elípticas (ECC), seguida de RSA, 3DES, AES y Otros.

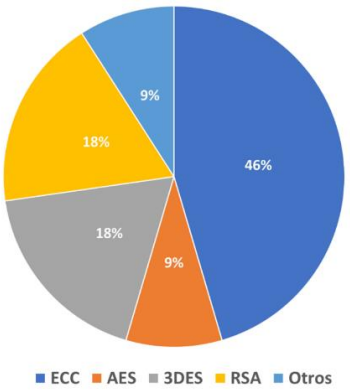

Figura 10: Algoritmos criptográficos usados en cada estudio

6.1.6. Determinación de algoritmo a utilizar.

Una vez se analizó cada documento resultado de la RSL, se evidencia que el algoritmo más utilizado es el basado en Curvas Elípticas (ECC).

En los estudios la utilización de ECC es por el ahorro de espacio de memoria, puesto que tiene el menor tamaño de cálculo y cantidad de transferencia lo que es más adecuado para dispositivos que tienen una capacidad limitada de cálculo y espacio de almacenamiento.

La utilización de ECC se adapta bien a todos los tipos de pagos como los mini, macro y micropagos que se hacen en un canal de extremo a extremo.

Tomando en cuenta los puntos antes mencionados se optó por utilizar ECC para en el desarrollo del presente trabajo de titulación.

6.2. Fase 2: Desarrollo de la aplicación móvil segura

Para el desarrollo de esta fase se analizó algunas metodologías para el desarrollo de software con el fin de seleccionar una, acorde a los requerimientos del TT, se optó por tomar como referencia el estudio hecho en [34] y [35], en la TABLA XXVII se puede ver una comparación entre las metodologías XP, RUP e ICONIX.

TABLA XXVII: ANÁLISIS COMPARATIVO ENTRE METODOLOGÍAS

XP	**RUP**	**ICONIX**
Exigencia de documentación		
Bajo nivel de exigencia de documentación, efectuándose el diseño mínimo para cumplir con los requerimientos actuales	Trabajo pesado en documentación de diseño y planificación rígida	Busca generar la documentación suficiente para el arranque del desarrollo
Tipos de metodología		
Ligera, ágil	Tradicional, pesada	Ágil, pesada-ligera
Tipo de proyecto		
Es recomendable para proyectos de corto plazo	Aún se implementa en proyectos de gran escala que no requiere resultados rápidos, pero si procesos críticos	Es adecuado para proyectos pequeños y medianos
Participación del cliente		
Requiere la participación a tiempo completo del cliente	El cliente interactúa, pero no es parte del equipo de desarrollo	Promueve la interacción del cliente con el desarrollo de software, mostrándoles versiones funcionales del sistema para que los pueda evaluar
Enfoque		
Potenciar las relaciones interpersonales como clave para el éxito	Enfoque disciplinado para asignar tareas y responsabilidades	En ir de los casos de uso al código de forma fiable, en el menor número de pasos posibles
Tamaño de equipo		
Pequeño	Medio o extenso	Pequeño o medio

Puesto que el presente TT es de pequeña escala, el desarrollo lo realiza una sola persona, no es de larga duración y tiene un nivel de complejidad medio se decidió utilizar la metodología XP.

Se tomó el proceso que sugiere la metodología XP (planeación, diseño, codificación y pruebas) se debe tener en cuenta que esta metodología no impone ninguna restricción en cuanto a la organización del ciclo de desarrollo de un proyecto de software por lo que, fue posible adaptarlo a las actividades para el cumplimiento de la presente fase.

6.2.1. Análisis de los requisitos necesarios para desarrollar la aplicación (Fase de planeación)

6.2.1.1. Roles:

Para la realización de este proyecto existe la participación de dos personas: tesista y director del proyecto, de acuerdo a la metodología XP los roles que se definirán serán los descritos en la TABLA XXVIII:

TABLA XXVIII: DESCRIPCIÓN DE ROLES

Nombre	**Rol**
Nixon Camilo Briceño Merino	Analista, diseñador y programador
Hernán Leonardo Torres	Director del trabajo de titulación

6.2.1.2. Especificación de requerimientos:

Para determinar las funciones que tendrá y cumplirá la aplicación móvil segura, se elaboró un documento correspondiente a la Especificación de Requisitos según el formato que provee el estándar IEEE 830 (Ver Anexo 1).

- **Requerimientos funcionales:**

TABLA XXIX: REQUERIMIENTOS FUNCIONALES

Requisito	**Nombre**	**Descripción**
RF01	Autentificación de usuario	Los usuarios podrán acceder a la aplicación utilizando las credenciales proporcionadas con anterioridad
RF02	Registrar usuarios	La aplicación permitirá al usuario registrarse. El usuario debe suministrar datos como: CI, Nombre, Apellido, E-mail, Usuario y Contraseña
RF03	Consultar información	La aplicación ofrecerá al usuario información general sobre sus datos personales
RF04	Consultar información	**Consultar Saldo:** Muestra toda la información sobre el saldo y los pagos que ha realizado el usuario
RF05	Modificar datos personales	La aplicación permitirá al usuario modificar los datos personales
RF06	Realizar transacciones de pago	Permite al usuario generar una transacción de pago
RF07	Integración de pago	La aplicación podrá coexistir con un aplicación o hardware que pueda ser la encargada de realizar las transacciones de pago
RF08	Gestionar reportes	Permite al usuario genera un reporte sobre todos los pagos que se han realizado en cierto tiempo

- **Requerimientos no funcionales:**

TABLA XXX: REQUERIMIENTO NO FUNCIONALES

Requisito	Nombre	Descripción
RNF01	Interfaz de la aplicación	La aplicación presentara una interfaz de usuario sencilla para que sea de fácil manejo a los usuarios del sistema
RNF02	Ayuda en el uso de la aplicación	La interfaz del usuario deberá de presentar una introducción de ayuda para que los mismos usuarios del sistema se les faciliten el manejo de la aplicación
RNF03	Desempeño	La aplicación garantizará a los usuarios un desempeño en cuanto a los datos almacenado en el sistema ofreciéndole una confiabilidad esta misma
RNF04	Seguridad en información	El sistema garantizara a los usuarios una seguridad en cuanto a la información que se procede en el sistema y a las transacciones que son realizadas a través de la misma

- **Características de los usuarios de la aplicación móvil segura:**

TABLA XXXI: CARACTERÍSTICAS DE LOS USUARIOS

Tipo de usuario	Descripción
Administrador	Persona con acceso a todo el sistema
Usuario	Manejo de la aplicación en general

6.2.1.3. Módulos de la aplicación móvil segura.

La aplicación móvil segura cuenta con tres módulos, consulta de saldo, gestión del perfil e historial de transacciones, los mismos que se detallan en la TABLA XXXII.

TABLA XXXII: MÓDULOS DE LA APLICACIÓN MÓVIL SEGURA

Módulo	**Descripción**
Transacciones	Realizar transacciones de pago y consultar el saldo disponible por parte del usuario
Gestión del perfil	Consulta, edición y registro de los datos del perfil del usuario
Historial de transacciones	Visualización de los movimientos presentes en la cuenta del usuario

6.2.1.4. Historias de usuario:

Las historias de usuario sirvieron para la representación de los requerimientos necesarios para la aplicación móvil segura.

- **Módulo de transacciones**

TABLA XXXIII: HISTORIA DE USUARIO AUTENTICACIÓN

Historia de usuario	
Numero: 1	**Nombre:** autentificar usuario
Usuario: usuario	Iteración asignada: 2
Prioridad de negocio: Alta	Puntos estimados: 1
Riesgo en Desarrollo: Media	Requisitos: RF01
Descripción: como usuario quieres acceder al sistema para poder realizar transacciones de pago	
Observaciones: el usuario podrá autentificarse en el sistema usando su usuario y contraseña almacenados en la base de datos del sistema, lo que se realizará a través de un recurso web	
Validación: El usuario debe ingresar su usuario y contraseña para acceder al sistema	

TABLA XXXIV: HISTORIA DE USUARIO REALIZAR PAGO

Historia de usuario	
Numero: 2	**Nombre:** Realizar pago
Usuario: usuario	Iteración asignada: 2
Prioridad de negocio: Alta	Puntos estimados: 1
Riesgo en Desarrollo: Alta/Media	Requisitos: RF06
Descripción: Como usuario quiero realizar pagos seguros utilizando la tecnología NFC para poder utilizar un servicio	
Observaciones: El usuario realizará las transacciones de pago utilizando un recurso web	
Validación: El usuario debe tener el saldo suficiente para realizar un pago El usuario tiene 30segundos para realizar el pago	

TABLA XXXV: HISTORIA DE USUARIO CONSULTADO DE SALDO

Historia de usuario	
Numero: 3	**Nombre:** Consulta de saldo
Usuario: usuario, administrador	Iteración asignada: 2
Prioridad de negocio: Alta/Media	Puntos estimados: 1
Riesgo en Desarrollo: Media/Baja	Requisitos: RF04
Descripción: Como usuario quiero conocer el saldo disponible en mi cuenta para saber cuánto necesito recargar	
Observaciones: El usuario podrá ver en la vista principal de la aplicación móvil el saldo que posee actualmente, para conocer este saldo se utilizará un recurso web	
Validación: El usuario puede ver su saldo en la vista principal de la aplicación	

- **Módulo de gestión del perfil**

TABLA XXXVI: HISTORIA DE USUARIO GESTIÓN DE DATOS PERSONALES

Historia de usuario	
Numero: 4	**Nombre:** gestión de datos personales
Usuario: usuario	Iteración asignada: 1
Prioridad de negocio: Media	Puntos estimados: 1
Riesgo en Desarrollo: Media	**Requisitos:** RF03 – RF05
Descripción: Como usuario quiero gestionar mis datos personales para poder tener control sobre los mismo	
Observaciones: El usuario podrá revisar y modificar sus datos necesarios para el sistema, los mismos que se encontrarán en la base de datos del sistema. El usuario podrá modificar sus datos personales utilizando un recurso web	
Validación: El usuario puede revisar sus datos personales El usuario puede modificar sus datos personales	

TABLA XXXVII: HISTORIA DE USUARIO REGISTRO DE DATOS

Historia de usuario	
Numero: 5	**Nombre:** Registro en el sistema
Usuario: usuario, administrador	Iteración asignada: 1
Prioridad de negocio: Media	Puntos estimados: 1
Riesgo en Desarrollo: Media	Requisitos: RF02
Descripción: Como usuario quiero registrar mis datos personales en el sistema para poder realizar transacciones de pago	
Observaciones: El usuario podrá registrar sus datos personales en el sistema utilizando un recurso web. Los datos del usuario se almacenarán en la base de datos del sistema	
Validación: El usuario puede registrar sus datos personales	

- **Módulo de historial de transacciones**

TABLA XXXVIII: HISTORIA DE USUARIO CONSULTA DE TRANSACCIONES

Historia de usuario	
Numero: 6	**Nombre:** Consulta de transacciones
Usuario: usuario, administrador	Iteración asignada: 2
Prioridad de negocio: Media	Puntos estimados: 1
Riesgo en Desarrollo: Media	Requisitos: RF07
Descripción: Como usuario quiero conocer el historial de mis transacciones de pago	
Observaciones: El usuario podrá consultar el historial de las transacciones de pago utilizando un recurso web	
Validación: El usuario puede seleccionar una fecha para ver las transacciones que realizó ese día	

6.2.2. Diseño de la aplicación

En esta fase está realizada de acuerdo a las pautas de diseño propuestas por la metodología XP.

6.2.2.1. Arquitectura del Sistema

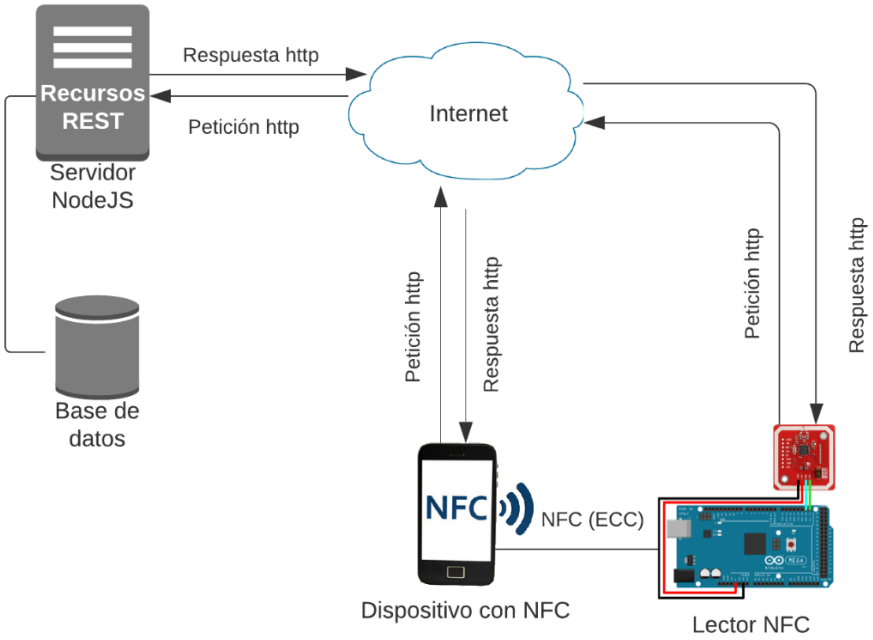

Figura 11: Arquitectura del sistema

A continuación, se describe cada uno de los componentes de la arquitectura:

- **Servidor Node JS:** Se conoce así al servidor configurado para procesar la información de datos y enviarla a los dispositivos con NFC y lector NFC mediante un API REST.
- **Dispositivo con NFC:** Se refiere a los clientes que muestran la información del usuario presente en la base de datos y recibida a través del protocolo HTTP mediante recursos REST.
- **Lector NFC:** Será el hardware utilizado y desarrollado para el presente TT, con el fin de simular el sistema de pagos seguro, se configuró para utilizar el protocolo HTTP para enviar información al servidor y con NFC para leer los datos del teléfono inteligente.
- **Internet:** Medio de comunicación por el cual, se transmitirá el tráfico de datos desde el dispositivo móvil y el lector NFC.

6.2.2.2. Diagrama de clases:

Sirve para comprender la relación entre las distintas clases u objetos que intervienen en el sistema.

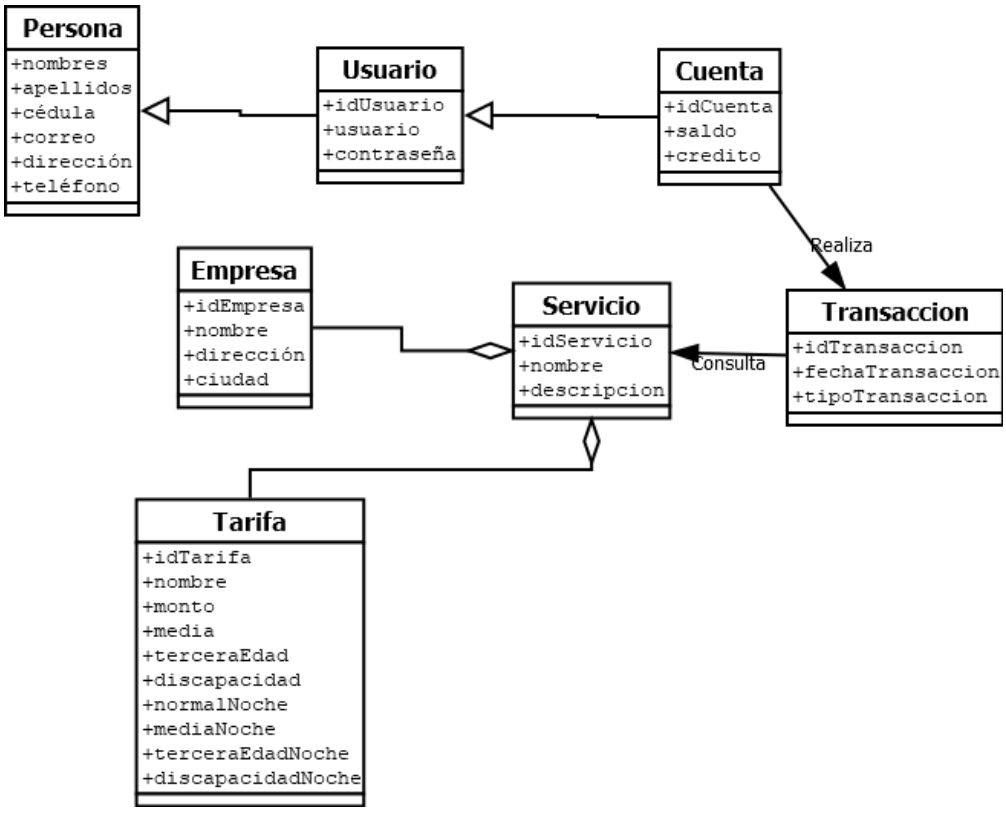

Figura 12: Diagrama de clases

6.2.2.3. Modelo Entidad Relación:

Sirve para mostrar las entidades y sus relaciones con las demás, estas entidades son objetos definidos por sus atributos.

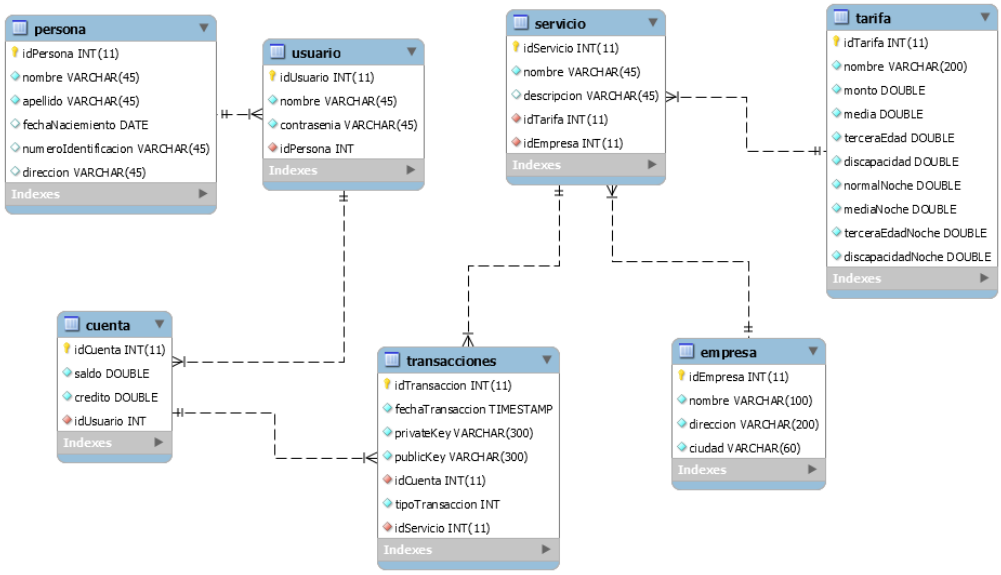

Figura 13: Diagrama entidad relación

6.2.2.4. Tarjetas Clase-Responsabilidad-Colaboración (CRC):

TABLA XXXIX: TARJETA CRC PERSONA

Persona	
Responsabilidad	Colaboración
Poseer información de persona	Usuario

TABLA XL: TARJETA CRC USUARIO

Usuario	
Responsabilidad	Colaboración
Poseer información personal Registrar cuenta Consultar datos de la cuenta Actualizar datos de la cuenta Realizar transacciones Consultar historia de transacciones	Persona cuenta

TABLA XLI: TARJETA CRC CUENTA

Cuenta	
Responsabilidad	Colaboración
Poseer información de usuario Realizar transacciones	Usuario Transacciones

TABLA XLII: TARJETA CRC TRANSACCIÓN

Transacción	
Responsabilidad	Colaboración
Poseer los datos de la transacción Realizar las transacciones de pago	Cuenta Servicio

TABLA XLIII: TARJETA CRC SERVICIO

Servicio	
Responsabilidad	Colaboración
Poseer los datos del servicio Poseer una tarifa	Transacciones Empresa Tarifa

TABLA XLIV: TARJETA CRC EMPRESA

Empresa	
Responsabilidad	Colaboración
Poseer los datos de la empresa Poseer un servicio	Servicio

TABLA XLV: TARJETA CRC TARIFA

Tarifa	
Responsabilidad	Colaboración
Poseer los datos de la transacción	servicio

6.2.2.5. Prototipo de la aplicación:

se presenta el prototipo realizado para la aplicación móvil a desarrollar en el presente TT.

Figura 14: Prototipo de pantalla de inicio de sesión

Figura 15: Prototipo de pantalla de registro de usuario

Figura 16: Prototipo de la pantalla en donde se muestra el saldo del usuario

Figura 17: Prototipo de la pantalla de realizar pago

6.2.3. Desarrollo de la aplicación (Fase de codificación)

Una vez que se realizó el diseño de la aplicación, en esta fase se procede a realizar la codificación de la misma. Para el desarrollo se utilizó el lenguaje de programación Java junto con el IDE Android Studio.

6.2.3.1. Selección de tecnologías:

Para la construcción del sistema se tomó en cuenta algunos parámetros considerados importantes, como el tiempo de desarrollo disponible para finalizar el software, los conocimientos del desarrollador y la facilidad de implementación utilizando la tecnología. En base a estos parámetros en la TABLA XLVI se definen las tecnologías seleccionadas por el desarrollador para la construcción del software, puesto que son las que mejor se acoplan a los parámetros antes mencionados.

TABLA XLVI: TECNOLOGÍA DE DESARROLLO UTILIZADAS

Tecnologías de desarrollo de software			
Software	Lenguaje de programación	Framework/Kit/Entorno	IDE
Aplicación móvil	Java	Android	Intellij IDEA
Servidor Node JS	JavaScript	Node JS	Visual Studio Code
Base de datos	SQL	MySQL	workbench
Programa Arduino	C++	Librería de los sensores	Arduino IDE

6.2.3.2. Patrón de Programación:

Se utilizó el modelo de programación Modelo-Vista-Controlador para poder separar los datos, las vistas y la lógica de negocio.

Para el desarrollo del servidor Node JS se utilizó un patrón modificado de MVC por el desarrollador, que se divide en Network direcciones de recursos apuntando a las funciones; controllers en donde se realizar la lógica y se definen las consultas SQL, este patrón modificado, así como el MVC mantiene cada una de las funcionalidades del servidor separadas y ordenadas.

Para la base de datos no se utilizó ningún patrón, en este caso se buscó realizar las consultas SQL de la forma más eficiente.

El desarrollo del programa para el arduino Mega2560 se basa en la estructura definida por defecto de la tecnología que consiste en declaración y definición de variables y librerías, setup() para la configuración e inicialización de funciones y loop() para la ejecución secuencial de los procesos.

6.2.3.3. Codificación de la aplicación móvil:

En la aplicación móvil se encuentran codificados los módulos de autenticación, registro y gestión del perfil del usuario, realización de transacciones de pago y por último el historial de transacciones. La misma que cuenta con la siguiente estructura:

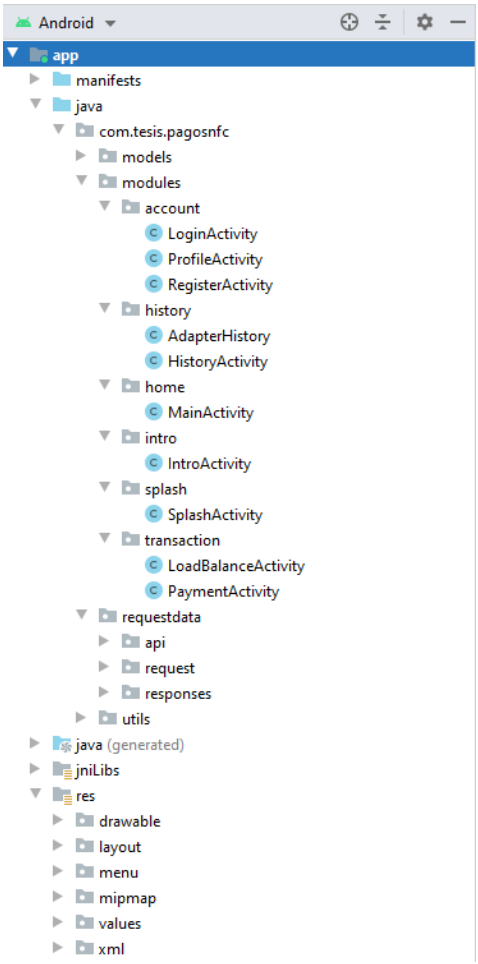

Figura 18: Estructura de la aplicación móvil

Lo primero que hace la aplicación al comenzar una transacción nueva de pago es generar la clave pública y privada para el intercambio de la clave a través de Diffie

Hellman, esto se encuentra en el método “onCreate” de la actividad “PaymentActivity” (Ver Figura 9).

```
@Override
protected void onCreate(@Nullable Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_payment);
    ButterKnife.bind(this);
    secret_key = ECDHCurve25519.generate_secret_key(random); //Llave privada
    public_key = ECDHCurve25519.generate_public_key(secret_key); //Llave publica

    serviceApduConnection = new ServiceConnection() {...};
    miContador = new MiContador(31000, 1000, new MiContador.CountListener() {...});
    miContador.start();
}
```

Figura 19: Porción de código, cómo se generan las claves pública y privada

Cuando el lector NFC intenta llamar a la aplicación, se recibe por un servicio que hereda de la clase “HostApduService” y se comunica con la vista principal a través de un Broadcast a continuación se puede ver la porción de código que se encarga de esta acción.

```
@Override
public byte[] processCommandApdu(byte[] commandApdu, Bundle extras) {
    LocalBroadcastManager lbm = LocalBroadcastManager.getInstance(getApplicationContext());
    Intent intent = new Intent(ACTION_PPSE_APDU_SEND);
    if (Arrays.equals(SELECT_APDU, commandApdu)) {
        intent.putExtra(NAME_KEY_ACTION, ACTION_PPSE_APDU_SELECT);
        messageCounter = 0;
    } else if (messageCounter == 0) {
        messageCounter++;
        intent.putExtra(NAME_KEY_ACTION, ACTION_PPSE_APDU_SEND_Pk);
        intent.putExtra("arduino_public_key", commandApdu);
    } else if (messageCounter == 1) {
        messageCounter++;
        intent.putExtra(NAME_KEY_ACTION, ACTION_PPSE_APDU_SEND_DATA);
        intent.putExtra("cipher_text", commandApdu);
    } else if (messageCounter == 2) {
        messageCounter++;
        intent.putExtra(NAME_KEY_ACTION, ACTION_PPSE_APDU_SEND_RESPONSE);
        intent.putExtra("response", commandApdu);
        if (messageCounter == 3){
            messageCounter = 0;
        }
    }
    lbm.sendBroadcast(intent);
    return null;
}
```

Figura 20: Porción de código que muestra como recibe la aplicación un comando

Al recibir a través del Broadcast la acción “ACTION_PPSE_APDU_SEND_PK” comienza el intercambio de claves desde el Arduino a la aplicación, en la aplicación móvil se crea el secreto compartido (shared_secret).

```
case ACTION_PPSE_APDU_SEND_Pk: //Arduino envía llave pública
    arduino_public_key = intent.getByteArrayExtra("arduino_public_key");
    if (arduino_public_key != null) {
        shared_secret = ECDHCurve25519.generate_shared_secret(
                secret_key, arduino_public_key);
        sendResponseApdu(public_key);
    } else {
        sendResponseApdu(UNKNOWN_CMD_SW);
    }
    break;
```

Figura 21: Porción de código que muestra cómo se realiza el intercambio de claves desde Android

Cuando recibe la acción “ACTION_PPSE_APDU_SEND_DATA” en la aplicación móvil se deriva la clave desde el secreto compartido utilizando SHA256 la cual será utilizada para la encriptación con AES, de igual manera se crear y encripta la trama enviada al Arduino (Ver Figura 22).

```
case ACTION_PPSE_APDU_SEND_DATA:
    byte[] cipherText = intent.getByteArrayExtra("cipher_text"); //Texto encriptado
    if (cipherText != null) {
        byte[] iv = {
                0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x01,
                0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x01,
        };
        derive_key = SHA256(shared_secret);
        String textoDecrypt = decrypt(cipherText, iv, derive_key);
        String[] split = textoDecrypt.split(">>");
        int length = 0;
        if (split.length >= 2) {
            length = Integer.parseInt(split[1]);
            textoDecrypt = textoDecrypt.substring(0, length);
        }
        JSONObject jsonUserData = null;
        try {
            JsonParser parser = new JsonParser();
            JsonElement jsonElement = parser.parse(textoDecrypt);
            jsonUserData = new JSONObject(jsonElement.toString());
            if (jsonUserData.has("nombre") && jsonUserData.has("monto")) {...}
        } catch (JSONException e) {
            e.printStackTrace();
        } catch (Exception e) {
        }
        //Data a encriptar
        String data = "\"idUser\":" +
                new SessionManager(getApplicationContext()).getSession().getIdUsuario() +
                ", \"nombre\":\"" +
                new SessionManager(getApplicationContext()).getSession().getNombre() + "\"";
        data += ">>" + data.length() + "<<";
        byte[] userDataCipher = encrypt(data, iv, derive_key, getApplicationContext());
        sendResponseApdu(userDataCipher);
    } else {
        sendResponseApdu(UNKNOWN_CMD_SW);
    }
    break;
```

Figura 22: Proción de código que muestra la desencriptación y encriptación en la transacción de pago

6.2.3.4. Codificación del Servicio Web API-REST:

El desarrollo del servicio Web API-REST es parte fundamental donde se controla la lógica del negocio. La aplicación cuenta con la siguiente estructura:

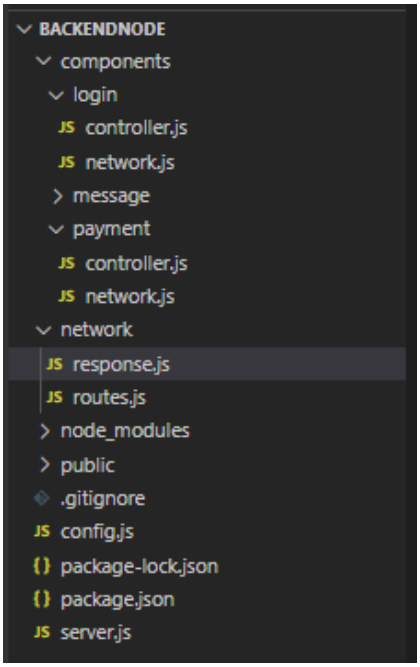

Figura 23: Estructura API-REST

Una de las partes más importantes de código dentro del servidor son las funciones que realizan una solicitud a la base de datos, extrae los registros y devuelve una respuesta al cliente en este caso la aplicación móvil o el lector NFC.

```
function transaction(idUser, idServicio){
    return new Promise((resolve, reject) => {
        var queryUpdate, querySearchAccount, querySelectMount, queryTransaction, queryGetTokenFirebase;
        querySearchAccount = "SELECT * " +
        "FROM pagosnfc.cuenta u INNER JOIN pagosnfc.usuario c ON c.idUsuario = u.idUsuario " +
        "WHERE u.idUsuario= ?;"

        querySelectMount = "SELECT t.monto, t.nombre as nombreServicio, e.nombre as nombreEmpresa from
        pagosnfc.tarifa t INNER JOIN pagosnfc.servicio s ON s.idTarifa = t.idTarifa INNER JOIN pagosnfc.
        empresa e ON s.idEmpresa = e.idEmpresa  WHERE s.idServicio = ?;"

        queryUpdate = "UPDATE `pagosnfc`.`cuenta` SET `saldo` = (saldo - ?) WHERE (`idCuenta` = ?);";

        queryTransaction = "INSERT INTO `pagosnfc`.`transacciones` (`idCuenta`, `idServicio`) VALUES (?, ?)
        ;"

        queryGetTokenFirebase = "SELECT * FROM pagosnfc.dispositivo WHERE idUsuario = 1;";

        configuraciones.ejecutarSQLCallback(querySearchAccount, idUser, (resAccount)=>{
            if(resAccount.length){
                if(resAccount[0]['saldo'] <= 0){
                    reject("No cuenta con el saldo suficiente para realizar esta transaccion");
                } else {
                    configuraciones.ejecutarSQLCallback(querySelectMount, idServicio, (resMount)=>{
                        if(resMount.length){
                            configuraciones.ejecutarConfirmacionSQL(queryUpdate, [resMount[0]['monto'],
                            resAccount[0]['idCuenta']], (resUpdate)=>{
                                configuraciones.ejecutarConfirmacionSQL(queryTransaction, [resAccount[0]
                                ['idCuenta'], idServicio], (resTransaction)=>{
                                    configuraciones.ejecutarSQLCallback(queryGetTokenFirebase, idUser,
                                    (resTk)=>{
                                        if(resTk.length){
                                            resTk.forEach(item => {
                                                enviarNotificacion(item['tokenFirebase'], "Transaccion
                                                realizada correctamente", "Se realizo un pago en " +
                                                resMount[0]['nombreEmpresa'] + " por " + resMount[0]
                                                ['nombreServicio'] , {
                                                    t: 1
                                                });
                                            });
                                        }
                                    });
                                    resolve("Pago realizado correctamente");
                                }, (confirmacion)=>{
                                    console.log(confirmacion);
                                    reject("Se produjó un error al realizar la transacción, transaccion no
                                    registrada");
                                });
                            }, (confirmacion)=>{
                                console.log(confirmacion);
                                reject("Se produjó un error al realizar la transacción, no se pudo hacer
                                el cobro");
                            });
                        } else {
                            reject("No cuenta con el saldo suficiente para realizar esta transaccion");
                        }
                    });
                }
            }
        });
    });
};
```

Figura 24: Código de función transacción de pago

En la Figura 25 se muestra el resultado de una petición HTTP hacia el servidor REST, el cual indica la URL con el método POST, que indica el saldo actual del usuario. El

servicio web se encarga de procesar la petición y envía a la aplicación cliente un objeto de tipo Json, que está compuesto por message, error, saldo (datos requeridos).

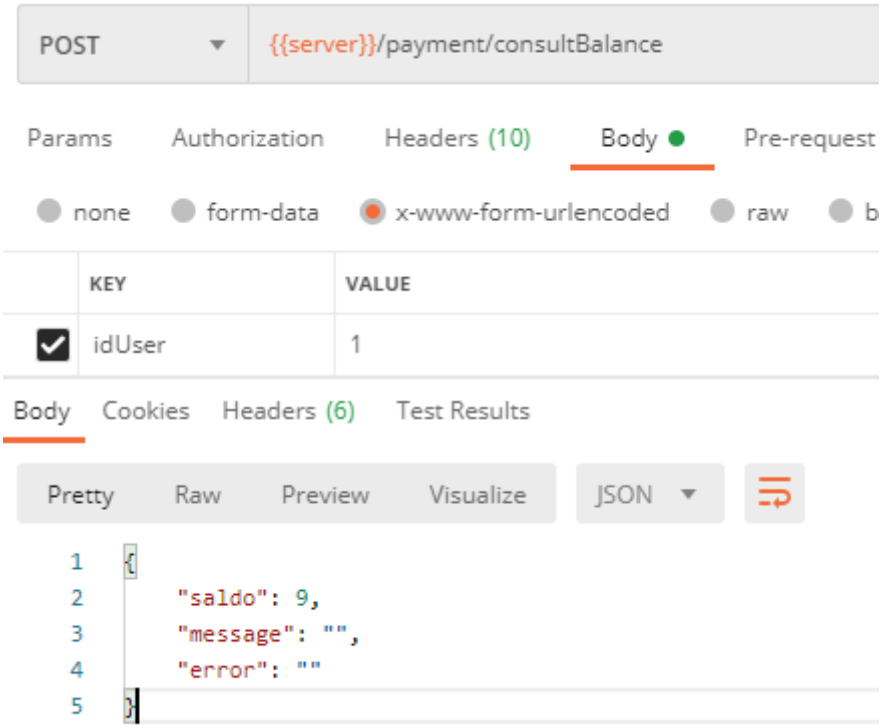

Figura 25: Resultado de la petición HTTP al API-REST

6.2.4. Implementación del algoritmo seleccionado

Para poder seleccionar la curva que se utilizaría en la implementación de la criptografía desde el dispositivo móvil con NFC hacia el lector, teniendo en cuenta el hardware a utilizar en el sistema de acuerdo a [36] en donde se indica las altas velocidades para el software de intercambio de claves Diffie-Hellman de curva elíptica segura de 128 bits en tres arquitecturas de microcontroladores populares diferentes, en donde se utiliza como curva elíptica la denominada Curva 25519.

En los estudios obtenidos en la RSL de este TT que utilizan ECC, se utiliza el intercambio seguro de claves denominado Elliptic Curve Diffie Hellman (ECDH), y AES para la encriptación de los datos.

6.2.4.1. Implementación de la curva 25519 en Android:

Para la implementación de está curva en la aplicación móvil fue necesario utilizar la librería externa llamada ECDH-Curve25519-Mobile [37], esta librería suple la falta de

implementación de los métodos necesarios de la propia API de Java en su paquete de java.security, en [8] se menciona que esta tiene limitaciones claras a la hora de generar curvas elípticas.

6.2.5. Análisis e implementación del Sistema de pagos

Con el propósito de demostrar el funcionamiento de la aplicación móvil dentro de un entorno simulado, se desarrolló un sistema de pagos como escenario de pruebas, el mismo que consta en la parte de Hardware por un Arduino mega 2560 conjuntamente con un módulo NFC PN532 y un módulo SIM900, a continuación, se procede a describir el proceso de análisis y desarrollo del mismo.

6.2.5.1. Distribución de sensor NFC PN532:

En la TABLA XLVII se muestra la distribución de las conexiones entre la placa Arduino Mega 2560 y el sensor NFC PN532. En este caso el módulo se trabajó en el modo HSU (Uart de alta velocidad), por ende, se necesitan solo 4 cables para su conexión, para el control se utilizó la librería PN532_HSU desarrollada por el mismo fabricante con el fin de no tener algún problema de compatibilidad durante el transcurso del desarrollo del sistema.

TABLA XLVII: CONEXIÓN DE PINES ENTRE ARDUINO MEGA Y SENSOR NFC

Sensor NFC PN532	**Arduino Mega 2560**	**Descripción**
GND	GND	Conexión a tierra entre el Arduino y el sensor nfc PN532
VCC	VCC	Conexión que sirve para proveer de energía al sensor nfc PN532 desde el Arduino
TX	RX3	La conexión entre estos pines sirve para establecer la comunicación por software serial entre el Arduino y el sensor NFC PN532
RX	TX3	

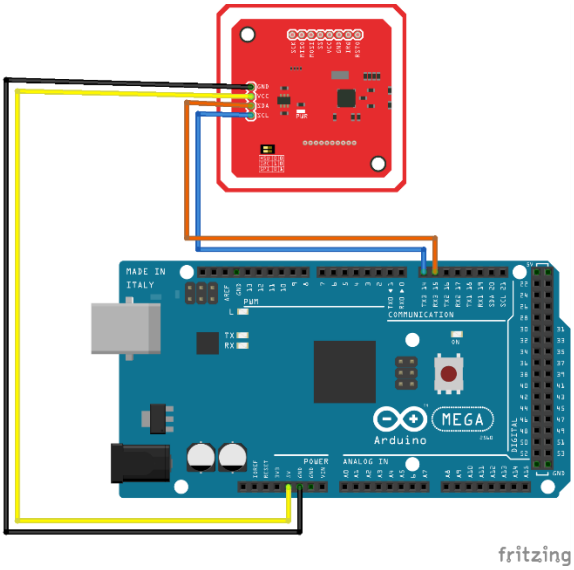

Figura 26: Esquema de la conexión del Arduino Mega 2560 y el sensor NFC PN532

6.2.5.2. Distribución de sensor SIM900:

En la TABLA XLVIII se muestra la distribución de las conexiones entre la placa Arduino Mega 2560 y el sensor NFC. Este módulo sirvió principalmente para la comunicación con el servidor, una vez que se termina el proceso de intercambio de llaves, encriptación y desencriptación de datos se procede a utilizar comandos AT para indicarle al sensor como enviar los datos, por esto no fue necesario importar alguna librería, la alimentación de es externa, puesto que el Arduino Mega ya se encuentra alimentando al Módulo NFC.

TABLA XLVIII: CONEXIÓN DE PINES ENTRE ARDUINO MEGA Y SENSOR NFC

Sensor SIM900	**Arduino Mega 2560**	**Descripción**
GND	GND	Conexión a tierra entre el Arduino y el sensor SIM900 PN532
VCC	_	Conexión que sirve para proveer de energía al sensor SIM900 desde una fuente de energía
TX	RX2	La conexión entre estos pines sirve para establecer la comunicación por software serial entre el Arduino y el sensor SIM900
RX	TX3	

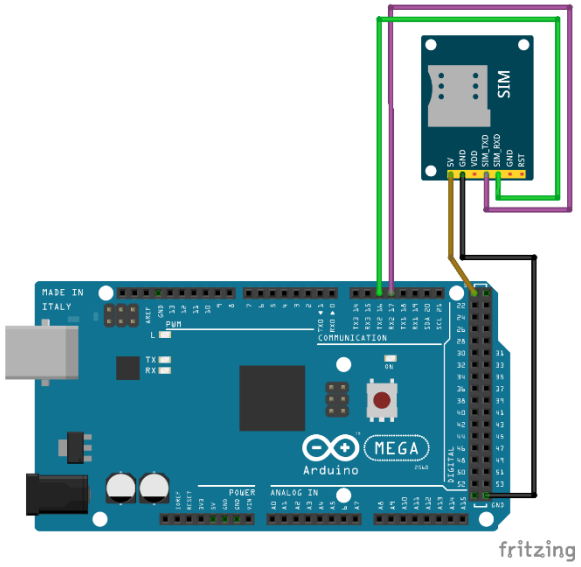

Figura 27: Esquema de la conexión del Arduino Mega 2560 con el sensor SIM900

6.2.5.3. Codificación de la aplicación Arduino:

Al iniciar el bucle (loop) lo primero que se hace es generar la clave pública y privada para el intercambio de la clave a través de Diffie Hellman (Ver Figura 28).

```
static uint8_t alice_k[32];
static uint8_t alice_f[32];
Curve25519::dhl(alice_k, alice_f);
```

Figura 28: Porción de código que muestra cómo se generan las claves pública y privada en Arduino

A continuación, se describe el protocolo ECDH: posterior a enviar la clave pública desde Arduino, se recibe una desde el dispositivo móvil con la que se genera un secreto compartido para luego derivar la llave que se utiliza con AES para encriptar los datos, en la Figura 29 se observa la porción de código que realiza este proceso.

```
//2. Enviar la clave publica al dispositivo movil
success = nfc.inDataExchange(alice_k, sizeof(alice_k), response2, &responseLength2);
if(success) {
  Serial.print("responseLength: "); Serial.println(responseLength2);
  nfc.PrintHexChar(response2, responseLength2);
  if(!Curve25519::dh2(response2, alice_f)){ //Generar secreto compartido
    return;
  }
  SHA256 sha256;
  sha256.update(response2, AES_KEY_LENGTH);
  sha256.finalize(keyHash, AES_KEY_LENGTH); //Generar clave AES
  byte iv_cbc[] = {
      0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x01,
      0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x01
  } ;

  byte cipher [padedLength] ;
  byte decrypted[padedLength];

  /*Padding data*/
  pad = aes.calc_pad(padedLength);
  size = aes.calc_size(padedLength, pad);
  byte plain_p[size];
  aes.padPlaintext(plain,plain_p, size, pad);

  cbc.setKey(keyHash, sizeof(keyHash));
  cbc.setIV(iv_cbc, sizeof(iv_cbc));
  cbc.encrypt(cipher, plain_p, padedLength);
```

Figura 29: Porción de código que describe el protocolo ECDH en Arduino

6.2.5.4. Implementación del Sistema de Pago:

Una vez realizada la instalación de los sensores, se procedió a codificar la lógica necesaria para la comunicación segura con el dispositivo móvil utilizando tecnología NFC, para utilizar Curvas Elípticas (ECC) se utilizó la librería Crypto, misma que cuenta con todos los métodos y funciones necesarias para poder realizar el intercambio de claves utilizando Elliptic-curve Diffie-Hellman (ECDH) y para la derivación de una clave se utilizó SHA256, necesaria para utilizar con el algoritmo de encriptación simétrico AES.

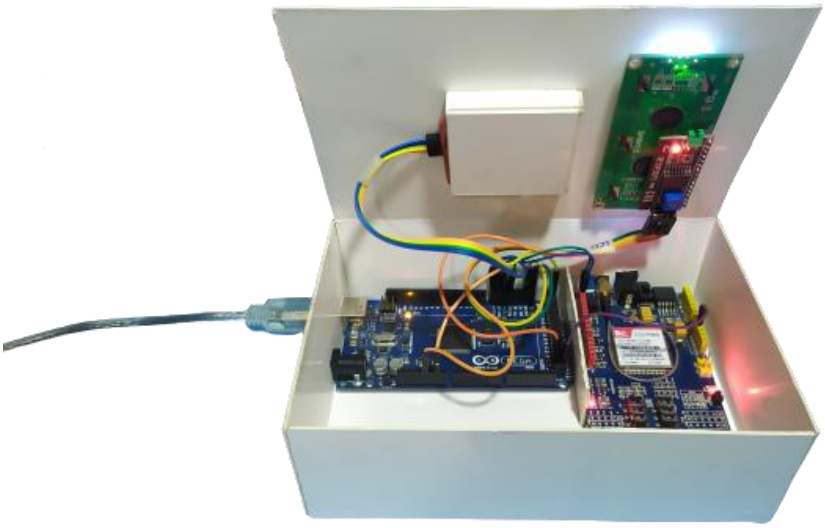

Figura 30: Implementación de Sistema de Pagos (Vista interna)

Figura 31: Implementación de Sistema de Pagos (Vista externa)

Figura 32: Implementación del Sistema de Pagos (Resultado final)

6.2.5.5. Registro de información de una transacción de pago:

A continuación, se muestra en un diagrama de bloques en donde indica como la información viaja y es procesada por los diferentes elementos que conforman el sistema de pagos.

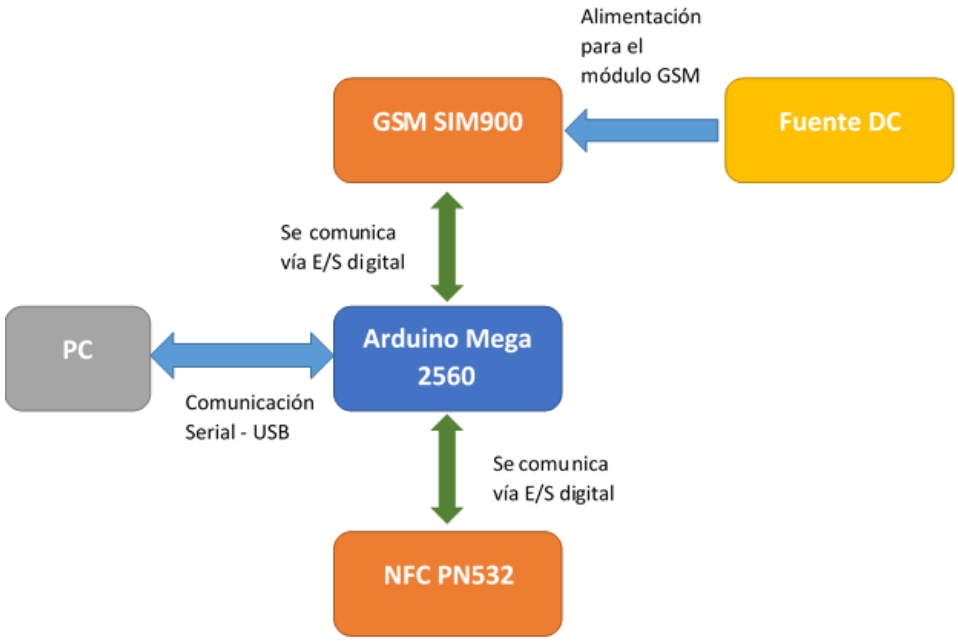

Figura 33: Diagrama de bloques del procesamiento de información

6.3. Fase 3: Realización de pruebas

En esta fase se realiza las pruebas necesarias para demostrar la seguridad del algoritmo de encriptación ECC seleccionado en el presente TT, se planteó dos casos de prueba denominados “inseguro” y “seguro” respectivamente, para lo cual fue necesario implementar un escenario compuesto por un dispositivo móvil con la aplicación desarrollada y un lector, para la parte del lector se utilizó un Arduino Mega 2560 conjuntamente con el módulo PN532 como receptor NFC y el módulo SIM900 para la conexión con el servidor.

6.3.1. Análisis de los requisitos de prueba

El objetivo principal de esta fase es demostrar la seguridad al utilizar el algoritmo basado en curvas elípticas (ECC) (Ver la sección 6.1). Para poder realizar las pruebas se montó un escenario, el cual consta de hadware y software que servirán para el propósito general de la presente fase, en la Figura 34 se muestra el flujo de procesos de una transacción de pago en el escenario propuesto.

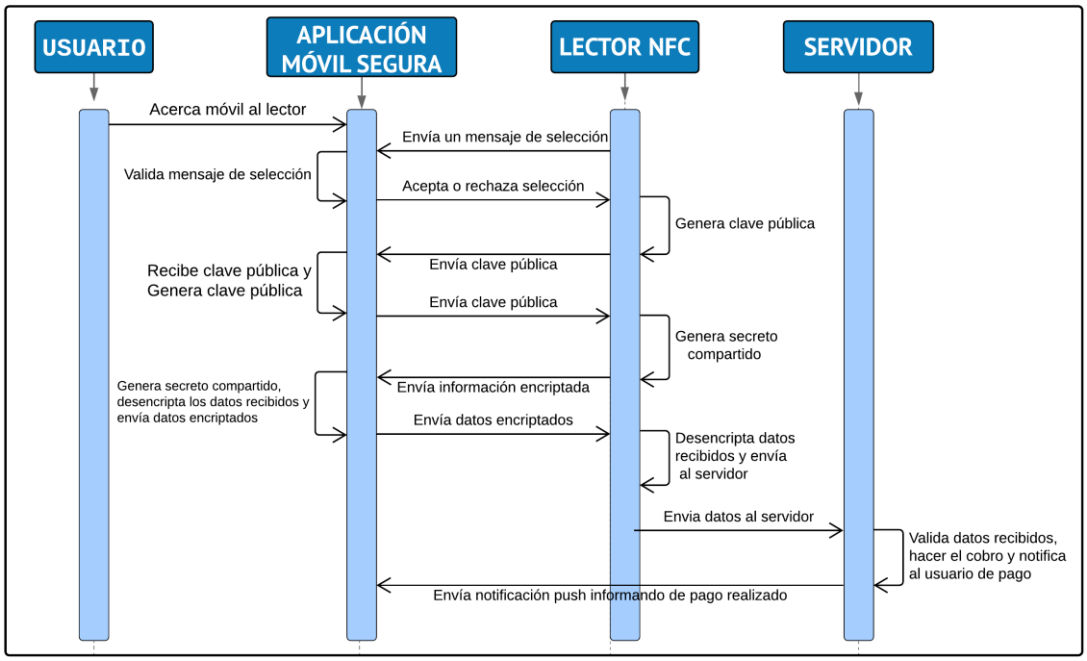

Figura 34: Flujo de procesos transacción de pagos segura utilizando dispositivo móvil con tecnología NFC

Para poder realizar un análisis estadístico de las vulnerabilidades reducidas utilizando ECC, se debe tener en cuenta la información que podría verse mayormente afectada durante un ataque, en la TABLA XLIX se muestran los datos involucrados en una transacción de pago agrupados por tipo de información, por ejemplo, los datos del usuario donde se encuentran el id de usuario y el nombre.

TABLA XLIX: INFORMACIÓN POSIBLEMENTE VULNERABLE

Información	**Tipo de información**	**Cantidad**
Datos del usuario	ID de usuario y nombre	2
Datos del pago	Monto a pagar	1
Datos de la empresa que cobra	Nombre, servicio	2
Datos de la aplicación	Claves púbicas	2

La tabla L, establece como se califica el nivel de integridad de la información en los casos de prueba, de acuerdo a los niveles establecidos en el estudio realizado en [2].

TABLA L: NIVEL DE INTEGRIDAD DE LA INFORMACIÓN

Nivel	Valor	Descripción
1	Nulo	Datos vulnerables
2	Bajo	Datos sensibles expuestos
3	Medio	Datos no relevantes expuestos
4	Alto	Datos sin riesgo

Donde:

- **Nivel 1:** La información es vulnerada en su totalidad
- **Nivel 2:** La información sensible es expuesta
- **Nivel 3:** La información no relevante es expuesta durante un ataque
- **Nivel 4:** La integridad de la información se encuentra intacta

6.3.2. Generar un plan de pruebas

Para el desarrollo de esta actividad se plantean dos casos de prueba:

- **Primer caso:** este caso será denominado “inseguro”, en la que se analizará la aplicación móvil de pago que utiliza la tecnología NFC donde no se toma en cuenta un mecanismo de seguridad.
- **Segundo caso:** este caso será denominado “seguro”, puesto que se analizará la aplicación móvil de pago que utiliza la tecnología NFC implementando el algoritmo de seguridad basado en curvas elípticas 6.1.6, para garantizar la integridad de los datos.

Las fases que se plantean para el análisis de las vulnerabilidades presentes en la tecnología NFC fueron:

- Simular un ataque
- Análisis de ataque NFC
- Aplicación de algoritmo criptográfico basado en Curvas Elípticas (ECC)
- Análisis comparativo de los resultados del escenario de pruebas

6.3.3. Desarrollar escenario de prueba

6.3.3.1. Escenario de prueba

El estudio realizado en [38] analiza los tipos de ataques para NFC y, de acuerdo a su investigación los ataques basados en man in the middle no son efectivos por las cortas distancias que se manejan en esta tecnología y la velocidad a la que se envían los datos, por lo que se decidió realizar este escenario basado en el indicador "Captura de información o data sniffing" (Ver Sección 4.4.1 de Revisión de Literatura), se realizó la simulación de un ataque de esta manera, en la TABLA LI se describen los instrumentos utilizados en el mismo.

TABLA LI: CASOS DE PRUEBA

Tipo caso	Implementos usados	Ataque
Caso inseguro	Aplicación móvil y lector NFC sin seguridad, conexión usb a Arduino	Captura de información (Data Sniffing)
Caso seguro	Aplicación móvil y lector NFC utilizando algoritmo criptográfico, conexión usb a Arduino	Captura de información (Data Sniffing)

- **Descripción de la simulación del ataque:** para la simulación de este ataque se utilizó la entrada usb del Arduino como acceso, luego se realizó los casos planteados para el escenario utilizando el Software Hércules para poder observar la transmisión de datos.

6.3.4. Ejecución de las pruebas

Para el desarrollo de esta actividad se utilizó dos variantes de la aplicación desarrollada, una no tiene encriptación alguna para fines de prueba y otra tiene la implementación con el objetivo de realizar el test necesario para los cálculos estadísticos que servirán como resultado de la fase de pruebas.

6.3.4.1. Caso de prueba inseguro

En este punto se muestran los resultados obtenidos en el caso propuesto, en el cual la comunicación del lector y el móvil con NFC no se encuentra asegurada por el algoritmo

criptográfico. En la Figura 35, se observa como luego de encontrar una nueva tarjeta NFC (en este caso la aplicación), se obtienen los datos {“idservicio”:1, “nombre”: PayAll, “monto”:1} que son compartidos desde el Arduino, luego se obtiene {“idUser”:1, “nombre”: “Nixon”} que son los datos compartidos desde el dispositivo móvil, estos datos podrían ser utilizados para hacer la suplantación como emisor o receptor de información.

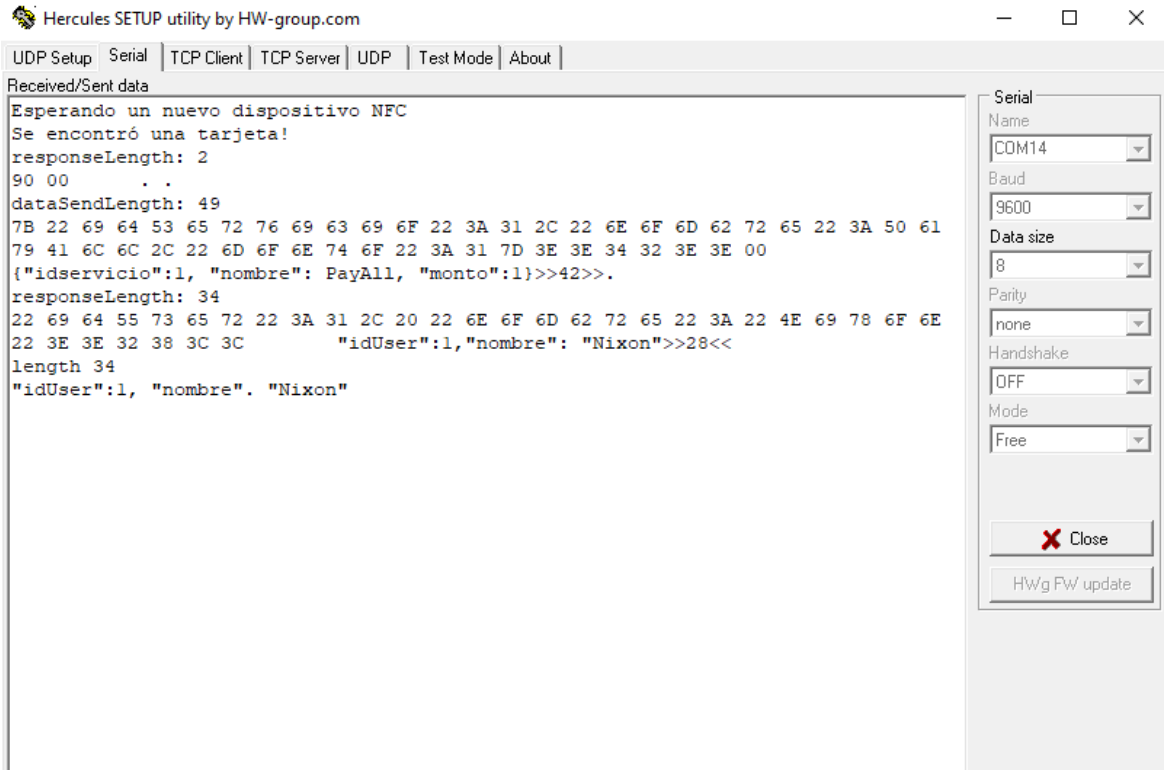

Figura 35: Captura de los datos sin seguridad en el monitor de serie Hercules

TABLA LII: DATOS DEL CASO INSEGURO

Caso	Información expuesta	Nivel
Caso inseguro	Datos del usuario	1
	Datos del pago	1
	Datos de la empresa que cobra	1

En la TABLA LII se indica el nivel de integridad de los datos obtenidos, en los cuales se observa que todos tiene un valor de 1 indicando que, la información es vulnerada en su totalidad TABLA L.

6.3.4.2. Caso de prueba seguro

En este apartado se muestra los resultados obtenidos del caso seguro, en donde se ha implementado el algoritmo de encriptación en la comunicación entre el lector y el dispositivo móvil con NFC.

En la Figura 36 se observa que, se obtiene datos representados en hexadecimal y con algunos caracteres imprimibles, esto es ocasionado por ECC, esta información se encuentra protegida contra ataques de captura.

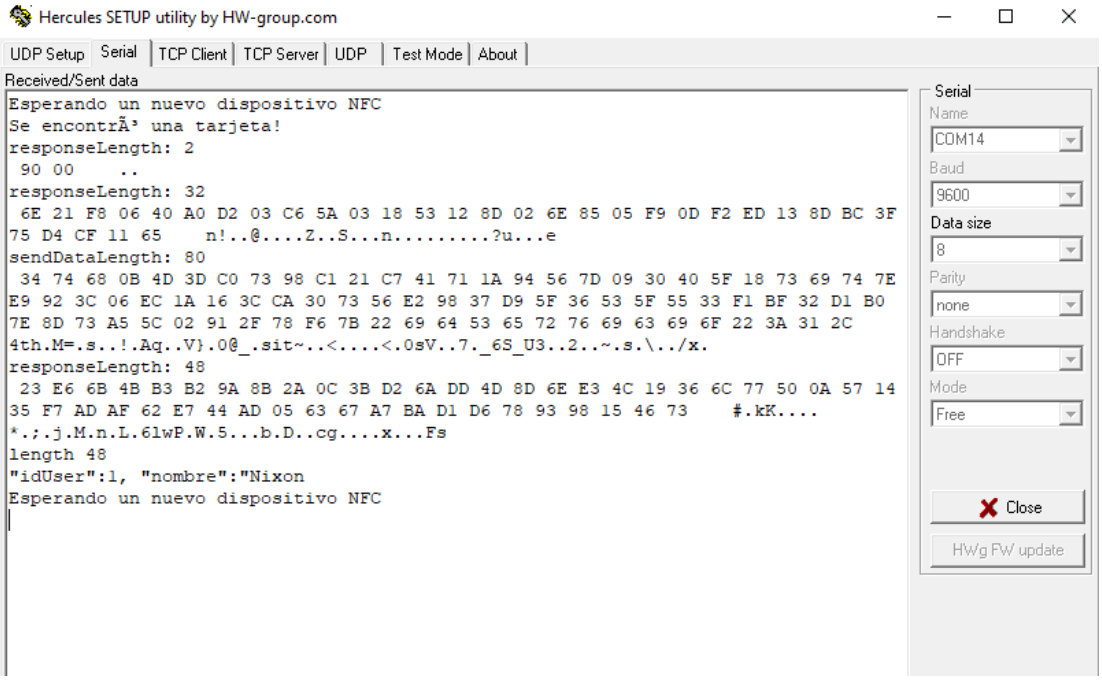

Figura 36: Captura de los datos con seguridad en el monitor de serie Hercules

En la TABLA LIII se indica el nivel de integridad de los datos obtenidos, en los cuales se observa valores de 4 indicando que, la información se encuentra sin riesgos, y 3 indica que se existen datos no relevantes expuestos (Ver TABLA L).

TABLA LIII: DATOS DEL CASO SEGURO

Caso	Información expuesta	Nivel
Caso seguro	Datos del usuario	4
	Datos del pago	4
	Datos de la empresa que cobra	4
	Datos de la aplicación	3

6.3.5. Presentación de resultados

Para poder representar los resultados de esta fase se tomó como punto de partida la estadística descriptiva, en donde se cuantifican los resultados de las pruebas realizadas en los casos planteados para cada uno de los indicadores definidos (Ver TABLA XLIX y TABLA L). De acuerdo a los resultados que se obtuvo en el escenario planteado y tomando en cuenta el caso de pruebas en donde se ha utilizado la implementación del algoritmo criptográfico seleccionado, se observa que es notoria la disminución de la exposición de la información con respecto al mismo caso, pero sin la implementación de la seguridad.

En la TABLA LIV se muestran la cantidad de datos vulnerables y el nivel de integridad que esto representa la (Ver TABLA L).

TABLA LIV: DATOS CONSOLIDADOS DEL ESCENARIO DE PRUEBAS

Información expuesta	App Vulnerable		App Segura	
	Cantidad	nivel	Número	Nivel
Datos del usuario	2	1	0	4
Datos del pago	1	1	0	4
Datos de la empresa que cobra	2	1	0	4
Datos de la aplicación	0	0	2	3

Tras la obtención de los resultados en el escenario de pruebas, se llevó a cabo el cálculo del promedio de los valores resultantes de los indicadores, tal como se puede ver en la TABLA LV**.**

TABLA LV: VALORES PROMEDIO DE LOS INDICADORES

Promedio	Caso	
	Vulnerable	Seguro
Cantidad de información expuesta	1.7	0.5
Nivel de integridad	1	3.75

Para poder obtener el porcentaje del nivel de integridad de los datos, se utilizó una regla de 3 obteniendo la siguiente formula:

nivel_de_integridad_mas_alto (Ver TABLA L) — 100%

promedio_nivel_de_integridad — porcentaje_nivel_de_integridad

$$porcentaje\_nivel\_de\_integridad = \frac{promedio\_nivel\_de\_integridad * 100\%}{nivel\_de\_integridad\_mas\_alto}$$

- **Caso inseguro:**

$$porcentaje\_nivel\_de\_integridad = \frac{1 * 100\%}{4}$$

$$porcentaje\_nivel\_de\_integridad = 25\% \rightarrow (P1)$$

- **Caso seguro:**

$$porcentaje\_nivel\_de\_integridad = \frac{3{,}75 * 100\%}{4}$$

$$porcentaje\_nivel\_de\_integridad = 94\% \rightarrow (P2)$$

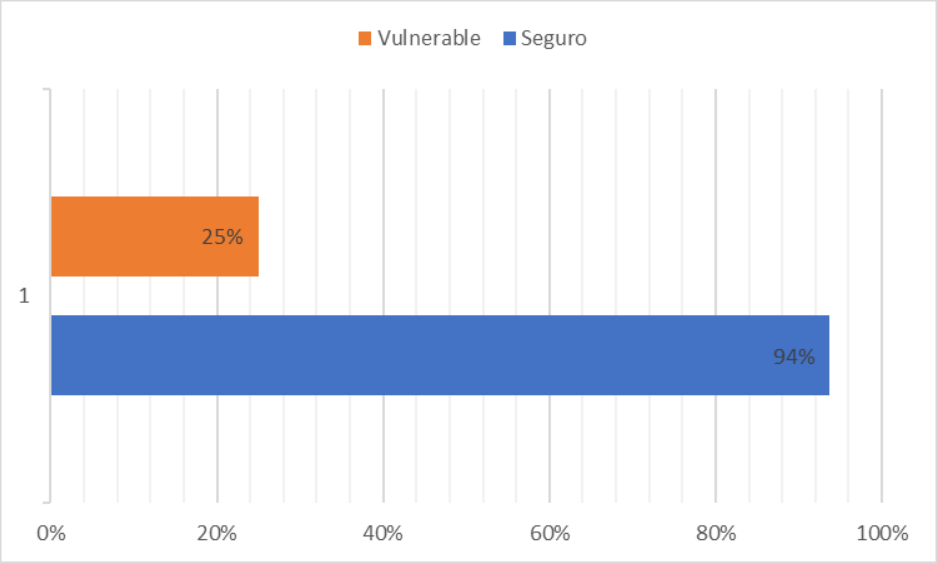

Figura 37: Porcentaje total de integridad del escenario

De acuerdo a la Figura 37 y utilizando la diferencia ($P1 - P2$), se concluye que al utilizar el algoritmo de encriptación basado en curvas elípticas seleccionado en la Sección 246.1 en una aplicación móvil de pago utilizando la tecnología NFC mejora en un 69% la integridad en el escenario propuesto para el presente TT.

6.3.6. Pruebas de rendimiento de la aplicación móvil

Las pruebas se realizaron con el servicio de Firebase Test Lab, que permiten ejecutar pruebas en diferentes dispositivos móviles, para verificar la funcionalidad y el rendimiento que tiene la aplicación móvil.

El resultado dado muestra que la aplicación móvil consume como máximo de memoria RAM 132.51 KiB, y de CPU consume el 15.63%, de red el valor máximo alcanzado es 2.257 Bytes/seg. Por tanto, este resultado indica que la aplicación no utiliza muchos recursos.

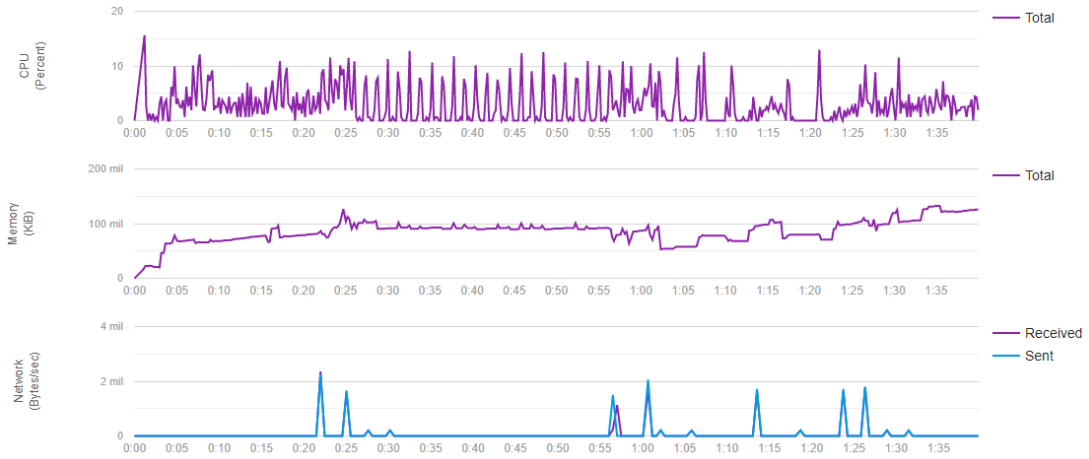

Figura 38: Resultados Test Aplicación Móvil

6.3.7. Pruebas de servidor Node JS

6.3.7.1. Pruebas de rendimiento y estrés

Para ejecutar esta sección de la fase de pruebas fue necesario utilizar la herramienta llamada Artillery [39], que es una herramienta implementada por Node JS que mediante la declaración de un fichero de configuración permite definir, el número de usuarios y peticiones que se van a simular y registrar los resultados de latencia y duración para el mínimo, máximo entre otros. Para ejecutar las pruebas se tomaron en cuenta dos parámetros importantes, el tiempo de ejecución de las pruebas (Duration), y el número de peticiones por segundo que se realizan (ArrivalRate), a continuación, se presenta una tabla con los resultados para los parámetros establecidos:

TABLA LVI: RESULTADO DE LAS PRUEBAS DE RENDIMIENTO Y ESTRÉS DEL SISTEMA

No. Fase	Duration	ArrivalRate	Resultados
1	30s	5	Escenarios lanzados: 150 Escenarios completados: 150 Peticiones completadas: 450 Latencia media: 2.6 ms Códigos de respuesta: 200: 450
2	30s	10	Escenarios lanzados: 300 Escenarios completados: 300 Peticiones completadas: 900 Latencia media: 2.3 ms Códigos de respuesta: 200: 900
3	30s	20	Escenarios lanzados: 600 Escenarios completados: 600 Peticiones completadas: 1800 Latencia media: 2.2 ms Códigos de respuesta: 200: 1800
4	30s	40	Escenarios lanzados: 1200 Escenarios completados: 1200 Peticiones completadas: 3600 Latencia media: 11.1 ms Códigos de respuesta: 200: 3600
Resultado final de peticiones			Escenarios lanzados: 2250 Escenarios completados: 2250 Peticiones completadas: 6750 Latencia media: 4.55 ms Códigos de respuesta: 200:6750

En la TABLA LVI se observa que, al aumentar el número de peticiones por segundo, también varia el tiempo de latencia media de la respuesta del servidor, en los 30 segundos delimitados para cada escenario se observa que se cumple con todas las peticiones, de igual manera se observa que se concretaron todos los escenarios que forman un total de 6750 peticiones con respuesta correcta (código 200), con una latencia media por petición de 4.55 milisegundos.

7. Discusión

En este apartado se procede a analizar cada uno de los objetivos propuestos para poder evidenciar el cumplimiento de los mismos, a continuación de describe el análisis realizado:

7.1. Desarrollo de la propuesta alternativa

7.1.1. Objetivo 1: Analizar algoritmos criptográficos que garanticen la seguridad en la transmisión de datos en NFC.

En este objetivo se analizó los algoritmos criptográficos que garanticen la seguridad en la transmisión de datos a través de la tecnología NFC, realizando una RSL (Ver Sección 6.1 de Resultados). Los documentos obtenidos en la RSL dicen que la seguridad es un pilar fundamental en los pagos que utilizan NFC como medio de transmisión, también que esta tecnología es vulnerable a ataques que afectan la seguridad de los datos transmitidos donde se encontró el uso de algoritmos criptográficos tales como: AES, 3DES y criptografía de curvas elípticas (ECC), de igual manera que el modo de operación para poder trabajar con el dispositivo móvil habilitado con NFC como medio de pago debe ser el Modo emulación de tarjeta NFC. Una vez analizadas las características de los algoritmos criptográficos se optó por utilizar la criptografía basada en curvas elípticas, debido a su gran ahorro de memoria y de procesamiento.

Este objetivo permitió principalmente conocer cuáles son los modelos y algoritmos criptográficos que se utilizan para garantizar la seguridad de los datos que se transmiten a través de la tecnología NFC, este es un punto importante dentro de este TT debido a que se pone en riesgo datos delicados que participan en la transacción de pagos.

7.1.2. Objetivo 2: Desarrollar la aplicación utilizando el algoritmo criptográfico seleccionado, que simule las transacciones de pago seguras realizadas a través de dispositivos móviles con tecnología NFC

Para el cumplimiento de este objetivo se utilizó, el Documento de Especificación de Requerimientos de Software (Ver Anexo 1), lo que ayudó a determinar los requerimientos necesarios para el desarrollo de la aplicación móvil segura, y adaptando

la metodología XP a las necesidades del presente TT se procedió a desarrollar la aplicación.

Puesto que este TT también tiene como objetivo demostrar el funcionamiento en un entorno simulado se optó por desarrollar el Sistema de Pagos utilizando hardware como Arduino y sus respectivos módulos.

7.1.3. Objetivo 3: Realizar las pruebas de funcionamiento en un entorno simulado

Para el cumplimiento a este objetivo se plantearon dos casos de prueba: uno denominado ``inseguro'' y el otro ``seguro'', en el primer caso se utilizó la aplicación móvil y el lector NFC sin seguridad, en donde se puede ver toda la información que se comunica del dispositivo hacia el lector NFC. En el segundo caso se analizó la comunicación entre el sistema de pagos y la aplicación móvil segura, puesto que en este caso ya se contaba con la implementación del algoritmo criptográfico ECC que fue de gran importancia para el intercambio de claves y así poder cifrar la información utilizando el algoritmo de encriptación simétrico AES. Se pudo evidenciar que al utilizar el algoritmo seleccionado (Ver Sección 6.3) en una aplicación móvil de pago utilizando tecnología NFC mejora considerablemente (Ver Sección 6.3.5).

7.2. Valoración técnica, económica y ambiental

7.2.1. Valoración técnica

El presente TT se valora técnicamente mediante el uso del método de RSL propuesto por Kitchenham para poder cumplir con la primera fase, así mismo con la integración de tecnologías para el desarrollo del Sistema de Pagos utilizando Arduino con los módulos NFC y SIM900, de igual manera se utilizó un dispositivo móvil con la aplicación desarrollada en este proyecto. Todas estas tecnologías hicieron posible la puesta en marcha del entorno simulado del Sistema de Pagos utilizando la tecnología NFC entre el lector y el dispositivo móvil con la aplicación segura.

7.2.2. Valoración económica

Para el desarrollo del presente TT se utilizaron recursos técnicos y económicos, a continuación, se procede a describirlos, algunos de los recursos utilizados durante el proceso de investigación son recursos libres, también existieron recursos que necesitaron realizar un pago.

En la TABLA LVII, se observan los recursos humanos que se necesitaron para el desarrollo del TT, en este caso la participación estuvo compuesta solo por el investigador y el director de TT.

TABLA LVII: RECURSOS HUMANOS

Personal	Tiempo (Horas)	Precio/hora ($)	Valor Total ($)
Investigador (Alumno)	480	$5.00	$2400.00
Director del TT	50	$12.00	$600.00
Subtotal			$3000.00

Como recursos materiales a continuación en la Tabla se detallan únicamente aquello que se utilizó para la elaboración de la memoria.

TABLA LVIII: SERVICIOS Y RECURSOS MATERIALES

Recursos	Cantidad	Valor unitario ($)	Valor Total ($)
Internet	6	$16.00	$96.00
Datos móviles	6	$16.80	$100.80
Transporte	60	$1.50	$90.00
Suministros de oficina	1	$4.00	$4.00
Subtotal			$290.80

A continuación, se detallan los recursos técnicos y tecnológicos que se utilizaron para el desarrollo de la aplicación de pago segura.

TABLA LIX: RECURSOS TECNOLÓGICOS

Recursos	Cantidad	Valor unitario ($)	Valor Total ($)
Hardware			
Computador	1	$1600.00	$1600.00
Servidor web	3 meses	$5.00	$15.00
Arduino Mega 2560	1	$20.00	$20.00
Módulo NFC PN532	1	$12.00	$12.00
Módulo GPRS/GSM	1	$12.00	$12.00
SOFTWARE			
Android Studio	1	0	0
Arduino IDE	1	0	0
Visual Code	1	0	0
Subtotal			$1659.00

Por último, se muestra un consolidado de todos los gastos realizados en la realización del presente TT.

TABLA LX: COSTO TOTAL APROXIMADO DEL PROYECTO

Recursos	Subtotal
Recursos humanos	$3000.00
Recursos materiales	$290.80
Recursos tecnológicos	$1659.00
SUBTOTAL	$4949.80
Imprevistos (5%)	$247.49
TOTAL	5197.29

7.2.3. Valoración ambiental

Se valora el proyecto ambientalmente puesto que todos los recursos utilizados son digitales, lo que permite el ahorro de los materiales derivados del papel, así mismo el proyecto en sí, incentiva al uso del dispositivo móvil para pagar utilizando la tecnología NFC lo que podría beneficiar mucho al medio ambiente puesto que no se utilizaría papel para boletos u otros medios.

8. Conclusiones

- Utilizar la metodología de revisión sistemática de literatura (RSL) propuesta por Barbara Kitchenham permitió, determinar y seleccionar el algoritmo de encriptación que se utilizaría en el TT, obteniendo como mejor resultado la criptografía basada en curvas elípticas debido a su ahorro de memoria y procesamiento.
- El estándar IEEE-830 permitió estructurar de manera clara el análisis de requerimientos, y poder plantear el alcance real de la aplicación móvil.
- Utilizar la metodología de programación XP, permitió el desarrollo ágil de la aplicación móvil, debido a su alto nivel de flexibilidad desde la fase de planeación como ayuda para la obtención de requerimientos hasta su finalización en la fase de pruebas.
- Utilizar la encriptación basada en Curvas Elípticas (ECC), incrementa considerablemente el nivel de integridad de los datos que participan en las transacciones de pago utilizando la tecnología NFC, al mitigar el acceso a los datos por parte de los atacantes y de los participantes.
- La encriptación basada en Curvas Elípticas puede ofrecer niveles de seguridad similar a otros algoritmos, pero con la peculiaridad que los tamaños de clave son relativamente más bajos, además ofrece ventajas como simplicidad, rentabilidad y bajos costos en el procesamiento.
- El intercambio de llaves Diffie-Hellman ayuda considerablemente en la creación de una clave privada entre dos dispositivos que se comunican a través de un canal inseguro.
- Los ataques man in the middle no son efectivos debido a las cortas distancias y la velocidad presentes en la transmisión de datos utilizando la tecnología NFC como medio de comunicación.
- Las librerías utilizadas de Arduino (Curve25519, CBC, AES, SHA256, PN532, LiquidCrystal_I2C) ayudaron en gran medida al desarrollo del sistema planteado, al contar con funciones preestablecidas facilitó la programación de los microcontroladores.

9. Recomendaciones

- Realizar un estudio de la información que podría verse mayormente afectada durante un ataque en un intercambio de información, esto ayudará a implementar de mejor manera un algoritmo de encriptación, evitando perdida de tiempos en desarrollos innecesarios.
- Para realizar el intercambio de claves a través de un canal de comunicación inseguro utilizar el método Diffie-Hellman.
- Utilizar la curva 25519 porque es óptimo para utilizarlo en un sistema de Internet de las cosas (IoT) debido a sus tamaños de claves y velocidad de procesamiento.
- Utilizar los mecanismos y métodos utilizados en el presente TT para asegurar la transmisión de datos en otros campos que utilicen la tecnología NFC como medio de comunicación, por ejemplo: control de acceso de personas, control de inventario, entre otros.
- Utilizar la librería ECDH-Curve25519-Mobile para implementar la encriptación basada en Curvas Elípticas puesto que en la propia API de Java en su paquete de java.security no existen los métodos necesarios.
- Aplicar medidas de seguridad a la comunicación con el servidor web para prevenir ataques DDoS y mantener protegido del acceso, uso, modificación, destrucción o interrupción no autorizada.
- Realizar una evaluación periódica de los nuevos algoritmos criptográficos, esto con el fin de evitar percances al momento de implementar una solución informática que involucre asegurar los datos utilizando.
- Utilizar una interfaz amigable, con colores llamativos que faciliten la usabilidad de la aplicación móvil.

10. Bibliografía

[1] B. Kitchenham, «Procedures for Performing Systematic Reviews».

[2] A. S. Cisneros Barahona, C. F. Castro Ortiz, M. I. Uvidia Fassler, G. N. Samaniego Erazo, C. D. Radicelli García y D. G. Barba Maggi, «Modelo de Seguridad para Garantizar la Integridad de Pagos Móviles sobre Near Field Communication (NFC),» 2018.

[3] B. O. Casilla Salazar y J. K. Guaman Ruiz, «Desarrollo de una aplicación móvil en plataforma android para la transferencia de información en las carreras tecnológicas de la facultad de ciencias matemáticas y físicas utilizando tecnología NFC,» 2016.

[4] F. Vásquez, «Desarrollo de Tecnologia NFC para medios de pago a traves de dispositivo moviles Alcatel One Touch,» 2013.

[5] J. Galán Figueroa y F. Venegas Martinez, «Impacto de los medios electronicos de pago sobre la demanda de dinero,» pp. 93-124, 2016.

[6] J. J. Herrera Mires, «Diseño e implementación de una aplicación móvil basada en la tecnología NFC para acceso a información de las piezas de arte de un museo,» p. 102, 2013.

[7] C. L. Valverde Ramírez, «Sistema De Control De Acceso De Personas Para Los Laboratorios De La Carrera De Ingeniería En Sistemas Computacionales De La Universidad De Guayaquil Utilizando Tecnología Nfc,» 2015.

[8] F. Abascal López, «Seguridad utilizando dispositivos NFC,» 2016.

[9] B. A. Arroyo Briones, G. A. Contreras Bernal y E. A. Espíritu de la Paz, «Control de acceso mediante NFC,» 2016.

[10] C. Aragonés Lacarta, «Aplicaciones para dispositivos móviles basadas en NFC para el control, gestión y monitorización de la medicación en pacientes de larga duración,» 2013.

[11] J. E. Padilla Contreras y W. A. Iñiguez López, «Near Field Communication-Teoría y Aplicaciones,» 2014.

[12] X. Chen, K. Choi y K. Chae, «A Secure and Efficient Key Authentication using Bilinear Pairing for NFC Mobile Payment Service,» 2017.

[13] CES, «Reglamento de Régimen Académico,» pp. 1-53, 2019.

[14] M. Genero Bocco, J. A. Cruz Lemus y M. G. Piattini Velthuis, «Métodos de investigación en ingeniería del software,» 2014.

[15] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner y J. L. S. Bailey, «Systematic literature reviews in software engineering - A systematic literature review,» 2009.

[16] S. M. Melendez Valladarez, M. E. Gaitan y N. N. Perez Reyes, «Metodologia Ágil De Desarrollo De Software Programacion Extrema,» 2016.

[17] J. D. Velásquez, «una Guía Corta Para Escribir Revisiones Sistemáticas de Literatura Parte 1,» vol. 81, nº 187, 2014.

[18] J. D. Velásquez, «Guía Corta para Escribir Revisiones Sitemáticas de Literatura Parte 2,» vol. 81, 2014.

[19] J. D. Velásquez, «Guía Corta para Escribir Revisiones Sitemáticas de Literatura Parte 3,» vol. 82, nº 189, 2014.

[20] J. D. Velásquez, «Guía Corta para Escribir Revisiones Sitemáticas de Literatura Parte 4,» vol. 82, nº 190, 2015.

[21] J. PT Higgins y G. Sally, «Manual Cochrane de revisiones sistemáticas de intervenciones,» 2011.

[22] J. Gonzalez Contreras y V. Vega Zepeda, «Ejecucion de una revision sistemática en mejoras de proceso de desarrollo de software para pequeñas y micro empresas,» 2011.

[23] M. C. Suntaxi Sarango, «Detección de técnicas de aprendizaje profundo aplicadas en las diferentes áreas del conocimiento, empleando el método de revisión sistemática de literatura,» 2009.

[24] N. Druml, M. Menghin, A. Kuleta, C. Steger, R. Weiss, H. Bock y J. Haid, «A flexible and lightweight ECC-based authentication solution for resource constrained systems,» 2014.

[25] S. Bojjagani y V. N. Sastry, «A secure end-to-end proximity NFC-based mobile payment protocol,» 2019.

[26] J. M. León-Coca, D. G. Reina, S. L. Toral, F. Barrero y N. Bessis, «Authentication systems using ID cards over NFC links: The Spanish experience using DNIe,» 2013.

[27] D. Veloz-cherrez y J. Suárez, «NFC-Based Payment System Using Smartphones for Public Transport Service,» 2019.

[28] Y. L. Chi, I. C. Lin, C. H. Chen y M. S. Hwang, «The Secure transaction protocol in NFC card emulation mode,» 2015.

[29] H. Eun, H. Lee y H. Oh, «Conditional privacy preserving security protocol for NFC applications,» 2013.

[30] E. Husni y A. Ariono, «Development of integrated mobile money system using Near Field Communication (NFC),» 2014.

[31] A. Al-Haj y M. A. Al-Tameemi, «Providing security for NFC-based payment systems using a management authentication server,» 2018.

[32] C. Arnosti, D. Gruntz y M. Hauri, «Secure Physical Access with NFC-enabled Smartphones,» 2015.

[33] D. Schürmann, S. Dechand y L. Wolf, «OpenKeychain: An Architecture for Cryptography with Smart Cards and NFC Rings on Android,» 2017.

[34] V. M. Sangucho Cueva, «Análisis, diseño e implementación de un sistema web, aplicando la tecnología java server faces (jsf), para la Gestión y control de transporte turístico de la compañía chrisland service and touring s.a.,» 2015.

[35] P. A. Quezada Sarmiento y S. Mengual Andrés, «Implementación de una solución web y móvil para la gestión vehicular basada en Arquitectura de Aspectos y metodologías ágiles: Un enfoque educativo de la teoría a la práctica,» 2017.

[36] M. Düll, B. Haase, G. Hinterwälder, M. Hutter, C. Paar, A. H. Sánchez y P. Schwabe, «High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers,» 2015.

[37] «ECDH-Curve25519-Mobile implements Diffie-Hellman key exchange based on the Elliptic Curve 25519 for Android devices.,» [En línea]. Available: https://github.com/duerrfk/ecdh-curve25519-mobile.

[38] E. Haselsteiner y K. BreitfuB, «Security in Near Field Communication (NFC) Strengths and Weaknesses,» 2006.

[39] R. Diaz, «Tests de rendimiento con Artillery - Adictos al trabajo,» 2018. [En línea]. Available: https://www.adictosaltrabajo.com/2018/02/22/tests-de-rendimiento-con-artillery/.

11. Anexos

11.1. Anexo 1: Especificación de requerimientos de software

Especificación de requisitos de software

Proyecto: Implementación de seguridad en las transacciones de pago realizadas a través de dispositivos móviles utilizando tecnología NFC.

Febrero del 2019

Ficha del documento

Fecha	Revisión	Autor	Verificado dep. Calidad.
	1.0	Nixon Camilo Briceño Merino	Ing. Hernán Leonardo Torres Carrión

Documento validado por las partes en fecha:

Por el encargado del departamento de informática	Por la Universidad Nacional de Loja

Contenido

Introducción

Este documento es una Especificación de Requisitos Software (ERS) para el **Prototipo de aplicación segura para realizar transacciones de pago utilizando la tecnología NFC**. Esta especificación se ha estructurado basándose en las directrices dadas por el estándar IEEE Práctica Recomendada para Especificaciones de Requisitos Software ANSI/IEEE 830, 1998.

1. Propósito

El presente documento tiene como propósito definir las especificaciones funcionales, no funcionales para el desarrollo de un prototipo que permita realizar transacciones de pago seguras a través de dispositivos móviles utilizando la tecnología NFC. Éste será utilizado por estudiantes, profesores y directivos.

2. Alcance

El alcance de la ERS comprende la definición de los requerimientos funcionales y no funcionales, como también otros aspectos que definen el producto, incluyendo objetivo del producto, restricciones, lo que el sistema no contemplará, modelo de negocio, requerimientos de interfaz, restricciones de diseño, requerimientos de licencia o componentes comprados necesarios para el producto a desarrollarse, entre otras cosas

3. Personal involucrado

Nombre	Nixon Camilo Briceño Merino
Rol	Analista, diseñador y programador
Categoría Profesional	Estudiante Universitario
Responsabilidad	Análisis de requisitos, diseño y programación
Información de contacto	ncbricenom@unl.edu.ec

4. Definiciones, acrónimos y abreviaturas

Nombre	*Descripción*
NFC	Near Field Comunication
ERS	Especificación de Requisitos Software
RF	Requerimiento Funcional
RNF	Requerimiento No Funcional

5. Referencias

Titulo del Documento	Referencia
Standard IEEE 830 - 1998	IEEE

6. Resumen

Este documento consta de tres secciones. En la primera sección se realiza una introducción al mismo y se proporciona una visión general de la especificación de recursos del sistema.

En la segunda sección del documento se realiza una descripción general del sistema, con el fin de conocer las principales funciones que éste debe realizar, los datos asociados y los factores, restricciones, supuestos y dependencias que afectan al desarrollo, sin entrar en excesivos detalles.

Por último, la tercera sección del documento es aquella en la que se definen detalladamente los requisitos que debe satisfacer el sistema.

Descripción general

7. Perspectiva del producto

El presente sistema de pago es un producto independiente que está diseñado para realizar transacciones de pago seguras a través de dispositivos móviles que utilizan la tecnología NFC, aplicando la técnica de criptografía basada en curvas elípticas.

8. Funcionalidad del producto

El siguiente prototipo permitirá realizar las siguientes funcionalidades
- Realizar el pago a través del dispositivo móvil utilizando la tecnología NFC
- Conocer a través de la aplicación el saldo con el que consta el usuario

9. Características de los usuarios

Tipo de usuario	Administrador
Formación	Estudiante Universitario
Actividades	Desarrollo y análisis

Tipo de usuario	Usuario
Formación	Cualquiera
Actividades	Manejo de la aplicación en general

10. Restricciones

- Interfaz para ser usada bajo el sistema operativo Android.
- El sistema debe tener un diseño e implementación sencillo.
- Lenguajes y tecnologías en uso: JAVA.
- El sistema debe brindar seguridad en las transacciones de pago

11. Suposiciones y dependencias

- Se asume que los requisitos aquí descritos son estables
- Los equipos en los que se vaya a ejecutar el sistema deben cumplir los requisitos antes indicados para garantizar una ejecución correcta de la misma

12. Evolución previsible del sistema

Requisitos específicos

Requerimientos Funcionales

Identificación del requerimiento:	RF01
Nombre del Requerimiento:	Autentificación de Usuario.
Características:	Los usuarios deberán identificarse para acceder a la aplicación.
Descripción del requerimiento:	Los usuario podrán acceder a la aplicación utilizando las credenciales proporcionadas con anterioridad.
Requerimiento NO funcional:	• RNF1 • RNF2
Prioridad del requerimiento: Alta	

Identificación del requerimiento:	RF02
Nombre del Requerimiento:	Registrar Usuarios.
Características:	Los usuarios deberán registrarse en la aplicación para acceder a cualquier parte de la misma.
Descripción del requerimiento:	La aplicación permitirá al usuario registrarse. El usuario debe suministrar datos como: CI, Nombre, Apellido, E-mail, Usuario y Contraseña.
Requerimiento NO funcional:	• RNF1 • RNF2
Prioridad del requerimiento: Alta	

Identificación del requerimiento:	RF03
Nombre del Requerimiento:	Consultar Información.
Características:	La aplicación ofrecerá al usuario información general sobre sus datos personales.
Descripción del requerimiento:	**Consultar perfil:** Muestra toda la información acerca de los datos personales subministrados por el usuario.
Requerimiento NO funcional:	• RNF1 • RNF2
Prioridad del requerimiento: Alta	

Identificación del requerimiento:	RF04
Nombre del Requerimiento:	Consultar Información.
Características:	La aplicación ofrecerá al usuario información general sobre el saldo existente
Descripción del requerimiento:	**Consultar Saldo:** Muestra toda la información sobre el saldo y los pagos que ha realizado el usuario.
Requerimiento NO funcional:	• RNF1 • RNF2
Prioridad del requerimiento: Alta	

Identificación del requerimiento:	RF05
Nombre del Requerimiento:	Modificar datos personales.
Características:	La aplicación permitirá al usuario modificar los datos personales.
Descripción del requerimiento:	Permite al usuario modificar sus datos personales en su cuenta creada.
Requerimiento NO funcional:	• RNF1 • RNF2
Prioridad del requerimiento: Alta	

Identificación del requerimiento:	RF06
Nombre del Requerimiento:	Integración de Componentes.
Características:	La aplicación podrá ser parte de un sistema de pagos.
Descripción del requerimiento:	La aplicación podrá coexistir con un aplicación o hardware que pueda ser la encargada de realizar las transacciones de pago.
Requerimiento NO funcional:	• RNF1 • RNF2
Prioridad del requerimiento: Alta	
Identificación del requerimiento:	RF07
Nombre del Requerimiento:	Gestionar Reportes.
Características:	El sistema permitirá generar reportes.

Descripción del requerimiento:	Permite al usuario genera un reporte sobre todos los pagos que se han realizado en cierto tiempo
Requerimiento NO funcional:	• RNF1 • RNF2
Prioridad del requerimiento: Alta	

Requerimientos No Funcionales.

Identificación del requerimiento:	RNF01
Nombre del Requerimiento:	Interfaz de la aplicación.
Características:	La aplicación presentara una interfaz de usuario sencilla para que sea de fácil manejo a los usuarios del sistema.
Descripción del requerimiento:	La aplicación debe tener una interfaz de uso intuitiva y sencilla.
Prioridad del requerimiento: Alta	

Identificación del requerimiento:	RNF02
Nombre del Requerimiento:	Ayuda en el uso de la aplicación.
Características:	La interfaz del usuario deberá de presentar un splash de ayuda para que los mismos usuarios del sistema se les faciliten el manejo de la aplicación.
Descripción del requerimiento:	La interfaz debe presentar buen sistema de ayuda, para que facilite el manejo de la aplicación.
Prioridad del requerimiento: Alta	
Identificación del requerimiento:	RNF03
Nombre del Requerimiento:	Desempeño

Características:	La aplicación garantizará a los usuarios un desempeño en cuanto a los datos almacenado en el sistema ofreciéndole una confiabilidad a esta misma.
Descripción del requerimiento:	Garantizar el desempeño del sistema informático a los diferentes usuarios. En este sentido la información almacenada o las transacciones realizadas podrán ser consultados y actualizados permanente y simultáneamente, sin que se afecte el tiempo de respuesta.
Prioridad del requerimiento: Alta	

Identificación del requerimiento:	RNF04
Nombre del Requerimiento:	Seguridad en información
Características:	El sistema garantizara a los usuarios una seguridad en cuanto a la información que se procede en el sistema y a las transacciones que son realizadas a través de la misma.
Descripción del requerimiento:	Garantizar la seguridad del sistema con respecto a la información y las transacciones que se realizan a través de la misma.
Prioridad del requerimiento: Alta	

13. Requisitos comunes de las interfaces

13.1. Interfaces de usuario

Las interfaces de la aplicación estarán compuestas por:

- Botones
- Mensajes de confirmación
- Mensajes de alerta
- Mensajes de error
- Cuadros de diálogo
- Formularios

13.2. Interfaces de hardware

Para un buen funcionamiento del software se usarán dispositivos móviles que soporten la tecnología NFC

13.3. Interfaces de software

La versión de Android necesaria para que la aplicación funciones deberá ser la 5.0 en adelante

13.4. Interfaces de comunicación

La comunicación se hará a través de la tecnología NFC, y las consultas de datos será en mediante consultas a un servidor utilizando el protocolo TCP/IP

14. Requisitos funcionales

14.1. Requisito funcional 1

- **Autentificación de Usuarios:** los usuarios deberán identificarse usando su usuario y contraseña para acceder a cualquier parte del sistema.

La aplicación mostrará mensajes de error en caso de que exista algún inconveniente al ingresar las credenciales.

14.2. Requisito funcional 2

- **Registro de Usuario:** el usuario deberá registrarse llenando un formulario que se presentará en la aplicación, si los datos introducidos (nombres y apellidos completos, cedula, celular, teléfono) no acreditan la validación, la aplicación mostrará un mensaje de error indicando cual es el dato incorrecto.

14.3. Requisito funcional 3

- **Consultar Información: Consultar perfil:** La aplicación contará con un perfil en el que se mostrará sus datos personales del usuario, si existe algún error en la consulta de los datos se mostrará un mensaje de error.

14.4. Requisito funcional 4

- **Consultar Información: Consultar saldo:** La aplicación permitirá al usuario consultar el saldo disponible, si existe algún error en la consulta se presentará un mensaje de error indicando porque se produjo el mismo.

14.5. Requisito funcional 5

- **Modificar datos personales:** La aplicación tendrá un apartado que permitirá al usuario revisar y modificar sus datos personales en caso de haber ingresado mal en la fase de registro.

14.6. Requisito funcional 6

- **Integración de componentes:** La aplicación será desarrollada para poder coexistir en un sistema de transacciones de pago ya implementado.

14.7. Requisito funcional 7

- **Gestionar reportes:** La aplicación tendrá un apartado que permitirá al usuario consultar reportes acerca de las transacciones que se han hecho a través de la aplicación.

15. Requisitos no funcionales

15.1. Rendimiento

Las transacciones y funcionalidades utilizadas a través de la aplicación deben responder al usuario en menos de 5 segundos.

15.2. Seguridad

Garantizar la confiabilidad, la seguridad y el desempeño de la aplicación a los diferentes usuarios.
Garantizar la seguridad de la aplicación con respecto a la información y datos que se manejan.
Garantizar la integridad de los datos en las transacciones que se realizan a través de la aplicación.

15.3. Fiabilidad

Garantizar que no se suspenda la aplicación al momento de realizar transacciones de pago a través del mismo.

15.4. Disponibilidad

La aplicación estará disponible para su funcionamiento cuando se necesite realizar transacciones a través de la mismas.

15.5. Mantenibilidad

A partir de la documentación con respecto a la implementación, se podrá dar el mantenimiento respectivo a la aplicación. Esta función le corresponde a un desarrollador de software.

15.6. Portabilidad

La aplicación será desarrollada exclusivamente para Android, constituyendo la versión 5.0 la base para ejecutar a partir de ella podrá funcionar en cualquier versión siempre y cuando sea superior.

11.2. Certificado de traducción del resumen

Loja, 02 de Febrero de 2021.

CERTIFICACIÓN

Yo, Yuri Silvana Correa Mijas, licenciada en "Ciencias de la Educación mención: Idioma Inglés", con cédula de ciudadanía 1104507676, por medio del presente certifico la veracidad de la traducción del resumen de la tesis titulada: Implementación de seguridad en las transacciones de pago realizadas a través de dispositivos móviles utilizando la tecnología NFC, del autor Nixon Camilo Briceño Merino.

Autorizo a la parte interesada a hacer del presente documento en lo que fuere conveniente.

Atentamente.

Licda. Yuri Silvana Correa Mijas