Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE DISPOSITIVO DE PAGO ELECTRÓNICO UTILIZANDO TARJETAS NFC CON AUTENTICACIÓN BIOMÉTRICA

Javier Andrés Rodríguez Mayén
Asesorado por la Inga. Ingrid Salomé Rodríguez de Loukota

Guatemala, septiembre de 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE DISPOSITIVO DE PAGO ELECTRÓNICO UTILIZANDO TARJETAS NFC CON AUTENTICACIÓN BIOMÉTRICA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JAVIER ANDRÉS RODRÍGUEZ MAYÉN
ASESORADO POR LA INGA. INGRID SALOMÉ RODRÍGUEZ DE LOUKOTA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, SEPTIEMBRE DE 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Jurgen Andoni Ramírez Ramírez
VOCAL V	Br. Oscar Humberto Galicia Nuñez
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Walter Giovanni Álvarez Marroquín
EXAMINADOR	Ing. Guillermo Antonio Puente Romero
EXAMINADOR	Ing. José Aníbal Silva de los Ángeles
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE DISPOSITIVO DE PAGO ELECTRÓNICO UTILIZANDO TARJETAS NFC CON AUTENTICACIÓN BIOMÉTRICA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 4 de noviembre de 2016.

Javier Andrés Rodríguez Mayén

Guatemala 19 de abril de 2017

Ingeniero
Carlos Eduardo Guzmán Salazar
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Estimado Ingeniero Guzmán.

Me permito dar aprobación al trabajo de graduación titular: ¨**Diseño de dispositivo de pago electrónico utilizando tarjetas NFC con autenticación biométrica**¨, del señor Javier Andrés Rodríguez Mayén, por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesora, nos hacemos responsables por el contenido y conclusiones del mismo.

Sin otro particular, me es grato saludarle.

Atentamente,

Inga. Ingrid Rodríguez de Loukota
Colegiada 5,356
Asesora

Ingrid Rodríguez de Loukota
Ingeniera en Electrónica
colegiado 5356

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Ref. EIME 46. 2017
Guatemala, 15 de MAYO 2017.

Señor Director
Ing. Francisco Javier González López
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: DISEÑO DE DISPOSITIVO DE PAGO ELECTRÓNICO UTILIZANDO TARJETAS NFC CON AUTENTICACIÓN BIOMÉTRICA, del estudiante Javier Andrés Rodriguez Mayén , que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

Ing. Carlos Eduardo Guzmán Salazar
Coordinador de Electrónica

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

sro

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 46 . 2017.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; JAVIER ANDRÉS RODRÍGUEZ MAYÉN titulado: DISEÑO DE DISPOSITIVO DE PAGO ELECTRÓNICO UTILIZANDO TARJETAS NFC CON AUTENTICACIÓN BIOMÉTRICA, procede a la autorización del mismo.

Ing. Otto Fernando Andrino González

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 4 DE SEPTIEMBRE 2,017.

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.D.448.2017

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica al trabajo de graduación titulado: **DISEÑO DE DISPOSITIVO DE PAGO ELECTRÓNICO UTILIZANDO TARJETAS NFC CON AUTENTICACIÓN BIOMÉTRICA,** presentado por el estudiante universitario: **Javier Andrés Rodríguez Mayén,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, septiembre, de 2017

/cc

ACTO QUE DEDICO A:

Dios	Por ser fuente de fortaleza y sabiduría para poder culminar mis estudios superiores.
Mis padres	Claudia Mayén y Ethelwaldo Rodríguez, por su incondicional amor y apoyo.
Mis hermanas	Veraly, Claudia y Rocío Rodríguez Mayén, por su apoyo y motivación para seguir adelante.
Mis abuelos	Dora de Mayén, Angélica de Rodríguez, Manuel Rodríguez y Carlos Mayén, por ser fuente de apoyo y ejemplo en mi vida.
Mi novia	Alejandra Morales, por su valioso apoyo durante la carrera y la realización de este trabajo.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la casa de estudios que me forjó como profesional.
Inga. Ingrid de Loukota	Por el tiempo brindado en la asesoría de este trabajo, su apoyo y conocimientos compartidos durante mi estadía en la Universidad.
Amigos de estudios y proyectos	Por los momentos compartidos durante la carrera y por el apoyo brindado para poder culminar esta etapa de mi vida.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES V
LISTA DE SÍMBOLOS IX
GLOSARIO XI
RESUMEN XIX
OBJETIVOS XXI
INTRODUCCIÓN XXIII

1. NEAR FIELD COMMUNICATION (NFC) 1
1.1. Beneficios de NFC 1
1.2. Especificaciones técnicas de NFC 2
1.2.1. Características principales 3
1.2.2. Arquitectura de NFC 4
1.3. Modos de comunicación 6
1.3.1. Comunicación pasiva 7
1.4. Modos de operación 8
1.4.1. Modo de lectura / escritura 8
1.4.1.1. Arquitectura del modo fr lectura/escritura 8
1.4.1.2. NDEF (NFC Data Exchange Format) 9
1.4.2. Modo punto a punto 11
1.4.2.1. Arquitectura del modo punto a punto 11
1.4.3. Modo de emulación de tarjeta 12
1.4.3.1. Arquitectura del modo de emulación de tarjeta 13
1.5. Tarjetas electrónicas NFC 13

1.6. RFID 15
1.6.1. Comparación entre NFC y RFID 17
1.7. Principales aplicaciones de NFC en el mundo actual 18

2. BIOMETRÍA Y SU APLICACIÓN EN SISTEMAS DE AUTENTICACIÓN 21
2.1. Reconocimiento biométrico 21
2.2. Rasgos biométricos 22
2.2.1. Rasgos biométricos comúnmente usados 22
2.3. La huella dactilar 24
2.4. Sistemas electrónicos biométricos 24
2.4.1. Sistemas de verificación 25
2.4.2. Sistemas de identificación 26
2.5. Proceso de matriculación 26

3. TARJETAS ELECTRÓNICAS DE PAGO 31
3.1. Tipos de tarjetas electrónicas de pago 32
3.1.1. Tarjetas de banda magnética 32
3.1.1.1. Funcionamiento 32
3.1.1.2. Ventajas y desventajas del uso de la tecnología de banda magnética 34
3.1.2. Tarjetas con *chip* integrado 35
3.1.2.1. Funcionamiento 36
3.1.2.2. Vulnerabilidades de las tarjetas con *chip* integrado 37
3.1.3. Tarjetas Contactless (NFC) 38
3.1.3.1. Funcionamiento 39
3.1.3.2. Vulnerabilidades y oportunidades 40
3.2. Máquina de punto de pago 41

3.3. Cajero automático 42

4. CONCEPTOS COMPLEMENTARIOS INVOLUCRADOS EN EL DISEÑO DEL DISPOSITIVO DE PAGO..... 43
4.1. Microcontrolador..... 43
4.1.1. Arquitecturas..... 44
4.1.2. Elementos básicos de un microcontrolador 44
4.2. Encriptación y seguridad de la información 48
4.2.1. AES 48
4.2.1.1. Descripción del cifrado AES 48
4.2.1.1.1. Pseudocódigo..... 49

5. DISEÑO DE DISPOSITIVO DE PAGO ELECTRÓNICO..... 53
5.1. Descripción de módulos electrónicos 53
5.1.1. Microcontrolador..... 53
5.1.1.1. Especificaciones técnicas..... 54
5.1.2. Módulo NFC..... 55
5.1.2.1. Especificaciones técnicas..... 55
5.1.2.2. Tarjetas NFC Mifare 57
5.1.3. Sensor de huella digital 58
5.1.3.1. Especificaciones técnicas..... 59
5.1.3.2. Comunicación con unidad de control... 59
5.1.4. LCD 60
5.1.4.1. Especificaciones técnicas..... 60
5.1.5. Teclado matricial..... 62
5.1.5.1. Especificaciones técnicas..... 62
5.1.6. Módulo auditivo y visual..... 63
5.1.7. Fuente de alimentación 64
5.2. Diagrama de bloques del dispositivo 66

5.3. Diagramas esquemáticos de circuitos electrónicos 67
5.3.1. Circuito de alimentación 67
5.3.2. Diagrama de conexiones del Módulo NFC 68
5.3.3. Diagrama de conexiones del sensor de huella digital 69
5.3.4. Diagrama de conexiones de la LCDPCD8544 70
5.3.5. Circuitos del módulo visual y auditivo 71
5.3.6. Diagrama de conexiones del teclado matricial 4x4 73
5.3.7. Diagrama esquemático de los circuitos interconectados 74
5.4. Placas de circuito impreso del dispositivo de pago 76
5.5. Programación del dispositivo de pago 78
5.5.1. Diagrama de flujo 78
5.5.2. Algoritmo del programa 79
5.6. Funcionamiento del dispositivo de pago 80
5.6.1. Procedimiento para cobro o retiro de dinero utilizando el dispositivo 80
5.6.2. Procedimiento de matriculación de un nuevo usuario 83
5.6.3. Interfaz de usuario, módulo visual y auditivo 84
5.6.3.1. Pantalla LCD 84
5.6.3.2. Indicaciones con led RGB y *buzzer* 88
5.7. Descripción económica del proyecto 89

CONCLUSIONES 93
RECOMENDACIONES 95
BIBLIOGRAFÍA 97
APÉNDICES 101

ÍNDICE DE ILUSTRACIONES

FIGURAS

1. Logotipo comercial de NFC 2
2. Pila de protocolos de arquitectura NFC 5
3. Tipos de dispositivos NFC 6
4. Arquitectura del modo lectura/escritura 9
5. Estructura de un mensaje NDEF 11
6. Arquitectura del modo punto a punto 12
7. Arquitectura del modo emulación de tarjeta 13
8. Componentes de un sistema RFID 16
9. Bondad de los rasgos biométricos de la cabeza 23
10. Bondad de los rasgos biométricos de la mano y dedos 23
11. Bondad de los rasgos biométricos del comportamiento 24
12. Proceso de un sistema de verificación 25
13. Proceso de un sistema de identificación 26
14. Proceso de matriculación 27
15. Partículas magnetizadas en una banda magnética 33
16. Valor de un *bit* en una banda magnética 33
17. Capas de un *chip* de circuito integrado 36
18. Identificación de contactos metálicos del *chip* 37
19. Chip Skimmer 38
20. Esquema de un sistema de pago inalámbrico básico 40
21. Máquina POS 41
22. Cajero automático (ATM) 42
23. Esquema básico de un microcontrolador 43

24. Bus SPI 47
25. Ejemplo de I2C con un maestro y tres esclavos 47
26. Paso Sub-bytes 49
27. Paso *Shift Rows* 50
28. Paso *Mix Columns* 50
29. Paso Add Round Key 51
30. Algoritmo de cifrado AES 52
31. Arduino Due y los puertos de programación 54
32. Módulo NFC 56
33. Ilustración del interruptor de selección de interfaz de comunicación 57
34. Tarjeta NFC Mifare 58
35. Diagrama de conexiones del sensor ZFM-20 59
36. Secuencias de escritura en la LCD 61
37. LCD PCD8544 62
38. Teclado matricial 63
39. *Buzzer* y led RGB 64
40. Esquema de módulo de alimentación 65
41. Diagrama de bloques del dispositivo de pago 67
42. Circuito de alimentación del dispositivo de pago 68
43. Conexiones del módulo NFC 69
44. Conexiones del sensor de huella digital 70
45. Conexiones de la LCD PDC8544 71
46. Circuito de control del *buzzer* 72
47. Circuito de control del led RGB 72
48. Conexiones del teclado matricial 4x4 73
49. Esquemático general del dispositivo de pago 74
50. PCB de circuito de alimentación del dispositivo 76
51. PCB del dispositivo de pago electrónico 77
52. Diagrama de flujo del programa de control 78

53. Diagrama de flujo del funcionamiento del dispositivo 82
54. Diagrama de flujo del proceso de matriculación 84
55. Interfaz para cobro o retiro de dinero utilizando el dispositivo 85
56. Interfaz para matriculación de nuevo usuario 87
57. Indicador visual y auditivo para una transacción rechazada 88
58. Indicador visual y auditivo para una transacción aceptada o matriculación exitosa 88
59. Indicador visual y auditivo para una lectura de rasgo biométrico exitosa 89

TABLAS

I. Principales características de NFC 3
II. Velocidad de transmisión, codificación y modulación en NFC 4
III. Modos de comunicación en NFC 7
IV. Rango de frecuencias de RFID 15
V. Comparación entre NFC y RFID 17
VI. Caracteristicas técnicas del microcontrolador 54
VII. Posición del *switch* de selección de interfaz 56
VIII. Caracteristicas técnicas del sensor ZFM-20 59
IX. Listado de pines del sensor ZFM-20 60
X. Asignación de pines para LCD PCD8544 61
XI. Voltajes de alimentación de módulos 65
XII. Pines utilizados en el microcontrolador 75
XIII. Listado de componentes electrónicos 90
XIV. Cotización de PCB industrial 90
XV. Listado de módulos electrónicos 91

LISTA DE SÍMBOLOS

Símbolo	Significado
A	Amperios
cm	Centímetros
$	Dólar estadounidense
°C	Grados Celsius
g	Gramos
Kbps	Kilobit por segundo
kB	Kilobyte
m	Metro
Mbps	Megabit por segundo
MB	MegabyteM
Hz	Megahertz
µF	Microfaradio
mA	Miliamperio
mm	Milímetro
Baudio	Número de símbolos por segundo
Oe	Oesterd
Ω	Ohmio
$\boldsymbol{in^2}$	Pulgadas cuadradas
Q	Quetzal
s	Segundos
Bit	Unidad mínima de información
VDC	Voltios de corriente directa
V	Voltios nominales

GLOSARIO

ADC	Conversión Analógica-Digital.
Arduino	Plataforma de código abierto que permite al usuario crear proyectos electrónicos interactivos mediante un microcontrolador.
ARM	Conjunto de instrucciones de 32 y 64 bits (Advance RISC Machine, en inglés).
ASK	Modulación por desplazamiento en amplitud en sistemas digitales (Amplitud-shiftkeying, en inglés).
ATM	Cajero automático (Automatic Teller Machine, en inglés).
Automatización	Aplicación de máquinas en la realización de un proceso.
Bluetooth	Protocolo de comunicaciones para dispositivos de bajo consumo.
Buzzer	Componente electrónico capaz de transformar la electricidad en sonido.

Contactless	Pago sin contacto por medio de identificación por radiofrecuencia.
CPU	Unidad Central de Procesamiento, es el *hardware* dentro de un dispositivo programable que interpreta las instrucciones de un programa informático.
DAC	Conversión Digital-Analógica.
DPI	Documento Personal de Identificación de los guatemaltecos.
EDC	Sistema informatizado diseñado para la recopilación de datos en formato electrónico (Electronic Data Capture, en inglés).
EEPROM	Tipo de memoria que puede ser programada, borrada y reprogramada eléctricamente (Electrically Erasable Programmable Read-Only Memory, en inglés).
EPROM	Tipo de memoria que puede ser programada eléctricamente y borrada por medio de luz ultravioleta (*Erasable Programmable Read-Only Memory*, en inglés).
FeliCa	Es un sistema de tarjeta inteligente RFID sin contacto de Sony, utilizado principalmente en tarjetas de pago electrónicas.

GND	Tierra, punto cero de todas las tensiones eléctricas presentes en un aparato eléctrico.
Hardware	Componentes eléctricos, electrónicos, electromecánicos y mecánicos de un sistema informático.
HF	Se refiere a la banda del espectro electromagnético que ocupa el rango de frecuencias de 1 megahercio a 30 megahercios (*High frequency*, en inglés).
IC	Estructura de pequeñas dimensiones de material semiconductor con superficie pequeña, en la cual se fabrican circuitos electrónicos que están protegidos dentro de un encapsulado (*Integrated Circuit*, en inglés).
ID (Identificador)	Elementos textuales que nombran entidades del lenguaje.
IDE	Entorno de desarrollo integrado que consiste en un editor de código fuente, herramientas de construcción automáticas y un depurador (*Integrated Development Environment*, en inglés).
ISM	Bandas reservadas internacionalmente para el uso no comercial de radiofrecuencia electromagnética (*Industrial, Scientific and Medical*, en inglés).

ISO / IEC	Directivas que definen los procedimientos básicos a seguir en el desarrollo de las Normas Internacionales y otras publicaciones.
LCD	Pantalla de cristal líquido, delgada y plana, formada por un número de píxeles monocromos (*Liquid Crystal Display*, en inglés).
Led	Componente optoelectrónico pasivo que emite luz.
Led RGB	Conjunto de tres ledes en un mismo empaque: rojo, verde y azul.
LF	Se refiere a la banda del espectro electromagnético que ocupa el rango de frecuencias entre 30 kilohercios y 300 kilohercios (*Low Frequency*, en inglés).
LLCP	Protocolo que permite comunicaciones multiplexadas entre dos dispositivos NFC (*Logical Link Control Protocol*, en inglés).
Microcontrolador (µC)	Circuito integrado programable, capaz de ejecutar instrucciones grabadas en su memoria.
Microondas	Ondas electromagnéticas entre 300 megahercios y 30 gigahercios.

NFC	Comunicación de campo cercano, inalámbrica, de corto alcance y alta frecuencia (*Near Field Communication*, en inglés).
Pay load	Parte de los datos transmitidos que es el mensaje real deseado.
PCB	Superficie constituida por pistas o buses de material conductor sobre una base no conductora (*Printed Circuit Board*, en inglés).
POS	Dispositivo que permite realizar cobros por tarjetas de crédito o débito.
PVC	Material termoplástico resistente, duradero y aislante.
PWM	Modulación por ancho de pulso en la que se modifica el ciclo de trabajo de una señal periódica (*Pulse With Modulation*, en inglés).
RAM	Memoria de acceso aleatorio en la que se cargan todas las instrucciones que ejecuta la unidad central de procesamiento (*Random Access Memory*, en inglés).
RF	Radiofrecuencia que se aplica a la porción menos energética del espectro electromagnético ubicada en los rangos de frecuencia entre 3 kilohercios y 300 gigahercios.

RFID	Identificación por radiofrecuencia en un sistema de almacenamiento y recuperación de datos remotamente mediante ondas de radio (*Radio Frequency Identification*, en inglés).
ROM	Memoria de solo lectura de información que no permite la escritura y es de acceso secuencial (*Read-Only Memory*, en inglés).
Skimmer	Robo de información de tarjetas de crédito usado al momento de la transacción, con el fin de reproducir o clonar la tarjeta para su uso fraudulento.
Smart card	Tarjeta inteligente del tamaño del bolsillo con circuitos integrados que realiza cierta lógica programada.
Software	Conjunto de los componentes lógicos necesarios en un sistema informático que hacen posible la realización de tareas.
Ticketing	Archivo contenido en el sistema de seguimiento que contiene información acerca de las intervenciones de *software* realizadas por el usuario.
Transistor NPN	Dispositivo electrónico de estado sólido consistente en dos uniones PN muy cercanas entre sí, permitiendo controlar el paso de corriente a través de sus terminales.

TTL	Lógica transistor a transistor, tecnología de construcción de circuitos electrónicos digitales (*Transistor-Transistor Logic*, en inglés).
UART	Dispositivo que controla los puertos y dispositivos serie (*Universal Asynchronous Receiver-Trasnmitter*, en inglés).
UHF	Banda del espectro electromagnético que ocupa el rango de frecuencias de 300 megahercios a 3 gigahercios (*Ultra High Frequency*, en inglés).
USART	Tipo de dispositivo de interfaz serial capaz de programarse para comunicarse de forma asíncrona o síncrona (*Universal Synchronous/Asynchronous Receiver/Transmitter*, en inglés).

RESUMEN

Este trabajo de graduación presenta el diseño de un dispositivo electrónico de pago que utiliza tarjetas NFC y autenticación por medio del rasgo biométrico de la huella digital.

En el primer capítulo se describe la tecnología NFC, sus conceptos fundamentales y sus especificaciones técnicas, de igual manera se describen las características de las tarjetas NFC y se realiza una comparación con RFID.

En el segundo capítulo se expone la teoría sobre biometría, los rasgos comúnmente usados, los tipos de sistemas biométricos existentes y sus aplicaciones.

En el tercer capítulo se describe la actualidad de las tarjetas de pago electrónicas, su funcionamiento y sus características técnicas, así como los dispositivos existentes para realizar transacciones monetarias.

En el cuarto capítulo se desarrollan conceptos complementarios involucrados en la realización del dispositivo.

En el quinto capítulo se detallan los módulos y circuitos electrónicos, explicando su funcionamiento, algoritmos de programación y las guías de operación del dispositivo. De igual manera, se incluye un presupuesto de la realización del proyecto.

OBJETIVOS

General

Diseñar un dispositivo de sistema de pago que utilice tecnologías de comunicación inalámbrica combinado con nuevos métodos de autenticación personal, para aumentar la confidencialidad y seguridad de los métodos actuales.

Específicos

1. Exponer la teoría sobre sistemas de pago existentes y la relación con un sistema de pago que utilice tecnología NFC junto con autenticación biométrica.

2. Mostrar los beneficios de la tecnología inalámbrica NFC en los sistemas de pago.

3. Aumentar la seguridad de los sistemas de pago actuales mediante el uso de autenticación de huella digital.

4. Diseñar un equipo electrónico que cumpla con la función de un sistema de pago inalámbrico con autenticación, describiendo el funcionamiento de sus circuitos y componentes electrónicos.

INTRODUCCIÓN

Las tarjetas de pago han revolucionado el consumo y las formas de pago. La mayoría de establecimientos comerciales cuentan con dispositivos capaces de recibir pagos de forma electrónica y, de la misma manera, en cualquier esquina se encuentra un cajero automático. Lastimosamente, el uso de las tarjetas de pago trae consigo ciertos peligros de seguridad relacionados con el robo de información, desgaste por uso y fraudes por falta de autenticación al momento de realizar un pago. Paralelamente, con el auge del uso de tarjetas de pago ha crecido la cantidad de dispositivos tecnológicos capaces de vulnerar la información del usuario.

Los sistemas de pago electrónicos actuales presentan muchas desventajas en cuanto a seguridad se refiere. Las tarjetas actuales poseen bandas magnéticas o *chips* que son susceptibles de robo de información por medio del uso de dispositivos para clonar tarjetas. La necesidad de contacto físico con el dispositivo receptor hace aún más desventajoso su uso, ya que el deterioro que todo dispositivo sufre por el constante uso puede complicar su funcionamiento.

Por esto se presenta una solución o alternativa para los sistemas de pago actuales. Mediante el uso de tecnología de comunicación inalámbrica de corto alcance y biometría, se plantea el diseño de un dispositivo de pago compuesto por tarjetas NFC y autenticación mediante huella digital, con el cual se pretende aumentar la seguridad de las tarjetas de pago y agregar mayor confiabilidad a la autenticación, para reducir la cantidad de fraudes que ocurren por el robo de información y mal uso de los dispositivos.

1. NEAR FIELD COMMUNICATION (NFC)

Near Field Communication (NFC, por sus siglas en inglés, o Comunicación de Campo Cercano, en español), es una tecnología de comunicación inalámbrica de corto alcance entre dos dispositivos, con reducido ancho de banda y baja velocidad de transmisión. NFC permite la comunicación entre dos dispositivos compatibles sin necesidad de autenticación previa y es capaz de realizar comunicación bidireccional. Es una tecnología relativamente nueva, aunque se basa en la tecnología de Identificación por Radiofrecuencia (RFID), sus características permiten que su uso sea más extendido debido al aumento de seguridad de la información. Actualmente, la tecnología NFC se ve mayormente reflejada en dispositivos móviles, sin embargo, su uso se ha extendido a diversos entornos, tales como sistemas de control de acceso, automatización, *ticketing*, publicidad, sistemas de pago, entre otros.

1.1. Beneficios de NFC

La aplicación de NFC en la tecnología presenta diversos beneficios generales como:

- Facilidad de uso: la tecnología NFC como tal no requiere de una autenticación o emparejamiento entre dispositivos para poder intercambiar información.
- Seguridad: el hecho de que NFC es un tipo de comunicación inalámbrica de corto alcance aumenta la seguridad de la información (no hay necesidad de contacto físico y sería necesario un acercamiento a pocos centímetros para interceptar la información). De igual forma, la

información contenida en tarjetas o dispositivos NFC puede encriptarse para aumentar la seguridad y privacidad de la misma.

- Adaptabilidad: la tecnología NFC es adaptable a diversos entornos y aplicaciones, tanto comerciales como industriales.
- Compatibilidad: NFC permite la activación y configuración de otras tecnologías inalámbricas (wifi, *Bluetooth*, entre otros) en dispositivos móviles.
- NFC es una tecnología basada en estándares, por lo tanto su funcionamiento y operatividad están garantizados.

Figura 1. **Logotipo comercial de NFC**

Fuente: NFC Forum, Inc. http://manuals.denon.com/PMA50/EU/ES/WBSPSYgvcekkuj.php. Consulta: 20 de febrero de 2017.

1.2. Especificaciones técnicas de NFC

La tecnología NFC permite interacciones bidireccionales simples y seguras entre dispositivos electrónicos, permitiendo a los consumidores realizar transacciones inalámbricas, acceder a contenido digital y conectarse a dispositivos electrónicos con un simple acercamiento. NFC complementa muchas tecnologías inalámbricas, utilizando elementos claves de las normas existentes para la tecnología de tarjetas sin contacto (ISO/IEC 14443).

1.2.1. Características principales

La comunicación inalámbrica en NFC emplea la inducción electromagnética entre dos antenas, operando dentro de la banda ISM (Industrial, Scientific and Medical, por sus siglas en inglés) de radiofrecuencia no licenciada de 13,56 MHz, bajo el estándar ISO/IEC 18000-3 de interfaz aérea, a velocidades de transmisión que van desde 106 hasta 424 kbps. La mayor parte de la energía de radiofrecuencia utilizada en NFC se encuentra concentrada en el margen de ancho de banda permitido de ± 7 kHz, sin embargo, la envolvente espectral puede ser de hasta 2 MHz cuando se utiliza la modulación ASK.

Tabla I. **Principales características de NFC**

Características técnicas de NFC	
Frecuencia de operación	13,56 MHz
Comunicación	Bidireccional
Velocidad de transmisión	106 a 424 kbps
Modulación	Principalmente ASK
Ancho de banda	Hasta 2 MHz
Estándares	ISO 14443
Distancia de escaneo	< 4 cm
Escaneo simultáneo de etiquetas	No
Modos de comunicación	Activo-activo / activo-pasivo
Consumo de corriente	< 15 mA
Tiempo de configuración	< 0,1 s

Fuente: elaboración propia.

NFC emplea dos sistemas de codificación diferentes en la señal de radiofrecuencia. En la mayoría de casos se utiliza la codificación Manchester con 10 % de modulación. Sin embargo, para un elemento activo transmitiendo información a 106 kbps, se utiliza el esquema de codificación Miller modificado con 100 % de modulación.

Tabla II. **Velocidad de transmisión, codificación y modulación en NFC**

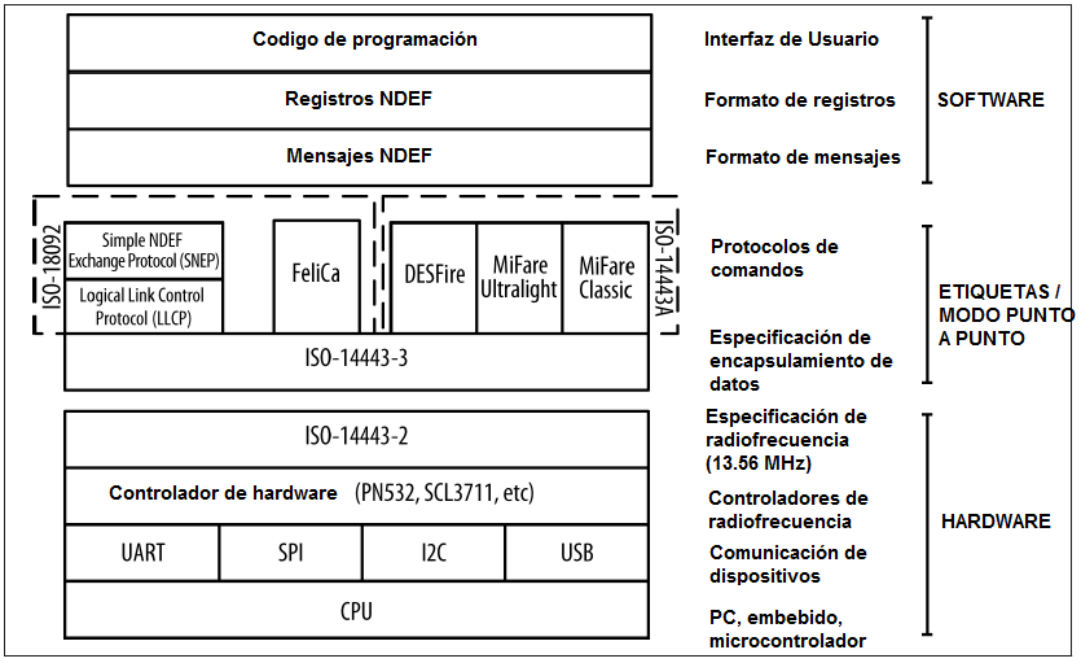
Velocidad (kbps)	Dispositivo Activo	Dispositivo Pasivo
106	Miller Modificado, 100 %, ASK	Manchester, 10 %, ASK
212	Manchester, 10 %, ASK	Manchester, 10 %, ASK
424	Manchester, 10 %, ASK	Manchester, 10 %, ASK

Fuente: POOLE, Ian. *NFC modulation and RF signal.* http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-modulation-rf-signal-interface.php. Consulta: 14 de diciembre de 2016.

1.2.2. Arquitectura de NFC

Para lograr entender el funcionamiento de NFC con detalle es necesario generar un modelo esquemático de su arquitectura. Dentro de la arquitectura de NFC existen múltiples capas. La primera capa es la capa física, conformada por el CPU y el *hardware* encargado de la comunicación por radiofrecuencia. En el medio, están las capas conformadas por el empaquetado y los protocolos de transmisión de información. Después de ellas se encuentran las capas que especifican el formato de la información a transmitir y, por último, se encuentran las capas de aplicación, conformadas por el código de programación.

Figura 2. **Pila de protocolos de arquitectura NFC**



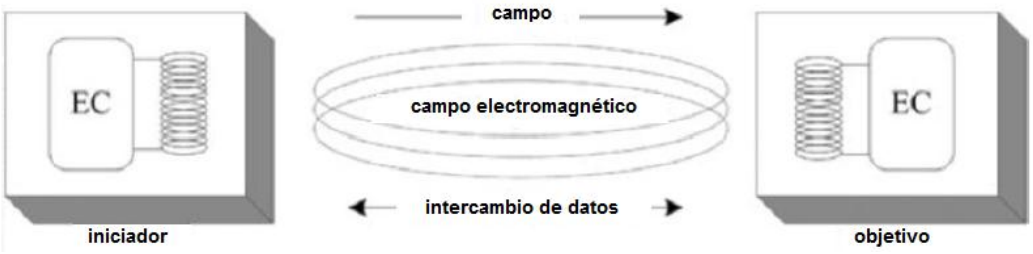
Fuente: IGOE, T.; COLEMAN, D.; JEPSON, B. *Beginning NFC, Near Field Communication with Arduino, Android, and PhoneGap*. p. 16

En la capa física, NFC trabaja bajo la especificación de radio RFID, ISO-14443-2, que describe radios de bajo consumo operando a 13,56 MHz. (Coleman, Igoe y Jepson, 2014). La capa de especificación de encapsulamiento de datos describe cómo la información es enviada a través de radiofrecuencia (ISO-14443-3). Los controladores de radiofrecuencia se comunican con el procesador principal por medio de protocolos seriales como: UART, SPI, I2C o USB.

1.3. Modos de comunicación

Los estándares establecidos alrededor de la tecnología *near field communication* definen dos tipos de dispositivos NFC. Estos dispositivos se conocen como el iniciador y el objetivo. Como su nombre lo indica, el iniciador es el dispositivo que inicia la comunicación y controla el intercambio de información. El dispositivo objetivo es el que responde a los requerimientos del iniciador.

Figura 3. **Tipos de dispositivos NFC**



Fuente: PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 45.

De igual forma, existe la clasificación de dispositivos según su capacidad de generar su propio campo de radiofrecuencia. Los dispositivos activos poseen su propia fuente de alimentación eléctrica y, por lo tanto, son capaces de generar un campo de radiofrecuencia. Por otro lado, los dispositivos pasivos no poseen fuente de alimentación y se alimentan por medio de la inducción del campo electromagnético generado por un dispositivo activo.

Habiendo expuesto los tipos de dispositivos NFC involucrados en la transferencia de información, a continuación se detallan los modos de comunicación:

Comunicación activa

Ambos dispositivos, tanto el emisor como el receptor, poseen fuentes de alimentación y, por lo tanto, son capaces de generar su propio campo de radiofrecuencia por medio de los cuales se comunican. Cada dispositivo debe desactivar su campo de radiofrecuencia mientras recibe datos del otro. Un ejemplo de este modo es la conexión entre dos teléfonos inteligentes, ambos poseen su propia fuente de alimentación y capacidades de procesamiento.

1.3.1. Comunicación pasiva

En el caso de la comunicación pasiva, únicamente un dispositivo es capaz de generar un campo de radiofrecuencia. “El dispositivo emisor proporciona un campo portador y el dispositivo receptor responde modulando el campo existente”[1]. El dispositivo receptor es capaz de operar mediante el campo electromagnético proporcionado por el dispositivo emisor. Un ejemplo de este modo es la comunicación entre un lector y una tarjeta o etiqueta NFC.

Tabla III. **Modos de comunicación en NFC**

Dispositivo A	Dispositivo B	Descripción	Modo de comunicación
Activo	Activo	El campo RF es generado por los dos dispositivos	Modo activo
Activo	Pasivo	El campo RF es generado por el dispositivo A	Modo pasivo
Pasivo	Activo	El campo RF es generado por el dispositivo B	Modo pasivo

Fuente: PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 45.

[1] PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 45.

1.4. Modos de operación

Además de los modos de comunicación, también se definen tres modos de operación en NFC.

1.4.1. Modo de lectura / escritura

En el modo de operación de lectura/escritura, un dispositivo activo inicia la comunicación y puede tanto leer como escribir mensajes en etiquetas NFC que actúan como receptores pasivos según el formato definido por el NFC Forum. En esto modo de operación la velocidad de transmisión de datos se aproxima a los 106 kbps. “El modo de operación de lectura/escritura está basado en la ISO/IEC 14443 tipo A, tipo B y el esquema FeliCa”[2]. Es importante mencionar que en este modo de operación no hay seguridad para la información, ya que cualquier dispositivo NFC activo puede leer, escribir o sobrescribir información.

1.4.1.1. Arquitectura del modo fr lectura/escritura

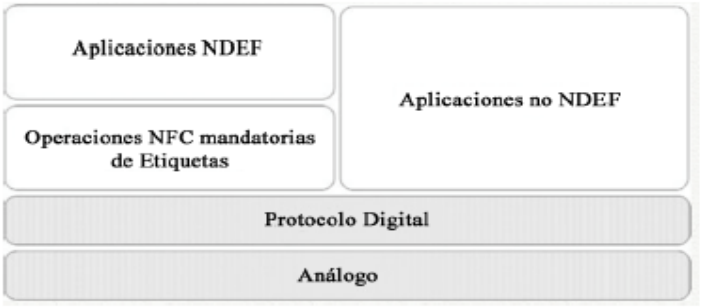
A continuación se especifican los protocolos incluidos en el modo de lectura/escritura:

- Protocolo análogo: se refiere a las características de radiofrecuencia de dispositivos NFC y establece el rango de operatividad de los mismos.
- “Protocolo digital: se refiere a los aspectos digitales establecidos en los estándares ISO/IEC 18092 e ISO/IEC 14443.

[2] PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 48.

- Operaciones NFC mandatorias de etiquetas: indican los comandos e instrucciones que deben utilizar los dispositivos para manejar y habilitar operaciones de lectura y escritura en etiquetas NFC"[3].
- Aplicaciones NDEF
- Aplicaciones no NDEF: aplicaciones no basadas en especificaciones NDEF.

Figura 4. **Arquitectura del modo lectura/escritura**



Fuente: PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 39.

1.4.1.2. NDEF (NFC Data Exchange Format)

NDEF es un estándar adoptado a nivel mundial para definir el formato de encapsulación de un mensaje para el intercambio de datos a través de un enlace NFC. NDEF es un formato ligero, ya que no agrega sobrecarga significativa a los mensajes. Consiste en un mensaje binario que encapsula paquetes llamados *payloads* o cargas útiles, en español, los cuales pueden variar en tipo y tamaño. Las cargas útiles se combinan en una sola estructura de mensaje. Cada carga útil es descrita por un tipo, una longitud o tamaño y un identificador opcional.

[3] PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 49.

Un mensaje NDEF está compuesto por uno o más registros NFED. El límite de registros que pueden ser guardados en un mensaje NDEF depende de la capacidad de memoria del dispositivo activo o del tipo de etiqueta pasiva que se esté utilizando. A fin de que el sistema identifique el inicio y el final de un mensaje NDEF, el primer registro del mensaje es etiquetado con la bandera MB y el último registro es etiquetado con la bandera ME. Cada registro encapsulado dentro de un mensaje NDEF consiste en dos partes:

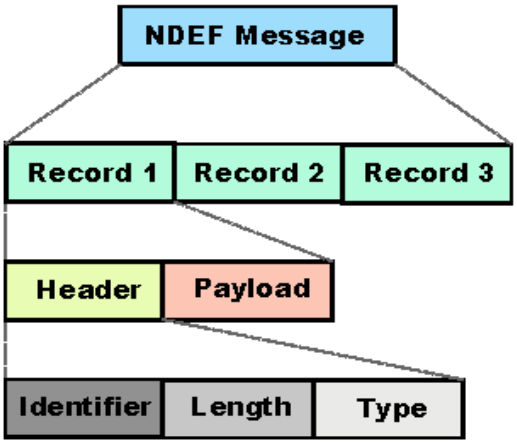
- Encabezado, que a su vez incluye tres elementos identificadores:

    - "Longitud de la carga útil, que es un campo compuesto de un octeto para registros pequeños y de cuatro octetos para registros grandes. Los registros pequeños son identificados por medio del bit SR (*Short Record*).
    - Tipo de carga útil, que indica el tipo de información contenida en el registro. El formato del tipo de carga útil es indicado por el campo TNF (*Type Name Format*).
    - Identificación de carga útil, que es un identificador opcional que permite a las aplicaciones identificar la carga útil contenida dentro de un registro NDEF"[4].

- Carga útil (*payload*), que es la carga útil contenida en un mensaje NDEF, puede ser de diferentes tipos: URL, MIME, texto plano, etc. Es importante mencionar que la carga útil es el contenido en sí y, según la seguridad que la información requiera, este puede ser encriptado o simplemente puede ser enviado como texto plano.

[4] POOLE, Ian. NDEF. http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-data-exchange-format-ndef.php. Consulta: 19 de diciembre de 2016.

Figura 5. **Estructura de un mensaje NDEF**



Fuente: POOLE, Ian. NDEF. http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-data-exchange-format-ndef.php. Consulta: 19 de diciembre de 2016.

1.4.2. Modo punto a punto

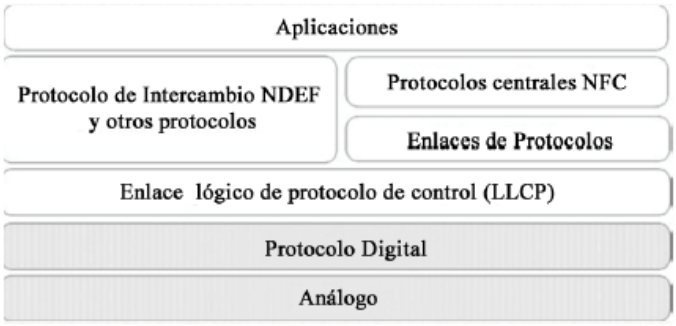
El modo de operación punto a punto en NFC permite una conexión bidireccional a una velocidad de 424 kbps. En este modo de funcionamiento dos dispositivos establecen una conexión para intercambiar información como tarjetas de negocios, fotografías, configuraciones, entre otros.

1.4.2.1. Arquitectura del modo punto a punto

En la capa física de este modo de funcionamiento se especifica que la interfaz de radiofrecuencia está bajo los estándares ISO/IEC 18092/NFCIP-1 e ISO/IEC 21481/NFCIP-2, los cuales habilitan un modelo de petición/respuesta entre dos dispositivos activos. También está incluido el estándar ISO/IEC 2148/NFCIP-2, el cual detecta y selecciona el protocolo de comunicación que se utilizará en la conexión punto a punto.

En la capa de enlace de datos del modo punto a punto, se especifica el protocolo de control de enlace lógico (LLCP). LLCP provee cinco importantes servicios: transporte sin conexión, transporte orientado a la conexión, activación de enlace, supervisión y desactivación, comunicación asíncrona balanceada y protocolo de multiplexación. La capa de aplicación del modo punto a punto permite hacer la combinación de diferentes tecnologías inalámbricas como NFC y Bluetooth, para crear aplicaciones seguras de intercambio de datos, como transferencias de dinero entre dispositivos móviles.

Figura 6. **Arquitectura del modo punto a punto**



Fuente: PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 37.

1.4.3. Modo de emulación de tarjeta

"En el modo de emulación de tarjeta un dispositivo NFC puede emular las propiedades y caracteristicas de una tarjeta inteligente con el estándar ISO/IEC 14443 y FeliCa"[5]. En este modo de operación un dispositivo NFC no genera su propio campo de radiofrecuencia, ya que el lector es el encargado de crearlo, por lo que el dispositivo emulador de tarjeta se comporta como una tarjeta o etiqueta convencional.

[5] PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 55.

1.4.3.1. Arquitectura del modo de emulación de tarjeta

La capa física la comunicación NFC se basa en el estándar ISO/IEC 14443 de tarjetas inteligentes inalámbricas y en estándares JIS X 6316-4 FeliCa. En este modo de funcionamiento se utilizan protocolos digitales y análogos, similares a los utilizados en tarjetas inteligentes, y son completamente compatibles con los estándares de tarjetas inteligentes basados en ISO/IEC 14443 tipo A, tipo B y FeliCa. En la capa de aplicación, el modo de emulación de tarjeta incluye propiedades de aplicaciones que permiten acciones inalámbricas, tales como, pagos, *ticketing* y control de acceso.

Figura 7. **Arquitectura del modo emulación de tarjeta**

Fuente: PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 41.

1.5. Tarjetas electrónicas NFC

"Las tarjetas o etiquetas NFC son dispositivos pasivos que permiten la comunicación con dispositivos NFC activos. Son capaces de almacenar información y consumen una mínima cantidad de energía. Por ser dispositivos pasivos, no cuentan con alimentación propia y dependen de ser alimentados por el campo electromagnético de un dispositivo activo. Existen cuatro tipos de tarjetas o etiquetas definidas por el NFC Forum. Todas ellas están basadas en

protocolos de control RFID. Existe un quinto tipo de tarjeta que es compatible, sin embargo, no es estrictamente parte de las especificaciones NFC"[6]. A continuación, se detallan las características de cada tipo de tarjeta o etiqueta NFC:

- Tipo 1
  - Basadas en la especificación ISO-14443 A
  - Capaz de funcionar en modo solo lectura o lectura/escritura
  - Memoria de 96 bytes a 2 kilobytes
  - Habilitada para una velocidad de comunicación de 106 kbps
  - No hay protección de colisión de datos

- Tipo 2
  - Basadas en NXP/Philips MifareUltralight(ISO-14443 A)
  - Capaz de funcionar en modo solo lectura o lectura/escritura
  - Memoria de 96 *bytes* a 2 *kilobytes*
  - Habilitada para una velocidad de comunicación de 106 kbps
  - Soporte anticolisión

- Tipo 3
  - Basadas en Sony FeliCa (ISO-18092 y JIS-X-6319-4), sin la encriptación y autenticación que brinda FeliCa.
  - Configuradas en fábrica para funcionar en modo solo lectura, y configurables para modo lectura/escritura.
  - Memoria variable, hasta 1MB.
  - Dos velocidades de comunicación, 212 o 424 kbps.
  - Soporte anticolisión.

[6] IGOE, Tom; COLEMAN, Don; JEPSON, Brian. *Beginning NFC, Near Field Communication with Arduino, Android, and Phone Gap.* p. 112.

- Tipo 4
    - Basadas en NXP DESFire (ISO-14443 A).
    - Configuradas en fábrica para funcionar en modo solo lectura o lectura/escritura.
    - 2, 4 o 6KB de memoria.
    - Tres velocidades de comunicación, 106, 212 o 424 kbps.
    - Soporte anticolisión.

1.6. RFID

Radio Frequency Identification (RFID) permite una comunicación inalámbrica unidireccional, comúnmente entre una tarjeta o etiqueta RFID no alimentada y un lector RFID. “Las tarjetas RFID pueden ser escaneadas a distancias de hasta 100 metros sin una línea directa de visión para el lector RFID”[7]. Por lo general, RFID se utiliza para el rastreo de equipaje en aeropuerto, identificación de productos, control de acceso, etc. Sin embargo, el hecho de que pueda ser escaneado a grandes distancias, no la hace una tecnología segura para la información. RFID opera en un rango específico de radiofrecuencia y posee sus propios estándares y protocolos.

Tabla IV. **Rango de frecuencias de RFID**

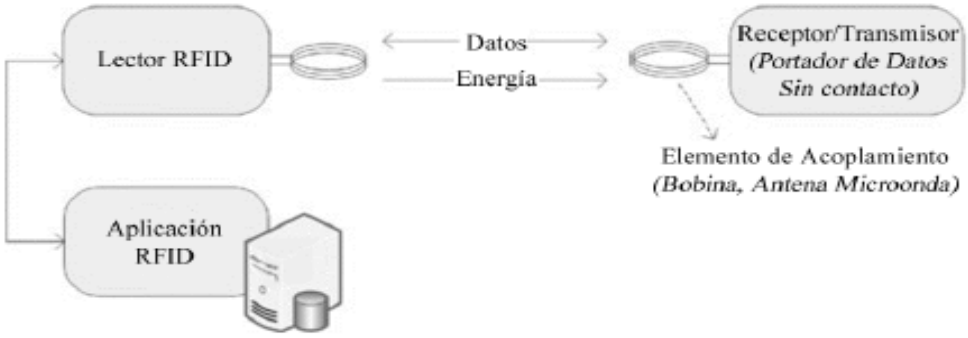
Banda de frecuencia RFID	Distancia de escaneo
120 – 150 kHz (Baja Frecuencia, LF)	Hasta 10 cm
13,56 MHz (Alta Frecuencia, HF)	Hasta 1 m
433 MHz (Ultra Alta Frecuencia, UHF)	1 – 100 m
860 – 960 MHz (Frecuencia Ultra Ligera Alta, UHF)	1 – 12 m
2 450 – 5 800 MHz (Microondas)	1 – 2 m
3,1 – 10 GHz (Microondas)	Hasta 200 m

Fuente: NFC Today. *The difference between NFC and RFID explained.* http://nfc.today/advice/difference-nfc-rfid-explained. Consulta: 28 de diciembre de 2016.

[7] NFC Today. *The difference between NFC and RFID explained.* http://nfc. today/ advice/difference-nfc-rfid-explained. Consulta: 28 de diciembre de 2016.

Las etiquetas RFID están compuestas de un circuito integrado y una antena. El circuito integrado proporciona el almacenamiento de datos y su procesamiento. Un sistema RFID está formado por 2 componentes, el transmisor y el lector. El transmisor es el componente que está localizado en un producto u objeto que va a ser identificado, y el lector es el componente que escaneará los datos del transmisor. El transmisor está compuesto de un elemento de unión y un circuito integrado, el cual almacena los datos. Realmente, el transmisor es llamado etiqueta o tarjeta RFID. “Una vez que la etiqueta está en el rango del lector RFID, este es activado por las señales de las etiquetas”[8]. Un dispositivo lector RFID está compuesto de un módulo de alta frecuencia, un decodificador, que es el encargado de interpretar los datos, una unidad de procesamiento y control, y una antena.

Figura 8. **Componentes de un sistema RFID**



Fuente: PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 42.

[8] PADILLA, Jorge; ÍÑIGUEZ, Wilber. *Near Field Communication-Teoría y aplicaciones*. p. 42.

1.6.1. Comparación entre NFC y RFID

NFC opera a 13,56 MHz y es una extensión de los estándares RFID de Alta Frecuencia (HF). A pesar de que NFC y RFID comparten muchas propiedades físicas similares, como la capacidad de comunicación sin una línea de visión directa y la comunicación unidireccional, existen tres diferencias importantes:

- NFC es capaz de realizar una comunicación bidireccional y puede ser utilizado para interacciones más complejas, como la emulación de tarjeta y la transferencia punto a punto.
- NFC está limitado a distancias cortas, comúnmente 5 cm o menos.
- Solo una etiqueta NFC puede ser escaneada a la vez.

Estas propiedades fueron desarrolladas principalmente para permitir transacciones seguras. Por esta misma razón NFC está restringido al escaneo individual y de corta distancia.

Tabla V. **Comparación entre NFC y RFID**

	RFID HF	**NFC**
Frecuencia de operación	13,56 MHz	13,56 MHz
Comunicación	Unidireccional	Bidireccional
Estándares	ISO 14443, 15693, 18000	ISO 14443
Distancia de escaneo	Hasta 1 m	Hasta 10 cm
Escaneo simultaneo	Si	No

Fuente: NFC Today. *The difference between NFC and RFID explained.* http://nfc.today/advice/difference-nfc-rfid-explained. Consulta: 28 de diciembre de 2016.

A continuación se detallan las principales semejanzas y diferencias entre NFC y RFID:

- Tanto NFC como RFID en HF operan en la frecuencia de 13,56 MHz.
- NFC posibilita una comunicación bidireccional, por lo que puede ser utilizado para transacciones complejas como emulación de tarjetas y comunicación punto a punto, en tanto que RFID está diseñado para una comunicación lectura/escritura simplemente.
- La comunicación NFC está diseñada para ser de corto alcance, lo cual da un mayor grado de seguridad para la información contenida en los dispositivos NFC. En cambio, RFID permite escaneos hasta distancias de 100 m y no brinda mayor seguridad a la información contenida en el dispositivo.
- Solo es posible el escaneo de una etiqueta NFC a la vez.
- Gracias a la capacidad de NF de operar en el modo emulación de tarjeta, es posible reemplazar tarjetas RFID con un teléfono inteligente o dispositivo con NFC habilitado.
- Las etiquetas RFID también pueden funcionar en modos activos o pasivos.
- La principal diferencia entre estas tecnologías es la consideración de limitar la distancia de escaneo para dispositivos NFC y así poder incluirla como alternativa de transacciones monetarias o entornos en donde se requiera mayor seguridad de la información contenida.

1.7. Principales aplicaciones de NFC en el mundo actual

NFC es una tecnología que ha mostrado auge en los últimos años, esto es notable ya que cada vez más dispositivos electrónicos (teléfonos celulares, computadoras, *tablets,* dispositivos de sonido, entre otros) cuentan con esta tecnología inalámbrica. A continuación, se enlistan varías aplicaciones de la tecnología NFC en el mundo actual:

- Sistemas de pago inalámbricos
- Identificación y control de acceso
- *Ticketing*
- Automatización de procesos
- Información digital

2. BIOMETRÍA Y SU APLICACIÓN EN SISTEMAS DE AUTENTICACIÓN

La biometría se define como una técnica que permite captar y analizar rasgos humanos y convertirlos en información que puede ser utilizada para identificar y autenticar a un individuo en específico. Las técnicas utilizadas en la biometría para adquirir rasgos humanos han evolucionado gracias a la aplicación de métodos de automatización basados en electrónica. Debido a la confiabilidad de los sistemas automatizados, los errores de seguridad de identificación y autenticación son mínimos.

2.1. Reconocimiento biométrico

El reconocimiento biométrico se refiere al uso de diferentes características anatómicas (como huellas dactilares, cara o iris) y de comportamiento (como habla, firma o teclear). Estas características se denominan identificadores biométricos o rasgos biométricos y sirven para reconocer automáticamente a los individuos.

La biometría es una técnica muy útil para la autenticación eficiente de los individuos. Esta eficacia se debe a que las características anatómicas de un individuo en particular no se pueden compartir o suplantar, los rasgos biométricos de un individuo representan las formas físicas inherentes. Por consiguiente, la biometría es una tecnología que, usada correctamente, puede permitir una sociedad más segura, reducir el fraude y proveer interfaces persona-máquina fáciles de usar. El objetivo de las aplicaciones biométricas es tener sistemas más cómodos, más seguros y más rápidos.

2.2. Rasgos biométricos

Cualquier rasgo humano puede ser utilizado como un identificador biométrico si cumple en cierto grado con las siguientes características:

- Universalidad: todos los individuos deben tener ese rasgo anatómico.
- Particularidad: debe existir exclusividad entre individuos de ese rasgo anatómico.
- Permanencia: el rasgo biométrico debe ser invariable en el tiempo.
- Medible: el rasgo debe estar en la posibilidad de ser medido cuantitativamente.
- Rendimiento: el rasgo biométrico debe garantizar precisión y robustez en diferentes factores ambientales.
- Aceptabilidad: debe ser un rasgo aceptado por los individuos que serán sometidos al proceso de identificación.
- No falsificable: debe ser un rasgo con alto grado de dificultad para ser falsificado o infalsificable.

2.2.1. Rasgos biométricos comúnmente usados

A continuación se enlistan los rasgos biométricos más utilizados para la identificación o verificación de individuos:

- Rasgos biométricos de la cabeza
    - Cara
    - Termograma facial (imagen térmica del rostro)
    - Oreja
    - Iris
    - Retina

Figura 9. **Bondad de los rasgos biométricos de la cabeza**

Rasgo	Característica						
	Universalidad	Particularidad	Permanencia	Medible	Rendimiento	Aceptabilidad	No falsificable
Cara	Alto	Bajo	Medio	Alto	Bajo	Alto	Alto
Termograma	Alto	Alto	Bajo	Alto	Medio	Alto	Alto
Oreja	Medio	Medio	Alto	Medio	Alto	Bajo	Alto
Iris	Alto	Alto	Alto	Medio	Alto	Bajo	Alto
Retina	Alto	Alto	Medio	Bajo	Alto	Bajo	Alto

Fuente: SERRATOSA, Francesc. *La biometría para la identificación de las personas.* p. 24.

- Rasgos biométricos de la mano y dedos
  - Geometría de la mano y de los dedos
  - Huella dactilar
  - Huella de la mano
  - Venas de la mano y de los dedos

Figura 10. **Bondad de los rasgos biométricos de la mano y dedos**

Rasgo	Característica						
	Universalidad	Particularidad	Permanencia	Medible	Rendimiento	Aceptabilidad	No falsificable
Geometría	Medio	Medio	Medio	Alto	Medio	Medio	Medio
H. dactilar	Medio	Alto	Alto	Medio	Alto	Medio	Medio
H. de mano	Medio	Alto	Alto	Bajo	Alto	Medio	Medio
Venas	Medio	Medio	Medio	Medio	Medio	Medio	Alto

Fuente: SERRATOSA, Francesc. *La biometría para la identificación de las personas.* p. 26.

- Rasgos biométricos del comportamiento
  - Tono de voz
  - Firma

- Tipo de pisada
- Manera de teclear

Figura 11. **Bondad de los rasgos biométricos del comportamiento**

Rasgo	Característica						
	Universalidad	Particularidad	Permanencia	Medible	Rendimiento	Aceptabilidad	No falsificable
Hablador	Medio	Bajo	Bajo	Medio	Bajo	Alto	Bajo
Firma	Bajo	Bajo	Bajo	Alto	Bajo	Alto	Bajo
F. de andar	Medio	Bajo	Bajo	Alto	Bajo	Alto	Medio
F. de teclear	Bajo	Bajo	Bajo	Medio	Bajo	Medio	Medio

Fuente: SERRATOSA, Francesc. *La biometría para la identificación de las personas.* p. 29.

2.3. La huella dactilar

La huella dactilar es un rasgo biométrico que cuenta con gran equilibrio entre todos los rasgos biométricos que actualmente son utilizados. Es un rasgo universal (exceptuando a las personas con discapacidades en sus extremidades). Las huellas dactilares son muy diversas y permanentes, a pesar de que ocurran accidentes en las yemas de los dedos, estas se regeneran en su totalidad. De igual manera, los sensores electrónicos de huellas dactilares son dispositivos económicamente asequibles y de alta confiabilidad. Por último, las huellas dactilares son rasgos biométricos difíciles de falsificar debido a la particularidad del rasgo y la tecnología utilizada.

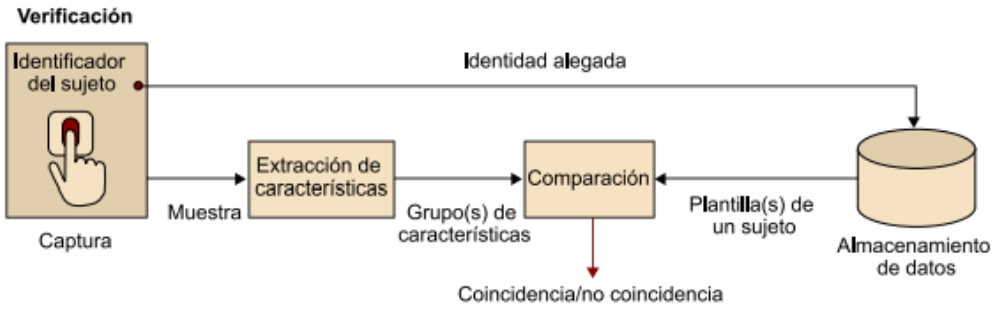
2.4. Sistemas electrónicos biométricos

Según la aplicación de la biometría, se pueden diferenciar dos tipos de sistemas:

2.4.1. Sistemas de verificación

Estos sistemas también son llamados sistemas de autenticación. Autentifican la identificación de la persona mediante la comparación del rasgo biométrico contenido acabado de capturar con el rasgo biométrico que el sistema ha capturado antes en el proceso de inscripción al sistema. Por ejemplo, el individuo presenta una identificación electrónica en la cual está almacenado un rasgo biométrico que identifica a este único usuario. De esta manera, el sistema encargado realiza una comparación entre el rasgo biométrico que el usuario acaba de presentar con el rasgo contenido en la identificación electrónica. Regularmente, la respuesta del sistema de verificación es binaria, se trata del mismo individuo si los rasgos biométricos concuerdan (tienen mucha similitud) o en caso contrario, son dos individuos distintos. Cuando los rasgos biométricos y la identificación del individuo se encuentran en la misma identificación electrónica de forma encriptada, se dice que la base de datos está distribuida entre las tarjetas electrónicas de los usuarios.

Figura 12. **Proceso de un sistema de verificación**

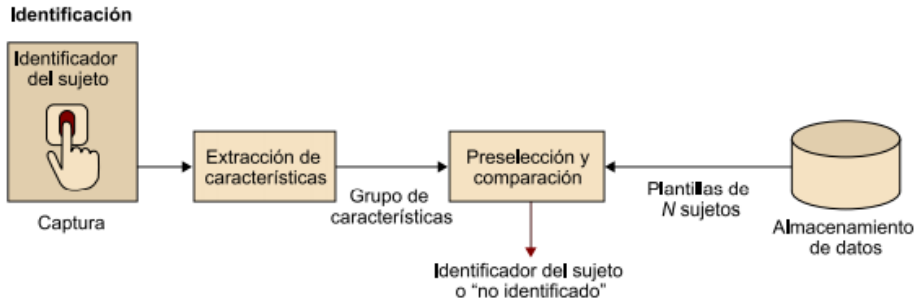


Fuente: SERRATOSA, Francesc. *La biometría para la identificación de las personas.* p. 20.

2.4.2. Sistemas de identificación

Estos sistemas reconocen a la persona a través de la búsqueda del rasgo biométrico que más se asemeja al usado para identificarlo en toda una base de datos. La tarjeta de identificación del individuo no proporciona ninguna información o rasgo con el cual poder comparar su identidad, en cambio, se realiza una comparación con muchos. Esto significa que el rasgo biométrico obtenido en ese instante se compara con una base de datos compuesta de muchos rasgos biométricos almacenados. Puede que la salida del sistema de identificación coincida con un único individuo, una lista de posibles individuos o ningún individuo.

Figura 13. **Proceso de un sistema de identificación**



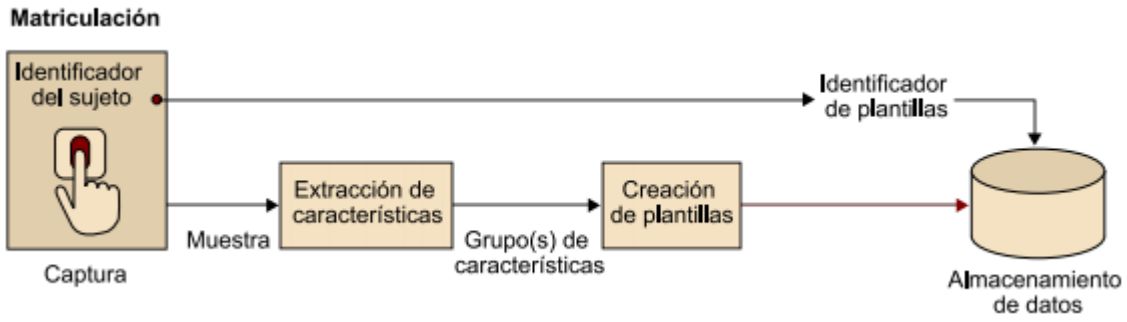
Fuente: SERRATOSA, Francesc. *La biometría para la identificación de las personas.* p. 20.

2.5. Proceso de matriculación

Todos los sistemas biométricos, incluyendo los sistemas de verificación y de identificación cuentan con un proceso precedente llamado “proceso de matriculación”. Está encargado de obtener el rasgo biométrico del individuo junto con su identificación y, posteriormente, de relacionar la información

obtenida. Este proceso debe ser realizado cuidadosamente para velar por la veracidad de la información del individuo, para asegurarse de la calidad del rasgo biométrico recopilado y para relacionar de forma correcta la información, ya que del éxito de este proceso depende la verificación o identificación de un individuo en específico.

Figura 14. **Proceso de matriculación**



Fuente: SERRATOSA, Francesc. *La biometría para la identificación de las personas.* p. 20.

Los sistemas biométricos cuentan con una serie de procesos que a continuación se detallan:

- Captura: el rasgo biométrico regularmente es captado por un dispositivo electrónico compuesto por un sensor especializado para la recolección de determinada característica anatómica.
- Obtención de características: con el propósito de facilitar la comparación de los rasgos biométricos de diferentes capturas, reducir la información innecesaria y aumentar la información útil, la captura original se procesa con un extractor de características para crear una representación compacta compuesta de los rasgos esenciales.

- Creación de plantilla: la plantilla es una forma compacta de representar un conjunto de muestras de una sola característica biométrica.
- Comparación: el proceso de comparación recibe como entrada un registro de identificación y una plantilla, y calcula una distancia entre los dos. En este proceso se define si el individuo sometido al sistema biométrico es identificable o produce una verificación positiva.
- Filtrado: este proceso es útil en sistemas de identificación con mucha información (por ejemplo, 50 millones de huellas dactilares), ya que permite aumentar el método de respuesta del sistema.
- Almacenamiento de la información: en este proceso se almacena la información del usuario. Esta información está compuesta por un identificador único (por ejemplo, número de DPI o pasaporte), la plantilla biométrica y otros datos (como dirección o teléfono de contacto).

Según la necesidad de la aplicación, la información se almacena en sistemas de almacenamiento centralizados (bases de datos estáticas) o en tarjetas electrónicas (base de datos distribuida). Las técnicas de encriptación son aplicadas regularmente a la información (identificación única y rasgo biométrico) para que los datos contenidos sean indivisibles. Según el contexto de aplicación, los sistemas biométricos pueden clasificarse como sistemas en línea o sistemas fuera de línea:

- Sistema en línea: requiere que la respuesta de la comparación de rasgos biométricos sea inmediata. Un ejemplo de este tipo de sistema biométrico es el utilizado en controles de acceso, para permitir o no el ingreso de una persona. Habitualmente, los sistemas de línea son utilizados en la verificación de individuos.

- Sistema fuera de línea: este tipo de sistema no demanda una respuesta inmediata y admite retrasos en la respuesta de comparación de rasgos biométricos. Normalmente, son sistemas de identificación. Los sistemas en línea están automatizados, ya que requieren de rapidez de procesamiento y de respuesta. En cambio, los sistemas fuera de línea pueden ser semiautomáticos, la captura y el análisis del rasgo biométrico puede ser realizada por medios no electrónicos.

3. TARJETAS ELECTRÓNICAS DE PAGO

Al mencionar tarjetas electrónicas de pago se hace referencia principalmente a las tarjetas de crédito o débito, que implican dispositivos electrónicos para completar transacciones financieras. Estos dispositivos fueron creados con la finalidad de facilitar las transacciones comerciales y reducir el flujo de efectivo entre los comerciantes y los compradores.

La tarjeta de crédito tal y como se conoce hoy en día se creó en el año 1949 por un grupo de socios y fue acogida mediante el nombre de Diner's Club. Tras el éxito de esta tarjeta, distintas instituciones bancarias emprendieron la emisión de tarjetas de crédito a lo largo de todo el mundo. Desde ese entonces, las transacciones comerciales evolucionaron hasta llegar a las modalidades de pago con que se cuenta hoy en día.

Dada la evolución de la tecnología, el usuario final tiene la capacidad de realizar transacciones sin necesidad de portar dinero en efectivo, ya sea mediante crédito con su entidad bancaria (tarjetas de crédito) o mediante el débito directo a una cuenta propia (tarjetas de débito).

Según la disponibilidad de la tecnología y la necesidad de proteger la información de cuentas bancarias del usuario, han existido diferentes tipos de tarjetas electrónicas, cada una con sus novedades y ventajas y, de igual manera, con ciertas vulnerabilidades y desventajas que han permitido el avance continuo en el uso de técnicas de seguridad de información.

3.1. Tipos de tarjetas electrónicas de pago

Las tarjetas electrónicas de pago se pueden categorizar según su tecnología de funcionamiento.

3.1.1. Tarjetas de banda magnética

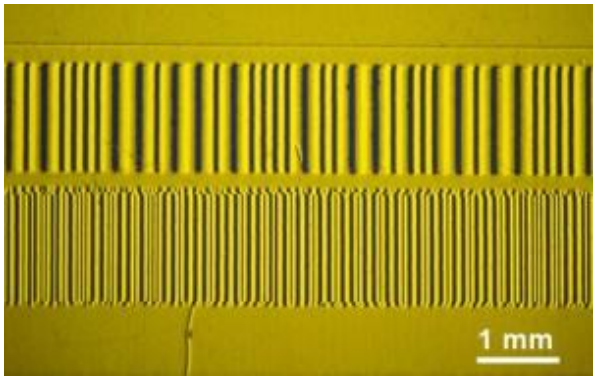
La banda magnética colocada en tarjetas de pago surgió de la necesidad de agilizar las operaciones en distintas entidades, tanto comerciales como financieras, ya que anteriormente un operador tenía que registrar todos los datos de forma manual en una bitácora.

3.1.1.1. Funcionamiento

La banda magnética de una tarjeta de pago emplea el mismo concepto que se usa en los casetes para el registro y reproducción de sonido. Está compuesta por partículas magnéticas en forma de barras sobre una película de plástico[9].

[9] ACOSTA, David. *¿Cómo funcionan las tarjetas de pago? Parte IV: banda magnética.* http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-iv-banda-magnetica/. Consulta: 16 de febrero de 2017.

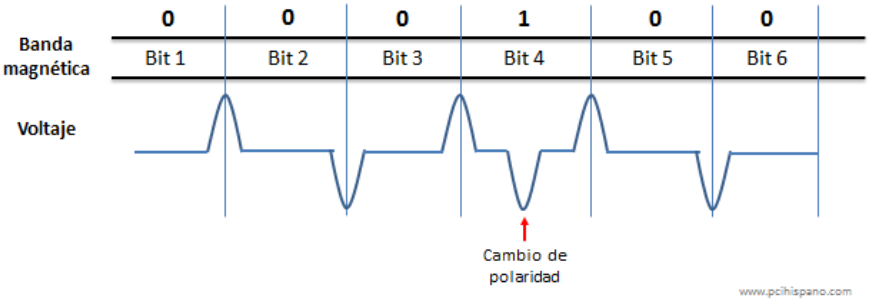
Figura 15. **Partículas magnetizadas en una banda magnética**



Fuente: ACOSTA, David. *¿Cómo funcionan las tarjetas de pago? Parte IV: banda magnética.* http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-iv-banda-magnetica/. Consulta: 16 de febrero de 2017.

Según la polaridad de cada partícula en dicha cinta, así es la codificación de los datos. Los *bits* están definidos por una longitud específica en la cinta. El valor de un *bit* (uno o cero), se define por la presencia o ausencia de un cambio de polaridad en la mitad del *bit* anterior.

Figura 16. **Valor de un *bit* en una banda magnética**



Fuente: ACOSTA, David. *¿Cómo funcionan las tarjetas de pago? Parte IV: banda magnética.* http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-iv-banda-magnetica/. Consulta: 17 de febrero de 2017.

La coercitividad, otro concepto trascendente en las bandas magnéticas, permite la medición de la resistencia del material utilizado en la desimanación. Las dimensionales de este valor son los Oersteds (Oe). Según el nivel de coercitividad, las tarjetas magnéticas se pueden separar en:

- Baja coercitividad (LoCo) – 300 Oe: este tipo de bandas magnéticas tienen un color marrón y para su funcionamiento requieren una baja cantidad de energía magnética para la lectura de datos, por lo que los lectores de este tipo de bandas suelen ser más baratos.
- Alta coercitividad (HiCo) – 2100-400 Oe: este modelo por lo general es de color negro. Son más difíciles de borrar y resistentes, por lo que son usadas en tarjetas que requieren una vida útil más larga. Sin embargo, son más costosas al igual que sus lectores.

La lectura de una tarjeta de banda magnética se hace mediante el deslizamiento de la banda magnética a través de un lector especial denominado *Electronic Data Capture* (EDC) a una cierta velocidad. Esto permite la generación de un fenómeno llamado inducción magnética, cuyo resultado será una serie de voltajes que posteriormente serán decodificados.

3.1.1.2. Ventajas y desventajas del uso de la tecnología de banda magnética

- Ventajas
  - Los costos de fabricación de una tarjeta con banda magnética y las unidades de lectura y escritura son relativamente baratos comparados con otras tecnologías.

- Los dispositivos de lectura y escritura poseen tecnologías compatibles para su fácil instalación en cajeros automáticos, centros de compra y centros financieros.
- Por ser la tecnología precursora, las tarjetas de banda magnética son las más utilizadas globalmente.

- Desventajas
  - La banda magnética contenida en las tarjetas es susceptible a daños causados por la temperatura, polvo, rayado, fricción y/o humedad que pueden alterar la lectura o la imanación de la cinta. La vida útil de una banda magnética es de unas 300-400 lecturas, después de lo cual empieza un proceso de deterioro hasta su inutilización.
  - La exposición de la banda magnética de una tarjeta a un imán o un dispositivo desmagnetizador podría afectar su funcionamiento.
  - La información de la banda magnética se encuentra almacenada en texto plano. No se emplea ningún algoritmo de cifrado para proteger esta información, por lo cual esta tecnología es susceptible a clonación empleando para ello dispositivos portátiles denominados *skimmers*. Estos dispositivos permiten la lectura y almacenamiento de bandas magnéticas para ser grabadas posteriormente en tarjetas vírgenes.

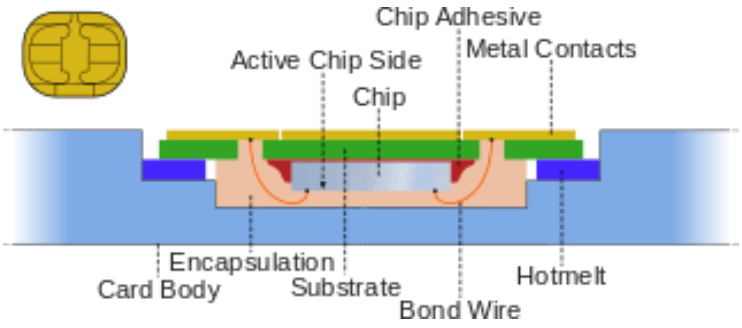
3.1.2. Tarjetas con *chip* integrado

Las tarjetas con *chip* integrado, también conocidas como *Smart Card,* surgieron debido a la necesidad de reforzar la seguridad de la información contenida en las tarjetas de banda magnética, debido a que se encontraron distintas vulnerabilidades que fueron aprovechadas para cometer fraudes.

3.1.2.1. Funcionamiento

De manera distinta a la forma de almacenamiento de información en la banda magnética (texto plano), en las tarjetas con *chip* integrado todos los datos son almacenados de forma cifrada, esto gracias a que los circuitos integrados permiten el uso de algoritmos de encriptación (DES, TripleDES, RSA y SHA). El componente clave de un *chip* es el circuito integrado (IC) que, por lo general, viene cubierto por una serie de capas protectoras de polivinilo, polietileno, poliéster o policarbonatos, acompañado de contactos metálicos que permiten su manipulación. Como tal, el *chip* de una tarjeta de pago no requiere de una batería para su funcionamiento, debido a que la energía requiere ser suministrada por el lector.

Figura 17. **Capas de un *chip* de circuito integrado**



Fuente: ACOSTA, David. *¿Cómo funcionan las tarjetas de pago? Parte V: smart card (chip) y EMV.* http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-v-smart-card-chip-y-emv/. Consulta: 17 de febrero de 2017.

El *chip* utilizado en las tarjetas de pago está bajo los estándares ISO/IEC 7816 e ISO/IEC 7810, que define las características físicas y lógicas de estos elementos:

- C1 – VCC, alimentación
- C2 – RST, reinicio de comunicación
- C3 – CLK, señal de reloj para comunicaciones síncronas
- C4, contacto auxiliar para uso con USB, por ejemplo
- C5 – GND, tierra
- C6 – VPP, programación de memoria no volátil
- C7 – I/O, entrada/salida serial (*halfduplex*)
- C8, contacto auxiliar

Figura 18. **Identificación de contactos metálicos del *chip***

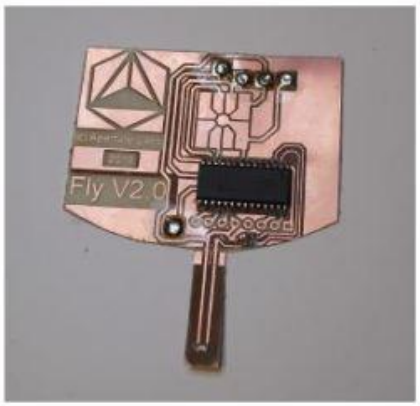
Fuente: ACOSTA, David. *¿Cómo funcionan las tarjetas de pago? Parte V: smart card (chip) y EMV.* http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-v-smart-card-chip-y-emv/. Consulta: 17 de febrero de 2017.

3.1.2.2. Vulnerabilidades de las tarjetas con *chip* integrado

- Migración de la banda magnética al sistema con *chip* integrado: debido a la falta de compatibilidad entre los dispositivos lectores de tarjetas de banda magnética y los dispositivos lectores de tarjetas con *chip*, existen muchas tarjetas que conviven con ambos sistemas, lo cual permite que los datos del usuario aún puedan ser vulnerados.
- Ataques *Yes-Card*: tipo de ataque que consiste en el aprovechamiento de un método de validación por medio de una firma digital estática.

- Ataque *Man-In-The-Middle* (MiTM): tipo de ataque intrusivo que permite que la validación de la tarjeta por medio de PIN siempre sea positiva, con lo cual la transacción es autorizada.
- Chip Skimmer y extracción de PIN: dispositivo diseñado exclusivamente para robar información de un *chip* y así poder clonar una tarjeta con *chip* integrado.

Figura 19. **Chip Skimmer**



Fuente: ACOSTA, David. *¿Cómo funcionan las tarjetas de pago? Parte V: smart card (chip) y EMV.* http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-v-smart-card-chip-y-emv/. Consulta: 17 de febrero de 2017.

3.1.3. Tarjetas Contactless (NFC)

Las tarjetas de pago Contactless o inalámbricas son el eje fundamental de este trabajo. La tecnología inalámbrica NFC posee de forma inherente características de seguridad de la información, esto debido a que no necesita ningún contacto físico para realizar una lectura de datos y, por lo mismo, reduce la vulnerabilidad ante uso de dispositivos que puedan sustraer información. De igual forma, un dispositivo que no requiere de contacto físico tiene mayor vida

útil (comparado con tarjetas de banda magnética que tienen cierta cantidad de lecturas efectivas antes de comenzar a fallar) y reduce las desventajas como la suciedad, desimanación, ataques de *hardware* con finalidad de sustraer información, etc.

3.1.3.1. Funcionamiento

Un sistema de pago inalámbrico está compuesto de tres elementos principales:

- Etiqueta inalámbrica: este elemento está compuesto por un dispositivo con un circuito integrado, un transductor y una antena. Contiene la información que será leída. Este dispositivo puede ser una tarjeta de pago o un dispositivo móvil que contenga la información de cierto usuario.
- Lector inalámbrico: este elemento consta de una antena, un transceptor y un decodificador. Requiere que sea un dispositivo con alimentación de energía continua. Se encarga de estar activo para leer etiquetas que estén a su alcance.
- *Middleware:* este elemento contiene la lógica que permite el procesamiento de la información obtenida por el lector desde la etiqueta.

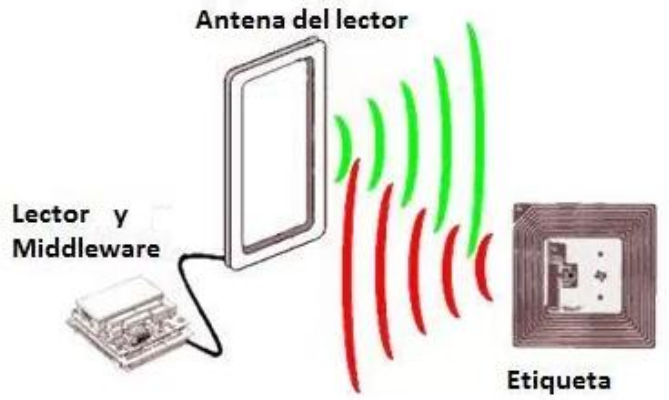
Un dispositivo inalámbrico de pago sigue el siguiente algoritmo:

- El usuario presenta una tarjeta inalámbrica para efectuar su pago.
- El usuario aproxima la tarjeta inalámbrica (a una distancia menor a 10 cm) al dispositivo lector.
- Se realiza la lectura de la información contenida en la tarjeta (de igual manera como se realizaría con una tarjeta de banda magnética o de *chip*

integrado), con la diferencia de que se realiza por medio inalámbrico a través de ondas electromagnéticas.

- Se autentica al usuario y posteriormente se rechaza o aprueba la transacción.

Figura 20. **Esquema de un sistema de pago inalámbrico básico**



Fuente: ACOSTA, David. *¿Cómo funcionan las tarjetas de pago? Parte VI: tarjetas contactless (RFID – NFC).* http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-vi-tarjetas-contactless-rfid-nfc/. Consulta: 20 de febrero de 2017.

3.1.3.2. Vulnerabilidades y oportunidades

Como todo dispositivo electrónico, los sistemas de pago con elementos inalámbricos tienen vulnerabilidades, a continuación se mencionan las más significativas:

- Obtención de información de la tarjeta: mediante un lector que opere en la frecuencia de NFC, es posible leer la información del circuito integrado contenido en la etiqueta, sin embargo, como principal medida de seguridad, la información se encuentra codificada.

- Pagos no autorizados debido a la ausencia de autenticación: la tecnología NFC no requiere ningún tipo de emparejamiento previo para la comunicación entre dispositivos, esto permitiría realizar pagos sin ninguna restricción. En vista de esta vulnerabilidad, se emplea el uso de un dispositivo biométrico que autentica al usuario titular de la tarjeta de pago y restringe su uso si la firma biométrica no coincide con la contenida dentro de la tarjeta.

3.2. Máquina de punto de pago

También conocida como máquina POS (*Point of Sale*), hace referencia a un dispositivo electrónico compuesto por una pantalla, teclado y lectores de tarjetas de pago electrónicas. La máquina POS permite que en un establecimiento se realicen pagos con tarjetas de crédito y débito.

Figura 21. **Máquina POS**

Fuente: POS. https://nationaldailyng.com/2015/armed-robbers-device-e-robbery-use-pos-to-confirms-atm-accounts/. Consulta: 04 de marzo de 2017.

3.3. Cajero automático

También conocido por sus siglas en inglés ATM (Automatic Teller Machine). Consta de una computadora adaptada de tal manera que permite hacer transacciones con dinero de forma automatizada. Utilizando una tarjeta electrónica de pago para la identificación de la cuenta, se pueden realizar diferentes transacciones en un ATM, tales como retiro y depósito de dinero en efectivo, consulta de saldo y pago de servicios.

Figura 22. **Cajero automático (ATM)**

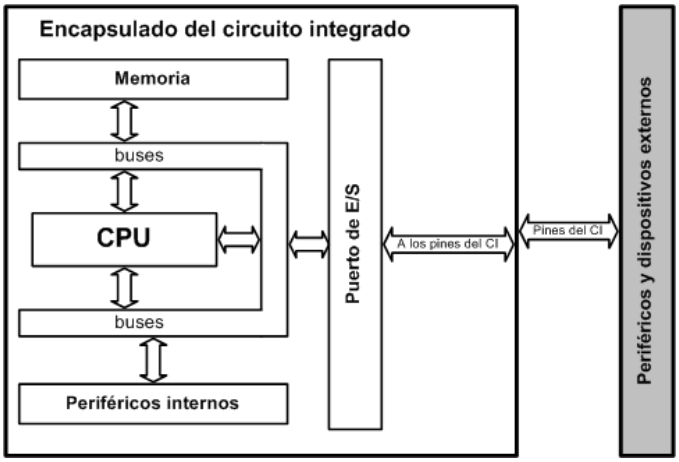
Fuente: *Cajero Automático en Guatemala.* http://www.deguate.com/artman/publish/noticias-guatemala/normalizan-servicio-de-cajeros-automaticos.shtml#.WLtXiVM1_IU. Consulta: 4 de marzo de 2017.

4. CONCEPTOS COMPLEMENTARIOS INVOLUCRADOS EN EL DISEÑO DEL DISPOSITIVO DE PAGO

4.1. Microcontrolador

Un microcontrolador (comúnmente abreviado como µC) es un dispositivo compuesto por circuitos integrados, que puede ser programado para ejecutar órdenes específicas grabadas en su memoria. Está compuesto por tres unidades principales: procesador o unidad central de procesamiento, memorias y puertos periféricos.

Figura 23. **Esquema básico de un microcontrolador**



Fuente: *Esquema de un microcontrolador.* http://juanluisolguin.blogspot.com/2012/11/4-memoria-compartida-distribuida.html. Consultada: 28 de febrero de 2017.

4.1.1. Arquitecturas

- Arquitectura Von Neumann

Este tipo de arquitectura se caracteriza porque tiene una memoria común para el almacenamiento de instrucciones y datos. De igual manera, únicamente posee un único bus para conectar la memoria con el procesador.

- Arquitectura Harvard

Es la arquitectura utilizada en microcontroladores actualmente. En esta arquitectura, cada tipo de memoria tiene un bus de datos, uno de direcciones y uno de control. Cada bus puede adecuarse en tamaño según las características de cada memoria y el acceso a las memorias puede hacerse de forma simultánea. Típicamente los dispositivos con arquitectura Harvard son dos veces más rápidos que dispositivos similares con arquitectura Von Neumann.

4.1.2. Elementos básicos de un microcontrolador

No todos los microcontroladores en el mercado poseen una misma estructura interna, ni mucho menos los mismos componentes. Sin embargo, todos comparten componentes fundamentales.

- Registros

Es un espacio de memoria reservado, en donde se almacenan los resultados de ejecución de instrucciones, se cargan o almacenan datos desde memoria externa.

- Unidad de control

Esta unidad es la encargada de la lógica necesaria para la decodificación y ejecución de las instrucciones, control de registros, la ALU, los buses, entre otros.

- Unidad aritmético-lógica (ALU)

Esta es la unidad encargada de la realización de las sumas, restas y operaciones lógicas relacionadas al álgebra de Boole.

- Buses

Son el medio de comunicación que utilizan los diferentes componentes del procesador para intercambiar información entre sí.

- Memoria

La memoria es un dispositivo que permite el almacenamiento de información, ya sea de forma permanente o de forma temporal.

  - Memoria RAM. Almacenamiento temporal de información.
  - Memoria ROM. Información invariante/permanente.
  - Memoria EPROM. Memoria reprogramable por medio de luz ultra violeta.
  - Memoria EEPROM. Memoria reprogramable eléctricamente.
  - Memoria Flash. Memoria reprogramable con la misma tensión de alimentación del microcontrolador.

- Periféricos

Los puertos periféricos permiten la comunicación del microcontrolador con fuentes externas:

  - Periféricos de entradas y salidas de propósito general.
  - Temporizadores y contadores.
  - ADC. Conversor analógico/digital.
  - PWM. Puertos con capacidad de modular una señal por ancho de pulso.

- Puertos de comunicación

  - Puerto serial

Este tipo de periférico está presente en la mayoría de microcontroladores en forma de UART (Universal Asynchronous Receiver Transmitter) o USART (Universal Synchronous Asynchronous Receiver Transmitter). La principal aplicación de este puerto es la comunicación con otro microcontrolador o con una computadora propiamente, aunque también se utiliza para la comunicación con módulos que permiten completar el funcionamiento del microcontrolador.

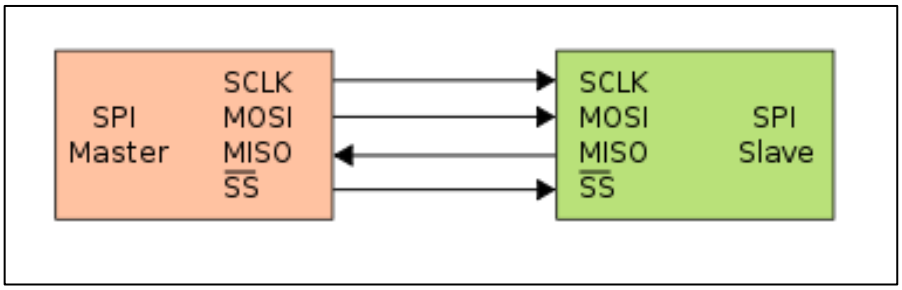
  - SPI

Por sus siglas en inglés, Serial Peripheral Interface es estándar de comunicación, utilizado principalmente en la transferencia de información entre circuitos integrados en equipos electrónicos. SPI es un protocolo síncrono.

- I2C

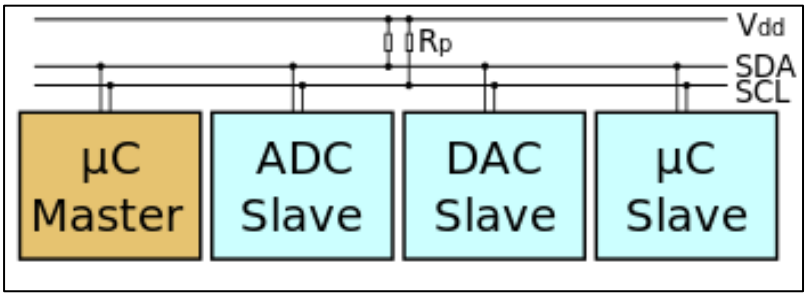
Por sus siglas en inglés, Inter-Integrated Circuit, comunicación utilizada internamente para la comunicación entre partes de un circuito. Está diseñado como un bus maestro-esclavo.

Figura 24. **Bus SPI**



Fuente: *Bus SPI.* Cburnett.https://commons.wikimedia.org/w/index.php?curid=1476502. Consulta: 28 de febrero de 2017.

Figura 25. **Ejemplo de I2C con un maestro y tres esclavos**



Fuente: *Ejemplo de I2C. Cburnett*. https://commons.wikimedia.org/w/index.php?curid=1472017 Consulta: 28 de febrero de 2017.

4.2. Encriptación y seguridad de la información

La encriptación se puede definir como un procedimiento en el cual información importante se vuelve ilegible mediante la aplicación de un código llave con la finalidad de brindar confidencialidad. En la actualidad, existen diferentes algoritmos de cifrado y estos se dividen en:

- Algoritmos de criptográfica simétrica. Se utiliza una misma llave para cifrar y descifrar mensajes.
- Algoritmos de criptografía asimétrica. Se utilizan dos llaves para el envío del mensaje.
- HASH. Cadenas de entrada y salida cifradas como cadenas de longitud fija.

4.2.1. AES

Por sus siglas en inglés, *Advanced Encryption Standard*, AES es un algoritmo de criptografía simétrica que opera con bloques de tamaño fijo de 128 *bits*, cuyas llaves pueden ser de 128, 192 y 256 bits. Este esquema de cifrado puede ser implementado tanto en *hardware* como en *software.* AES consiste en 10 rondas de cifrado para llaves de 128 *bits*, 12 rondas para llaves de 192 *bits* y 14 rondas para llaves de 256 *bits.*

4.2.1.1. Descripción del cifrado AES

El resultado intermedio del cifrado constituye una matriz de *bytes* de cuatro filas por cuatro columnas. A esta matriz se le vuelve a aplicar una serie de ciclos de cifrado basada en operaciones matemáticas (sustituciones no lineales de *bytes*, desplazamiento de filas de la matriz, combinaciones de las

columnas mediante multiplicaciones lógicas y sumas XOR con base en claves intermedias).

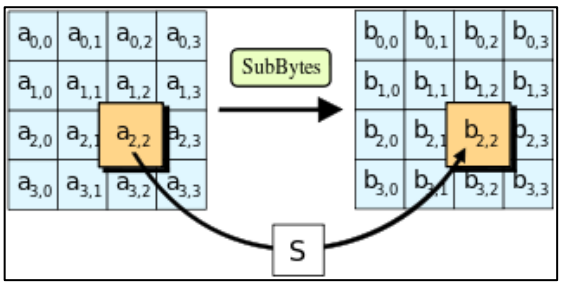
4.2.1.1.1. Pseudocódigo

El cifrado AES se basa en una matriz estado (*state*) y se realiza con el operador lógico XOR (OR exclusivo).

- Etapa Inicial
  - Add Round Key

- Rondas
  - *"Sub-bytes*: en este paso se realiza una sustitución no lineal donde cada *byte* es reemplazado con otro de acuerdo a una tabla de búsqueda"[10].

Figura 26. **Paso Sub-bytes**

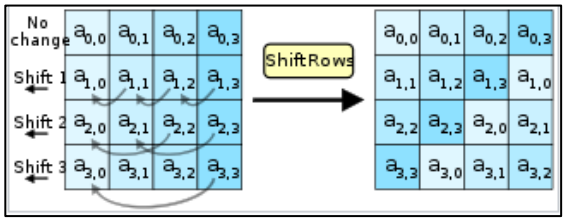


Fuente: *Paso Sub-bytes.* https://es.wikipedia.org/wiki/Advanced_Encryption_Standard. Consulta: 1 de marzo de 2017.

[10] *Paso Sub-bytes.* https://es.wikipedia.org/wiki/Advanced_Encryption_Standard. Consulta: 1 de marzo de 2017.

- *"Shift Rows*: en este paso se realiza una transposición en que cada fila de la matriz estado es rotada de manera cíclica un número determinado de veces[11].

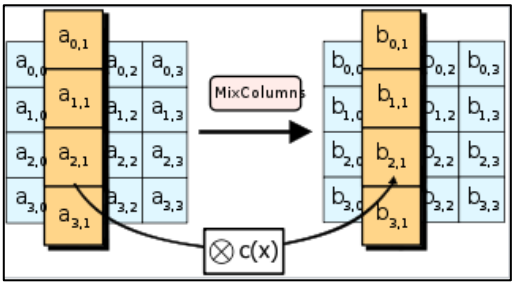
Figura 27. **Paso *Shift Rows***



Fuente: *Paso Shift Rows.* https://es.wikipedia.org/wiki/Advanced_Encryption_Standard. Consulta: 1 de marzo de 2017.

- *"Mix Columns:* operación de mezclado que opera en las columnas de la matriz estado, combinando los cuatro *bytes* en cada columna usando una transformación lineal"[12].

Figura 28. **Paso *Mix Columns***



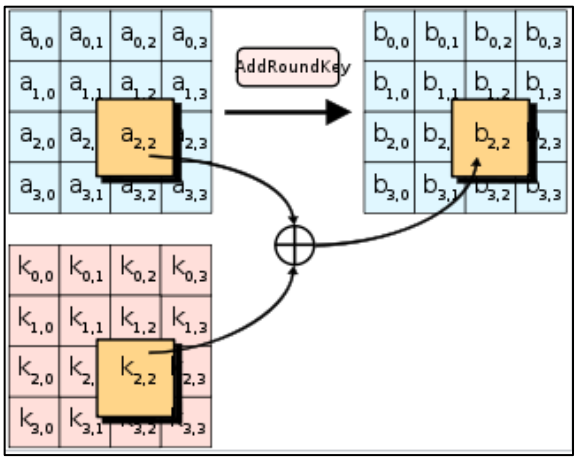
Fuente: *Paso Mix Columns.* https://es.wikipedia.org/wiki/Advanced_Encryption_Standard. Consulta: 1 de marzo de 2017.

[11] *Paso Sub-bytes.* https://es.wikipedia.org/wiki/Advanced_Encryption_Standard. Consulta: 1 de marzo de 2017.
[12] Ibíd.

- *Add Round Key*: cada *byte* de la matriz estado es combinado con la clave de una ronda previa; cada clave de ronda previa se deriva de la clave de cifrado usando una iteración de la clave.

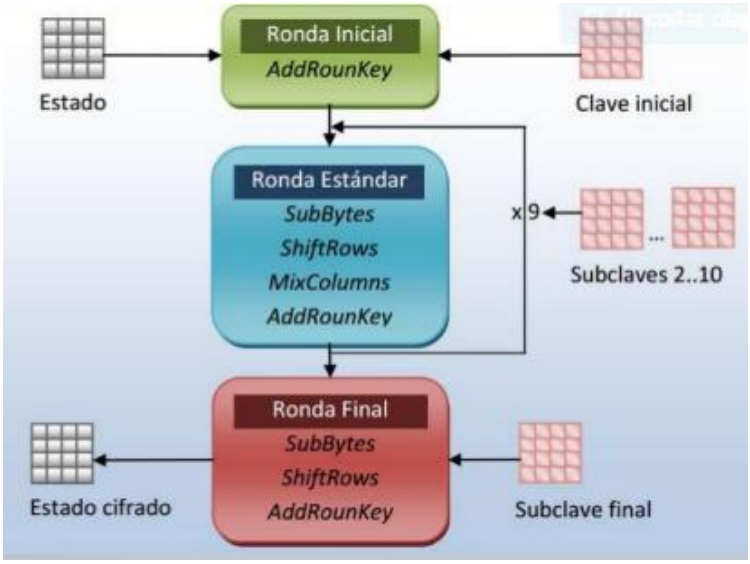
- Etapa Final
  - Sub-bytes
  - Shift Rows
  - Add Round Key

Figura 29. **Paso Add Round Key**



Fuente: *Paso Add Round Key.* https://es.wikipedia.org/wiki/Advanced_Encryption_Standard. Consulta: 1 de marzo de 2017.

Figura 30. **Algoritmo de cifrado AES**



Fuente: VINDA, Elvis. *Explicación AES.* https://es.slideshare.net/elvisvinda/sencilla-explicacin-sobre-aes Consulta: 1 de marzo de 2017.

5. DISEÑO DE DISPOSITIVO DE PAGO ELECTRÓNICO

El dispositivo de pago electrónico propuesto está contemplado para ser utilizado como máquina POS, o bien, para ser adaptado para su uso en cajeros automáticos. Para que el dispositivo sea versátil y adaptable se ha planteado un diseño que consta de diferentes módulos. De igual manera, se presentan los diagramas esquemáticos de los circuitos electrónicos, así como los circuitos en placa impresa, el algoritmo de funcionamiento del dispositivo, las conexiones entre módulos, las indicaciones de uso según la aplicación del dispositivo y, por último, una cotización del proyecto.

5.1. Descripción de módulos electrónicos

5.1.1. Microcontrolador

El microcontrolador propuesto dentro del diseño del dispositivo de pago es el Arduino Due, el cual está basado en un procesador ARM CortexM3 de 32 *bits* y es programable mediante el IDE de Arduino. El microcontrolador dispone de 54 pines digitales de entrada / salida (de los cuales 12 pueden utilizarse para salidas PWM), 12 entradas analógicas, 4 UART (puertas seriales), un reloj de 84 MHz, una conexión USB OTG, 2 DAC, 2 puertos I2C, un puerto SPI, botón de reinicio, un botón de borrado y un conector de alimentación.

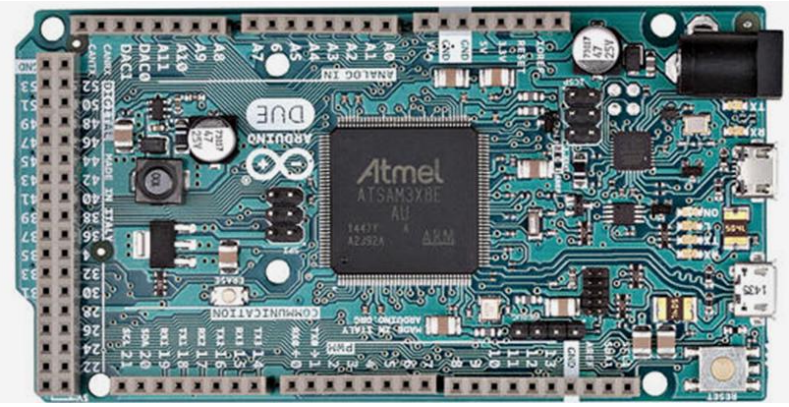
5.1.1.1. Especificaciones técnicas

Tabla VI. **Caracteristicas técnicas del microcontrolador**

Microcontrolador	**AT91SAM3X8E**
Voltaje de operación	3.3 V
Voltaje de alimentación	7-12 V
Límites de voltaje de alimentación	6-16 V
Pines digitales I/O	54
Pines análogos de entrada	12
Pines de salidas analógicas	2 (DAC)
Corriente para pines de 3.3 V	800 mA
Corriente para pines de 5 V	800 mA
Memoria Flash	512 KB
SRAM	96 KB
Velocidad de reloj	84 MHz
Dimensiones	101.52 x 53.3 mm
Peso	36 g

Fuente: *Especificaciones técnicas Arduino Due.*
https://www.arduino.cc/en/Main/ArduinoBoardDue. Consulta: 6 de marzo de 2017.

Figura 31. **Arduino Due y los puertos de programación**



Fuente: *Arduino Due.* https://www.arduino.cc/en/Main/ArduinoBoardDue.
Consulta: 6 de marzo de 2017.

5.1.2. Módulo NFC

Para realizar la lectura y escritura de las tarjetas de pago se propone el uso de un módulo NFC basado en el circuito integrado PN532. Dicho circuito integrado está diseñado para establecer comunicación inalámbrica entre dispositivos que operen a la frecuencia de 13,56 MHz. Dentro del PN532 se encuentra embebido un microcontrolador 80C51. El IC PN532 posee diferentes interfaces para el intercambio de información:

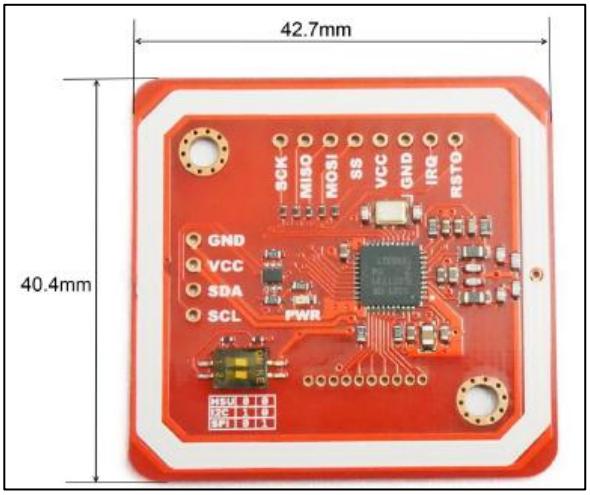
- Interfaz SPI
- Interfaz I2C
- UART

5.1.2.1. Especificaciones técnicas

A continuación se especifican las principales caracteristicas técnicas del módulo de comunicación inalámbrica NFC:

- Microcontrolador 80C51 embebido con ROM de 40 kB y RAM de 1 kB.
- Circuitería analógica dedicada a demodulación y decodificación.
- Distintas interfaces de comunicación: SPI, I2C y UART.
- Oscilador interno de 27,12 MHz.
- Alimentación de 3,3 a 5 V.
- Pines de comunicación para control con dispositivos externos.
- Antena empotrada en PCB.
- Distancia de comunicación de 5 a 7 cm.
- Distintos modos de funcionamiento: lectura/escritura, punto a punto y emulación de tarjeta.
- Dimensiones: 42,7 x 40,4 x 4 mm.

Figura 32. **Módulo NFC**



Fuente: *PN532* Manual. www.elechouse.com. Consulta: 7 de marzo de 2017.

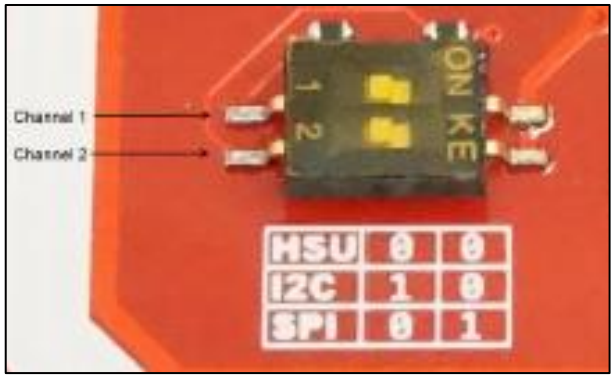
Para seleccionar el modo de funcionamiento del módulo NFC, se debe ajustar el estado del *switch* como se especifica en la tabla VII y se ilustra en la figura 33.

Tabla VII. **Posición del *switch* de selección de interfaz**

Interfaz	Interruptor 1	Interruptor 2
UART	0	0
SPI	0	1
I2C	1	0

Fuente: elaboración propia.

Figura 33. **Ilustración del interruptor de selección de interfaz de comunicación**

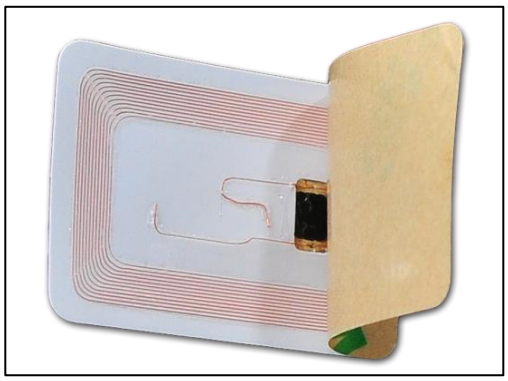


Fuente: *PN532 Manual.* www.elechouse.com. Consulta: 7 de marzo de 2017.

5.1.2.2. Tarjetas NFC Mifare

Para emular tarjetas de crédito o débito se propone el uso de tarjetas NFC Mifare, las cuales son tarjetas de PVC con dimensiones de 85 x 54 mm. Estas tarjetas tienen la peculiaridad de ser de color blanco y permiten la impresión de cualquier diseño de tarjeta de pago sobre su superficie, sin dañar la antena que contiene en el interior. Tienen la capacidad de almacenar 1 kb de información, la cual estaría compuesta por el número de tarjeta, la fecha de vencimiento, el ID del usuario y el ID biométrico encriptado. Además, tienen un vida útil de hasta 10 años, son impermeables y, debido a la naturaleza de su funcionamiento, no sufren desgaste por uso. La escritura de la tarjeta se puede realizar una única vez con el dispositivo de pago propuesto, esto para evitar que se sobrescriba información con el fin de realizar fraudes. Las tarjetas de los usuarios funcionarán como una base de datos distribuida, ya que en ella portarán la información de su rasgo biométrico encriptado con AES, para evitar clonaciones o fraudes de información.

Figura 34. **Tarjeta NFC Mifare**



Fuente: *Tarjeta NFC Mifare.* http://www.mitarjeta.eu/. Consulta: 20 de marzo de 2017.

5.1.3. Sensor de huella digital

Para poder efectuar la autenticación de un usuario se propone el uso de un sensor biométrico capaz de captar la huella digital de un individuo. Específicamente se plantea la utilización del sensor ZFM-20. El ZFM-20 utiliza comunicación asíncrona (UART) semiduplex y la velocidad de comunicación puede ser ajustada de 9600 a 115200 baudios. El sensor incluye un principio de funcionamiento basado en dos etapas: registro de una nueva huella y comparación de huellas. Cuando se hace el registro de una nueva huella digital, el usuario debe colocar su dedo para captar rasgos dos veces, el sistema procesa ambas imágenes, genera una plantilla de la huella y almacena esa plantilla. Cuando se realiza la comparación de huellas, el usuario coloca su dedo en el sensor óptico, el sistema genera una plantilla del rasgo obtenido en ese instante, lo compara con las plantillas almacenadas previamente y el sistema retorna un resultado de comparación.

5.1.3.1. Especificaciones técnicas

Tabla VIII. **Caracteristicas técnicas del sensor ZFM-20**

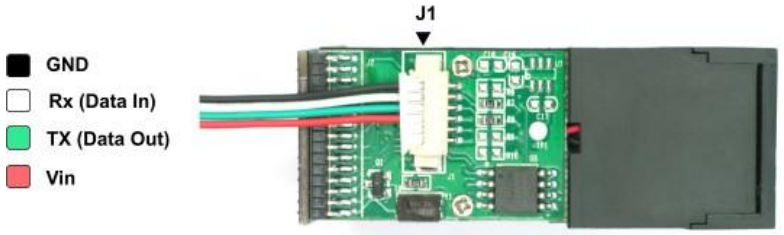
Alimentación	DC 3,6 – 6 V
Corriente de funcionamiento	100 – 150 mA
Baud Rate	9600 – 115200 baudios
Tiempo de adquisición de imagen	< 1 s
Capacidad de almacenamiento	1000 huellas
Tiempo de comparación de huellas	< 1 s
Temperatura de funcionamiento	-10 °C - +40 °C
Interfaz	UART

Fuente: elaboración propia.

5.1.3.2. Comunicación con unidad de control

Para conectar el sensor ZFM-20 al microcontrolador para programar su funcionamiento se debe atender el esquema de conexiones ilustrado en la figura 35. De igual manera, los pines del sensor se especifican en la Tabla IX.

Figura 35. **Diagrama de conexiones del sensor ZFM-20**



Fuente: *ZFM-20.* https://www.robotics.org.za/fingerprint-reader.html. Consulta: 7 de marzo de 2017.

Tabla IX. **Listado de pines del sensor ZFM-20**

Pin	Nombre	Tipo	Descripción
1	VCC	Entrada	Alimentación
2	TX	Salida	Transmisor de UART
3	RX	Entrada	Receptor de UART
4	GND	-	Señal de tierra

Fuente: elaboración propia.

5.1.4. LCD

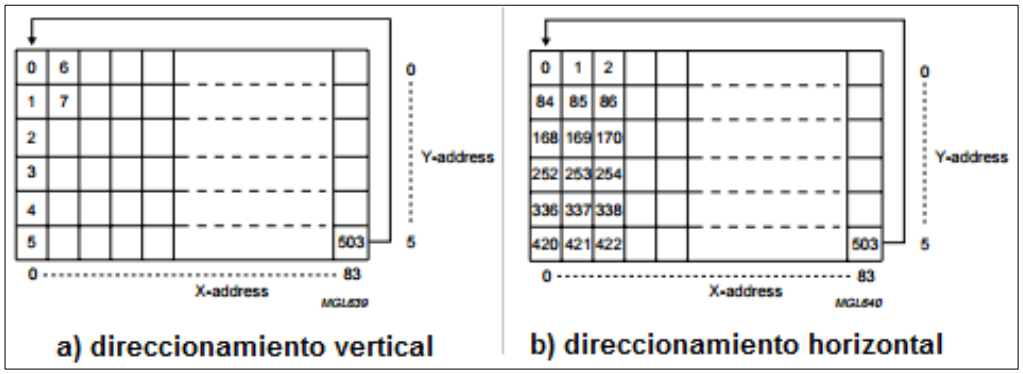
Para la interfaz de comunicación con el usuario, se propone el uso de la LCD PCD8544. Comúnmente esta LCD es conocida porque se encontraba integrada en los celulares Nokia 5110 y, actualmente, se utiliza en proyectos de electrónica que requieren un módulo de visualización. La característica principal de este dispositivo es que presenta un bajo consumo de energía y la interfaz de comunicación que utiliza con un controlador es SPI.

5.1.4.1. Especificaciones técnicas

- Pantalla conformada por 48 filas y 84 columnas.
- RAM de visualización de datos de 48 x 84 bits.
- Pin externo de RESET.
- Velocidad de comunicación serial de 4 Mbps.
- Voltaje de alimentación de circuitos lógicos, 2,7 a 3,3 V.
- Voltaje de alimentación de la pantalla, 6 a 9 V.
- Bajo consumo de energía, ideal para dispositivos alimentados con baterías.
- Temperatura de operación, -25 a + 70 °C.

Existen dos formas de escribir en la pantalla del PCD8544, haciendo una secuencia de escritura de información en la memoria RAM con direccionamiento vertical o con direccionamiento horizontal (ver figura 36).

Figura 36. **Secuencias de escritura en la LCD**



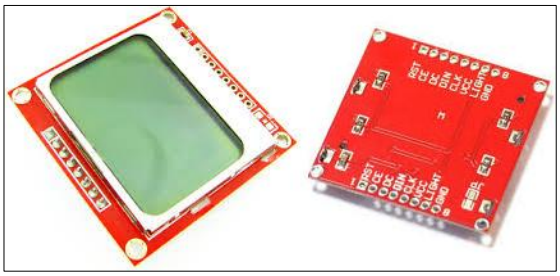
Fuente: elaboración propia, utilizando programa Eagle.

Tabla X. **Asignación de pines para LCD PCD8544**

Pin	Nombre	Descripción
1	VCC	2,7 a 3,3 VDC
2	GND	Tierra
3	SCE	Habilitar *chip*
4	RST	Reset
5	D/C	Comando de selección Bajo – Escribir comando Alto – Escribir información
6	MOSI	Entrada serial
7	SCLK	Entrada de reloj
8	LED	2,7 a 3,2 V

Fuente: elaboración propia.

Figura 37. **LCD PCD8544**



Fuente: *LCD pcd8544.* https://www.espruino.com/PCD8544. Consulta: 8 de marzo de 2017.

5.1.5. Teclado matricial

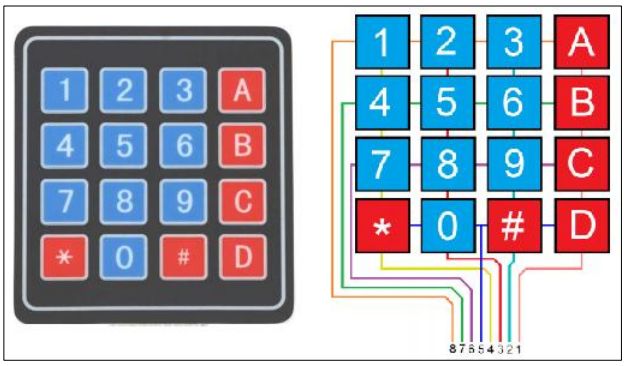
Para que el operador o usuario del dispositivo de pago pueda ingresar valores numéricos relacionados a cantidades de transacciones, se propone la utilización de un teclado matricial de 4 filas x 4 columnas, el cual está compuesto por los números del 0 al 9 más las letras A, B, C, D y los símbolos # y *. El teclado matricial cuenta con 8 pines de conexión, los cuales se conectan a entradas digitales del microcontrolador. Su funcionamiento está basado en una combinación de 4 filas x 4 columnas. Cada botón es un interruptor que está conectado a una fila y una columna específica, verificando el estado del voltaje en cada una de las filas y columnas; el microcontrolador puede establecer qué botón ha sido presionado.

5.1.5.1. Especificaciones técnicas

- Alimentación hasta 24 VDC.
- Vida útil hasta 1 millón de presiones.
- Teclado de 4 filas x 4 columnas, con 8 pines de conexión.
- Temperatura de operación, 0 a 50 °C.

- Dimensiones del teclado 6,9 x 7,6 cm.

Figura 38. **Teclado matricial**

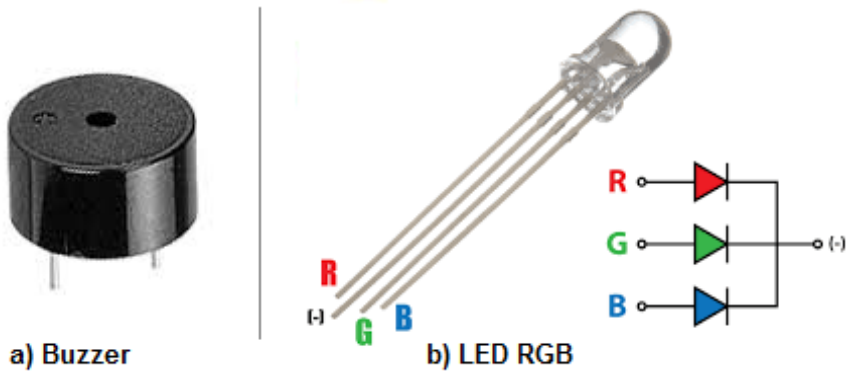


Fuente: *4x4 Matrix Membrane Keypad.* http://www.electronicoscaldas.com/datasheet/Teclado-membrana-matricial-4x4.pdf. Consulta: 08 de marzo de 2017.

5.1.6. Módulo auditivo y visual

Este módulo consiste de un dispositivo de sonido y un dispositivo visual que permiten al operador o usuario del dispositivo de pago estar al tanto del estado de cualquier operación realizada (lectura o escritura de tarjeta, aprobación de transacción, error en operación, etc.). Se propone el uso de un transductor electroacústico, comúnmente conocido como *buzzer*, para generar un sonido indicativo de operaciones y un led RGB (ver figura 39), para generar diferentes colores de luces indicativas según el estado de la operación.

Figura 39. ***Buzzer* y led RGB**



Fuente: elaboración propia, utilizando programa Eagle.

Para generar un sonido en el *buzzer* se debe generar una señal utilizando un pin con capacidad de PWM en el microcontrolador. De igual manera sucede con el led RGB, únicamente que este requiere de 3 pines PWM para generar variaciones de colores en el led.

5.1.7. Fuente de alimentación

Debido a la diversidad de voltajes presentes en los módulos involucrados en el dispositivo de pago electrónico, se propone utilizar un módulo compuesto por reguladores de tensión capaz de brindar diferentes voltajes de alimentación.

En la tabla XI se muestra el rango de voltajes de alimentación permisibles de los módulos involucrados en el dispositivo de pago y la estandarización del voltaje utilizado para cada uno, para así reducir la cantidad de reguladores de tensión a utilizar.

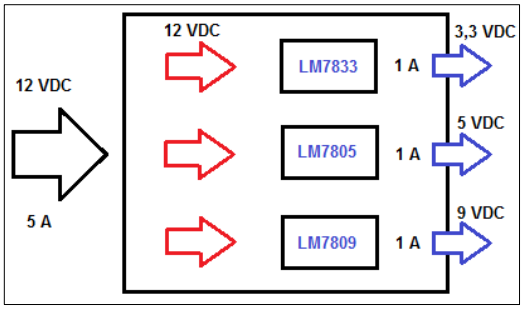
Tabla XI. **Voltajes de alimentación de módulos**

Módulo	Rango de voltaje de alimentación	Voltaje estandarizado
Microcontrolador	7 – 12 VDC	9 VDC
NFC	3,3 – 5 VDC	5 VDC
Sensor de huella	3,6 – 6 VDC	5 VDC
Pantalla de LCD	6 – 9 VDC	9 VDC
Lógica de LCD	3,3 VDC	3,3 VDC
Visual y Audio	3,3 – 12 VDC	5 VDC

Fuente: elaboración propia.

Según la columna de voltajes estandarizados de la tabla XI, se debe crear un módulo con la capacidad de entregar tres diferentes niveles de tensión, 3,3, 5 y 9 VDC. Según estos datos, y considerando una corriente de consumo máxima por nivel de tensión de 1 A, se propone el uso de los siguientes modelos de reguladores de tensión: LM7833 (regulador de 3,3 VDC), LM7805 (regulador de 5 VDC) y LM7809 (regulador de 9 VDC), tomando en consideración una fuente de alimentación general de 12 VDC con 5 A de capacidad. En la figura 40 se ilustra el módulo de alimentación anteriormente descrito:

Figura 40. **Esquema de módulo de alimentación**



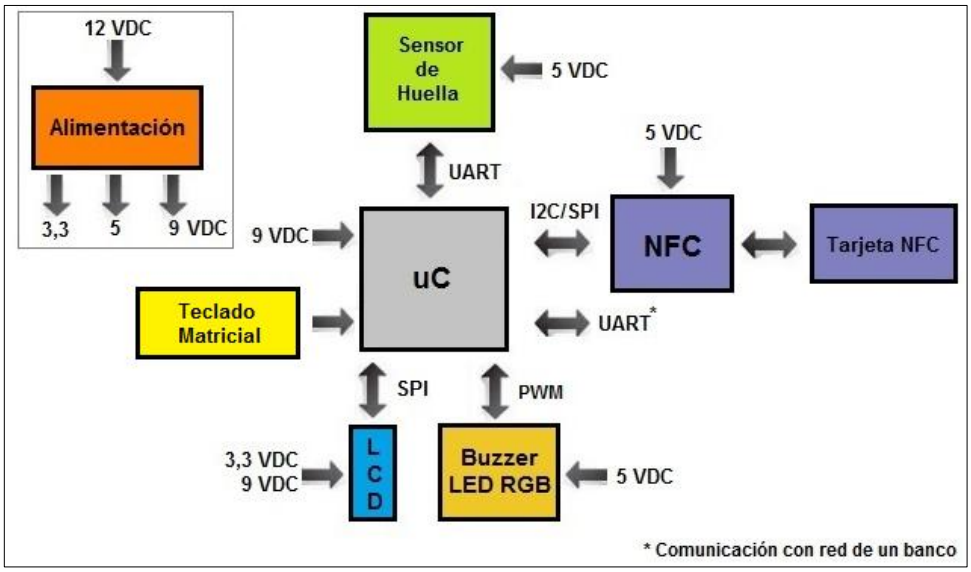
Fuente: elaboración propia, utilizando programa Eagle.

5.2. Diagrama de bloques del dispositivo

Como se describió en la sección anterior, el dispositivo de pago está compuesto por varios módulos electrónicos. En la figura 41 se presenta un diagrama de bloques en el cual se especifica la jerarquía del diseño, la interfaz de comunicación entre módulos y el voltaje de alimentación.

Como se puede observar en dicha figura, el microcontrolador es la unidad de control del dispositivo, de este se derivan los módulos periféricos que cumplen diversas funciones. El módulo de alimentación es el encargado de adaptar los niveles de voltaje y de alimentar a cada uno de los módulos periféricos (3,3, 5 y 9 VDC). El sensor de huella cumple la función de recolectar el rasgo biométrico del usuario (tanto en el registro de un nuevo usuario, como en la autenticación de un usuario existente) y enviarlo como un código al microcontrolador por medio de UART. La LCD es la encargada de presentar gráficamente en una pantalla la información del proceso de pago y autenticación; se comunica por medio de SPI con el microcontrolador. La unidad auditiva y visual está compuesta por un *buzzer* y un LED RGB, y estos son controlados por medio de pulsos modulados (PWM). El módulo NFC es el encargado de la lectura y escritura (únicamente cuando se registra un nuevo usuario) de información contenida en la tarjeta de pago; se comunica por medio de I2C o SPI con el microcontrolador. Al mismo tiempo, el módulo NFC se comunica con la tarjeta de pago por medio de radiofrecuencia. El teclado matricial permite el ingreso de datos numéricos. El microcontrolador también envía la información recolectada de la tarjeta de pago por medio de UART para hacer posible las operaciones de seguridad y las transacciones con la red bancaria.

Figura 41. **Diagrama de bloques del dispositivo de pago**



Fuente: elaboración propia, utilizando programa Eagle.

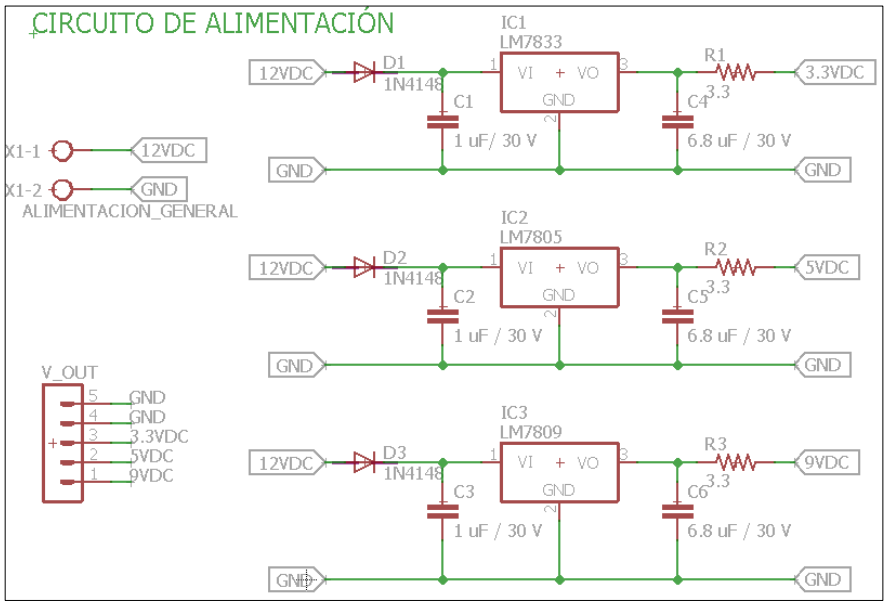
5.3. Diagramas esquemáticos de circuitos electrónicos

5.3.1. Circuito de alimentación

El circuito de alimentación representado en la figura 42 está compuesto principalmente por tres reguladores de tensión, esto debido a la variedad de voltajes de alimentación de los circuitos integrados involucrados (tabla XI). El circuito integrado LM7833 está diseñado para brindar una tensión de salida de 3,3 VDC, el CI LM7805 brinda una tensión de salida de 5 VDC y el LM7809 permite obtener un nivel de tensión de 9 VDC. Cada uno de los reguladores posee un pin de voltaje de entrada, un pin de referencia (GND) y otro pin de voltaje de salida. Los diodos 1N4148 se utilizan con el propósito de proteger contra cortocircuitos al regulador. De igual forma, se considera la utilización de dos capacitores, uno de 1 µF conectado en paralelo a la entrada de cada

regulador, con el propósito de mejorar el rechazo al rizado de la señal de entrada, y otro de 6,8 µF con el propósito de mejorar la respuesta a transitorios.

Figura 42. **Circuito de alimentación del dispositivo de pago**

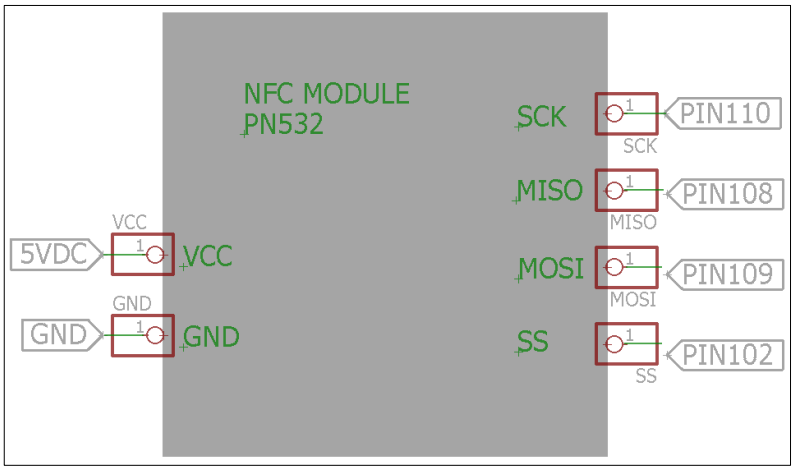


Fuente: elaboración propia, utilizando programa Eagle.

5.3.2. Diagrama de conexiones del Módulo NFC

El diagrama presentado en la figura 43 muestra las conexiones del módulo NFC. Este módulo es alimentado con 5 VDC. Debido a que la comunicación del módulo con el microcontrolador se realiza con el protocolo SPI, se requiere el uso de cuatro pines del microcontrolador: SCLK, que es el pulso que marca la sincronización entre los dispositivos; MOSI, que es la salida de datos del microcontrolador hacia el módulo NFC; MISO, que es la salida de datos del módulo NFC hacia el microcontrolador, y SS, que es el seleccionador de módulo esclavo controlado por el microcontrolador.

Figura 43. **Conexiones del módulo NFC**



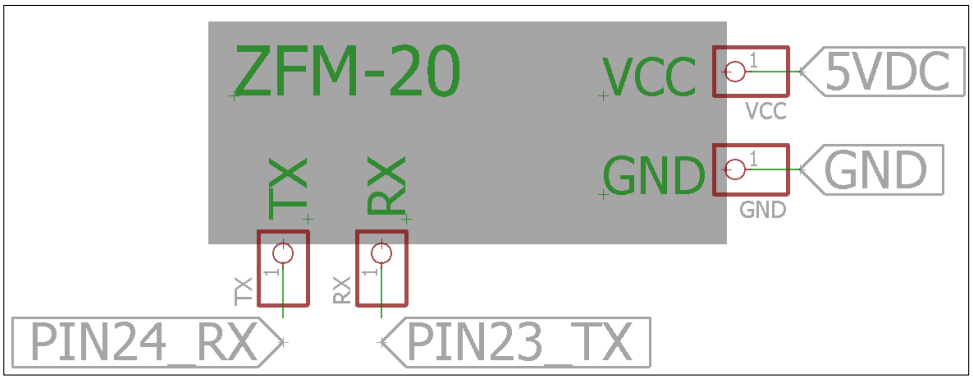
Fuente: elaboración propia, utilizando programa Eagle.

5.3.3. Diagrama de conexiones del sensor de huella digital

El diagrama presentado en la figura 44 muestra las conexiones del sensor de huella digital. Este módulo requiere una alimentación de 5 VDC, por lo tanto posee un pin de voltaje de alimentación y otro de nivel de referencia (GND). El módulo sensor de huella digital se comunica con el microcontrolador mediante el sistema de comunicación serial Transmisor-Receptor Asíncrono Universal (UART).

El microntrolador propuesto en el diseño del dispositivo de pago (figura 31) cuenta con cuatro puertos de comunicación UART, los cuales intercambian información serial TTL a un nivel de tensión de 3,3 V. Un puerto UART del microcontrolador se utiliza exclusivamente para la comunicación entre el sensor de huella digital y el microcontrolador. El transmisor del sensor (Tx) se conecta con el receptor del microcontrolador (pin 24) y el receptor del sensor (Rx) se conecta con el transmisor del microcontrolador (pin 23).

Figura 44. **Conexiones del sensor de huella digital**



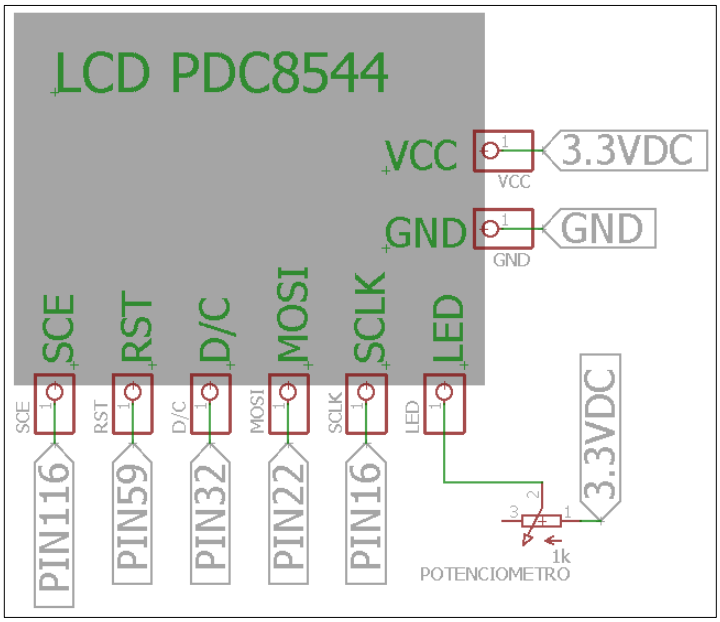
Fuente: elaboración propia, utilizando programa Eagle.

5.3.4. Diagrama de conexiones de la LCDPCD8544

El diagrama de la figura 45 representa las conexiones de la LCD PCD8544. Este módulo de visualización requiere de un voltaje de alimentación de 3,3 VDC. La LCD se basa en el protocolo SPI para comunicarse con el microcontrolador. El pin SCLK es el pulso que marca la sincronización entre los dispositivos; MOSI es la salida de datos del microcontrolador hacia la LCD; MISO es la salida de datos de la LCD hacia el microcontrolador, y SCE es el seleccionador de módulo esclavo controlado por el microcontrolador.

Además de los pines de comunicación SPI, esta pantalla incluye el pin de entrada (D/C), que corresponde a la selección de comandos de información, y el pin de reseteo (RST). Para controlar la iluminación de la LCD, este módulo posee un pin de entrada que está conectado a un led interno. Para tener la opción de ajustar el nivel de iluminación de la pantalla se conecta un potenciómetro al pin led, como se muestra en la figura 45, con el fin de regular la corriente que llega al led interno de la pantalla.

Figura 45. **Conexiones de la LCD PDC8544**

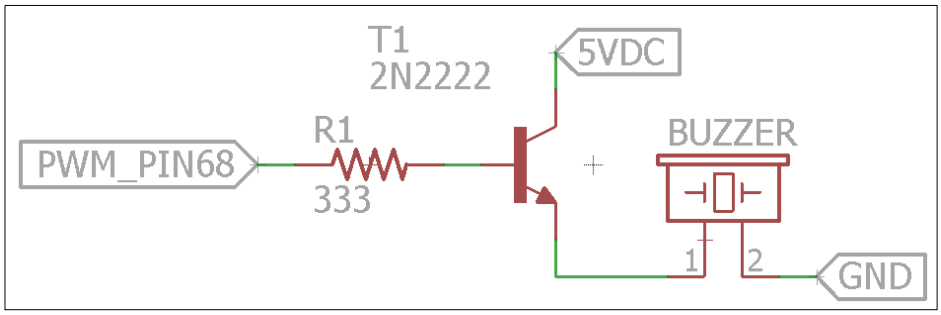


Fuente: elaboración propia, utilizando programa Eagle.

5.3.5. Circuitos del módulo visual y auditivo

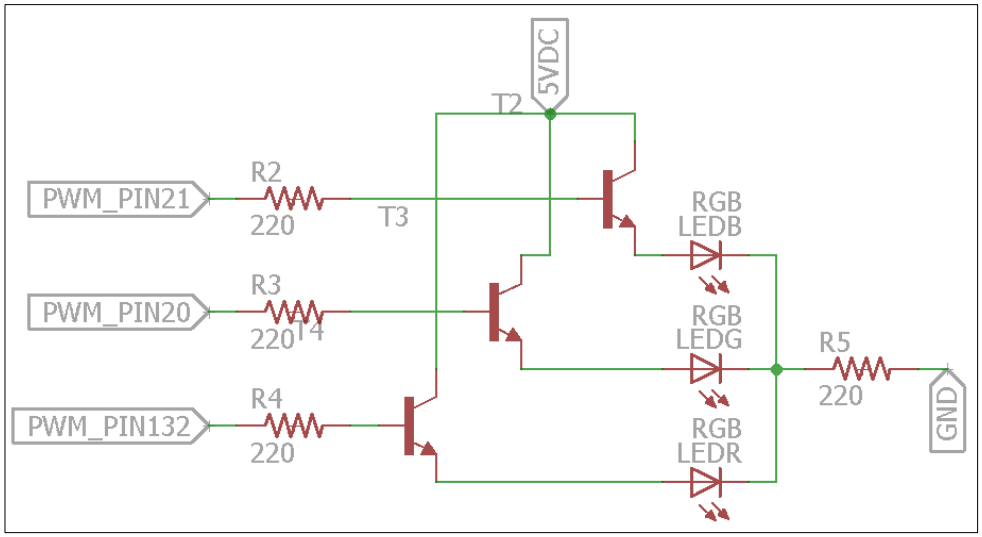
El módulo visual y auditivo está compuesto por dos circuitos electrónicos. El circuito del *buzzer* se muestra en la figura 46. El *buzzer* cumple la función de transductor de señales eléctricas a señales auditivas. La señal eléctrica es generada por el microcontrolador y puede variar el ancho de los pulsos que componen a la señal mediante el uso de la modulación por ancho de pulsos (PWM). El transistor T1 presente en el circuito de la figura 46 funciona como un interruptor. Con la incidencia de corriente en la base del transistor se genera continuidad de corriente entre el colector y el emisor, permitiendo la alimentación del *buzzer* con 5 VDC, generando un sonido en particular. Un pin del buzzer se conecta hacía el emisor del transistor y el otro pin se conecta a tierra (GND).

Figura 46. **Circuito de control del *buzzer***



Fuente: elaboración propia, utilizando programa Eagle.

Figura 47. **Circuito de control del led RGB**



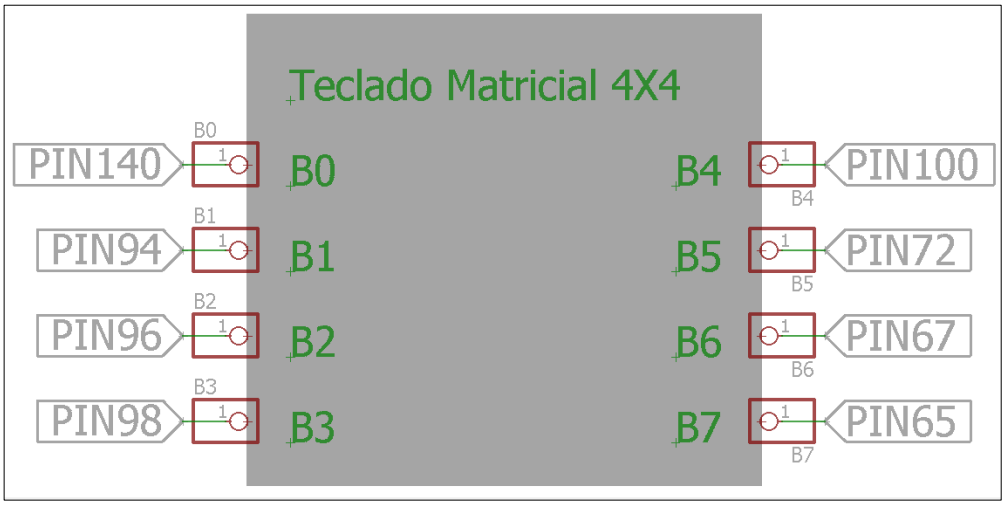
Fuente: elaboración propia, utilizando programa Eagle.

En la figura 47 se muestra el circuito del led RGB, este funciona de la misma manera que el circuito de la figura 46, únicamente con la particularidad de que la carga en uno es el *buzzer* y en el otro son tres diodos que componen al led RGB. Las resistencias colocadas entre el pin del microcontrolador y la

base de cada transistor se encargan de regular la corriente que llega hacía cada una de las bases. En el caso del led RGB, cada ánodo de los diodos se conecta a los emisores respectivos y el cátodo común se conecta a una resistencia conectada a tierra (GND). Esta última tiene la función de regular la corriente que atraviesa cada uno de los diodos para así evitar el daño por sobrecorrientes.

5.3.6. Diagrama de conexiones del teclado matricial 4x4

Figura 48. **Conexiones del teclado matricial 4x4**

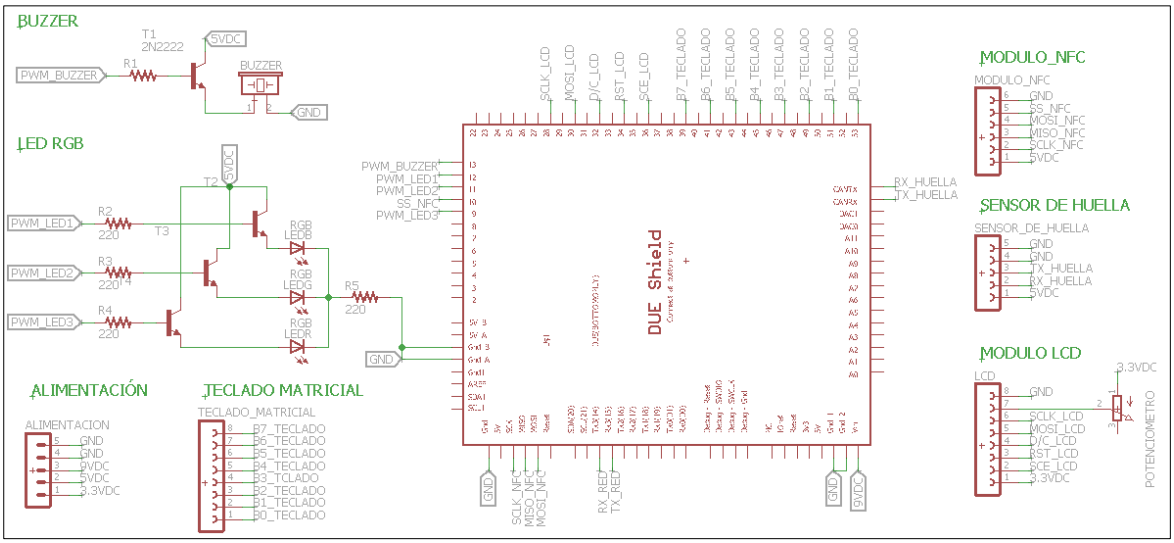


Fuente: elaboración propia, utilizando programa Eagle.

En la figura 48 se muestran las conexiones del teclado matricial con el microcontrolador. El teclado matricial propuesto en el diseño del dispositivo de pago consta de un arreglo de botones conectados en filas y columnas. Para comunicar el teclado con el microcontrolador son necesarios ocho pines, o bien, un puerto del microcontrolador. En el diagrama de la figura 48 se muestra la asignación de *bits* del teclado a pines del microcontrolador.

5.3.7. Diagrama esquemático de los circuitos interconectados

Figura 49. **Esquemático general del dispositivo de pago**



Fuente: elaboración propia, utilizando programa Eagle.

En la figura 49 se muestra un diagrama esquemático de todos los circuitos y conexiones entre los módulos que componen el dispositivo de pago electrónico. Este diagrama se utiliza para el diseño de la placa de circuito impreso del dispositivo de pago.

Tabla XII. **Pines utilizados en el microcontrolador**

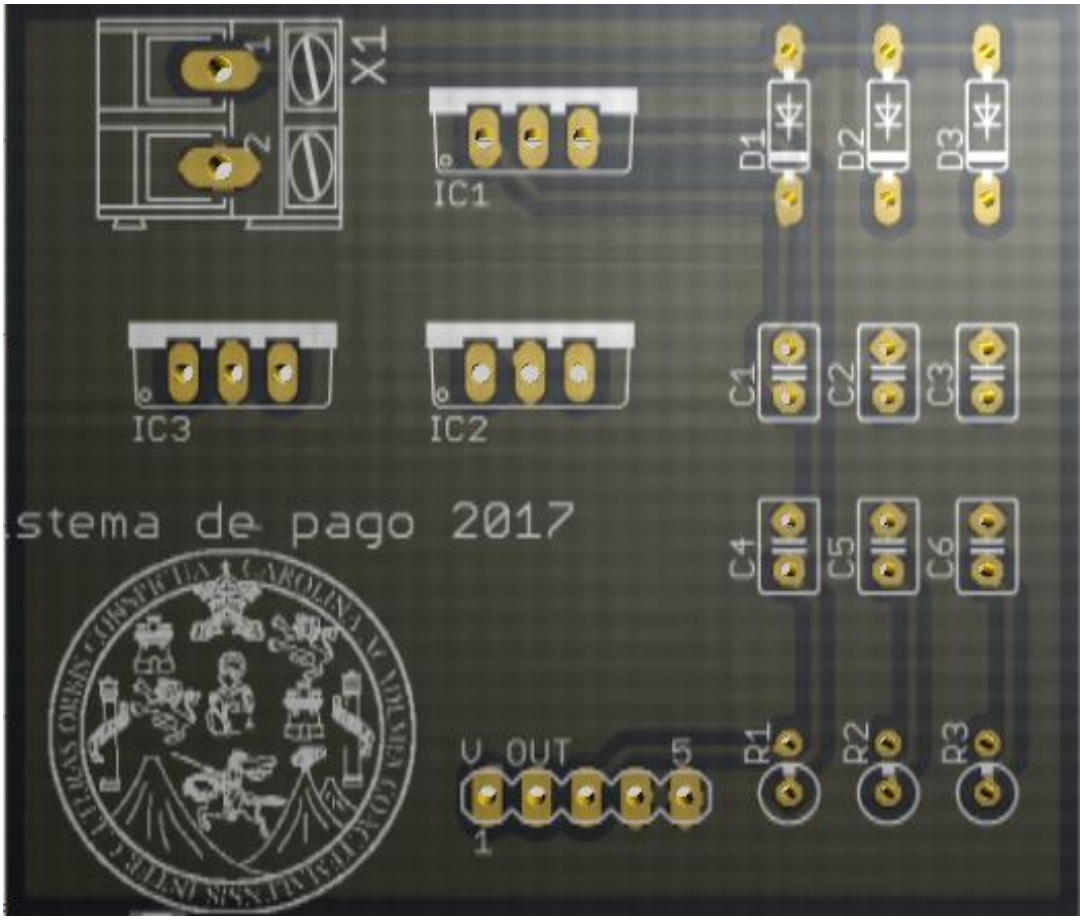
Pines utilizados en el microcontrolador Arduino Due	
Número de pin físico	**Descripción**
VIN	Voltaje de alimentación 9 VDC
GND	Nivel de referencia, tierra
16	SCLK de LCD
17	Datos hacia red bancaria (Tx)
18	Datos desde red bancaria (Rx)
20	PWM del LED 2 RGB
21	PWM del LED 1 RGB
22	MOSI de LCD
23	Datos desde el sensor de huella (Rx)
24	Datos hacia el sensor de huella (Tx)
32	D/C de LCD
59	Reset de LCD (RST)
65	Bit 7 del teclado matricial (B7)
67	Bit 6 del teclado matricial (B6)
68	PWM del Buzzer
72	Bit 5 del teclado matricial (B5)
94	Bit 1 del teclado matricial (B1)
96	Bit 2 del teclado matricial (B2)
98	Bit 3 del teclado matricial (B3)
100	Bit 4 del teclado matricial (B4)
102	Seleccionador de módulo NFC (SS)
108	MISO módulo NFC
109	MOSI módulo NFC
110	SCLK módulo NFC
116	Seleccionador de módulo de LCD (SCE)
132	PWM LED 3 RGB
140	Bit 0 del teclado matricial (B0)

Fuente: elaboración propia, utilizando mapa de pines del Arduino DUE.

En la tabla XII se muestra una lista de los pines utilizados en el microcontrolador y la descripción de cada uno de ellos.

5.4. Placas de circuito impreso del dispositivo de pago

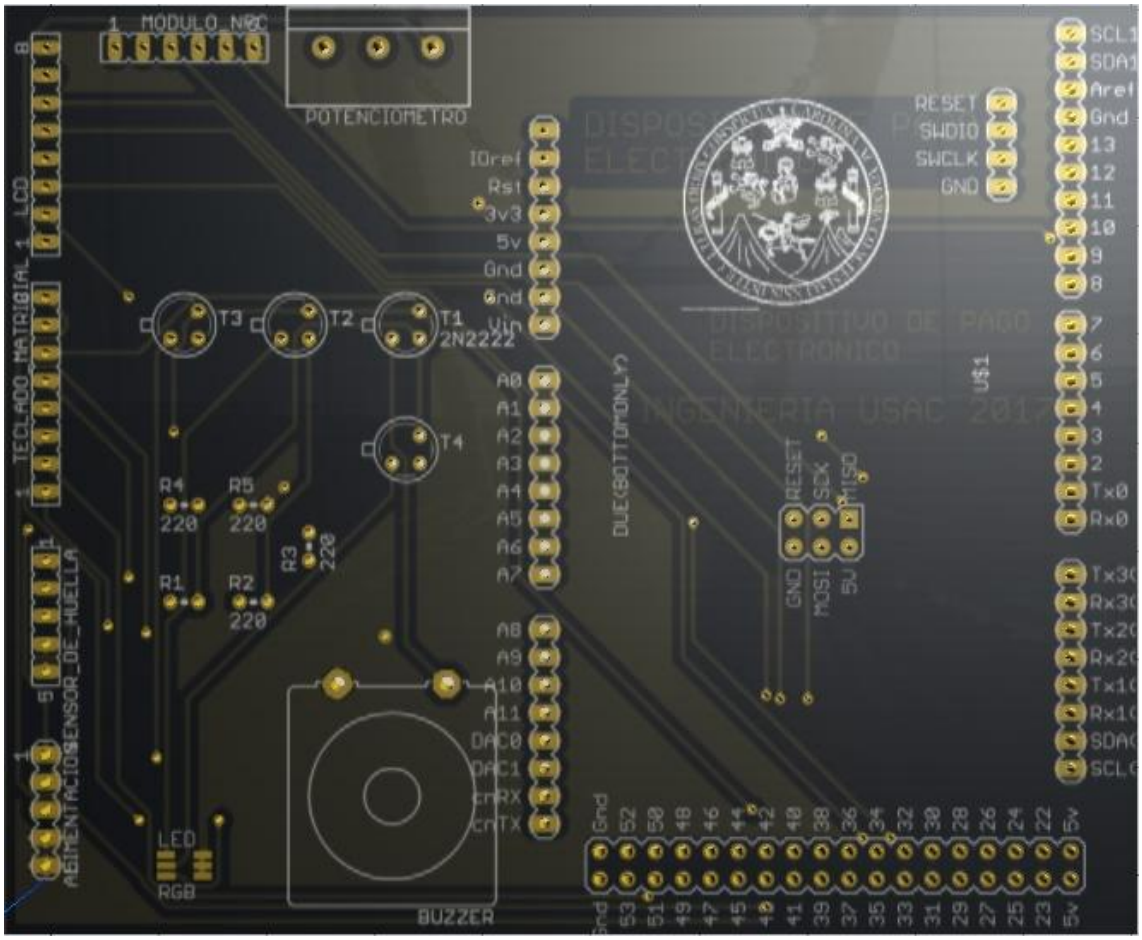
Figura 50. **PCB de circuito de alimentación del dispositivo**



Fuente: elaboración propia, utilizando programa Eagle y visualizador online 3D BRD.

En la figura 50 se muestra la placa de circuito impreso (PCB) del circuito de alimentación del dispositivo y, de igual forma, se indica la ubicación de cada uno de los componentes electrónicos que la componen.

Figura 51. **PCB del dispositivo de pago electrónico**



Fuente: elaboración propia, utilizando programa Eagle y visualizador online 3D BRD.

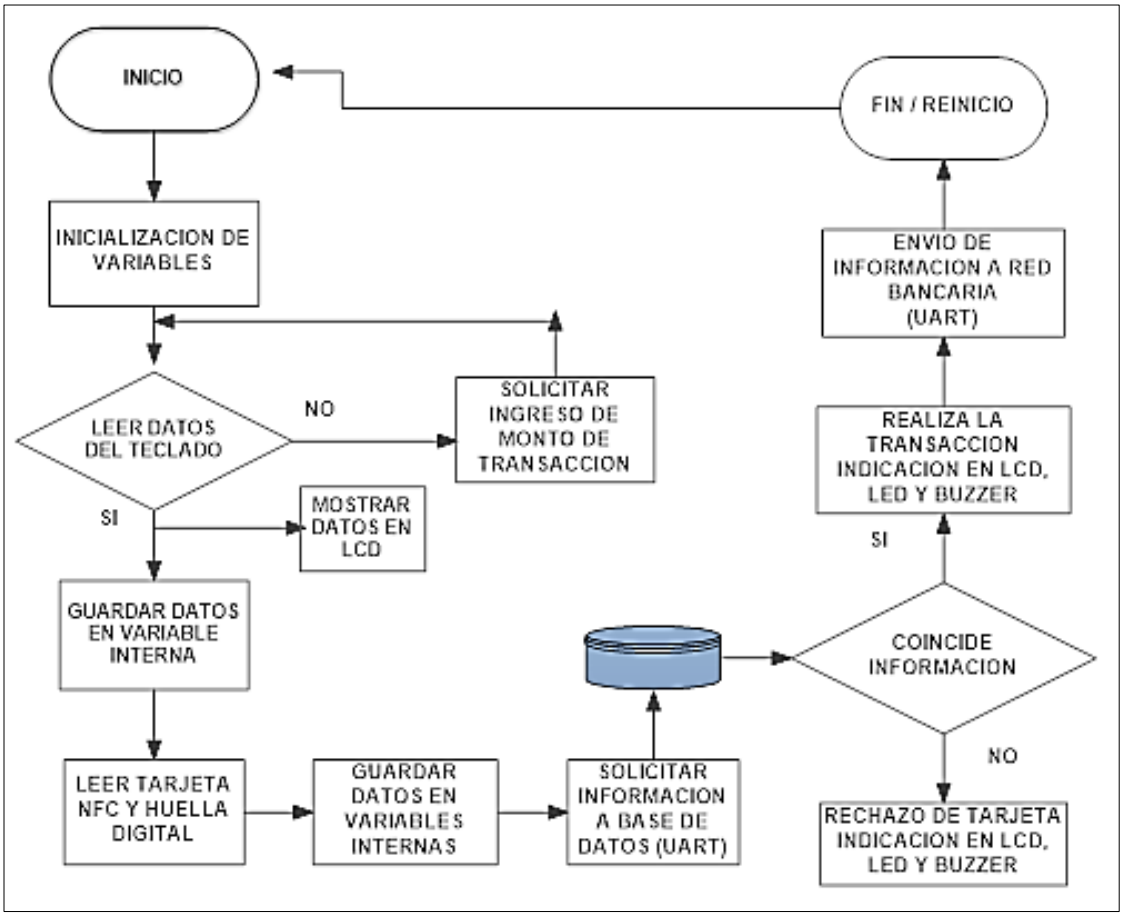
En la figura 51 se muestra el diseño de la placa de circuito impreso que incluye el módulo del microcontrolador, el módulo visual y auditivo, y las conexiones con la LCD, así como el módulo NFC, el módulo de alimentación, el teclado matricial y el sensor de huella digital. De igual forma se indica la posición de cada uno de los componentes electrónicos.

5.5. Programación del dispositivo de pago

5.5.1. Diagrama de flujo

El microcontrolador debe ser programado para poder controlar los módulos que componen al sistema de pago en general. En la figura 52 se muestra el diagrama de flujo del programa de control.

Figura 52. **Diagrama de flujo del programa de control**



Fuente: elaboración propia, empleando Microsoft Visio.

5.5.2. Algoritmo del programa

A continuación se describe el algoritmo del programa de control propuesto para el dispositivo de pago electrónico. Este algoritmo está basado en el diagrama de flujo representado en la figura 52.

- Inicio del programa.
- Importación de librerías y módulos, declaración e inicialización de variables.
- Declaración e inicialización de pines de puertos a utilizar para los módulos electrónicos.
- Inicialización de módulos de comunicación serial (establecer velocidad de transmisión, puerto serial a utilizar, entre otros).
- Lectura de datos provenientes del teclado matricial (cantidad de cobro o retiro de dinero).
- Impresión de datos ingresados en LCD.
- Almacenamiento de datos en variables internas.
- Lectura de tarjeta NFC y sensor de huella digital.
- Lectura de datos provenientes de la tarjeta NFC y el sensor de huella digital y almacenamiento en variables internas.
- Impresión de datos de usuario en LCD.
- Solicitud de datos utilizando comunicación serial asíncrona (ID de usuario y llave de desencriptación).
- Desencriptación de información.
- Comparación entre datos para autenticar la tarjeta de pago (rasgo biométrico obtenido y rasgo desencriptado y almacenado en tarjeta).
- Impresión en pantalla del resultado del paso anterior (aceptación o rechazo de transacción).

- Envío de información por medio de UART hacía la red bancaria, para actualización de datos.
- Fin de programa y reinicio.

En los anexos se incluye una reseña del IDE de programación del microcontrolador y ejemplos de códigos de programación para cada módulo involucrado en el dispositivo de pago.

5.6. Funcionamiento del dispositivo de pago

A continuación se describen los pasos a seguir para el correcto funcionamiento del dispositivo de pago electrónico. Por medio de diagramas de flujo se realiza una representación gráfica de los pasos que deben ejecutarse para utilizar el dispositivo, e igualmente los pasos a seguir en el proceso de matriculación de un nuevo usuario. De igual forma, se exponen imágenes de la interfaz de usuario del dispositivo y se indican las señales visuales y auditivas que este genera al realizar determinada acción.

5.6.1. Procedimiento para cobro o retiro de dinero utilizando el dispositivo

El siguiente algoritmo está basado en el diagrama de flujo de la figura 53 e indica el procedimiento a seguir para utilizar el dispositivo de pago.

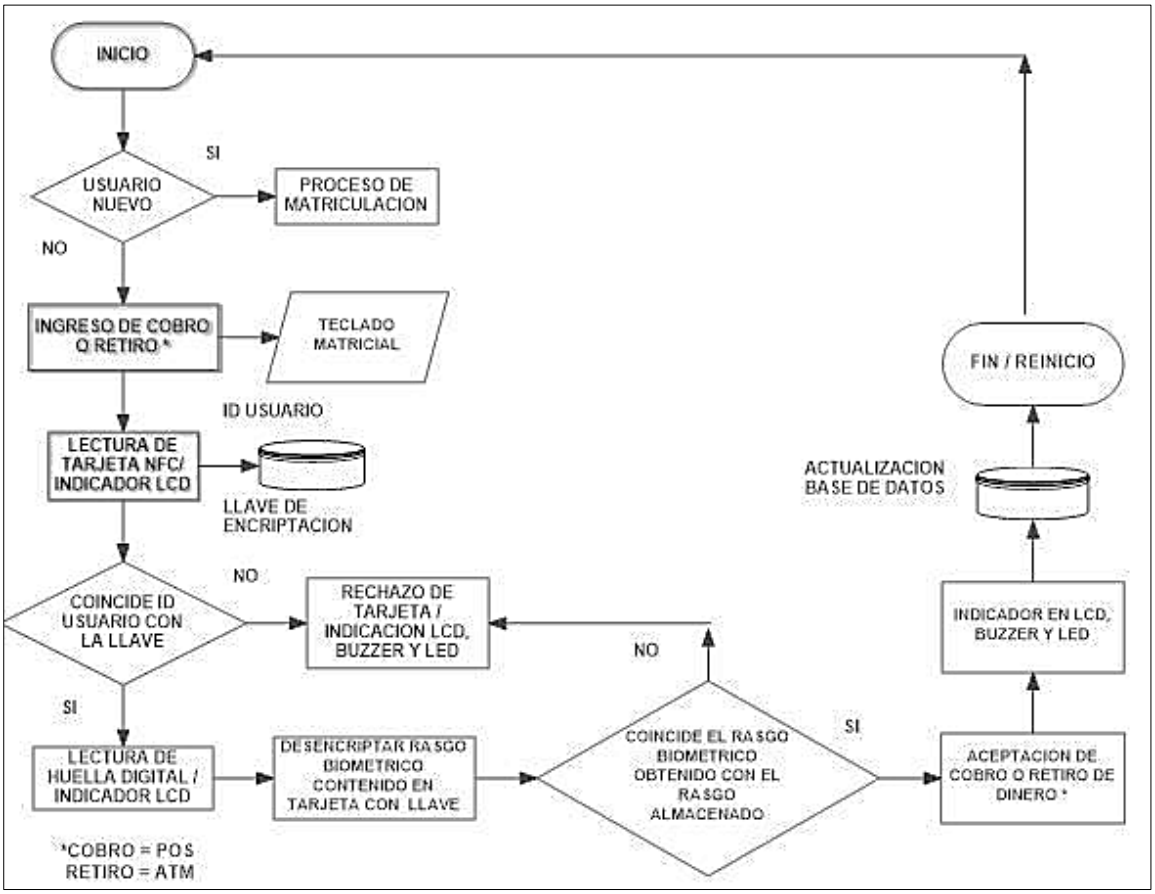
- El proceso inicia con el pago de un usuario por medio de tarjeta electrónica NFC o el retiro de efectivo en un ATM utilizando tarjeta electrónica inalámbrica.
- Si el usuario es nuevo, procede el proceso de matriculación (figura 54). En cambio, si el usuario ya existe, se debe ingresar el monto a cobrar

(POS) o el monto a retirar (ATM) por medio del teclado matricial y presionar la tecla A para proceder.

- En la pantalla LCD se muestra la cantidad ingresada y como confirmación se debe presionar la tecla “A”. Si la cantidad ingresada no es la correcta, se debe presionar la tecla “B” y se ingresa la cantidad correcta. El proceso anterior se repite hasta que la cantidad sea confirmada.
- En la pantalla LCD se indica al usuario que coloque su tarjeta a 5 cm aproximadamente del lector NFC para proseguir con el pago. Con el ID de usuario obtenido, se solicita a la base de datos de la red bancaria la llave simétrica de encriptación.
- En el procesamiento interno de información, se realiza una comparación entre el ID de usuario y la llave simétrica correspondiente. Si esta información no coincide con la contenida en la tarjeta NFC, se rechaza la transacción y se indica en la LCD, el led RGB enciende en color rojo y el *buzzer* reproduce tres tonos continuos.
- Si la información coincide después de la comparación, se indica al usuario por medio de la LCD que coloque su huella digital para obtener un rasgo biométrico instantáneo. Cuando el rasgo es obtenido con éxito, se indica en la LCD, el led RGB enciende en color naranja y el *buzzer* reproduce dos tonos continuos.
- El rasgo biométrico contenido en la tarjeta NFC se desencripta utilizando la llave simétrica obtenida con anterioridad y se compara con el rasgo obtenido en ese momento. Si los rasgos no coinciden dentro de un margen de aceptación, se rechaza la transacción y se indica en la LCD, el led RGB enciende en color rojo y el *buzzer* reproduce tres tonos continuos.

- Si los rasgos biométricos coinciden, la transacción es aceptada. Se indica en la LCD, el led RGB enciende en color verde y el *buzzer* reproduce un único tono.
- En el procesamiento interno del dispositivo, se envía una actualización de información a la base de datos y finaliza el proceso de funcionamiento del dispositivo.

Figura 53. **Diagrama de flujo del funcionamiento del dispositivo**



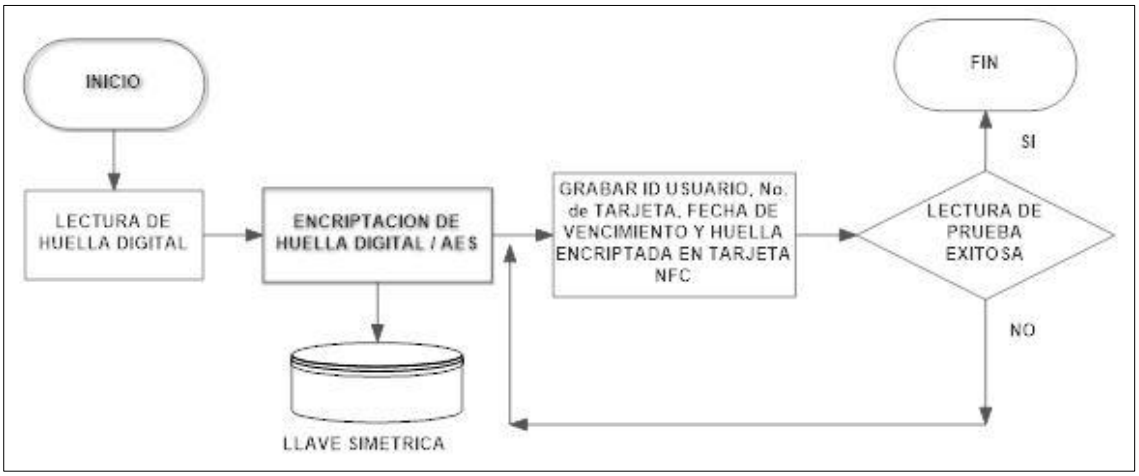
Fuente: elaboración propia, empleando Microsoft Visio.

5.6.2. Procedimiento de matriculación de un nuevo usuario

El proceso de matriculación de un nuevo usuario se indica en el siguiente algoritmo. El algoritmo de matriculación de un nuevo usuario se representa en el diagrama de flujo de la figura 54. Cabe mencionar que el proceso de matriculación de un nuevo usuario únicamente puede ser efectuado por un ente emisor de tarjetas de pago.

- El proceso inicia con la necesidad de crear un nuevo usuario para registrar sus datos en una tarjeta de pago inalámbrica.
- Se solicita al usuario colocar su dedo sobre el sensor de huella digital para obtener el rasgo biométrico. Este paso se realiza dos veces para corroborar la huella del usuario.
- El rasgo biométrico es encriptado utilizando una llave simétrica por medio del método AES. La llave simétrica es almacenada en la base de datos de la red bancaria o del ente emisor de la tarjeta de pago.
- Por medio de un dispositivo NFC se realiza la grabación de información en la tarjeta de pago. La información contenida dentro de la tarjeta es: identificador de usuario (ID usuario), número de tarjeta, fecha de vencimiento y el rasgo biométrico encriptado. Asimismo, es válido acotar que únicamente se puede realizar una grabación en la tarjeta NFC, ya que no se permite sobreescritura de información, para evitar vulnerabilidades de información.
- Con un lector NFC se realiza una prueba de la información contenida y la información se muestra en la pantalla LCD para su verificación. Si la información es errónea, se presiona la letra “C” del teclado matricial para realizar una nueva escritura de información en una tarjeta NFC nueva. Si la información es correcta, la tarjeta NFC está lista para ser utilizada en cualquier punto de pago (POS) o cajero automático (ATM).

Figura 54. **Diagrama de flujo del proceso de matriculación**



Fuente: elaboración propia, empleando Microsoft Visio.

5.6.3. Interfaz de usuario, módulo visual y auditivo

En esta sección se muestran las diferentes interfaces con las que el usuario interactúa. El dispositivo cuenta con tres módulos de información para el usuario, además de un módulo de ingreso de datos que está compuesto por el teclado matricial.

5.6.3.1. Pantalla LCD

La pantalla LCD del dispositivo es la principal interfaz gráfica de comunicación con el usuario, ya que en ella se pueden desplegar mensajes que le indican al usuario instrucciones claras del procedimiento que debe realizar para poder utilizar el dispositivo de pago. A continuación se muestran los mensajes que el usuario podría visualizar si estuviera utilizando el dispositivo.

Figura 55. **Interfaz para cobro o retiro de dinero utilizando el dispositivo**

Fuente: elaboración propia, empleando Adobe Photoshop.

En la figura 55 se muestran las diferentes pantallas que se pueden mostrar al usuario cuando está realizando una transacción de pago en un POS o de retiro de dinero en un ATM:

- Pantalla de bienvenida e ingreso de monto de transacción.
- Pantalla de impresión y verificación de monto de transacción.
- Pantalla de validación y confirmación de monto de transacción.
- Pantalla de solicitud de lectura de tarjeta NFC.
- Pantalla de solicitud de lectura de rasgo biométrico.
- Pantalla de confirmación de rasgo leído de forma exitosa.
- Pantalla de aceptación de transacción.
- Pantalla de rechazo de transacción.

En la figura 56 se muestran las diferentes pantallas que pueden ser mostradas al operador de registros cuando se está realizando la matriculación de un nuevo usuario del sistema bancario:

- Pantalla de bienvenida para matriculación de nuevo usuario.
- Pantalla de solicitud de colocación de dedo para toma de rasgo biométrico (paso 1).
- Pantalla de solicitud de colocación de dedo para toma de rasgo biométrico (paso 2).
- Pantalla de indicación de grabación de información en tarjeta NFC.
- Pantalla de impresión de datos leídos de tarjeta NFC en fase de prueba de información contenida.
- Pantalla de validación y confirmación de datos contenidos en tarjeta NFC.
- Pantalla de indicación de matriculación exitosa de nuevo usuario.

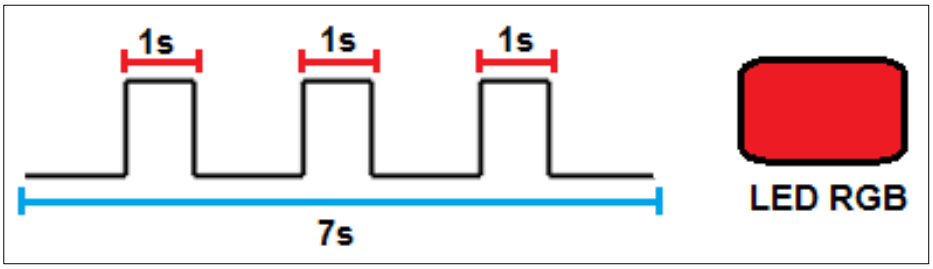
Figura 56. **Interfaz para matriculación de nuevo usuario**

Fuente: elaboración propia, empleando Adobe Photoshop.

5.6.3.2. Indicaciones con led RGB y *buzzer*

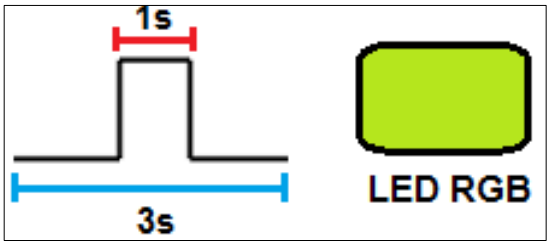
Además de la pantalla LCD, el dispositivo cuenta con un indicador visual conformado por un led RGB y un indicador auditivo que consta de un *buzzer*. Estos elementos generan indicativos sonoros y visuales según el resultado de un proceso dentro del procedimiento de uso del dispositivo. En la figura 57 se muestra el color del led y la señal de sonido generada por el *buzzer* en el caso de que una transacción sea rechazada.

Figura 57. **Indicador visual y auditivo para una transacción rechazada**



Fuente: elaboración propia, utilizando programa Eagle.

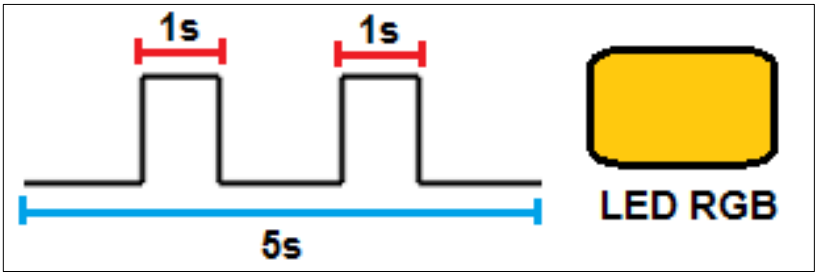
Figura 58. **Indicador visual y auditivo para una transacción aceptada o matriculación exitosa**



Fuente: elaboración propia, utilizando programa Eagle.

En la figura 58 se muestra el color del led y la señal de sonido generada por el *buzzer* cuando una transacción es aceptada o la matriculación de un nuevo usuario es exitosa.

Figura 59. **Indicador visual y auditivo para una lectura de rasgo biométrico exitosa**



Fuente: elaboración propia, utilizando programa Eagle.

En la figura 59 se representa gráficamente el color del led y la señal de sonido reproducida por el *buzzer* cuando la lectura del rasgo biométrico del usuario es exitosa.

5.7. Descripción económica del proyecto

En el siguiente apartado se muestra el presupuesto del dispositivo de pago electrónico. Este incluye los componentes y módulos electrónicos involucrados en la realización del proyecto.

Cabe mencionar que dentro de este presupuesto únicamente están incluidos los componentes de hardware del dispositivo, ya que el software utilizado para la programación y configuración de los distintos módulos es de distribución libre y, por lo tanto, no representa ningún gasto económico.

Tabla XIII. **Listado de componentes electrónicos**

Descripción de componente	Cantidad	Precio en quetzales
Jack tipobornera 5,5 x 2,1 mm	1	Q 5,00
Pines macho rectos 40 x 1	4	Q 16,00
Regulador LM7833	1	Q9,00
Regulador LM7805	1	Q 9,00
Regulador LM7809	1	Q 9,00
Diodo 1N4148	3	Q4,50
Capacitor de 1 µF 30 V	3	Q 3,00
Capacitor de 6,8 µF 30 V	3	Q 6,00
Resistencia de 3,3 Ω ½ W	3	Q3,00
Resistencia 333 Ω ¼ W	1	Q 1,00
Resistencia 220 Ω ¼ W	4	Q4,00
Potenciómetro de 1 kΩ	1	Q 5,00
Transistor NPN 2N2222	4	Q 6,00
LED RGB de alta intensidad	1	Q 11,00
Buzzer de 5 VDC	1	Q 5,00
Fuente de poder 12 VDC 5 A	1	Q360,00
Cable Dupont hembra/hembra	24	Q28,50
Cable Dupont hembra/macho	8	Q 9,50
Metro de estaño	2	Q 12,00
Total	-	Q 506,50

Fuente: *Steren Guatemala*. http://www.steren.com.gt/catalogo. Consulta: 25 de marzo de 2017.

Tabla XIV. **Cotización de PCB industrial**

Descripción	Precio por in^2	Dimensiones de PCB en in^2	Precio en dólares	Precio en quetzales
PCB de circuito de alimentación	$ 5,00	4,07	$ 20,35	Q 149,45
PCB del dispositivo de pago	$ 5,00	14,00	$ 70,00	Q 514,07
Total	-	-	$ 90,35	Q 663,52

Fuente: *Precio de PCB industrial por* in^2. http://docs.oshpark.com/services/ . Tipo de cambio según: http://www.banguat.gob.gt/cambio/7,34394. Consulta: 25 de marzo de 2017.

Tabla XV. **Listado de módulos electrónicos**

Descripción de componente	Cantidad	Precio en dólares	Precio en quetzales
Microcontrolador Arduino DUE	1	$ 54,95	Q 403,55
Módulo de lectura/escritura NFC	1	$ 11,99	Q 88,05
Tarjetas NFC Mifare	10	$ 10,98	Q 80,64
Sensor de huella digital ZFM-20	1	$ 37,70	Q 276,84
LCD PCD8544	1	$ 1,97	Q 14,47
Teclado Matricial 4x4	1	$ 1,28	Q 9,40
Total	-	$ 118,87	Q 872,95

Fuente: *Cotización de módulos realizada en*: http://www.ebay.com . Tipo de cambio según: http://www.banguat.gob.gt/cambio/7,34394. Consulta: 25 de marzo de 2017.

En la tabla XIII se enlistan los componentes electrónicos que conforman las placas de alimentación y la placa del dispositivo propiamente, estos fueron cotizados en un negocio local. En la tabla XIV se indica el precio de las PCB fabricadas de forma industrial por una empresa internacional dedicada a ello. Por último, en la tabla XV se enlistan los módulos electrónicos, los cuales fueron cotizados en una página internacional de ventas por Internet. El monto total del proyecto puede variar dependiendo del lugar de compra, marca de los componentes y el valor actual del cambio, sin embargo, se aproxima un costo total de Q. 2 042,97.

CONCLUSIONES

1. Con la integración de nuevas tecnologías para autenticación de usuarios se aumenta la seguridad de la información contenida en las tarjetas electrónicas de pago.

2. Actualmente, la estructura de sistemas de pago electrónico está basada en tecnologías de banda magnética y *chips* electrónicos, sin embargo, estos muestran deficiencia en la seguridad y la vida útil de los dispositivos.

3. NFC es una tecnología relativamente nueva y su principal beneficio es que permite la comunicación inalámbrica de corto alcance entre dispositivos, aumentando la vida útil de estos y aportando mayor seguridad debido a la naturaleza de funcionamiento.

4. El uso de la huella digital permite tener mayor seguridad al momento de realizar transacciones, ya que es un rasgo biométrico único de cada usuario.

5. Se logró realizar el diseño del equipo electrónico, sin embargo, en Guatemala no existe en el mercado disponibilidad de los módulos electrónicos que componen el dispositivo, por ello se realizó una cotización de los módulos en el mercado internacional.

RECOMENDACIONES

1. La persona que desee implementar el dispositivo debe verificar el voltaje de lógica del microcontrolador, la configuración de los pines y el voltaje de alimentación de todos los módulos periféricos, para asegurar el funcionamiento y evitar posibles daños a los componentes.

2. Las tarjetas NFC tienen un alcance de comunicación de hasta 10 cm, por lo tanto, el usuario debe tener en consideración la distancia al momento de realizar el pago.

3. El sensor de recepción del módulo biométrico debe encontrarse libre de suciedad para evitar lecturas erróneas.

4. El módulo de lectura/escritura NFC funciona por medio de radiofrecuencia, por lo tanto no debe haber ningún objeto metálico entre la antena del módulo y la tarjeta NFC, ya que esto impediría la lectura o escritura de información desde o hacia la tarjeta.

5. Para garantizar un buen funcionamiento del dispositivo, se recomienda que el usuario siga los pasos descritos en el apartado “Procedimiento para cobro o retiro de dinero utilizando el dispositivo”, del capítulo 5.

6. Para garantizar la correcta matriculación de un usuario nuevo se recomienda seguir los pasos descritos en el apartado “Procedimiento de matriculación de un nuevo usuario”, del capítulo 5.

7. El diseño del dispositivo es flexible y adaptable a los módulos que lo componen, ya que en el mercado de productos electrónicos se encuentra diversidad de marcas y precios, sin embargo, se recomienda utilizar los especificados en este texto, ya que se realizaron investigaciones, pruebas y análisis de funcionamiento.

8. Una institución comercial que desee implementar el dispositivo debe conectarse a una red bancaria para poder completar las transacciones.

BIBLIOGRAFÍA

1. *Acerca de NFC.* [en línea]. <http://nfc-forum.org/what-is-nfc/about-the-technology/>. [Consulta: 14 de diciembre de 2016].

2. ACOSTA, David. *¿Cómo funcionan las tarjetas de pago? Parte I: PAN (Primary Account Number).* [en línea]. <http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-i-pan-primary-account-number/>. [Consulta: 16 de febrero de 2017].

3. _____. *¿Cómo funcionan las tarjetas de pago? Parte IV: banda magnética*. [en línea]. <http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-iv-banda-magnetica/>. [Consulta: 16 de febrero de 2017].

4. _____. *¿Cómo funcionan las tarjetas de pago? Parte V: smart card (chip) y EMV*. [en línea]. <http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-v-smart-card-chip-y-emv/>. [Consulta: 17 de febrero de 2017].

5. _____. *¿Cómo funcionan las tarjetas de pago? Parte VI: tarjetas contactless (RFID – NFC).* [en línea]. <http://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-vi-tarjetas-contactless-rfid-nfc/>. [Consulta: 20 de febrero de 2017].

6. *Advanced Encryption Standard.* [en línea]. <https://es.wikipedia.org/wiki/Advanced_Encryption_Standard>. [Consulta: 1 de marzo de 2017].

7. *Algoritmo criptográfico.* [en línea]. <https://es.wikipedia.org/wiki/Algoritmo_criptogr%C3%A1fico>. [Consulta: 27 de febrero de 2017].

8. COSKUN, Vedat; OZDENIZCI, Busra; OK, Kerem. *The survey on near field communication.* Turquía: Department of Information Technolgies. ISIK University, 2015. [en línea].<http://www.mdpi.com/1424-8220/15/6/13348/htm>. [Consulta: 20 de diciembre de 2016].

9. DE LUZ, Sergio. *Criptografía: algoritmos de cifrado de clave simétrica.* [en línea]. <https://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/>. [Consulta: 1 de marzo de 2017].

10. IGOE, Tom; COLEMAN, Don; JEPSON, Brian. *Beginning NFC, Near Field Communication with Arduino, Android, and Phone Gap.* Estados Unidos: O'Reilly, 2014. 227 p.

11. *Microcontrolador.* [en línea]. <https://es.wikipedia.org/wiki/Microcontrolador>. [Consulta: 28 de febrero de 2017].

12. Microsoft. *¿Qué es NDEF?* [en línea]. <https://nfcfirststeps.codeplex.com/wikipage?title=%C2%BFQu%C3%A9%20es%20NDEF?>. [Consulta: 19 de diciembre de 2016].

13. *Origen e historia de las tarjetas de crédito.* [en línea]. <http://www.ennaranja.com/economia-facil/origen-e-historia-de-las-tarjetas-de-credito/>. [Consulta: 14 de febrero de 2017].

14. PADILLA, J.; Íñiguez, W. Near Field Communication-Teoría y aplicaciones. Ecuador: Universidad del Azuay, Facultad de Ingeniería de Sistemas y Telemática, 2014. 216 p.

15. Phillips Semiconductors. *PCD8544 datasheet, 1999*. [en línea]. <http://eia.udg.edu/~forest/PCD8544_1.pdf >. [Consulta: 17 de marzo de 2017].

16. POOLE, Ian. *Near Field Communication Modulation*. [en línea]. <http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-modulation-rf-signal-interface.php>. [Consulta: 14 de diciembre de 2016].

17. SERRATOSA, Francesc. *La biometría para la identificación de las personas.* España: Universitat Oberta de Catalunya, 2010. 50 p.

18. THAYER, Luis. *Arduino Due.* [en línea]. <http://arduino.cl/arduino-due/>. [Consulta: 6 de marzo de 2017].

19. *The difference between NFC and RFID explained.* [en línea]. <http://nfc.today/advice/difference-nfc-rfid-explained>. [Consulta: 28 de diciembre de 2016].

20. ZABALA, Enrique. *Rijndael inspector.* [en línea]. <http://www.formaestudio.com/rijndaelinspector/>. [Consulta: 1 de marzo de 2017].

APÉNDICES

Apéndice 1. **Descripción de IDE del microcontrolador**

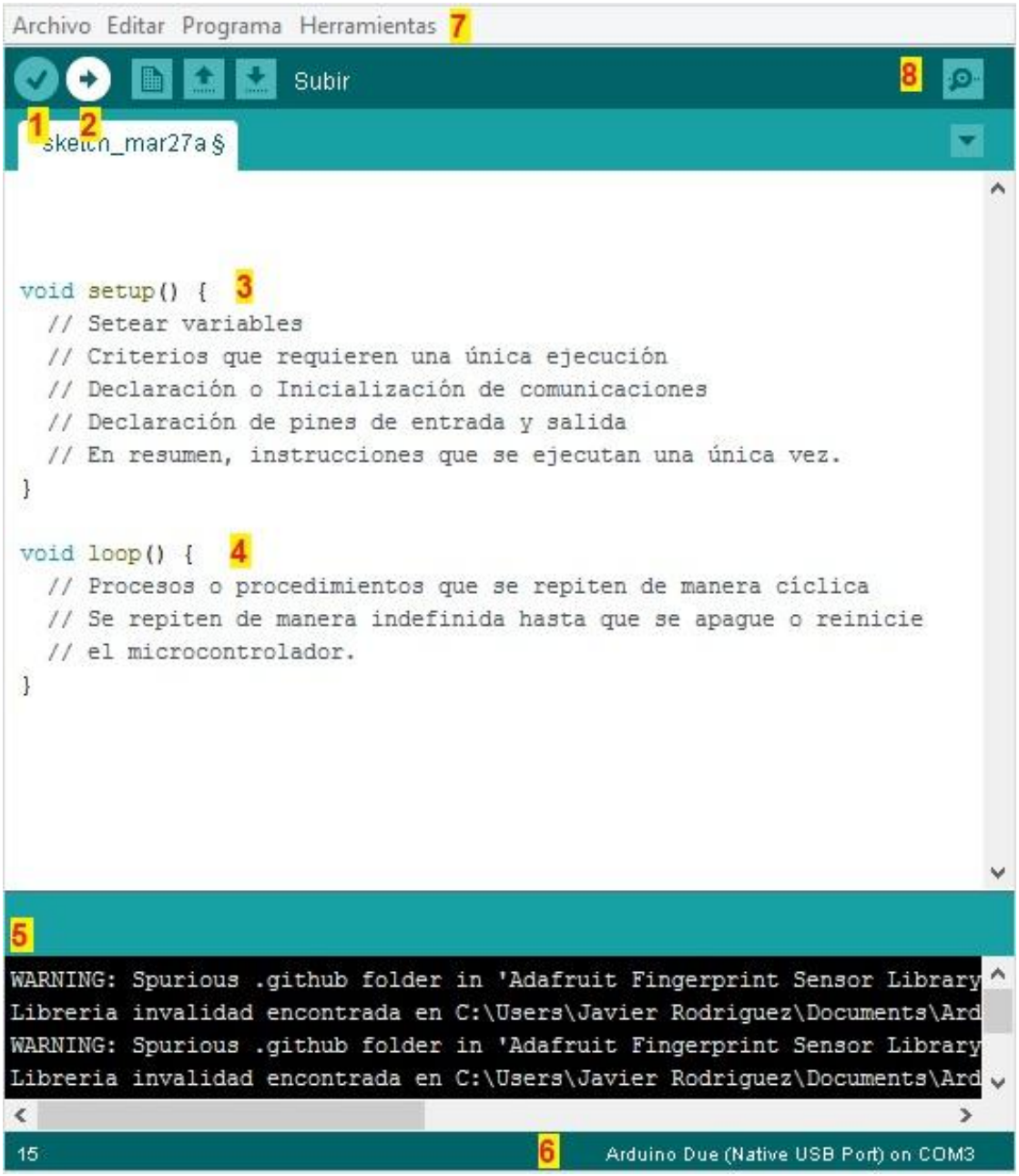
A continuación se describe el *software* de programación del microcontrolador propuesto en el diseño del dispositivo.

En la figura del anexo 1a se muestra la ventana del IDE de Arduino. El indicador (1) de la figura señala el botón para compilar el programa, esta función permite verificar si existen errores en el código de programación para realizar su corrección antes de cargar el programa al microcontrolador.

El indicador (2) muestra el botón correspondiente a cargar el programa en el microcontrolador. El indicador (3) muestra la función *set up*, la cual contiene instrucciones que se ejecutan una única vez dentro del programa. El indicador (4) muestra la función *loop*, la cual contiene procedimientos que se repiten de manera cíclica en el programa.

El indicador (5) muestra la consola de mensajes del IDE. El indicador (6) muestra la sección del IDE Arduino donde se especifica qué microcontrolador Arduino y en qué puerto serial se encuentra conectado. El indicador (7) muestra el menú “Herramientas”, mediante este se puede escoger el microcontrolador Arduino a utilizar y el puerto serial al que se encuentra conectado. Y, por último, el indicador (8) muestra el botón para desplegar el monitor serial del IDE y así poder visualizar la información transmitida por UART.

Apéndice 1a. **Imagen de ventana del IDE de Arduino**



Fuente: elaboración propia.

Apéndice 2. **Programas propuestos**

Programa para escritura de una tarjeta NFC

En el código 1 se muestra el código del programa propuesto para escritura de una tarjeta NFC.

Código 1: **Programa para escritura de tarjeta NFC**

```
// Inclusión de Librerías
#include<SPI.h>
#include <PN532_SPI.h>
#include <PN532.h>
#include<NfcAdapter.h>

//Inicialización de parámetros
PN532_SPI pn532spi(SPI,10);
NfcAdapternfc=NfcAdapter(pn532spi);

voidsetup(){
//Inicialización de puerto serial
        Serial.begin(9600);

        nfc.begin();
        //Impresión en monitor serial
Serial.println("Escritor NFC");
        //Inicialización de módulo NFC
nfc.begin();
}
voidloop(){
        //Impresión en monitor serial
Serial.println("\nColocar un tarjeta NFC para grabar");
        //Detección de tarjeta NFC
if(nfc.tagPresent()){
NdefMessagemessage=NdefMessage();
                //Escribe en tarjeta
message.addUriRecord("ID USUARIO...");
                //Resultado de grabación
bool success =nfc.write(message);
if(success){
                Serial.println("Tarjeta grabada con éxito");
}else{
                Serial.println("Escritura fallida");
}
}
delay(5000);
}
```

Continuación del apéndice 2.

Programa para lectura de una tarjeta NFC

En el código 2 se muestra el código del programa propuesto para lectura de una tarjeta NFC.

Código 2: **Programa para lectura de una tarjeta NFC**

```
//Inclusión de librerías
#include<SPI.h>
#include <PN532_SPI.h>
#include <PN532.h>
#include<NfcAdapter.h>

//Inicialización de parámetros
PN532_SPI pn532spi(SPI,10);
NfcAdapternfc=NfcAdapter(pn532spi);

voidsetup(void){
        //Inicialización de puerto serial
Serial.begin(9600);
Serial.println("Lector NFC");
        //Inicialización de módulo NFC
nfc.begin();
}

voidloop(void){
        //Impresión en pantalla
Serial.println("\nLeer una tarjeta NFC\n");
        //Detección de tarjeta NFC
if(nfc.tagPresent())
{
                //Asignación de data a variable
NfcTagtag=nfc.read();
                //Impresión de información contenida en tarjeta
tag.print();
}
        //Retraso en milisegundos entre procesos de lectura
delay(5000);
}
```

Continuación del apéndice 2.

Programa para grabación de huella digital de un nuevo usuario

En el código 3 se muestra el código del programa propuesto para grabar la huella digital de un nuevo usuario (proceso de matriculación).

Código 3: **Programa para grabación de nuevo rasgo biométrico**

```
//Inclusión de librerias
#include<Adafruit_Fingerprint.h>
#include<SoftwareSerial.h>

//Enteros representados en 8 bits
uint8_t id;
uint8_tgetFingerprintEnroll();

//Selección de pines UART
SoftwareSerialmySerial(8,9);
//Inicialización de librerías
Adafruit_Fingerprintfinger=Adafruit_Fingerprint(&mySerial);

voidsetup()
{
	//Mientras este disponible puerto serial
	while(!Serial);
		delay(500);

		Serial.begin(9600);
		Serial.println("Matriculación de huella");

		//Velocidad de transmisión de pto. serial
		finger.begin(57600);

		if(finger.verifyPassword()){
			Serial.println("Found fingerprint sensor!");
		}else{
			Serial.println("Did not find fingerprint sensor :(");
			while(1);
		}
}

//Lectura de ID asignado a rasgo de nuevo usuario
uint8_treadnumber(void){
uint8_tnum=0;
booleanvalidnum= false;
while(1){
```

Continuación del apéndice 2.

```
while(!Serial.available());
                    char c =Serial.read();
if(isdigit(c)){
num*=10;
num+= c -'0';
validnum= true;
}elseif(validnum){
returnnum;
}
}
}

//Asignación de ID a un rasgo biometrico
voidloop()
{
Serial.println("Porfavor ingrese el ID del rasgo biometrico");
id=readnumber();
//Se imprime el # de ID del rasgo a guardar
Serial.print("Guardando ID #");
Serial.println(id);

while(!getFingerprintEnroll());
}

uint8_tgetFingerprintEnroll(){

int p =-1;
Serial.print("Esperando por una huella valida");
Serial.println(id);
//Mientras la huella sea leída sin errores
while(p != FINGERPRINT_OK){
p =finger.getImage();
          //Casos de posibles errores en este proceso
switch(p){
case FINGERPRINT_OK:
Serial.println("Imagen tomada");
break;
case FINGERPRINT_NOFINGER:
Serial.println("Esperando huella");
break;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Error de comunicación");
break;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Error de imagen");
break;
default:
Serial.println("Error desconocido");
break;
}
```

Continuación del apéndice 2.

```
}


        //Captura de huella exitosa
p =finger.image2Tz(1);
switch(p){
case FINGERPRINT_OK:
Serial.println("Imagen convertida");
break;
case FINGERPRINT_IMAGEMESS:
Serial.println("Imagen ilegible");
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Error de comunicación");
return p;
case FINGERPRINT_FEATUREFAIL:
Serial.println("No se pueden leer caracteristicas de la huella");
return p;
case FINGERPRINT_INVALIDIMAGE:
Serial.println("No se pueden encontrar caracteristicas de la huella");
return p;
default:
Serial.println("Error desconocido");
return p;
}

//Segunda lectura del rasgo
Serial.println("Remover dedo");
delay(2000);
p =0;
while(p != FINGERPRINT_NOFINGER){
p =finger.getImage();
}
Serial.print("ID de huella ");Serial.println(id);
  p =-1;
Serial.println("Colocar nuevamente el dedo");
while(p != FINGERPRINT_OK){
    p =finger.getImage();
switch(p){
case FINGERPRINT_OK:
Serial.println("Imagen guardada");
break;
case FINGERPRINT_NOFINGER:
Serial.print(".");
break;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Error de comunicación");
break;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Error de imagen");
```

Continuación del apéndice 2.

```
break;
default:
Serial.println("Error desconocido");
break;
}
}

//Lectura de huella exitosa
p =finger.image2Tz(2);
switch(p){
case FINGERPRINT_OK:
Serial.println("Imagen convertida");
break;
case FINGERPRINT_IMAGEMESS:
Serial.println("Imagen ilegible");
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Error de comunicación");
return p;
case FINGERPRINT_FEATUREFAIL:
Serial.println("No se pueden leer caracteristicas de la huella");
return p;
case FINGERPRINT_INVALIDIMAGE:
Serial.println("No se pueden encontrar caracteristicas de la huella");
return p;
default:
Serial.println("Error desconocido");
return p;
}

//Huella convertida
Serial.print("Creando modelo para huella #");
Serial.println(id);

  p =finger.createModel();
if(p == FINGERPRINT_OK){
Serial.println("Coinciden las imagenes");
}elseif(p == FINGERPRINT_PACKETRECIEVEERR){
Serial.println("Error de comunicación");
return p;
}elseif(p == FINGERPRINT_ENROLLMISMATCH){
Serial.println("No coinciden las huellas");
return p;
}else{
Serial.println("Error desconocido");
return p;
}

Serial.print("Huella #");
Serial.println(id);
```

Continuación del apéndice 2.

```
p =finger.storeModel(id);
if(p == FINGERPRINT_OK){
Serial.println("HuellaGuardada.");
}elseif(p == FINGERPRINT_PACKETRECIEVEERR){
Serial.println("Error de comunicación");
return p;
}elseif(p == FINGERPRINT_BADLOCATION){
Serial.println("No se puede almacenar huella con ese ID");
return p;
}elseif(p == FINGERPRINT_FLASHERR){
Serial.println("Error de escritura en memoria flash");
return p;
}else{
Serial.println("Error desconocido");
return p;
}
}
```

Programa para lectura y comparación de huella digital

En el código 4 se muestra el programa para leer una huella digital y compararla con la base de datos de huellas almacenadas. Este programa retorna como respuesta una coincidencia o un incompatibilidad de huellas.

Código 4: **Programa para lectura y comparación de huella digital**

```
//Inclusión de librerías
#include<Adafruit_Fingerprint.h>
#include<SoftwareSerial.h>

//Declaración de variable entera
intgetFingerprintIDez();

//Declaración de pines UART
SoftwareSerialmySerial(2,3);
//Inicialización de librerías
Adafruit_Fingerprint finger =Adafruit_Fingerprint(&mySerial);

void setup()
{
        //Si el puerto serial está disponible
        while(!Serial);

                Serial.begin(9600);
```

Continuación del apéndice 2.

```
                Serial.println("Prueba de detección de huella");

                //Velocidad de transmisión de pto. serial
                finger.begin(57600);

//Detección de sensor de huella conectado
if(finger.verifyPassword()){
Serial.println("Sensor de huella disponible");
}else{
Serial.println("Sensor de huella no disponible");
while(1);
}
Serial.println("Esperando por huella valida...");
}

//Función cíclica
voidloop()
{
getFingerprintIDez();
delay(50);
}

//Lectura de huella digital a comparar con DB
uint8_tgetFingerprintID(){
uint8_t p =finger.getImage();
switch(p){
case FINGERPRINT_OK:
Serial.println("Imagen guardada");
break;
case FINGERPRINT_NOFINGER:
Serial.println("No se ha detectado huella digital");
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Error de comunicación");
return p;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Error de imagen");
return p;
default:
Serial.println("Error desconocido");
return p;
}

        //Éxito de lectura
        p =finger.image2Tz();
        switch(p){
                case FINGERPRINT_OK:
                Serial.println("Imagen convertida");
                break;
                case FINGERPRINT_IMAGEMESS:
```

Continuación del apéndice 2.

```
                    Serial.println("Imagen ilegible");
                    return p;
                    case FINGERPRINT_PACKETRECIEVEERR:
                    Serial.println("Error de comunicación");
                    return p;
                    case FINGERPRINT_FEATUREFAIL:
                    Serial.println("No se pueden leer caracteristicas de la huella");
                    return p;
                    case FINGERPRINT_INVALIDIMAGE:
                    Serial.println("No se pueden encontrar caracteristicas de la huella");
                    return p;
                    default:
                    Serial.println("Error desconocido");
                    return p;
}

        //Exito en la conversión
        p =finger.fingerFastSearch();
                if(p == FINGERPRINT_OK){
                        Serial.println("Se encontró coincidencia en huellas");
                }elseif(p == FINGERPRINT_PACKETRECIEVEERR){
                        Serial.println("Error de comunicación");
                        return p;
                }elseif(p == FINGERPRINT_NOTFOUND){
                        Serial.println("No se encontró coincidencia en huellas");
                        return p;
                }else{
                        Serial.println("Error desconocido");
                        return p;
                }

        //Se encontró coincidencia de huellas
        Serial.print("Se encontró coincidencia con huella ID#");
        Serial.print(finger.fingerID);
        Serial.print("Con un nivel de confianza de: ");
        //Porcentaje de igualdad
        Serial.println(finger.confidence);
}

// Regresa -1 si hay fallo, si no hay fallo, retorna # de ID
intgetFingerprintIDez(){
uint8_t p =finger.getImage();
if(p != FINGERPRINT_OK)return-1;

  p =finger.image2Tz();
if(p != FINGERPRINT_OK)return-1;

  p =finger.fingerFastSearch();
if(p != FINGERPRINT_OK)return-1;
```

Continuación del apéndice 2.

```
        //Se encontró coincidencia de huellas
        Serial.print("Se encontró coincidencia con huella ID#");
        Serial.print(finger.fingerID);
        Serial.print("Con un nivel de confianza de: ");
        Serial.println(finger.confidence);
return finger.fingerID;
}
```

Programa para impresión de información en LCD PCD8544

En el código 5 se muestra el programa para escritura de información en la pantalla LCD PCD8544.

Código 5: **Programa para escritura de datos en pantalla de LCD**

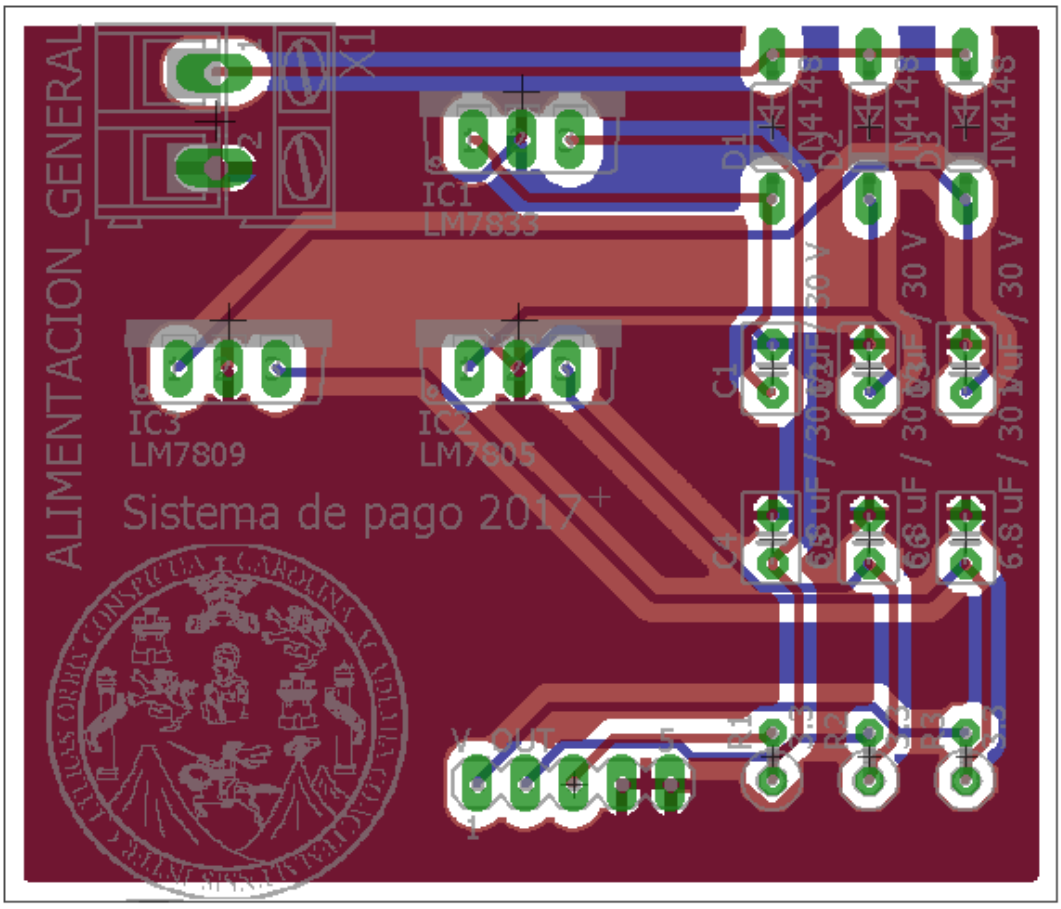
```
//Inclusión de librerías
#include<ASCII.h>
#include<Clase911_PCD6544.h>

//Inicialización de librerías
// y asignación de parámetros
// (CLK, MOSI, DC, RST, CE)
NokiaLCDNokiaLCD(4,5,6,7,8);

void setup(){
        //Inicialización de LCD
        NokiaLCD.init();
        //Limpieza de pantalla
        NokiaLCD.clear();
}

void loop(){
        //Colocación de cursor en coordenadas (0,0)-(x,y)
        NokiaLCD.setCursor(0,0);
        //Impresión en LCD
        NokiaLCD.print("Sistema de pago");
        NokiaLCD.setCursor(15,3);
        NokiaLCD.print("usuario: @");
        NokiaLCD.setCursor(1,4);
        NokiaLCD.print("transaccion: ");
}
```

Fuente: elaboración propia.

Apéndice 3. **Circuitos impresos en Eagle**

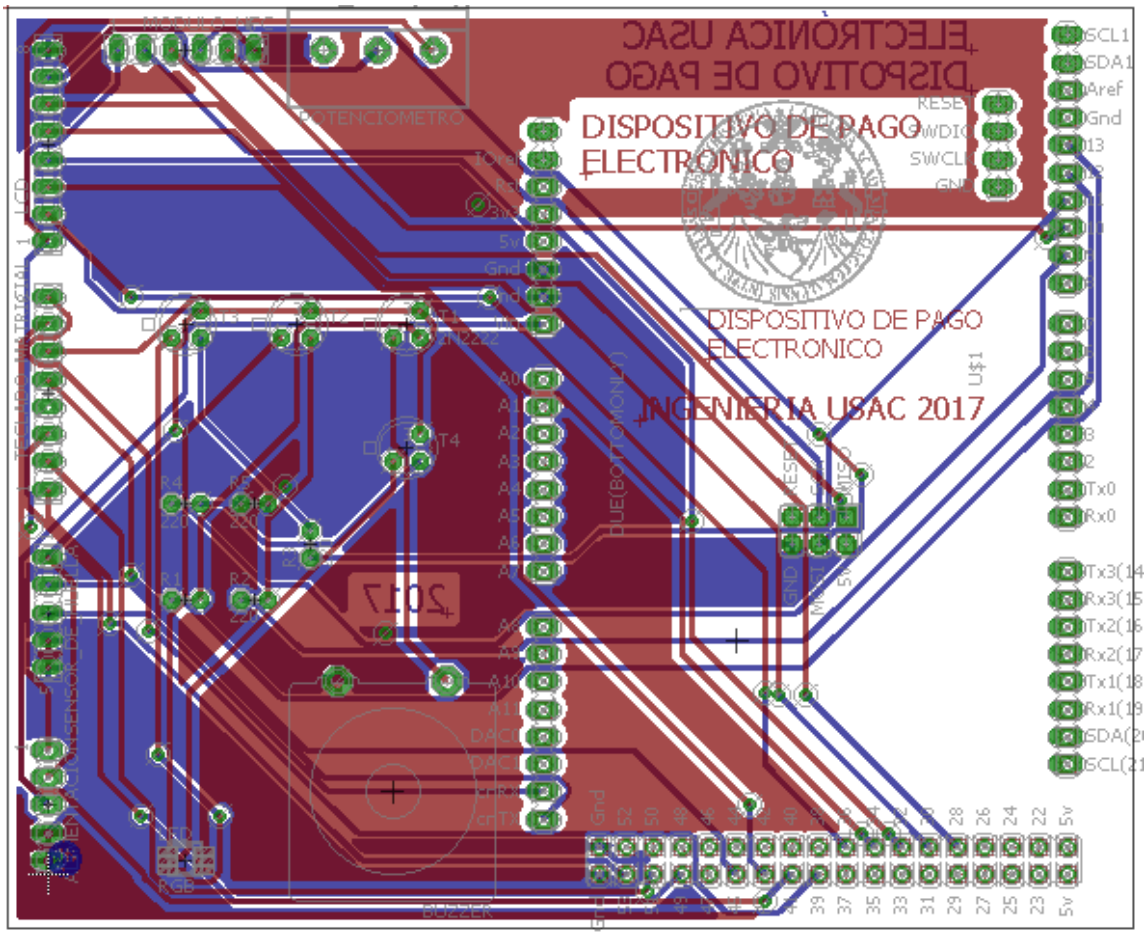
A continuación se muestran los dos diagramas de circuitos impresos realizados en el *software* Eagle. Cabe mencionar que ambas placas fueron realizadas con conexiones de doble cara para reducir el tamaño de las mismas.

Apéndice 3a. **PCB de circuito de alimentación**



Fuente: elaboración propia, utilizando el editor de circuitos impresos de Eagle.

Apéndice 3b. **PCB de circuito del dispositivo de pago**



Fuente: elaboración propia, utilizando el editor de circuitos impresos de Eagle.