ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

MODELO DE SEGURIDAD PARA GARANTIZAR LA INTEGRIDAD DE LOS PAGOS MÓVILES BASADOS EN NEAR FIELD COMMUNICATION (NFC)

CRISTHIAN FERNANDO CASTRO ORTIZ

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA - ECUADOR

Diciembre - 2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado "MODELO DE SEGURIDAD PARA GARANTIZAR LA INTEGRIDAD DE LOS PAGOS MÓVILES BASADOS EN NEAR FIELD COMMUNICATION (NFC)", de responsabilidad del Ing. Cristhian Fernando Castro Ortiz ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ing. Wilson Zúñiga Vinueza, M.Sc.	_____
PRESIDENTE	**FIRMA**
Ing. Santiago Cisneros Barahona, M.Sc.	_____
DIRECTOR DE TESIS	**FIRMA**
Ing. Alfredo Colcha Ortiz, M.Sc.	_____
MIEMBRO DEL TRIBUNAL	**FIRMA**
Dr. Javier Moreno Barreno, M.Sc.	_____
MIEMBRO DEL TRIBUNAL	**FIRMA**

Riobamba, Diciembre 2017

DERECHOS INTELECTUALES

Yo, Cristhian Fernando Castro Ortiz, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo y que el patrimonio intelectual generado por la misma pertenecen exclusivamente a la Escuela Superior Politécnica de Chimborazo.

_____

Cristhian Fernando Castro Ortiz
No. Cédula: 0603001678

DECLARACIÓN DE AUTENTICIDAD

Yo, Cristhian Fernando Castro Ortiz, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

_____

Cristhian Fernando Castro Ortiz
No. Cédula: 0603001678

DEDICATORIA

Dedico este trabajo de Investigación a mi esposa Andrea y a mis hijos Andrés Sebastián y Ana Paula por su amor infinito y apoyo incondicional en cada uno de los retos y desafíos que me he propuesto, y a mis padres Magdalena y Wilson quienes jamás dejaron de creer en mí y siempre me ayudaron a levantarme tras las caídas que tuve a lo largo de mi vida.

Cristhian

AGRADECIMIENTO

Agradezco a la Escuela Superior Politécnica de Chimborazo, al Instituto de Posgrado, por darme la oportunidad de crecer profesionalmente y permitido alcanzar esta nueva meta.
Mi gratitud y reconocimiento especial a mi tutor Santiago, y a los miembros del tribunal Alfredo y Javier, quienes me guiaron y apoyaron durante el desarrollo del trabajo investigativo.

Cristhian

TABLA DE CONTENIDO

CAPITULO III

CAPITULO IV

INDICE DE TABLAS

INDICE DE GRÁFICOS

RESUMEN

Se propuso un modelo de seguridad para garantizar la integridad de los pagos móviles basados en Near Field Communication (NFC) denominado NRioSec, que establece tres niveles de protección con un alto grado de compatibilidad y fácil integración en el desarrollo de aplicaciones de pago móviles. Sus componentes permiten controlar la autenticación con certificados digitales, la unicidad de transacciones mediante la tokenización y el cifrado de datos mediante algoritmos robustos, y que sumados a las normas de seguridad de aceptación de pagos móviles del PCI SSC, determinan la eficacia de su aplicación para mitigar las vulnerabilidades analizadas. Se comprobó que el modelo de seguridad NRioSec incrementa el nivel de integridad de los pagos móviles basados en NFC porque mediante cifrado protege la información sensible que se transmite durante una transacción; al ser transmitida la información únicamente entre el emisor y el receptor se protege la información confidencial de los atacantes o de las entidades participantes, pues éstas no tienen necesidad de acceder a dicha información; el modelo proporciona cifrado y autenticación de origen para que el receptor los pueda validar y, se asegura al receptor que los detalles del pago son correctos y corresponden a los datos proporcionados por el emisor mediante una pantalla donde se confirme que los datos son correctos.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <SEGURIDAD TELEMÁTICA>, < Near Field Communication (NFC)>, <PAGOS MÓVILES>, <PAGOS SIN CONTACTO>, <MODELO DE SEGURIDAD>, <INTEGRIDAD DE DATOS>

ABSTRACT

A security model was proposed to guarantee the integrity of mobile payments based on Near Field Communication (NFC) called NRioSec, which establishes three levels of protection with a high degree of compatibility and easy integration in the development of mobile payment applications. Its components allow controlling authentication with digital certificates, the uniqueness of transactions through tokenization and data encryption using robust algorithms, and that added to the PCISSC mobile payment acceptance security standards, determine the efficiency of its application to mitigate the vulnerabilities analyzed it was possible to verify that the NRioSec security model increases the integrity level of mobile payments based on NFC because encryption protects the sensitive information transmitted during a transaction; When the information is transmitted only between the sender and the receiver, the confidential information of the attackers or participating entities is protected. Because they have no need to access said information; the model provides encryption and authentication of origin so that the receiver can validate them, and the receiver is assured that the details of the payment are correct and correspond to the data provided by the issuer through a screen where the data is confirmed to be correct.

Keywords: <ENGINEERING TECHNOLOGY AND SCIENCE>, <TELEMATIC SECURITY>, <Near Field Communication (NFC)>, <MOBILE PAYMENTS>, <NON-CONTACT PAYMENTS>, <SECURITY MODEL>, <SECURITY MODEL>, <INTEGRITY OF DATA>

CAPITULO I

1. INTRODUCCIÓN

En la última década el avance en el área de las comunicaciones ha logrado una integración casi natural de las herramientas tecnológicas y las tareas cotidianas que realizan los seres humanos. Y una parte fundamental de ello son los teléfonos móviles inteligentes (smartphones) que procesan información y datos en tiempo real, facilitando las actividades de las personas.

Sin embargo, la introducción de los teléfonos móviles en sus inicios tenía otro objetivo muy simple, permitir la comunicación de voz en redes entre los teléfonos móviles y la telefonía fija.

Pero con el uso del sistema de comunicaciones GSM (Global System for Mobile Communications) se activaron varias funcionalidades adicionales y servicios en los teléfonos móviles además de la comunicación por voz, tales como los SMS (Short Messaging Service), MMS (Multimedia Messaging Service) e incluso el acceso a Internet. La tecnología Bluetooth se introdujo más tarde con el objetivo de crear redes inalámbricas de área personal, para la conexión de los periféricos con los dispositivos informáticos, incluyendo los teléfonos móviles (Coskun, Ozdenizci, & Ok, 2012).

Hoy en día las funcionalidades de un teléfono móvil inteligente son muy amplias, y entre ellas destacan las que hacen uso de la tecnología NFC (Near Field Communication), que permiten simplificar el proceso de pagos de servicios públicos y financieros.

Con NFC, la posibilidad de vincular un número de cuenta bancaria en el teléfono móvil inteligente del usuario y ejecutar la autorización del débito bancario al momento de realizar el pago, con tan solo acercar durante pocos segundos el dispositivo móvil al equipo que procesa el pedido, genera un ahorro significativo de tiempo a los usuarios y a su vez, de recursos a las empresas.

Pero esta nueva tendencia de pagos móviles conlleva a la necesidad de contar con un modelo de seguridad que permita interactuar con la tecnología NFC, bajo un entorno que garantice la integridad de los datos personales y privados del usuario al momento de procesar un pago.

1.1 Planteamiento del Problema

1.1.1 Situación Problemática

La introducción de la tecnología digital en los sistemas de comunicaciones móviles producidos a partir de principios de la década de los noventa ha permitido crear una sinergia en los aspectos relacionados a la interacción con el sistema financiero, el acceso a los servicios públicos, los procesos de aprendizaje en las escuelas, la medicina, la vivienda, los medios audiovisuales y de entretenimiento.

Esto sumado al avance tecnológico ha permitido simplificar la manera en que las personas realizan sus actividades cotidianas, con innumerables aplicaciones y servicios que pueden ser controlados desde un dispositivo móvil.

En este ámbito los pagos móviles han tenido un despunte significativo debido al uso de NFC (Near Field Communication), que es una tecnología de comunicación inalámbrica de corto alcance. NFC se basa en el estándar RFID (Radio Frequency Identification) que permite la transmisión de datos a través de campos de radio frecuencia (Coskun et al., 2012).

(Garfinkel, Juels, & Pappu, 2005) indican que la tecnología NFC permite la conectividad entre dispositivos móviles y equipos destinados a realizar transacciones electrónicas. NFC es considerado un medio de transmisión inalámbrico bastante seguro, debido a la corta distancia que necesita para transmitir información entre un emisor y un receptor, donde resulta muy difícil que un tercer dispositivo interfiera en la conexión.

Sin embargo, no existen estándares de seguridad definidos para garantizar la integridad de los pagos móviles. El interés que actualmente existe por el uso de NFC es muy alto, y es ampliamente referenciada en las transacciones que se realizan entre dispositivos móviles. Pero a su vez, esto genera dudas sobre la seguridad, al momento de aplicar esta tecnología.

En el año 2012, durante el evento de seguridad el investigador Charlie Miller brindó una conferencia, sobre ataques a NFC, donde demostró importantes vulnerabilidades en distintos sistemas y equipos, basados en esta tecnología (SecTor, 2012).

Entre las vulnerabilidades de seguridad de NFC más conocidas están la interceptación de comunicaciones (eavesdropping), modificación de datos (data modification), ataque relay (relay

attack) o ataques de hombre en el medio (man-in-the-middle), a pesar de que las posibilidades de que este último ataque son bajas debido a la distancia en la que debe interactuar una transacción entre dispositivos NFC.

(Coskun et al., 2012) detallan las vulnerabilidades, ataques y posibles soluciones que podrían ser aplicadas:

Tabla 1-1 Vulnerabilidades de seguridad NFC y posibles soluciones

Vulnerabilidades y ataques	Posibles soluciones
Manipulación de etiquetas NFC URI spoofing URL spoofing	Etiquetas con firmas basadas en técnicas de cifrado
Clonación, suplantación, reemplazo y ocultación de etiquetas NFC	Uso de protocolos de autenticación de etiquetas cifradas
Interceptación de comunicaciones (eavesdropping) Alteración, modificación e inserción de datos Ataques de denegación de servicios (DOS) Ataques de relay (relay attacsk) Suplantación de identidad por ingeniería social (pishing)	Establecimiento de un canal seguro de comunicación entre dispositivos NFC. Uso de protocolos de acuerdo a claves específicas NFC
Ejecución de aplicaciones en el dispositivo sin conocimiento del usuario Instalación de aplicaciones de malware	Mecanismos de autenticación basados en certificados. Políticas de gestión de claves para la autenticación
Ataques al controlador NFC de los dispositivos	Obligatoriedad de firma de código al usar el API de comunicación de NFC
Skimming y ataques de clonación de tokens	Enlace de aplicaciones cifrados con identificadores únicos

Realizado por: Castro Cristhian, 2017

Dado que son varios los escenarios donde una transacción basada en NFC podría ser vulnerable, (Ottoy et al., 2011) plantean una plataforma modular para validar la seguridad en aplicaciones basadas en NFC, a través de la implementación de un canal seguro, con la utilización de algoritmos criptográficos y de seguridad construido mediante hardware. Sin embargo, no siempre

se puede contar con los recursos ni las herramientas adecuadas para implementar la seguridad mediante hardware.

En el ámbito de los pagos móviles basadas en NFC, (Günther & Borchert, 2013) establecen un modelo con algunas características interesantes:

- Una pantalla para mostrar que la operación que se firmará.
- Un módulo de cifrado para firmar la transacción mostrada.
- Una firma que puede ser desechada únicamente por el usuario.
- Almacenamiento seguro de las credenciales, a prueba de falsificaciones.

Pero dado que el modelo planteado únicamente se enfoca en transacciones bancarias, resulta compleja su integración y los costos de su implementación, a pesar de que estos son relativamente bajos ya que no se requiere un sistema de administración adicional para el manejo de credenciales.

A su vez, (Nguyen, Seo, & Kim, 2014) proponen un modelo de seguridad basado en LEA, Lightweight Encryption Algorithm (Hong et al., 2014), que permite aplicar un bloque cifrado con LEA para proteger la comunicación entre dispositivos NFC y el sistema de base de datos, asegurando alta disponibilidad y un alto rendimiento. A pesar de que los resultados de rendimiento del cifrado con LEA respecto al cifrado con AES son muy buenos, no se han validado con grandes volúmenes de datos.

Si bien existen modelos de seguridad para NFC, estos se enfocan únicamente a entornos específicos, limitando así su aplicación para escenarios de aplicación más comunes. Por ello, el presente trabajo de investigación aportará con un modelo de seguridad, que pueda ser aplicado en diferentes escenarios y tipos de pagos móviles, que se realicen mediante el uso de la tecnología NFC, para garantizar la integridad de los datos procesados durante el intercambio de información.

1.1.2 Formulación del Problema

¿Cuál es el nivel de integridad de los pagos móviles basados en NFC al aplicar un modelo de seguridad?

1.1.3 Preguntas directrices o específicas de la Investigación

¿Existen modelos de seguridad para pagos móviles basados en NFC?
¿Cuáles son las principales vulnerabilidades que se presentan en NFC?

¿Qué dispositivos móviles soportan la tecnología NFC?
¿Cuáles son las ventajas y desventajas de utilizar NFC para pagos móviles?
¿Qué elementos se deben tomar en cuenta para considerar un entorno seguro basado en NFC?

1.1.4 Justificación de la Investigación

En la actualidad nuevas tecnologías como NFC, ofrecen avances significativos y mucha versatilidad en los pagos móviles, brindando accesibilidad inmediata y facilidades de uso a los usuarios, que utilizan servicios de esta índole.

Por ello NFC ha dado lugar a la creación de distintas aplicaciones que facilitan las actividades de la vida cotidiana de las personas, como por ejemplo transacciones bancarias, pagos de servicios básicos, pago de pasajes de transporte, pago en puntos de venta, etc.

El uso de la tecnología NFC está enfocada principalmente en dispositivos móviles, por ello resulta de vital importancia, contar con un modelo aplicable para asegurar este tipo de transacciones.

El beneficio tecnológico que resultará de este trabajo de investigación será la elaboración de un modelo de seguridad que permitirá garantizar la integridad de los pagos móviles basados en NFC, el cual proveerá los componentes necesarios, para ser aplicados de manera exitosa en entornos similares.

1.1.5 Objetivo general de la Investigación

- Proponer un modelo de seguridad para garantizar la integridad de los pagos móviles basados en Near Field Communication (NFC).

1.1.6 Objetivos específicos de la Investigación

- Analizar los modelos de seguridad existentes para NFC.
- Determinar los componentes para el modelo de seguridad que garantizará la integridad de los pagos móviles.
- Implementar el modelo de seguridad, con todos sus elementos.
- Validar el modelo de seguridad NRioSec.

1.1.7 Hipótesis

El modelo de seguridad NRioSec incrementará el nivel de integridad de los pagos móviles basados en NFC.

1.1.7.1 Operacionalización Conceptual

Tabla 2-1 Operacionalización conceptual de variables

VARIABLE	TIPO	CONCEPTO
Modelo de Seguridad	Independiente	Un modelo de seguridad es la presentación formal de una política de seguridad. La integridad en un sistema basado en NFC no es completa hasta que se provea la seguridad en todos los elementos del sistema (Ok, Coskun, Ozdenizci, & Aydin, 2011)
Integridad	Dependiente	Integridad significa que el contenido o información solicitada de acuerdo a una petición, no ha sido alterada (S.-C. Cha et al., 2014)

Realizado por: Castro Cristhian, 2017

1.1.7.2 Operacionalización Metodológica

Tabla 3-1 Operacionalización metodológica de variables

VARIABLE	CATEGORIA	INDICADOR	TECNICA	INSTRUMENTO
Modelo de Seguridad	Independiente Simple	Calidad Coherencia Homogeneidad	Observación Científica	Cálculo de medición de variables, número de transacciones y calidad, entre otras
Integridad	Dependiente Compleja	Captura de información (data sniffing) Alteración de información (data modification)	Comparación de escenarios Test de Penetración	Escenario de Prueba Prototipo

Realizado por: Castro Cristhian, 2017

CAPITULO II

2. MARCO TEÓRICO

2.1 Antecedentes del Problema

Near Field Communication (NFC) provee un canal de comunicación inalámbrica en un rango máximo de 10 cm en la frecuencia de 13,56 MHz, con velocidades de transmisión de datos de hasta 424 kbps (Nikitin, Rao, & Lazar, 2007).

Los teléfonos móviles inteligentes (smartphones), tarjetas inteligentes (smartcards) y chips de identificación electrónica son algunos de los dispositivos que en la actualidad vienen equipados con tecnología NFC y que a nivel mundial son utilizados en transacciones susceptibles a la seguridad, como pagos móviles, sistemas de identificación y control de acceso.

Debido al corto alcance de la señal de comunicación de NFC, se ha restado importancia al análisis de seguridad de dicha tecnología, ya que se piensa que esta no puede ser alterada. Este concepto se basa en la publicación del sitio web del NFC Forum donde afirman que NFC es intrínsecamente seguro (NFC Forum, 2016a).

Sin embargo, se ha demostrado que en una transacción basada en NFC es posible obtener información sensible, alterarla y reproducirla cuando no se aplica un modelo de seguridad adecuado (SecTor, 2012).

2.2 Bases Teóricas

2.2.1 Sistemas de Comunicación Inalámbricos

El crecimiento registrado en los últimos años por los sistemas de comunicación inalámbricos ha multiplicado significativamente los servicios basados en este medio de comunicación, ya que están al alcance de la mayoría de las personas.

Una de las principales ventajas de los sistemas inalámbricos es la movilidad, debido a que el medio de transmisión está listo para ser usado y su punto de entrada en la red de comunicaciones no es fijo, logrando de esta manera que su expansión sea más rápida que la de cualquier otro tipo de sistema de comunicación.

Para (Prieto, Ramírez, Morillo, & Domingo, 2011) el intercambio de información que se realiza a través del espectro electromagnético entre uno o más actores (dispositivos o personas), es lo que se denomina un sistema de comunicación inalámbrica.

2.2.1.1 *Clasificación*

Considerando el alcance o distancia de conexión, los sistemas de comunicación inalámbricos se clasifican en 4 grupos: WPAN, WLAN, WMAN y WWAN.

2.2.1.1.1 Red inalámbrica de área personal (WPAN: wireless personal area networks)

Las redes inalámbricas de área personal (WPAN) son redes de corto alcance que se usan para la conexión de dispositivos periféricos a un ordenador o entre dos dispositivos móviles, sin la necesidad de cables.

Este tipo de redes se han constituido es una tecnología de uso cotidiano, dado que permite realizar comunicaciones e intercambio de información de manera cómoda y fácil de usar. Sin embargo, presentan una gran limitante en cuanto al alcance, ya que requiere la interacción de los dispositivos a pocos centímetros o metros de distancia.

Entre las tecnologías más conocidas y utilizadas de las redes inalámbricas de área personal se encuentran (Prieto et al., 2011):

- ***Bluetooth:*** tecnología que usa la radiofrecuencia de 2,4 GHz para el intercambio de voz y datos entre 2 o más dispositivos. Existen tres clases: Clase 1 (alcance aproximado de 100 metros), Clase 2 (alcance de hasta 10 metros) y Clase 3 (alcance de hasta 1 metro).

- ***Infrared Data Association (IrDA):*** define un estándar físico en la forma de transmisión y recepción de datos mediante rayo infrarrojo, permitiendo una conexión bidireccional a velocidades de entre 9.600 bps y los 4 Mbps con un alcance de 1 metro.

- ***Near Field Communication (NFC):*** permite la transmisión de datos de una manera simple entre diferentes dispositivos mediante un enlace de radiofrecuencia de 13,56 MHz. La tecnología NFC permite que un mismo dispositivo actúe como una tarjeta de proximidad inteligente y como lector, basado en el estándar ISO/IEC-14443 que define las tarjetas de identificación electrónicas, lo que la hace compatible con las infraestructuras de pago móvil existentes en el mercado.

- ***Zigbee:*** se utiliza para conectar dispositivos en forma inalámbrica a un costo y consumo de energía bajo. Funciona en una radiofrecuencia de 2,4 GHz pudiendo alcanzar una velocidad de transferencia de hasta 250 Kbps con un alcance máximo de 100 metros.

2.2.1.1.2 Red de área local inalámbrica (WLAN: wireless local area network)

Una red de área local inalámbrica (WLAN) es una red que cubre un área equivalente a una red local (LAN), con un alcance de hasta cien metros, permitiendo que los dispositivos que encuentran dentro del área de cobertura puedan conectarse e interactuar entre sí sin la necesidad de cables.

El uso de estas redes se ha vuelto común en las empresas, hogares y sitios públicos debido a que además de ofrecer a sus usuarios la posibilidad de estar conectados sin cables, brinda ciertas ventajas con respecto a las redes de área local, como lo menciona (Prieto et al., 2011):

- ***Movilidad:*** la información puede ser obtenida desde cualquier punto de la zona de cobertura en tiempo real.

- ***Flexibilidad:*** la cobertura abarca lugares donde resulta poco probable que una LAN pueda llegar.

- ***Economía:*** su implementación en lugares donde a menudo los equipos tecnológicos cambian de lugar, supone una ventaja y ahorro a largo plazo.

- ***Escalabilidad:*** permite una integración transparente y sencilla con otros tipos de conexiones de red, según los requerimientos.

A pesar de las ventajas que representa la instalación de una red local inalámbrica, también poseen algunas limitaciones según (Benavides, 2016):

- ***Velocidad:*** no pueden transmitir información a las mismas velocidades de una red LAN cableada.

- ***Retardos:*** al usar el espectro electromagnético para la trasmisión de información, estas pueden sufrir retardos.

- ***Interferencias:*** producidas generalmente por colisiones (transferencias simultáneas) o cuando una misma frecuencia es utilizada por 2 emisores al mismo tiempo.

- ***Cobertura máxima:*** el rango de cobertura oscila entre 10 m^2 a 100 m^2, lo que a su vez determina retardos de propagación de muy poca duración.

- ***Seguridad:*** dado que el espectro por el que viaja la información es accesible dentro del rango de cobertura, se requieren algoritmos de cifrado para garantizar la seguridad.

El estándar IEEE 802.11 para redes locales inalámbricas desarrollada por el IEEE (Institute of Electrical and Electronics Engineers) garantiza la interoperabilidad entre diferentes fabricantes, sin considerar el tipo de comunicación (cableada o inalámbrica).

(Benavides, 2016) hace referencia la familia de especificaciones del estándar 802.11, entre las cuales destacan:

- ***IEEE 802.11a:*** trabaja en la frecuencia de 5GHz, permitiendo velocidades de transmisión de hasta 54 Mbps.

- ***IEEE 802.11b:*** velocidad de transmisión de hasta 11 Mbps en la frecuencia de 2,4GHz.

- ***IEEE 802.11g:*** es una mejora del 802.11b con una velocidad superior de hasta 54 Mbps en la frecuencia de 2,4GHz.

- ***IEEE 802.11i:*** incluye los protocolos 802.1x, TKIP y AES con la implementación de WPA2, incrementando la seguridad de cifrado en los protocolos de autenticación.

- ***IEEE 802.11n:*** admite velocidades de transmisión de hasta 600 Mbps, tanto en el rango de frecuencias de 2,4 GHz y 5 GHz. 802.11n, siendo compatible con aquellos dispositivos basados en todas las especificaciones 802.11.

2.2.1.1.3 Red inalámbrica de área metropolitana (WMAN: wireless metropolitan area network)

Las WMAN o redes inalámbricas de área metropolitana usan el estándar WiMAX (Worldwide Interoperability for Microwave Access) basado en la norma IEEE 802.16, cuya cobertura es de hasta 50 km en las frecuencias de 2,3 a 3,5 GHz.

Existen dos variantes de la norma IEEE 802.16:

- ***802.16d:*** de acceso fijo, establece un radio enlace entre la estación base y un equipo situado en el domicilio del usuario. Teóricamente las velocidades máximas que se pueden obtener son de 70 Mbit/s con una frecuencia de 20 MHz. Sin embargo, en entornos reales se consiguen velocidades de hasta 20 Mbit/s, que es compartida por todos los usuarios.

- ***802.16e:*** de movilidad completa, que permite el desplazamiento del usuario de un modo similar al que se puede dar en GSM/UMTS. Es considerada una alternativa para las operadoras de telecomunicaciones que apuestan por los servicios en movilidad.

2.2.1.1.4 Red inalámbrica de área extendida (WWAN: wireless wide area network)

Las redes inalámbricas de área extensa (WWAN) tienen el alcance más amplio de todas las redes inalámbricas y usan tecnologías de red celular de comunicaciones móviles para transferir los datos.

En este tipo de redes, el dispositivo que envía y recibe la información está en movimiento, y pueden estar conectados de manera simultánea varios usuarios a la vez.

Dado que las redes WWAN usan la tecnología de red celular, estas pueden ser agrupadas por generaciones (Benavides, 2016):

- ***2G:*** tecnología de segunda generación diseñadas para la transmisión de voz y mensajes de texto (SMS) que reemplazó a las redes móviles de primera generación (analógicas). Esta generación abarca el sistema GSM (Global System for Mobile Communications).

- ***2.5G:*** se sitúa entre la tecnología 2G y 3G, y mejora la eficacia y la velocidad de transmisión con respecto a su antecesora. Esta generación abarca los sistemas GPRS (General Packet Radio Service) y EDGE (Enhanced GPRS).

- ***3G:*** la tecnología de tercera generación permite a la telefonía móvil disponer de banda ancha para transmitir grandes volúmenes de información mediante la red celular. Con ello es posible escuchar música y ver videos en tiempo real mediante streaming, así como las funciones de voz y texto desde el móvil. Esta generación abarca el sistema UMTS (Universal Mobile Telecommunications System).

- ***3.5G:*** es considerada la evolución de la tecnología 3G, la misma que provee un aumento considerable de la velocidad de transmisión de datos. Esta generación abarca los sistemas HSPA (High-Speed Packet Access) y HSDPA (High Speed Downlink Packet Access).

- ***4G:*** su tecnología es basada en Internet mediante el protocolo IP, combinándose con otros usos y tecnologías, como Wi-Fi y WiMAX. Esta generación abarca los sistemas LTE (Long Term Evolution) y WiMAX (Worldwide Interoperability for Microwave Access).

2.2.2 Teléfonos móviles inteligentes

La movilidad es la cualidad de un dispositivo para ser transportado o movido con frecuencia y facilidad, por tanto, los teléfonos móviles son aquellos que pueden ser transportados con facilidad y utilizados al mismo tiempo, pero que a su vez ofrecen una serie de funcionalidades que lo diferencian de los teléfonos celulares comunes.

2.2.2.1 *Características*

Las principales características de los teléfonos inteligentes son:

- Son aparatos electrónicos pequeños, que se pueden transportar en el bolsillo o en un pequeño bolso.

- Tienen alta capacidad de procesamiento.

- Establecen conexión con redes de datos inalámbricos.

- Poseen memoria interna (RAM, ROM, flash) y en ciertos casos capacidad de memoria externa (ranuras para tarjetas MicroSD).

- Tienen una alta capacidad de interacción mediante la pantalla o el teclado.

2.2.2.2 *Evolución de los teléfonos inteligentes*

En sus inicios, la idea de un smartphone o teléfono inteligente consistía en integrar las funciones de un teléfono celular y un asistente personal o PDA (Personal Digital Assistant) en un solo dispositivo.

En 1922 salió a la luz el IBM Simon, el primer dispositivo que integró las funciones de un PDA con capacidad para llamadas telefónicas y mensajería instantánea, con una pantalla táctil la cual podía ser manipulada por la mano, o mediante un lápiz digital (stylus).

El primer teléfono móvil considerado inteligente fue el Ericsson GS88 en el año de 1997, que incorporó las funciones básicas de acceso a Internet como correo electrónico, navegación, así como también la conexión a PC y un teclado QWERTY físico para su uso.

En el año 2000 se lanzó al mercado el sistema operativo Windows Pocket PC de Microsoft, junto con una cantidad de dispositivos y teléfonos inteligentes que adaptaron este sistema a las necesidades de los usuarios.

Entre el 2002 y el 2004, la empresa Palm Inc., con sus smartphones y PDAs basados en Palm OS, y la empresa RIM (Research In Motion) con sus teléfonos inteligentes Blackberry, serían las de mayor auge entre los usuarios empresariales a nivel mundial.

Y no fue hasta el 2007 donde la empresa Apple creó un punto de inflexión, con el anuncio de la primera versión del sistema operativo iOS y su primer teléfono inteligente iPhone, logrando una revolucionando en la industria de la telefonía móvil y de los smartphones.

Google no se quedó atrás, y en el 2008 lanzó al mercado el sistema operativo Android, que hasta la actualidad es el mayor competidor del sistema iOS de Apple. Por su parte Microsoft, dos años más tarde lanzó el sistema operativo Windows Phone.

2.2.3 Near Field Communication (NFC)

Con la popularidad de los teléfonos inteligentes y el Internet de las Cosas (IOT), la tecnología NFC ha sido adoptada como parte de las configuraciones básicas de los smartphones.

Esta tecnología hace posible la integración de tarjetas inteligentes (smart cards) en los teléfonos móviles.

2.2.3.1 *Historia*

En el año 2002 la empresa japonesa Sony y la neerlandesa Philips, realizaron una alianza estratégica con el fin de desarrollar un protocolo compatible con las tecnologías de comunicación inalámbrica, FeliCa y Mifare respectivamente, que en esa época poseían dichas empresas.

Es así, que un año más tarde, este protocolo fue adoptado como el estándar ISO/IEC 18092 (ISO/IEC 18092, 2013). Tras ello, se consolidó el NFC Forum con la participación de varios operadores de telefonía a nivel mundial, grandes empresas tecnológicas e instituciones financieras de renombre (NFC Forum, 2016b), que harían pública la primera especificación oficial del estándar Near Field Communication o NFC.

Con tecnología de corto alcance e inalámbrica, NFC opera en una frecuencia de 13.56 MHz, a una distancia máxima de 10 cm y a velocidades de 106kbit/s, 212kbit/s y 424 kbit/s (Nikitin et al., 2007).

NFC a su vez, es compatible con la tecnología de Identificación por Radiofrecuecia (RFID - Radio Frecuency Identification) y con las tarjetas inteligentes (Smart Card), las mismas que en los países desarrollados se utilizan para el control de acceso de personal, pago de servicios, compra de tickets, entre otros (Halgaonkar, Jain, & Wadhai, 2013).

2.2.3.2 *Modos de Operación de NFC*

NFC tiene 2 tipos de funcionamiento: activo y pasivo. Esto a su vez, permiten generar 3 diferentes modos de operación (Kerem Ok, 2011):

- ***Simulación de tarjeta (Card Emulation):*** Un dispositivo con tecnología NFC simula una tarjeta inteligente (modo pasivo), que podrá interactuar con otro dispositivo NFC.

- ***Lectura/Escritura (Reader/Writer):*** Permite leer información de un dispositivo NFC o tarjetas inteligentes.

- ***Punto a punto (Peer to peer):*** Permite la conexión entre dos dispositivos, para intercambiar información.

Tabla 1-2 Modos de Operación de NFC

MODO	TIPO	FUNCIONALIDAD
NFC Card Emulation	Pasivo: se comporta como una etiqueta RFID	Lectura
NFC Reader/Writer	Activo: tiene la capacidad de leer/escribir una etiqueta	Lectura/Escritura
NFC Peer to peer	Activo	Lectura/Escritura Bidireccional

Elaborado por: Castro Cristhian, 2017

2.2.3.3 *Etiquetas NFC*

Las etiquetas NFC (tags) son dispositivos conformados por 3 elementos: circuito integrado, antena y contenedor de energía. (Halgaonkar et al., 2013) describen los 4 tipos de etiquetas NFC existentes:

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

Tabla 2-2. Etiquetas NFC

	TIPO 1	TIPO 2	TIPO 3	TIPO 4
Estándar	ISO 14443 A	ISO 14443 A	FeliCa ISO 18092	ISO 14443 A y B
Memoria	96 Bytes hasta 2 KBytes	48 Bytes hasta 2 KBytes	Hasta 1 MB	32 KBytes
Velocidad	106 Kbit/s	106 Kbit/s	212 Kbit/s	106 - 424 Kbit/s
Operación	Lectura y Escritura o solo lectura	Lectura y Escritura o solo lectura	Preconfigurados para lectura y escritura o solo lectura	Preconfigurados para lectura y escritura o solo lectura

Elaborado por: Castro Cristhian, 2017

2.2.3.4 *Formato de intercambio de datos NDEF*

El formato de intercambio de datos NDEF (NFC Data Exchange Format) fue creado por el NFC Forum, con la finalidad que los dispositivos NFC puedan almacenar y transportar diferentes tipos de elementos, a su vez intercambiarlos con otros dispositivos o con las etiquetas.

(Roland & Langer, 2010) consideran a NDEF como un formato de encapsulación de mensaje para el intercambio de datos de un dispositivo NFC con otro, o con una etiqueta. Además, define las reglas para la creación de un mensaje NDEF válido y para una cadena ordenada de registros NDEF.

La estructura de NDEF empieza por una cabecera de datos, a partir de la cual se ubican los bloques de información. A su vez, cada bloque de información se agrupa en registros, que contienen los datos en mensajes NDEF, caracterizados por un tipo MIME definido.

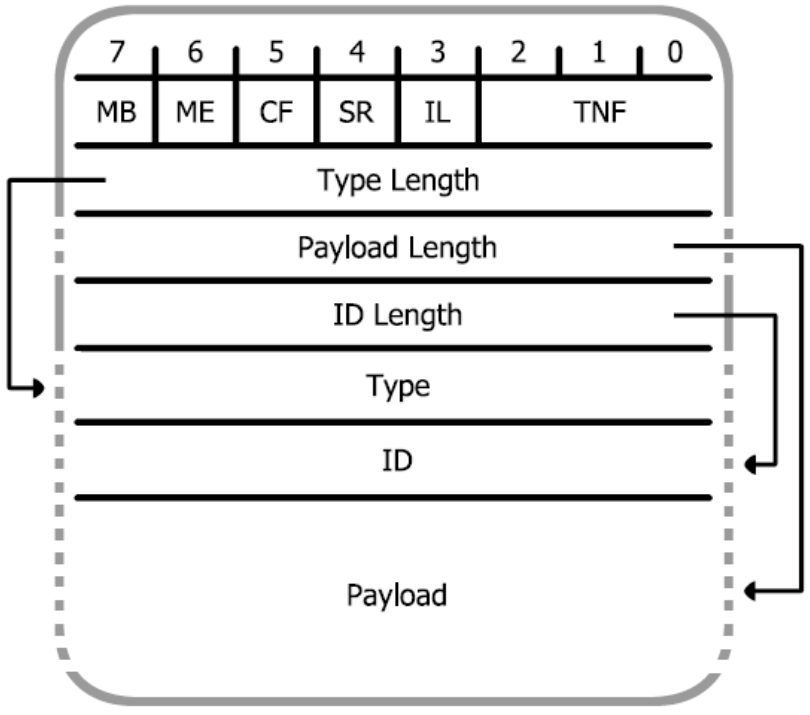


Gráfico 1-2. Formato de un registro NDEF
Fuente: (Roland & Langer, 2010)

El formato de intercambio de datos NDEF es similar tanto para etiquetas como para dispositivos NFC, por lo que la información transmitida es independiente del tipo de dispositivo que participe en el intercambio de información.

2.2.3.5 *Vulnerabilidades en NFC*

A pesar de que la tecnología NFC se limita a un rango de comunicación de tan solo 10 cm, existen algunas amenazas de seguridad y privacidad sobre los dispositivos pasivos (ej. etiquetas). Por su parte, en los dispositivos que trabajan en modo lectura/escritura, se puede vulnerar la seguridad, insertando etiquetas manipuladas en sustitución de las etiquetas originales.

(AbdAllah, 2011) aborda algunas de las amenazas que se podrían dar al momento del intercambio de información entre dispositivos NFC, entra ellas destacan:

- ***Interceptación de comunicaciones (Eavesdropping / sniffing):*** En este tipo de amenaza, un atacante sería capaz de interceptar y leer la información transmitida entre los dispositivos.

- ***Modificación de datos (Data Modification):*** Un atacante, en lugar de únicamente escuchar, podría modificar los datos que se transmiten entre los dispositivos NFC.

- ***Ataque de hombre en el medio (Man-in-the-Middle):*** En teoría un ataque poco probable, dada la distancia a la que se debe realizar la transferencia de información entre los dispositivos, sin embargo, no se la descarta como una posible amenaza para la integridad.

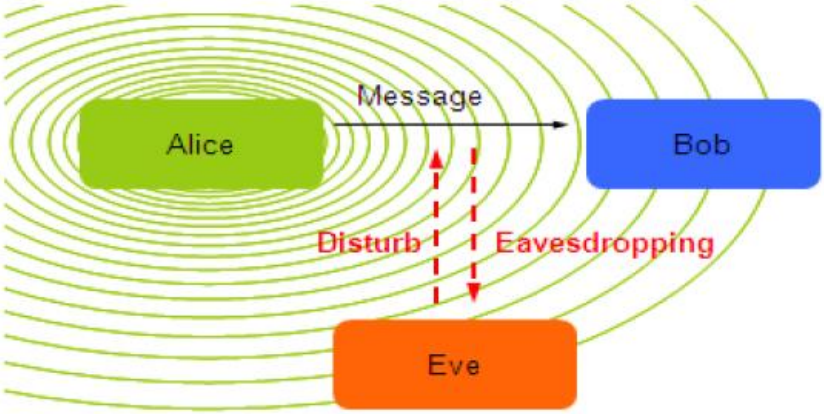


Gráfico 2-2. Ataques de infiltración y modificación de datos
Fuente: (AbdAllah, 2011)

(Chen, Lin, & Yang, 2014) manifiestan que, aunque los sistemas basados en NFC se consideran seguros, estos no están exentos de ataques o problemas de seguridad, y por ello determina algunos tipos de problemas:

- ***Identificador único (Unique ID):*** Un atacante podría clonar el identificador único de una tarjeta inteligente, para ser utilizado en otra aplicación.

- ***Ataque de denegación de servicios (DoS):*** Un atacante podría generar miles de solicitudes lo que hará que el servicio NFC pase a un estado suspendido.

- ***Autenticación de identidad (Identity Authentication):*** La autenticación de identificación necesita fabricantes de tarjetas IC para proteger la privacidad de los usuarios.

- ***Ataque Relay (Relay Attack):*** Un atacante podría obtener la información usando comandos de la unidad de datos de protocolo de aplicación (APDU).

- ***Estafa (Phishing):*** Un atacante podría modificar una etiqueta para que se redirija a sitios fraudulentos, para robar la información del usuario.

- ***Clonación de tickets (Ticket cloning):*** Un ticket generado en un sistema NFC podría ser clonado y compartido con otros atacantes, antes de ser verificado.

Tabla 3-2. Tipos de ataques en los modos de operación NFC

MODO DE OPERACIÓN	TIPO DE ATAQUE
NFC Card Emulation	Denegación de Servicios (DoS)
	Interceptación de comunicaciones (Eavesdropping)
	Ataque relay
NFC Reader/Writer	Autenticación de identidad
	Estafa (Phishing)
	Clonación de tickets

Elaborado por: Castro Cristhian, 2017

Para contrarrestar las vulnerabilidades de seguridad de NFC, (Abu-Saymeh, Abou-Tair, & Zmily, 2013) presentan un framework de seguridad que recoge los datos de seguridad y datos biométricos, manteniendo una medida de seguridad en el dispositivo. Cuando una transacción NFC es iniciada por un usuario, la aplicación solicita autorización al framework. El framework a su vez analiza el nivel de seguridad del dispositivo, y responde con la autorización o denegación de la solicitud.

Este framework, se conforma de los siguientes componentes:

- ***Autenticación:*** El framework maneja la autenticación utilizando métodos invasivos, como exigir el ingreso de una contraseña, o mediante métodos no invasivos, tales como el análisis del comportamiento.

- ***Seguridad de la aplicación:*** El framework de seguridad clasifica las aplicaciones en varias zonas de seguridad. A su vez, las transacciones NFC son preclasificadas y asignadas a una de las zonas de seguridad disponibles.

- ***Autorización:*** Las solicitudes de las transacciones NFC que son receptadas por el framework de seguridad, son comparadas entre el nivel de seguridad actual, y la zona de seguridad de las transacciones o aplicaciones.

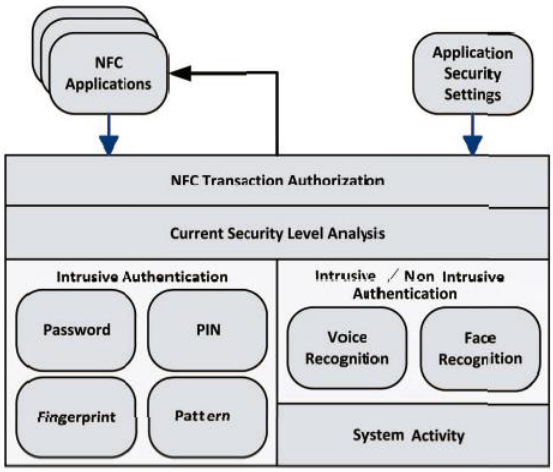


Gráfico 3-2. Framework de seguridad para NFC
Fuente: (Abu-Saymeh et al., 2013)

2.2.4 Evolución de los Pagos Móviles en el mundo

La progresiva evolución y el uso creciente de smartphones, junto con el acceso a internet de alta velocidad desde el móvil, han contribuido al crecimiento de las transacciones móviles. Es por ello que las entidades financieras invierten en modelos de negocio digitales, ganando cada vez más adeptos con los métodos de pagos móviles.

Hay que destacar que la innovación en los pagos móviles, van más allá de la simplicidad y ahorro de tiempo, se trata de la forma de manejar y utilizar el dinero a través de los móviles. Esto implica, desde tener registrada una tarjeta de crédito en el teléfono móvil, o de poder administrar eficientemente las cuentas bancarias que los usuarios utilizan a la hora de hacer compras y pagos (Pedreño, 2013).

Sin embargo, un paso previo a la proliferación de los pagos móviles fue el uso de medios electrónicos para realizar las transacciones por parte de los consumidores, específicamente los pagos realizados a través de internet o también conocidos como pagos en línea o pagos online.

1994, considerado como el año en que se realizó el primer pago en línea de la historia por parte de Pizza Hut. No han pasado más de 25 años de eso y el escenario sobre los pagos en línea ha cambiado enormemente y en la actualidad las transacciones financieras y comerciales están apuntando hacia los sistemas de pagos móviles.

A continuación, se detalla cronológicamente la evolución de los pagos móviles (Media Telecom, 2016):

- 1983: El criptógrafo estadounidense David Chaum, comenzó a investigar sobre la creación de dinero electrónico y la importancia de la privacidad en las transacciones. Inventó la "fórmula cegadora" (blinding formula) basada en la extensión del algoritmo RSA utilizado para la encriptación de páginas web, que permitía a una persona enviar dinero a otra sin dejar rastro del origen. De esta forma, el dinero podría ser modificado para que no se pudiese rastrear, a la vez que mantendría su firma original que lo haría único.

- 1994: La primera compra en línea de la historia realizada por Pizza Hut, cuya orden consistía en una pizza de pepperoni y champiñones.

- 1997: Coca Cola crea el primer sistema de pago móvil, el mismo que permitía a los usuarios adquirir una bebida en una cantidad limitada de máquinas expendedoras, mediante el envío de un SMS o mensaje de texto.

- **1997:** Exxon Mobile introduce Speedpass, el primer sistema de pago móvil con tecnología RFID, que permite a los usuarios pagar de manera rápida sus consumos de gasolina (Exxon and Mobil, 2014).

- 1998: PayPal es fundada por Peter Thiel y Max Levchin inicialmente bajo el nombre de Confinity y posteriormente pasaría a llamarse PayPal. Inicialmente se limitaba a ofrecer el servicio de transferencias de dinero a través de PDAs (Personal Digital Assistant o), pero en poco tiempo dieron un giro completo enfocado en el comercio electrónico.

- 1999: los teléfonos empezaron a ser usados para adquirir entradas de cine, con la tecnología de Ericsson en conjunto con Telnor Mobil.

- 2001: El comercio móvil alcanza los 2.400 millones de dólares en todo el mundo. Domino's Pizza comienza a tomar pedidos a través de teléfono celular.

- 2003: al menos 95 millones de usuarios a nivel mundial, han ejecutado una transacción de compra mediante su teléfono celular.

- 2004: Los mensajes de textos (SMS) son usados para realizar donaciones a organizaciones sin fines de lucro.

- **2004:** Nokia, Sony y Philips se unieron para formar el NFC Forum a fin de promover la seguridad y facilidad de uso de la comunicación de campo cercano (Square Inc., 2012).

- **2005:** Nokia lanza el primer teléfono habilitado con NFC para pagos móviles de boletos y pasajes, en su modelo 3220 (Nokia, 2005).

- 2009: Se crea Bitcoin (BTC), una moneda virtual encriptada cuyo valor está basado en el cálculo de un algoritmo complejo propuesto por Satoshi Nakamoto.

- 2009: El mercado de pagos móviles alcanza los 69 mil millones de dólares en ventas.

- **2011:** Google lanza oficialmente su primer servicio de pagos móviles denominado Google Wallet, basado en la tecnología NFC (Google, 2011).

- **2014:** Apple anuncia el lanzamiento de Apple Pay, servicio que permite a los usuarios del iPhone realizar pagos móviles mediante la tecnología NFC, y de la mano de las aplicaciones Touch ID y Passbook (Apple, 2014).

- **2015:** Samsung Pay se incorpora al mercado de los pagos móviles, los consumidores pueden ahora utilizar sus dispositivos móviles basados en NFC junto con la tecnología MST (Magnetic Secure Transmission) permitiendo que los pagos móviles sean más accesibles para los consumidores (Electronics Co., 2015).

- **2015:** Android Pay es anunciado oficialmente para smartphones que tengan la tecnología NFC y el sistema operativo KitKat 4.4 o superior de Google (Google, 2015).

- 2017: Se estiman 60 mil millones de dólares en ventas a través de pagos móviles.

- Y para el año 2020, se prevé que el 90 por ciento de los usuarios de smartphones habrá realizado al menos un pago móvil.

El uso de dispositivos móviles se ha convertido en una tendencia a nivel mundial, donde el 68% de los adultos poseen un smartphone, el 45% tienen tablets y aproximadamente el 90% de los propietarios de smartphones llevan sus teléfonos consigo la mayor parte del tiempo. Los pagos móviles tendrán un crecimiento exponencial a medida que las personas se vuelven más dependientes de sus dispositivos móviles para llevar a cabo las tareas cotidianas.

Actualmente, se consideran hay tres tipos de pagos móviles: m-commerce, m-payments y m-wallets.

- **M-Commerce:** se realizan usando el navegador del móvil para compras en sitios que almacenen su información del pago en la nube. Por ejemplo, cuando se realiza una compra en Amazon.com donde toda la información de pago ya se encuentra almacenada en el sitio.

- **M-Payments:** utilizan la tecnología de tokens para crear un identificador único por cada transacción a fin de asegurar la información sensible como datos bancarios o de tarjeta de crédito. Al realizar una transacción, por lo generar se utiliza un pin o huella digital para verificar la identidad del usuario y completar la transacción.

- **M-Wallets:** o también conocidas como billeteras móviles. Almacenan toda la información de pago en el dispositivo móvil para interactuar con un sistema de venta (POS) cercano para realizar una transacción.

Las capacidades y funcionalidades de los teléfonos inteligentes están provocando grandes cambios en el ámbito financiero, gracias al avance en el desarrollo de tecnologías como NFC que potencian los pagos móviles.

Las grandes empresas tecnológicas presentan alternativas relevantes para pagos móviles basados en NFC en teléfonos inteligentes que de a poco se van incorporando en los países con más desarrollo tecnológico en el mundo. Google Wallet, Apple Pay, Samsung Pay y Android Pay han logrado dar un respaldo importante a los pagos móviles con NFC, por lo que en la actualidad se consideran como una asociación de servicios y sistemas de pagos avanzados, ligada a la movilidad y ubicuidad (Pedreño, 2013).

2.2.4.1 *Pagos Móviles con tecnología NFC*

La tecnología NFC actualmente se encuentra integrada en tarjetas de viajero, tarjetas inteligentes, boletos de autobús, etc. Y la mayoría de teléfonos inteligentes o smartphones también incorporan un chip NFC. Las capacidades de la tecnología NFC son ahora más relevantes que nunca, particularmente cuando se trata de los pagos móviles. Con esta tecnología, dos dispositivos equipados con un chip NFC y colocados a pocos centímetros el uno del otro, permite el envío y recepción de datos en simultáneo a alta velocidad, por lo que es adecuada para la realización de transacciones y pagos.

Para el proceso de un pago móvil basado en NFC, se requieren al menos 2 dispositivos con tecnología NFC, el primero que será el dispositivo del adquiriente, y el segundo que será el terminal de punto de venta (TPV) del comercio. Este proceso por lo general se basa en el siguiente esquema (BBVA, 2015):

1. En el dispositivo del adquiriente, se registran los datos solicitados por el aplicativo, como por ejemplo datos básicos del usuario, y datos sensibles de las formas de pago, que pueden ser tarjetas de crédito, débito o cuentas bancarias.
2. Se acerca el dispositivo (adquiriente) a unos pocos centímetros del terminal de punto de venta (TPV del comercio)
3. El TPV lee automáticamente la información de pago almacenada en el chip inteligente del teléfono.
4. Se genera un token con un identificador único para la transacción y se confirma el pago por parte del comercio.
5. Todo este proceso ocurre en fracciones de minuto.

Los TPV emiten una onda de radio de alta frecuencia que facilita la comunicación entre el terminal y el teléfono. Cuando el dispositivo móvil está en rango, se ejecuta un protocolo de comunicación inalámbrica entre el terminal y el teléfono, para intercambiar información y realizar una transacción segura.

Gráfico 4-2. Proceso de un pago móvil basado en NFC
Fuente: http://www.centrodeinnovacionbbva.com/infografia/infografia-pagos-moviles-sin-contacto-nfc

Durante la última década, los principales emisores de tarjetas de crédito y débito a nivel mundial han agregado la función de pago sin contacto (contactless payments), permitiendo a sus usuarios procesar los pagos con tan solo colocar su tarjeta cerca del terminal del punto de venta.

Gráfico 5-2. Claves de los pagos móviles
Fuente: http://blogunisono.com/2016/03/despega-el-pago-por-movil-un-must-en-la-experiencia-de-cliente/

Una de las principales claves de los pagos móviles es que se basen en una tecnología común para facilitar su compatibilidad, y es por ello por lo que NFC está expandiendo su uso en estas formas de pago. Cuando se realiza un pago móvil con NFC, se establece una conexión con el TPV del vendedor, donde los pasos que siguen para procesar este tipo de pagos son idénticos a los que se usan en las transacciones que a diario cada día se realizan con tarjetas de crédito con chip y banda magnética.

Sin embargo, las transacciones con NFC tienen la ventaja de que los datos de tarjeta de crédito del comprador no son mostrados en ningún momento al vendedor, ya que el chip NFC cifra la información sensible antes de enviarla, tornándola inútil para cualquier intento de fraude.

2.2.4.2 *Google Wallet*

En 2011 Google lanzó de manera oficial Google Wallet, una aplicación que permitía a los usuarios almacenar en el teléfono los datos sus tarjetas de crédito, para eliminar la necesidad de llevarlas físicamente en una billetera, y por ello es considerada como una "billetera virtual" que permite realizar transacciones de manera rápida, sencilla y segura, en puntos de venta o tiendas.

De acuerdo con sus creadores, Google Wallet *"es parte de un esfuerzo continuo para mejorar las compras de consumidores y negocios. Está orientado en hacer las cosas más fáciles para que page y ahorre en los productos que desee, a la vez que le brinda al comerciante más formas para ofrecer a los consumidores cupones y programas de lealtad, así como reducir la brecha entre comercio online y tradicional"* (Google, 2011).

Gráfico 6-2. Google Wallet
Fuente: http://www.madridesnoticia.es/ciencia_y_tecnologia/redes_sociales/asi-funciona-google-wallet-dinero-via-gmail

Google Wallet permite almacenar dinero en el teléfono móvil a través de una aplicación, la cual se asocia con una tarjeta de crédito y permite mantener un saldo de efectivo a disposición en cualquier momento. Adicionalmente se puede almacenar cupones de descuento y de promoción, así como acumular puntos de descuento en locales que disponen de esta opción.

La tecnología NFC es parte Google Wallet, por lo que su uso está enfocado para smartphones con sistema operativo Android 4.4 o superior, y a las tiendas físicas que dispongan de un TPV con chip NFC integrado. El usuario simplemente acerca el equipo al TPV para realizar el pago y se descuenta el saldo desde la aplicación.

Para los pagos en línea, se accede mediante la aplicación del móvil y de descuenta el monto a pagar Google Wallet. Y la última incorporación es la transferencia de dinero a un amigo o familiar, que dispongan de una cuenta de correo de Gmail, y el monto a transferir se debita de la billetera virtual y se envía al destinatario.

Google Wallet ofrece un nivel de seguridad alto ya que los datos de tarjetas o bancarios no son enviadas directamente, si no que la aplicación sirve como puente y desde ahí se realizar todo el intercambio de información con las tiendas o comercios.

En el caso que el usuario pierda el teléfono donde se encuentra instalada la aplicación, esta no podrá ser accesible ya que además de tener que desbloquear la pantalla de inicio del equipo, es necesario ingresar un pin de seguridad para acceder a la aplicación.

Google Wallet permite una forma rápida de pago en tiendas físicas y tiendas en línea, con solo acercar el smartphone a pocos centímetros del TPV con NFC para procesar la compra, sin necesidad de ingresar códigos o claves adicionales.

2.2.4.3 *Apple Pay*

En septiembre del 2014, Tim Cook hacía la presentación del iPhone 6, y como un aditamento especial, anunciaba al mundo el lanzamiento de una solución de pagos denominada Apple Pay, que se basa en la tecnología NFC y está integrada en la aplicación Passbook, y para activarla únicamente se requiere asociar un número de tarjeta de crédito o débito (Apple, 2014).

Apple Pay se convirtió en una pasarela de pagos novedosa para los propietarios de los dispositivos móviles de la empresa de Cupertino, para completar los procesos de pago en las aplicaciones y los pagos en línea en un solo paso, de manera rápida y sencilla.

Al tener la información de las tarjetas almacenadas en la aplicación, el proceso de pago se reduce a colocar el dispositivo Apple cerca del TPV y confirmar la transacción mediante la huella digital de Touch ID. El dispositivo reproduce una vibración notificando que la transacción fue realizada de manera exitosa. Las operaciones son sencillas, fáciles y seguras gracias al hardware de seguridad integrado y a Touch ID.

Gráfico 7-2. Tim Cook en la presentación de Apple Pay
Fuente: https://www.nytimes.com/2014/09/11/upshot/apple-pay-tries-to-solve-a-problem-that-really-isnt-a-problem.html

Apple Pay aprovecha la tecnología inalámbrica NFC y el sistema Touch ID para un funcionamiento sencillo para sus usuarios.

A continuación, se detalla el proceso de funcionamiento de Apple Pay:

1. Los usuarios vinculan en Apple Pay sus tarjetas de crédito MasterCard, Visa o American Express, ya sea directamente en la aplicación, o mediante la importación de la información desde las cuentas de iTunes.
2. Se configura un nivel de seguridad mediante el registro de la huella dactilar a través de Touch ID. Este es el sustituto del código PIN tradicional.
3. En los comercios establecimientos habilitados para Apple Pay, solo será necesario acercar los dispositivos a los TPV, para posteriormente confirmar el pago con la huella dactilar.

En referencia a la seguridad de la Apple Pay, la empresa aclara que:

- Cuando el usuario agrega información de tarjetas de crédito o débito, esta no se almacena en los servidores de Apple, ya que se le asigna un número de cuenta al dispositivo, que será cifrado y almacenado de forma segura en el dispositivo.
- En cada transacción, se crea un identificador único de un solo uso con el número de cuenta del dispositivo, para ello Apple Pay utiliza la tokenización.

2.2.4.4 *Samsung Pay*

Samsung Pay facilita las transacciones seguras para sus clientes, mediante el uso de sus dispositivos móviles para pagar en puntos de venta, que dispongan de un chip NFC y junto con la tecnología MST (Magnetic Secure Transmission). Samsung Pay permite hacer pagos móviles más accesibles a comercios y consumidores (Argentina. Samsung, 2015).

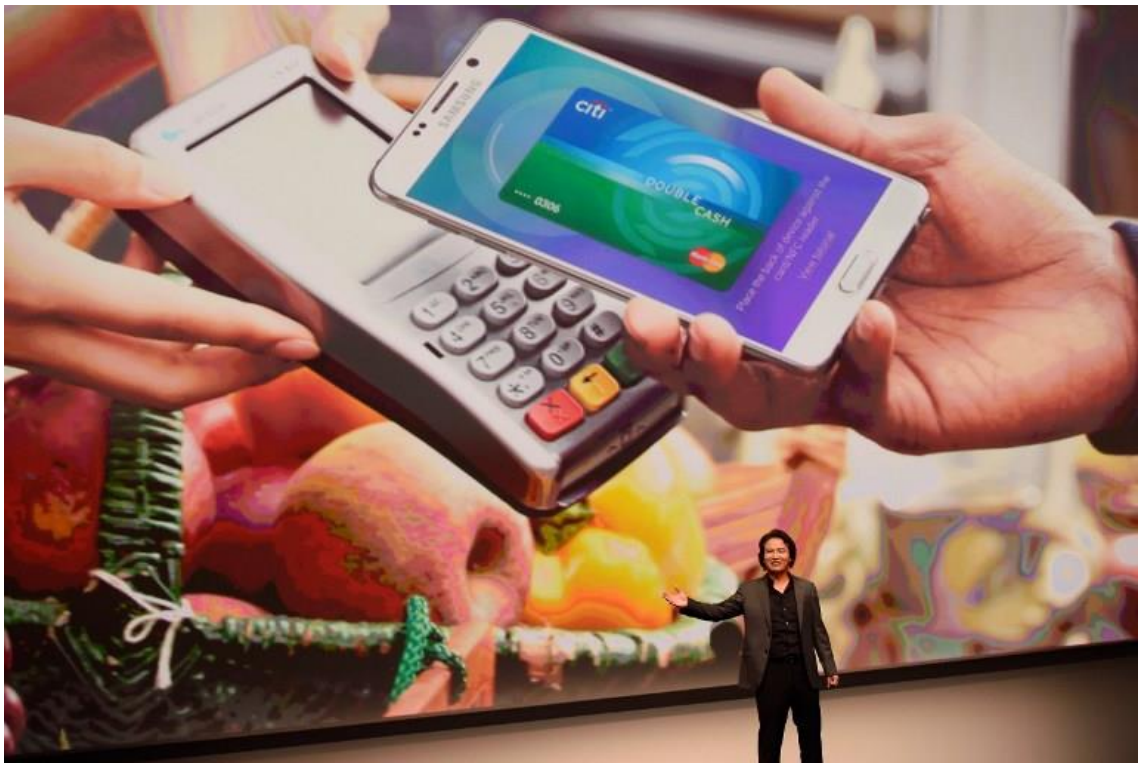


Gráfico 8-2. InJong Rhee en la presentación de Samsung Pay
Fuente: http://www.mediospublicos.ec/noticias/variedades/samsung-presento-dos-nuevos-smartphones-y-nuevo-servicio-de-pagos

La gran ventaja de Samsung Pay sobre sus rivales, se debe a la incorporación de la tecnología MST que fue desarrollada por la empresa LoopPay, quienes fabrican carcasas para celular en las que incluyen dispositivo electrónico que permite a los usuarios hacer pagos en casi cualquier TPV, ya sea que disponga de la tecnología NFC o sea un lector tradicional de tarjetas con banda magnética.

La tecnología MST genera campos magnéticos variables en un corto periodo de tiempo. Para ello generan una corriente alterna para que atraviese un bucle inductivo, y que pueda ser procesado por el receptor magnético del lector de tarjetas. La señal que recibe simula el mismo cambio del campo magnético que generaría una tarjeta tradicional. LoopPay funciona con un alcance de 7,5 cm respecto al receptor magnético. El campo se disipa rápidamente y sólo existe durante una transmisión iniciada por el usuario (Samsung Electronics Co., 2015).

En cuanto a seguridad, Samsung Pay trabaja con tres capas de seguridad:

1. Los datos codificados de las tarjetas de crédito se almacenan en el elemento seguro.
2. Se realiza un monitoreo en tiempo real del dispositivo gracias a la integración con Samsung Knox.
3. El uso de la huella dactilar añade un nivel extra de seguridad para completar los pagos.

Los pasos para el uso de Samsung Pay son:

1. Registrar los datos de las tarjetas de crédito en la aplicación.
2. Deslizar hacia arriba en la pantalla principal para seleccionar la tarjeta para el pago.
3. Autorizar el pago de forma segura mediante la huella dactilar.
4. Acercar el teléfono al TPV para completar la transacción.

2.2.4.5 *Android Pay*

En el marco de la conferencia I/O que se desarrolló en San Francisco en 2015, Google hizo el lanzamiento de Android Pay, un sistema de pago para todos los dispositivos con sistema operativo Android habilitados con NFC.

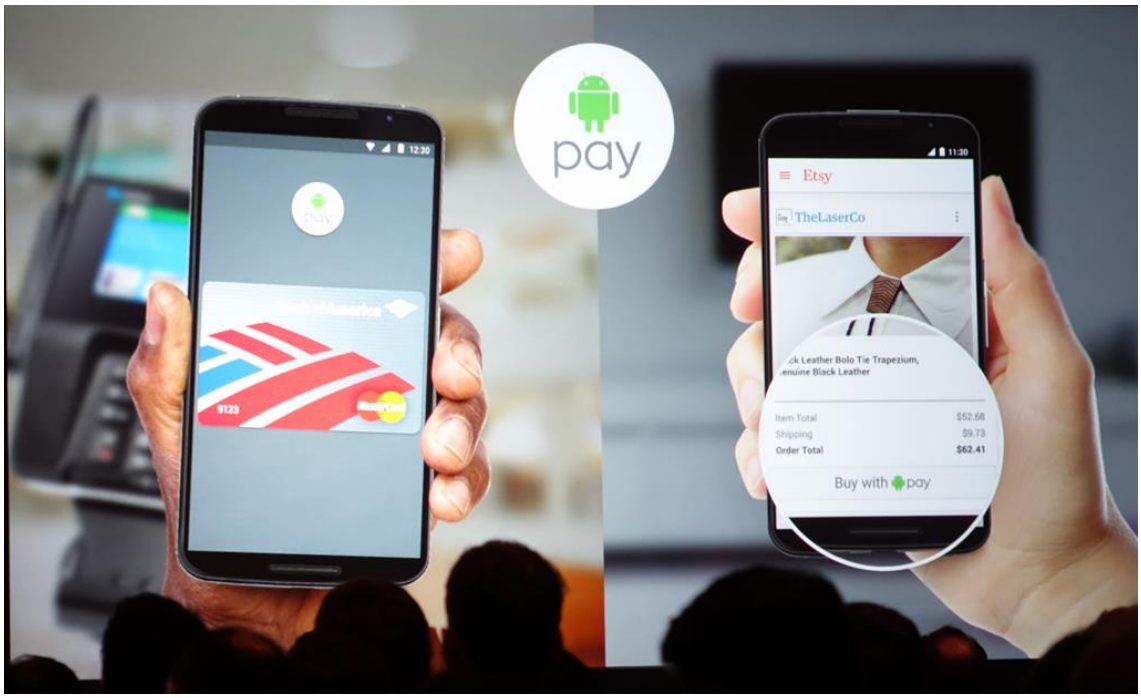


Gráfico 9-2. Presentación de Android Pay
Fuente: http://mobilesyrup.com/2016/10/11/latest-version-of-android-pay-suggests-the-platform-could-soon-come-to-canada/

Android Pay hace uso del Host Card Emulation (HCE) que permite a las aplicaciones móviles que se ejecutan en sistemas operativos compatibles representar virtualmente y de forma segura a través del NFC una tarjeta inteligente para poder realizar una transacción aprovechando los

procesos criptográficos basados en hardware sin necesidad de usar el elemento seguro físico (SE o Secure Element).

Para realizar un pago con Android Pay, simplemente será necesario acercar el teléfono al TPV de forma que se realice una conexión a través de NFC. Entre sus ventajas destaca la capacidad para almacenar tarjetas de fidelización, ofertas especiales y detalles sobre las tarjetas bancarias, centralizando las experiencias de compra de los usuarios.

En cuanto a seguridad, Android Pay está basada en tokens, de forma que los detalles de las tarjetas de crédito o débito no se envían con el pago, sino que se utiliza un identificador único que reemplaza el número de la tarjeta de crédito con 16 dígitos, proporcionando una capa extra de seguridad. Al momento de realizar una compra, el usuario podrá ver una confirmación del pago que muestra dónde se ha realizado la transacción, de forma que una actividad sospechosa sea rápidamente detectada.

Los representantes de Google comentaron que "los pagos móviles son su prioridad, y trabajan en conjunto con MasterCard para ofrecer una experiencia de compra fácil y segura para sus usuarios a través de sus teléfonos Android (MasterCard, 2015).

2.2.5 Evolución de los Pagos Móviles en el Ecuador

La constante evolución tecnológica ha permitido que, durante los últimos 5 años, en el Ecuador tome fuerza la aplicación de servicios y pagos mediante dispositivos móviles.

El uso de smartphones se ha vuelto común en el desempeño de las actividades de uso cotidiano por parte de los usuarios, hasta llegarse a convertir en una herramienta de comunicación, trabajo y también diversión. Según el INEC (Ecuador. Instituto Nacional de Estadística y Censos, 2017), el número de usuarios de smartphones creció más de 700% en los últimos 5 años, pasando de 500 mil personas a casi 4,5 millones de usuarios. Solo de diciembre de 2015 a diciembre de 2016, este número se incrementó en 45.3%, es decir casi 1,4 millones de usuarios nuevos.

Gráfico 10-2. Número de usuarios de smartphones en el Ecuador
Fuente: https://twitter.com/Ecuadorencifras/status/829688887102566402/photo/1

El uso de los pagos móviles pretende aumentar los movimientos financieros de los usuarios, sin embargo, su implementación en el país aún no ha despuntado debido al estado actual del mercado ecuatoriano, así como las tecnologías que se encuentran actualmente vigentes en el país, sin olvidar la seguridad, que es primordial al momento de implementar servicios de pagos móviles.

Se han identificado 3 estrategias en torno a su implementación en el Ecuador:

1. La primera es mejorar la seguridad de las transacciones, disminuyendo el nivel de fraudes en las compras, para de esta manera permitir que los vendedores, los compradores y las instituciones financieras sientan seguridad al momento de transaccionar mediante dispositivos móviles.

2. La segunda es mejorar la experiencia del usuario durante el proceso de compra, ya que la principal causa por la que el usuario no usa un pago de esta manera puede deberse a la cantidad de pasos que debe realizar o por que le resulta demasiado compleja.

3. Y la tercera es convencer al usuario que los pagos en efectivo son cosas del pasado, pese a que representan el 90% de las transacciones en el Ecuador. El usuario debe estar convencido que al utilizar su smartphone tendrá mayor seguridad y efectividad en las transacciones.

Uno de los principales obstáculos que han enfrentado los pagos móviles, es la falta de acceso a los sistemas financieros por parte de los usuarios. Aún existe una brecha importante entre la cantidad de negocios que ofertan este tipo de servicios de pago electrónico, con respecto a aquellos que aún no aceptan pagos electrónicos o con tarjeta, y que no se sienten seguras con los sistemas digitales, y no quieren cambiar los hábitos de sus negocios.

2.2.5.1 *Dinero Electrónico*

En noviembre del 2014, se puso en funcionamiento la primera etapa del dinero electrónico como forma de pago en el Ecuador, el mismo que es definido como aquél que se almacena e intercambia a través de dispositivos móviles, entre otros, producto del avance tecnológico (Ecuador. Junta de Regulación Monetaria Financiera, 2014).

El dinero electrónico es un medio alternativo de pago en dólares de los Estados Unidos, cuyo único administrador es el Banco Central del Ecuador. Para su funcionamiento no es necesario que el usuario disponga de una cuenta bancaria o que requiera de una conexión a Internet. El dinero electrónico podrá ser canjeado por dinero físico a petición del usuario (Ecuador. El Telégrafo, 2016).

Gráfico 11-2. Dinero Electrónico en Ecuador
Fuente: http://www.cre.com.ec/noticias/2016/06/01/137632/efectivo-desde-celular-dinero-electronico/ei

El dinero electrónico es un instrumento de pago virtual que se guarda, moviliza y transfiere por medio de dispositivos electrónicos y que sirve para saldar de contado la compra de bienes, servicios y valores, sin utilizar billetes, monedas, cheques de banco, tarjetas de crédito u otros instrumentos convencionales (Ecuador. Superintendencia de control del Poder de Mercado, 2014).

A inicios del 2015 el Banco Central del Ecuador puso en marcha la segunda etapa del sistema de dinero electrónico para la carga y descarga de dinero, para consultar los últimos movimientos, consultas de saldo, envío de dinero a otro usuario, y para realizar compras en locales comerciales. Y la tercera fase arrancó a mediados del 2015 con la posibilidad de usar el dinero electrónico para pagos de servicios y obligaciones tributarias.

Tras el terremoto ocurrido en el Ecuador el 16 de abril del 2016, entró en vigor la Ley Orgánica de Solidaridad y de Corresponsabilidad Ciudadana para la Reconstrucción y Reactivación de las Zonas Afectadas por el Terremoto, donde se establece el aumento del IVA del 12 al 14 por ciento. Adicionalmente estipula que aquellas personas que realicen transacciones mediante el dinero electrónico paguen únicamente el 10% del IVA. Por ejemplo, por la compra de $100, el valor normal del IVA es de $14, pero si cancela con dinero electrónico, únicamente se paga $10 por IVA, es decir se le devuelve al usuario 4 puntos del IVA por cada transacción realizada con este sistema (Ecuador. El Telégrafo, 2016).

Con esta ley, que promueve la devolución de 1 a 4 puntos del IVA, tanto para consumos con tarjetas de crédito, débito y con dinero electrónico, el crecimiento del uso de este sistema ha sido significativo. Hasta enero de 2017 las transacciones realizadas llegaron a 15 millones de dólares y el saldo a la fecha del dinero electrónico en el Banco Central del Ecuador, se encuentra a $ 6,1 millones.

El funcionamiento del dinero electrónico tiene el siguiente esquema:

1. Marcar desde el celular *153# y seguir los pasos para la apertura de la cuenta.
2. Aceptar el mensaje para activar la cuenta, donde se solicitarán datos como cédula y nombre, y la respuesta para las preguntas de seguridad del sistema.
3. Posteriormente se genera una clave personal de 4 dígitos que será utilizada para realizar las transacciones en el sistema.
4. Para recargar dinero a la cuenta, es necesario que el usuario se acerque a un establecimiento autorizado por el BCE (macro agente, como bancos, cooperativas, entre otros) donde entregará el dinero físico para que sea acreditado a la cuenta del usuario.
5. Ahí mismo, para la descarga, el usuario se acercará a un macro agente donde gestionará el cambio del dinero electrónico por dinero físico.
6. El canje de dinero electrónico por físico no tendrá costo hasta por cuatro transacciones al mes, al igual que la consulta de saldos y movimientos hasta 10 veces al mes.

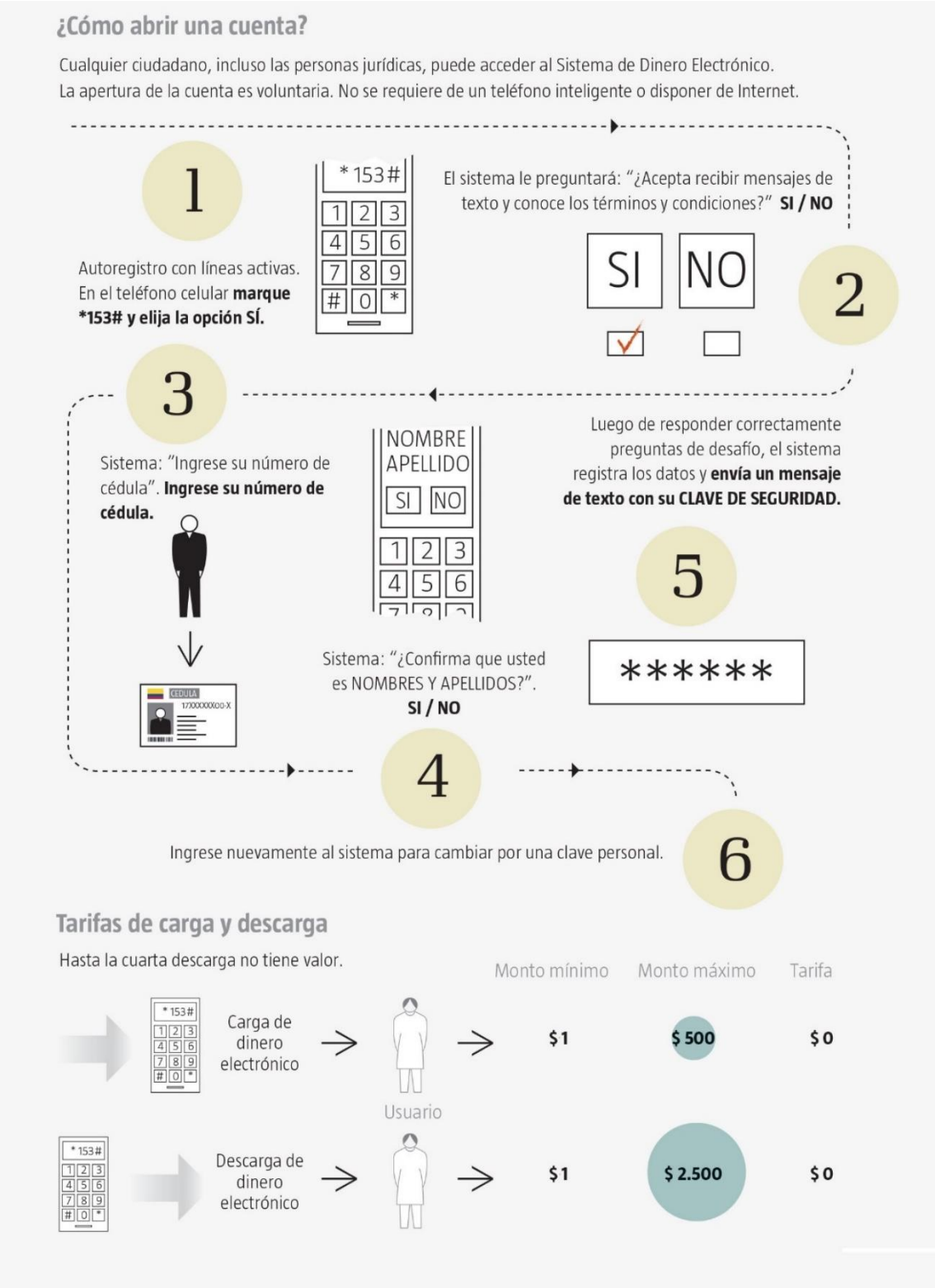


Gráfico 12-2. Abrir cuenta de Dinero Electrónico del Banco Central del Ecuador

Fuente: http://www.eltelegrafo.com.ec/noticias/economia/8/el-dinero-electronico-se-activa-al-marcar-153

2.2.5.2 *PayClub Móvil*

A finales del 2015, Diners Club del Ecuador presentó PayClub Móvil es una aplicación para smartphones, que permite realizar transacciones sin la necesidad de la tarjeta de crédito física, sino mediante un código temporal que autoriza la compra de un producto o servicio. PayClub Móvil no almacena la información en el celular, sino en el sistema desarrollado por la aplicación, de tal manera que otorga mayor seguridad y reduce la posibilidad de fraudes.

Los usuarios de PayClub Móvil pueden registrar las tarjetas de crédito Diners, Discover, MasterCard y Visa (Banco Pichincha) y Visa Interdin para realizar los pagos. Adicional a la experiencia de pago tecnológica, sencilla y diferente, los usuarios tienen acceso a servicios complementarios como promociones con geolocalización y notificaciones de seguridad, así como también al historial de las transacciones realizadas y el registro de gastos que realizan.

Gráfico 13-2. PayClub Móvil
Fuente: https://pbs.twimg.com/media/Cmjcyp7W8AAfXjP.jpg

PayClub Móvil permite pagar con el smartphone, tan solo registrando las tarjetas de crédito en la aplicación, para lo cual se deben seguir los siguientes pasos:

1. Descargar la aplicación PayClub desde App Store (iOS) o Play Store (Android).
2. Activar la aplicación en el teléfono celular, siguiendo los pasos de registro.
3. Seleccionar la opción “gestionar tarjetas” para registrar las tarjetas de crédito.
4. Para realizar un pago, seleccionar la opción “generar código” sobre la tarjeta con la que se va a realizar el pago.

5. En la pantalla se desplegará el código temporal que deberá ser ingresado por el vendedor en el terminal del punto de venta (TPV)
6. A continuación, se debe confirmar el pago presionando la opción “Aceptar” en la pantalla que muestra el detalle de la compra”.
7. En el TPV se imprimirá el voucher de compra donde se debe incluir la firma.

Gráfico 14-2. Pasos para el uso de PayClub Móvil
Fuente: http://www.itahora.com/actualidad/movilidad/nueva-modalidad-de-pagos-en-ecuador/

PayClub Móvil se convierte en un complemento para otras formas de pago tradicionales, pero que brinda los siguientes beneficios (Ecuador. Diners Club, 2015):

- Agilidad: Con solo acceder a la aplicación móvil y seleccionar la tarjeta con la que realizará el pago, obtendrá su código de compras de un solo uso (OTT).
- Seguridad Ni el establecimiento ni el sistema operativo del teléfono acceden nunca a la información de su tarjeta de crédito.
- Comodidad: Usted podrá pagar en todos los establecimientos habilitados para proporcionar este servicio sin necesidad de presentar su tarjeta físicamente.

PayClub Móvil es una aplicación que busca que los usuarios lleguen a un nuevo nivel tecnológico de transacciones, que actualmente ya se usa en varios países del mundo.

2.2.5.3 *PayPhone*

En mayo del 2014, se conforma la empresa EcuaPayPhone producto de la sociedad de 3 ingenieros ecuatorianos con amplia experiencia en el desarrollo de aplicaciones móviles, quienes identificaron la necesidad de la gente para usar su smartphone como medio de pago. Producto de esto nace PayPhone, aplicación móvil que permite realizar transacciones desde un smartphone con tan solo registrar las tarjetas al número de la línea móvil del propietario.

PayPhone maneja el concepto de que para realizar un pago se requieren de 2 componentes: una tarjeta de crédito y un terminal de punto de venta (TPV) y la aplicación sustituye el uso físico de las tarjetas de crédito de los usuarios al momento de procesar los pagos.

Gráfico 15-2. PayPhone Ecuador
Fuente: https://www.facebook.com/PayphoneEc/photos/a.754851057902652.1073741827.754847617902996/1223621467692273/

En 2015, PayPhone obtuvo la certificación de Visa Internacional y posteriormente de MasterCard Internacional, lo que llamó la atención del Grupo Promerica-Produbanco quienes apoyaron el emprendimiento y ahora lo ofrecen dentro de su amplia gama de servicios financieros. Adicionalmente PayPhone cuenta con la certificación del Banco Central del Ecuador para la utilización del dinero electrónico.

PayPhone está disponible para las tarjetas de crédito Visa y MasterCard de Produbanco y para los smartphones con sistemas operativos Android, iOS y Windows Phone. Los pasos para utilizarla como forma de pago son (Produbanco - Grupo Promerica, 2016):

1. Con la aplicación descargada, crear un usuario y clave de acceso para la aplicación.

2. Ingresar la información personal y de validación que solicita el sistema.

3. Registrar los números de tarjetas de crédito o débito y el código de seguridad CVV localizado en el reverso de la tarjeta.

4. Si la información registrada es correcta, el servicio se habilita para que el usuario puede realizar compras en los establecimientos afiliados.

5. Para procesar un pago, el usuario únicamente debe proporcionar el número de celular en el establecimiento y la aplicación le notificará el consumo y solicitará la clave de acceso a la aplicación.

6. Posteriormente se selecciona la tarjeta con la que se desea pagar, el sistema envía un mensaje de autorización al punto de venta y el pago se hace efectivo.

En cuanto a la seguridad, PayPhone garantiza la seguridad de la información de las tarjetas del usuario, ya que trabaja bajo el estándar de seguridad PCI DSS, que permite cifrar toda la información que se envía durante la transacción. El usuario únicamente proporciona el número de celular y en ningún momento entrega la información de sus tarjetas de crédito al establecimiento. Adicionalmente, cada transacción requiere de la clave de ingreso creada por el usuario, la cual corresponde al código de usuario de PayPhone.

En el 2015, durante el Digital Bank Colombia 2015, PayPhone recibió su primer reconocimiento internacional, donde 22 emprendedores de Iberoamérica presentaron las diversas plataformas de solución tecnológica para la rama financiera. Al final, el jurado decidió que la mejor plataforma fue la de PayPhone (Ecuador. Grupo El Comercio, 2015).

CAPITULO III

3. METODOLOGÍA DE INVESTIGACIÓN

Este capítulo tiene como objetivo fundamental describir el proceso metodológico empleado en la investigación, los procedimientos, métodos y técnicas que permitieron recopilar resultados tendientes a comprobar la hipótesis planteada a través de pruebas y mediciones.

3.1 Diseños de la Investigación

La presente investigación corresponde a un diseño Cuasi-experimental, en el cual se desarrolla el estudio de una variable que, a medida que se realizan las pruebas, va permitiendo la comprobación de su hipótesis base, ya que la integridad va a estar en función del modelo que se propone implementar. Es decir, en base a la manipulación de la variable independiente se evidencia el comportamiento de la variable dependiente. Se trabajó con grupos que estaban formados previamente, es decir grupos intactos no elegidos al azar.

3.2 Tipo de Investigación

El tipo de estudio de este trabajo es una investigación correlacional ya que indica el nivel de relación entre las dos variables a fin de determinar cómo se puede comportar la una variable conociendo el comportamiento de la otra. En este caso, se pone en evidencia la relación que existe entre el nivel de integridad de los pagos móviles con la aplicación del modelo de seguridad utilizando la tecnología NFC.

Se utiliza también la investigación experimental pues se desarrollan sus procesos, como son la observación, análisis e interpretación de los resultados en cuanto al comportamiento de la variable en el criterio de integridad garantizado por la tecnología NFC en los pagos móviles.

3.3 Población y Muestra

Uno de los principales componentes de esta investigación es la población, es decir, aquellas unidades de análisis que proporcionarán los datos sobre los cuales se enfoca este estudio, y la

correspondiente parte representativa de dicha población, o sea la muestra que facilite su análisis e interpretación. A continuación, se describe a cada una de ellas.

3.3.1 Población

La población es el conjunto total de individuos, objetos o medidas que poseen algunas características comunes, observables en un lugar y en un momento determinado; ésta constituye el objeto de la investigación de donde se extrae la información requerida para el estudio. En la presente investigación, la población está constituida por todas las vulnerabilidades que se presentan en distintos sistemas y equipos basados en tecnología NFC.

3.3.2 Muestra

La muestra es una parte representativa de la población en la que se reproduce de la mejor manera sus rasgos esenciales, datos que son importantes para la investigación. La función básica del muestreo es determinar que parte de una población debe examinarse, con la finalidad de hacer inferencias sobre dicha población.

En el presente trabajo investigativo se emplea un Muestreo Dirigido o Intencional, ya que los elementos representativos están determinados por el tipo de investigación realizada, por lo tanto, se considerarán las vulnerabilidades de NFC como eavesdropping, data modification, relay attack y man-in-the-middle.

3.4 Métodos, Técnicas e Instrumentos

La investigación se fundamenta en la aplicación de métodos, técnicas e instrumentos que facilitan la interpretación final de la misma.

3.4.1 Métodos

Los principales métodos que se utilizan para el estudio planteado se describen a continuación.

3.4.1.1 *Método Científico*

Determinado como una sucesión ordenada de fases en la investigación, está constituido por principios, reglas y procedimientos que orientan el proceso investigativo. Siendo una estrategia general para abordar un problema científico, su aplicación en este trabajo sigue el camino de la duda sistemática. Su nivel de desglose es evidente desde la identificación y planteamiento del problema en cuanto a la integridad de pagos móviles utilizando la tecnología NFC.

Revisión de conceptos relacionados a los sistemas de comunicación inalámbricos, teléfonos móviles inteligentes, pagos móviles con estos dispositivos, la tecnología NFC, las vulnerabilidades y ataques en los modos de operación NFC, y la propuesta de un modelo que utilizando la tecnología NFC garantice mayor integridad en los pagos móviles. Hipótesis, elección de técnicas, recolección y análisis de la información para finalmente llegar a concluir y establecer soluciones.

En consecuencia, las fases previstas para la aplicación de este método de detallan a continuación:

1. Planteamiento del problema
2. Formulación de hipótesis
3. Levantamiento de información
4. Análisis e interpretación de resultados
5. Comprobación de la hipótesis
6. Difusión de resultados.

3.4.1.2 *Método Analítico*

Permite observar las características y relaciones de los modos de operación de NFC y su comportamiento en un pago móvil. Está conformado por las etapas de observación, descripción, descomposición, ordenación y clasificación de todo lo que conduce al objeto de estudio.

3.4.1.3 *Método Sintético*

La síntesis permite integrar alternativa nueva de solución para las vulnerabilidades previamente analizadas en los procesos de pagos mediante la aplicación de la tecnología NFC.

3.4.1.4 *Método Experimental*

Mediante la aplicación de este método se obtienen pautas para realizar las pruebas en base a un escenario que tendrá dos momentos:

1) Escenario donde se manifiestan las vulnerabilidades susceptibles en los pagos móviles.
2) Escenario que determina si las vulnerabilidades son corregidas, mitigadas en base al modelo de seguridad NRioSec.

3.4.1.5 *Método Comparativo*

Se establece al identificar un escenario sin la aplicación del modelo que garantiza mayor integridad en los pagos móviles, frente al mismo escenario con la implementación del modelo de seguridad NRioSec.

3.4.1.6 *Técnicas*

Los métodos seleccionados para la presente investigación se complementan con la aplicación de las técnicas correspondientes, que son las siguientes:

- Observación
- Experimentación
- Comparación de escenarios
- Análisis
- Test de penetración

3.4.2 Instrumentos

Los instrumentos son las herramientas utilizadas para realizar las pruebas dentro del escenario y a su vez facilitarán el análisis y el desarrollo del test de penetración para validar el modelo de seguridad NRioSec.

3.4.2.1 *Instrumentos Software*

Tabla 1-3. Instrumentos Software

NOMBRE	VERSIÓN	DESCRIPCIÓN	FUNCIONALIDAD
Visual Studio + Xamarin	2015	Entorno de desarrollo integrado multiplataforma con leguaje C#	Desarrollar la aplicación para dispositivos Android que simula un pago basado en NFC.
Windows	10	Sistema Operativo	Alojar los servicios necesarios para el ejecución del punto de venta.
Wireshark	2.0.2	Sniffer	Capturar tráfico y analizar una transacción NFC.
Hyper-V	10.0.1	Software de virtualización	Crear una máquina virtual que simula ser un atacante.

Elaborado por: Castro Cristhian, 2017

3.4.2.2 *Instrumentos Hardware*

Tabla 2-3. Instrumentos Hardware

NOMBRE	DESCRIPCIÓN	FUNCIONALIDAD
Servidor	Computadora Personal	Ejecutar la máquina virtual que funcionará como atacante y el servidor del punto de venta.
Punto de venta	Smartphone Sony Xperia Z1 Compact	Simular el punto de venta para la recepción un pago con NFC
Teléfono para pago	Smartphone Samsung Galaxy S7	Simular el pago móvil basado en NFC
Atacante	Smartphone Samsung Galaxy S4	Simular un ataque mediante la alteración de la información

Elaborado por: Castro Cristhian, 2017

3.4.2.3 *Instrumentos Bibliográficos*

Se emplearán como instrumentos los modelos de seguridad de NFC descritos en tesis y artículos científicos a fin de determinar los componentes que formarán parte del modelo de seguridad que garantice la integridad en los pagos móviles.

3.5 Validación de los Instrumentos

La aplicación de los instrumentos mencionados el apartado 3.4 permitirán realizar el análisis de datos, mediciones y comparaciones de los factores de seguridad que forman parte del objeto de estudio, a fin de llegar a la evaluación de la hipótesis planteada.

3.6 Procedimiento

Para la realización del presente estudio de investigación se establecen lineamientos y pasos que otorgarán una secuencia lógica de cada proceso y que podrá ser tomada como guía de referencia.

Los pasos establecidos se describen a continuación:

1) Configuración de los instrumentos hardware.
2) Configuración de los instrumentos software.
3) Configuración del escenario de prueba 1.
    - 3.1 Captura de información (data sniffing) de un pago móvil basado en NFC con el sniffer Wireshark.
    - 3.2 Observación y análisis de vulnerabilidades.
    - 3.3 Aplicación del modelo de seguridad NRioSec al escenario de prueba 1.
4) Configuración del escenario de prueba 2.
    - 4.1 Alteración de información (data modification) durante el proceso de intercambio de datos en un pago móvil basado en NFC.
    - 4.2 Observación y análisis de vulnerabilidades.
    - 4.3 Aplicación del modelo de seguridad NRioSec al escenario de prueba 2.
5) Observación y análisis de resultados mediante la tabulación de toma de muestras y generación de datos estadísticos.

3.7 Planteamiento de la Hipótesis

El modelo de seguridad NRioSec incrementará el nivel de integridad de los pagos móviles basados en NFC.

3.8 Operacionalización de las Variables

Para el análisis de la investigación se consideran las siguientes variables:

3.8.1 Variable Independiente

La aplicación de un modelo de seguridad es la variable independiente en la presente investigación, ya que la variable independiente permite manipular las características de otras variables que estarán en función de esta y variarán según su manipulación.

3.8.2 Variable Dependiente

La integridad es la variable dependiente en la presente investigación, ya que al momento de aplicar un modelo de seguridad en un pago móvil basado en NFC se puede medir si la integridad aumenta, se mantiene o disminuye.

3.8.3 Operacionalización Conceptual

Para la realización de la presente investigación se consideran las siguientes variables:

Tabla 3-3. Operacionalización Conceptual de Variables

VARIABLE	TIPO	CONCEPTO
Modelo de Seguridad	Independiente	Un modelo de seguridad es la presentación formal de una política de seguridad. La integridad en un sistema basado en NFC no es completa hasta que se provea la seguridad en todos los elementos del sistema (Ok et al., 2011)
Integridad	Dependiente	Integridad significa que el contenido o información solicitada de acuerdo a una petición, no ha sido alterada (S.-C. Cha et al., 2014)

Elaborado por: Castro Cristhian, 2017

3.8.4 Operacionalización Metodológica

Tabla 4-3. Operacionalización Metodológica de Variables

VARIABLE	CATEGORIA	INDICADOR	TECNICA	INSTRUMENTO
Modelo de Seguridad	Independiente Simple	Calidad	Observación Científica	Cálculo de medición de variables, número de transacciones y calidad, entre otras
		Coherencia		
		Homogeneidad		
Integridad	Dependiente Compleja	Captura de información (data sniffing)	Comparación de escenarios prueba	Escenario de Prueba Prototipo
		Alteración de información (data modification)		

Elaborado por: Castro Cristhian, 2017

3.9 Escenarios de Prueba

Para el desarrollo de la presente investigación se plantean dos escenarios de prueba:

- ***Primer escenario:*** denominado *Escenario Vulnerable*, se analizará la aplicación de pagos móviles basada en NFC en la que no se considera ninguna medida de seguridad adicional a la proporcionada por los dispositivos móviles.
- ***Segundo escenario:*** denominado *Escenario Seguro*, se analizará la aplicación móvil implementada con el modelo de seguridad NRioSec, para evidenciar si se garantiza o no la integridad de los pagos móviles basados en NFC.

Las fases para analizar las vulnerabilidades presentes en la tecnología NFC son:

1) Generación de ataques.
2) Análisis de los ataques NFC.
3) Aplicación del modelo de seguridad NRioSec.
4) Análisis comparativo de los resultados de los escenarios de prueba.

3.9.1 Escenario de Prueba 1

A continuación, se describen los instrumentos utilizados y el esquema del escenario de prueba 1:

Tabla 5-3. Escenario de Prueba 1

ESCENARIO	INSTRUMENTOS HW / SW	TIPO DE ATAQUE
Escenario Vulnerable	Aplicación NFC sin modelo de seguridad Wireshark	Captura de información (data sniffing)
Escenario Seguro	Aplicación NFC con modelo de seguridad aplicado Wireshark	Captura de información (data sniffing)

Elaborado por: Castro Cristhian, 2017

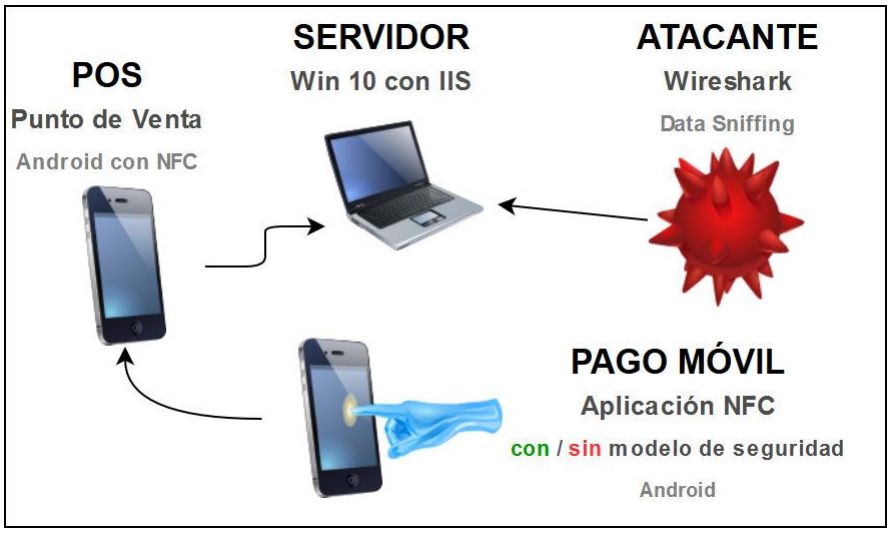


Gráfico 1-3. Esquema del Escenario de Prueba 1
Elaborado por: Castro Cristhian, 2017

3.9.2 Escenario de Prueba 2

A continuación, se describen los instrumentos utilizados y el esquema del escenario de prueba 2:

Tabla 6-3. Escenario de Prueba 2

ESCENARIO	INSTRUMENTOS HW / SW	TIPO DE ATAQUE
Escenario Vulnerable	Aplicación NFC sin modelo de seguridad Aplicación Android tipo malware	Alteración de información (data modification)
Escenario Seguro	Aplicación NFC con modelo de seguridad aplicado Aplicación Android tipo malware	Alteración de información (data modification)

Elaborado por: Castro Cristhian, 2017

Gráfico 2-3. Esquema del Escenario de Prueba 2
Elaborado por: Castro Cristhian, 2017

3.10 Modelo de Seguridad NRioSec

Gráfico 3-3. Logotipo NRioSec – NFC Security Model
Elaborado por: Castro Cristhian, 2017

El Modelo de Seguridad NRioSec fue desarrollado en base a las normas de seguridad de aceptación de pagos móviles elaborada por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC, Payment Card Industry Security Standards Council) que fue fundado por las principales compañías emisoras de tarjetas (crédito y débito) a nivel mundial con el objetivo de establecer estándares de seguridad y guías para la protección de los datos de las tarjetas, independientemente de la forma o canal utilizado para el pago (Liu et al., 2010).

Estas normas tienen como objetivo proporcionar directrices y mejores prácticas sobre el desarrollo de soluciones de pagos seguras, incluyendo mecanismos tradicionales y otros menos convencionales que evitan la exposición de los datos sensible, mejorando considerablemente la integridad y la mitigación de vulnerabilidades (Payment Card Industry Security Standards Council, 2014).

3.10.1 Objetivos de Seguridad del Modelo NRioSec

En base a las normas del PCI SSC, el Modelo de Seguridad NRioSec contempla 18 objetivos de seguridad para garantizar la integridad de los pagos móviles basados en NFC.

Tabla 7-3. Objetivos de Seguridad del Modelo NRioSec

#	OBJETIVOS DE SEGURIDAD	
1	Evitar que los datos sean interceptados cuando se ingresen en un dispositivo móvil	✓
2	Evitar que los datos se comprometan mientras se procesan o almacenan en el dispositivo móvil	✓
3	Evitar que los datos sean interceptados tras la transmisión del dispositivo móvil	✓
4	Evitar el acceso a dispositivos lógicos no autorizados	✓
5	Crear controles del lado del servidor y reportar accesos no autorizado	✓
6	Evitar la escalada de privilegios	✓
7	Deshabilitar remotamente la aplicación de pago	✓
8	Detectar robo o pérdida	✓
9	Fortalecer la infraestructura de los sistemas	✓
10	Validar el estado del servidor	✓
11	Codificación, ingeniería y pruebas seguras	✓
12	Protección contra vulnerabilidades conocidas	✓
13	Protección del dispositivo móvil de aplicaciones no autorizadas	✓
14	Protección del dispositivo móvil contra malware	✓
15	Protección del dispositivo móvil de accesorios no autorizados	✓
16	Crear materiales de instrucción para su implementación y uso	✓
17	Soporte de recibos seguros	✓
18	Proporcionar un indicador de estado seguro	✓

Elaborado por: Castro Cristhian, 2017

3.10.1.1 *Evitar que los datos sean interceptados cuando se ingresen en un dispositivo móvil*

Asegura que los datos del usuario estén debidamente cifrados antes de su registro en el dispositivo móvil. Si se utiliza un dispositivo externo para el registro de datos en el dispositivo móvil, dicho dispositivo también mostrará que está autorizado a comunicarse con la aplicación de pago. Si el dispositivo externo es inalámbrico, el canal de comunicación inalámbrico debe asegurarse mediante cifrado adicional.

3.10.1.2 *Evitar que los datos se comprometan mientras se procesan o almacenan en el dispositivo móvil*

Genera un entorno de ejecución de confianza en un elemento seguro (SE) para el almacenamiento temporal de los datos antes del procesamiento y durante la transacción, para evitar el sniffing de atacantes. Los datos cifrados de cuentas que son almacenados tienen una gestión de las claves criptográficas relacionadas para que no sean accesibles a personas, aplicaciones y / o procesos no autorizados.

3.10.1.3 *Evitar que los datos sean interceptados tras la transmisión del dispositivo móvil*

Los datos de la cuenta son cifrados (simétrica o asimétricamente) antes que la transmisión se realice fuera del entorno de ejecución de confianza del dispositivo móvil.

3.10.1.4 *Evitar el acceso a dispositivos lógicos no autorizados*

Protege el dispositivo móvil del acceso lógico no autorizado, mediante una pantalla de bloqueo como el ingreso de un “Patrón” o un “PIN” de seguridad, y que a su vez obliga al usuario a volver a autenticarse en el dispositivo después de un tiempo determinado. Adicionalmente incluye la capacidad para determinar si la depuración USB está desactivada y si está habilitado el cifrado de los datos.

3.10.1.5 *Crear controles del lado del servidor y reportar accesos no autorizado*

Incluye controles para prevenir y reportar intentos de acceso no autorizados, identificar y reportar actividad inusual e interrumpir los accesos. Los controles además estipulan:

- Soporte para acceso autorizado (ej.: lista de control de acceso).
- Capacidad para monitorear eventos y para distinguir eventos inusuales.
- Capacidad para reportar eventos (por ejemplo, a través de un registro, mensaje o señal) incluyendo cambios de claves, escalada de privilegios, intentos de inicio de sesión no válidos que exceden un umbral, actualizaciones de software de aplicación o firmware y acciones similares

3.10.1.6 *Evitar la escalada de privilegios*

Evita la escalada de privilegios en el dispositivo (privilegios de root o de grupo) desactivando el dispositivo cuando se ha detectado una intrusión, y mostrando una advertencia en caso de que se intente rootear o realizar un jail-break al dispositivo.

3.10.1.7 *Deshabilitar remotamente la aplicación de pago*

Incluye un mecanismo para que la aplicación sea deshabilitada de forma remota, sin interferir con otras funcionalidades del dispositivo móvil que no tengan relación con el sistema de pago.

3.10.1.8 *Detectar robo o pérdida*

Incluye el uso de la tecnología de localización GPS con la capacidad de establecer límites geográficos, re-autenticación periódica del usuario y re-autenticación periódica del dispositivo, en caso del robo o pérdida del dispositivo móvil, a fin de que se desactiven los servicios asociados.

3.10.1.9 *Fortalecer la infraestructura de los sistemas*

Fortalece o realiza un "hardening" de los sistemas de pago móviles que reciben datos de tarjetas para evitar el acceso no deseado o la exposición de datos de una transacción, manteniendo una infraestructura segura y al margen de atacantes.

3.10.1.10 *Validar el estado del servidor*

Valida la conexión con el servidor a fin de que las transacciones se realicen en línea, y en caso de que el servidor se encuentra inaccesible, la aplicación de pago móvil no autoriza las transacciones ni almacena datos para su posterior transmisión y procesamiento.

3.10.1.11 *Codificación, ingeniería y pruebas seguras*

Abarca las mejores prácticas de codificación segura para prevenir las vulnerabilidades de codificación comunes en los procesos de desarrollo de software como fallas de inyección, desbordamiento de búfer, almacenamiento de cifrado inseguro, manejo incorrecto de errores y control de acceso inadecuado. Además, permite establecer un proceso formal para identificar y asignar una clasificación de riesgo a las nuevas vulnerabilidades de seguridad descubiertas y que puedan ser documentadas.

3.10.1.12 *Protección contra vulnerabilidades conocidas*

Proporciona un medio seguro para mantener actualizada de manera oportuna la aplicación de pago en el dispositivo móvil a través de actualizaciones automáticas que son notificadas al usuario, para evitar que el dispositivo móvil pueda ser vulnerado por un atacante.

3.10.1.13 *Protección del dispositivo móvil de aplicaciones no autorizadas*

Evitar la carga y posterior ejecución de aplicaciones que no pueden ser autenticadas, mediante un proceso que permite la distribución segura de las aplicaciones de tal manera que un usuario final pueda determinar que la aplicación procede de una fuente de confianza antes de instalarla.

3.10.1.14 *Protección del dispositivo móvil contra malware*

Implementa procesos de autenticación para proteger los sistemas de amenazas de software malicioso actuales y en evolución, basándose en soluciones MAM (Mobile Application Management) para la gestión segura mediante autenticación, autorización y acceso. Los usuarios obtienen acceso basado en nombres de usuario, contraseñas, dirección IP y autenticación de dispositivos en el servidor. Estas soluciones normalmente utilizan métodos de autenticación de múltiples factores para conceder y administrar el acceso, a fin de que puedan monitorear, evaluar y eliminar software malicioso y aplicaciones del dispositivo.

3.10.1.15 *Protección del dispositivo móvil de accesorios no autorizados*

Permite asegurar que el dispositivo de entrada que se encuentra conectado al dispositivo móvil (ej.: lector de tarjetas) independientemente si la conexión es física o inalámbrica, esté emparejado de manera correcta con el dispositivo móvil, mediante la validación a través de un número de serie u otro identificador único.

3.10.1.16 *Crear materiales de instrucción para su implementación y uso*

Elaboración de documentación para abordar el uso adecuado y seguro tanto en el entorno del comerciante, como en el entorno del usuario final.

3.10.1.17 *Soporte de recibos seguros*

Permite enmascarar la información sensible de la forma de pago al momento de la generación de recibos, ya sea que esta se imprima o se envíe mediante correo electrónico.

3.10.1.18 *Proporcionar un indicador de estado seguro*

Incluye un mecanismo para notificar al usuario del dispositivo móvil que la aplicación móvil de pagos está ejecutando en un estado seguro, similar al indicador cuando una compra se realizar en un sitio con certificados SSL.

3.10.2 Componentes del Modelo NRioSec

El Modelo de Seguridad NRioSec utiliza la autenticación y verificación de identidad, la tokenización y la criptografía, sumados a las normas de seguridad de aceptación de pagos móviles del PCI SSC, que permiten determinar su alto grado de compatibilidad y fácil integración en el desarrollo de aplicaciones de pago móviles.

Con la implementación de NRioSec, se logra cubrir las necesidades de seguridad definidas para los pagos móviles (Attard & Leung, 2012):

- **Confidencialidad:** la información sensible que se transmite durante una transacción, como los datos de la tarjeta de crédito, se protegen mediante cifrado. Esto evita a un atacante acceder a la información confidencial.
- **Privacidad:** la información es transmitida únicamente entre el emisor y el receptor. De esta manera, se protege la información confidencial de los atacantes o de los actores que participan legítimamente en la transacción pero que no tienen necesidad de acceder a dicha información.
- **Integridad:** se proporciona cifrado y autenticación de dos vías, donde los mensajes intercambiados durante una transacción incluyen una firma o certificado digital, para que el receptor pueda validarlos.
- **Confiabilidad:** se asegura al receptor que los detalles del pago son correctos y corresponden a los datos proporcionados por el emisor, mediante una pantalla donde se confirme que los datos son correctos.
- **Auditoría:** el modelo proporciona registros de auditoría para respaldar las transacciones realizadas.

A fin de que el modelo sea compatible con diferentes tipos de aplicaciones para pagos móviles con NFC, debe ofrecer protección suficiente contra las amenazas analizadas (AbdAllah, 2011). Para ello se establecieron los componentes que conforman los tres niveles de seguridad del Modelo NRioSec.

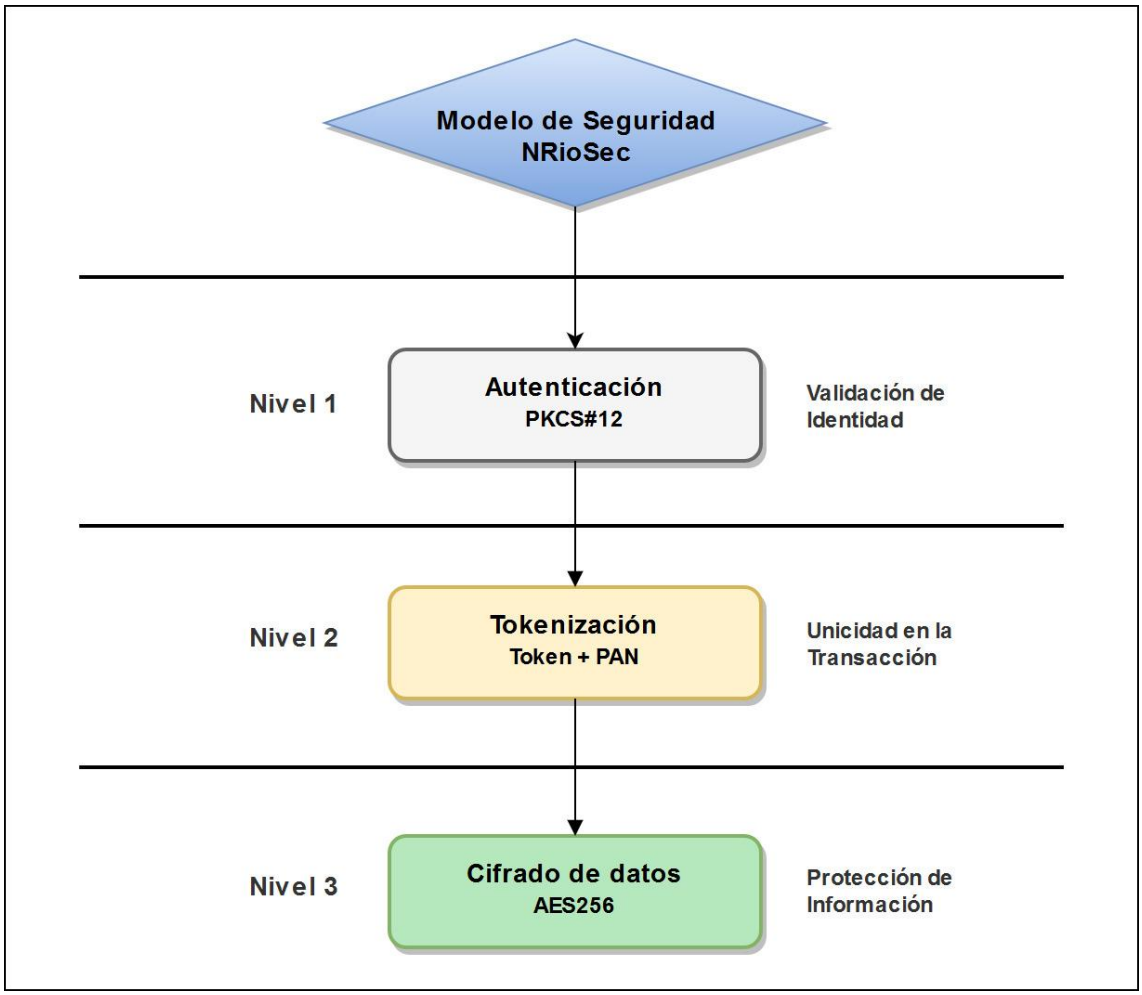


Gráfico 4-3. Componentes del modelo de seguridad NRioSec
Elaborado por: Castro Cristhian, 2017

3.10.2.1 *Nivel de Seguridad 1 – Autenticación*

Objetivo del Nivel: *Validación de Identidad*

Este nivel constituye la base para todas las aplicaciones que realizan transacciones de datos de dos vías, a fin de garantizar la identidad del emisor y el receptor y para ello se requiere un certificado digital con el estándar PKCS#12. Este estándar fue desarrollado por la empresa de seguridad RSA y especifica un formato portátil para almacenar o transportar claves privadas y certificados de un usuario (Dell EMC, 2014).

El estándar PKCS#12 admite la transferencia directa de información personal en varios modos de privacidad e integridad. El modo más seguro de privacidad e integridad requiere que las plataformas de origen y destino tengan un par de claves públicas/privadas confiables para la firma y cifrado, respectivamente. El estándar también admite modos de privacidad y de integridad

basados en contraseña para aquellos casos en los que no se dispone de pares de claves públicas/privadas de confianza (Yinghui, 2009).

La extensión para archivos PKCS#12 es usualmente ".p12" aunque también puede ser ".pfx". El archivo ".p12" contiene tanto la clave privada como la pública, así como información sobre el propietario (nombre, dirección de correo electrónico, etc.), todas certificadas por un tercero (Entidad Certificadora). Con dicho certificado, el usuario puede identificarse y autenticarse en la aplicación de manera segura.

Gráfico 5-3. Nivel de Seguridad 1 - Autenticación
Elaborado por: Castro Cristhian, 2017

3.10.2.2 *Nivel de Seguridad 2 – Tokenización*

Objetivo del Nivel: *Unicidad en la Transacción*

En este nivel se consideran aplicaciones que transmiten datos cuyo valor se elimina tras un periodo de tiempo después del procesamiento de la información, como por ejemplo un identificador que brinde unicidad a la transacción.

La Tokenización surgió en el 2005 con el objetivo de proteger la información de transacciones financieras y aseguramiento de datos, reemplazándolos con un conjunto de valores no sensibles y no descriptivos. Los datos sensibles reales se almacenan localmente en una ubicación protegida o en un servidor (B. Cha & Kim, 2013). La tokenización en ámbitos digitales se usan para prevenir el acceso no autorizado a información personal como números de tarjetas de crédito, transacciones financieras, expedientes médicos, antecedentes penales e incluso registros de votantes. Con este proceso, un token se genera en una diversidad de maneras, ya sea para coincidir con el formato de los datos originales que está protegiendo o para generar un conjunto de valores arbitrarios sin orden o secuencia lógica, que se asignan de nuevo a la información sensible.

La seguridad de la tokenización se basa en tres aspectos (B. Cha & Kim, 2013):

- Cumple con las especificaciones de PCI-DSS.
- La privacidad se almacena y gestiona con seguridad en el servidor de tokens.
- Se obtiene mediante generación de números aleatorios y no hay fallas de privacidad.

La tokenización en los pagos móviles permite que el número de tarjeta del usuario, que vendría a ser el número de cuenta principal o PAN (Primary Account Number) sea reemplazado por un identificador único o token. La de-tokenización a su vez es el proceso inverso de redimir un token para su valor PAN asociado. En otras palabras, un token de pago oculta la información de la tarjeta principal, como el PAN, el nombre del portador y la fecha de caducidad (Urien, 2015).

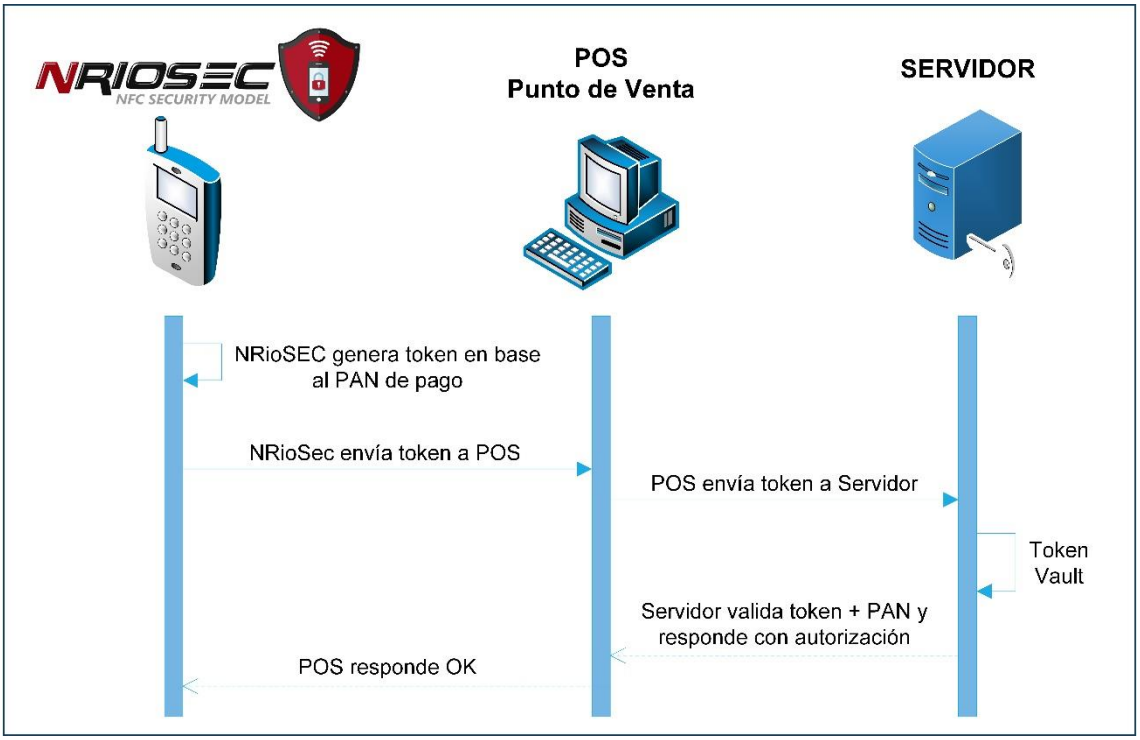


Gráfico 6-3. Nivel de Seguridad 2 - Tokenización
Elaborado por: Castro Cristhian, 2017

3.10.2.3 *Nivel de Seguridad 3 – Cifrado de datos*

Objetivo del Nivel: *Protección de Información*

Este nivel permite la protección a largo plazo de los datos transmitidos como los datos de la transacción de un pago móvil. Para ello se utilizará el estándar de cifrado en bloque de clave simétrica publicada por el Instituto Nacional de Estándares y Tecnología (NIST) en diciembre de 2001 denominado AES (Advanced Encryption Standard) (Mantoro, Ayu, & Mahmod, 2014).

Si bien los dispositivos móviles van mejorando constantemente, tienen recursos limitados, sobre todo en la energía que requieren para funcionar. Estos criterios permiten que AES con una fuerza de 256 bits se ajuste a las necesidades del modelo, porque es mucho más rápido, consume menos recursos y es adecuado para diferentes longitudes en el procesamiento de palabras.

Un cifrado de clave asimétrica como RSA o de curva elíptica (ECC) no son adecuados porque los dispositivos móviles no pueden dedicar su energía limitada para implementar un cifrado de clave pública complejos y que por lo general están orientados a los recursos (Mantoro et al., 2014).

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

AES con una clave de 256 es fácil de implementar y es extremadamente rápido ya que no se experimenta disminución en el rendimiento en comparación con otros algoritmos de cifrado. Su ventaja radica en que resulta casi imposible de descifrar si no se conoce la clave, lo que brinda un alto nivel de seguridad.

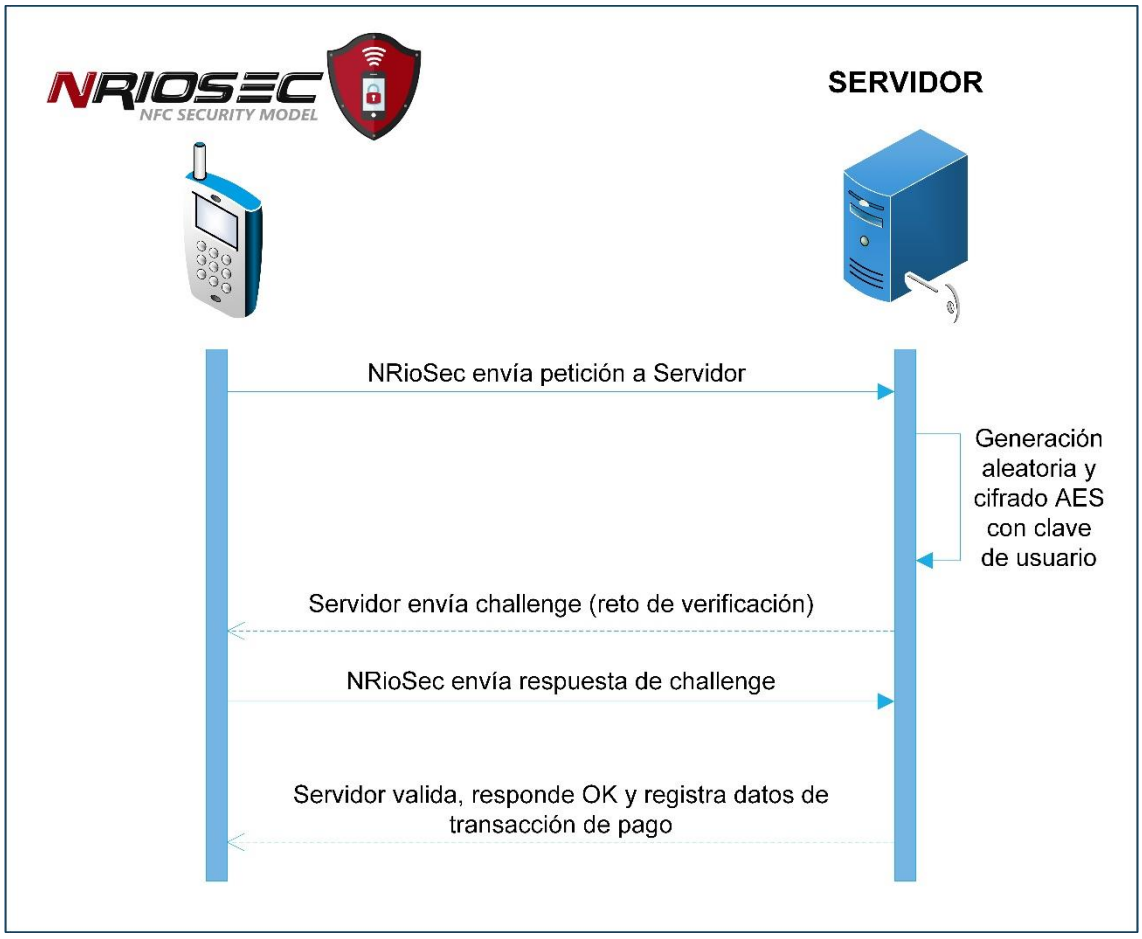


Gráfico 7-3. Nivel de Seguridad 3 – Cifrado de datos
Elaborado por: Castro Cristhian, 2017

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

La seguridad es un pilar fundamental en los pagos móviles basados en NFC, sin embargo, esta tecnología es vulnerable a ataques que afectan la integridad de la información sensible que se transmite en una transacción con esta tecnología.

Esta afirmación se deriva de la investigación realizada y de la implementación de los escenarios de prueba, cuyos resultados serán tratados en este capítulo.

4.1 Prototipo de Pago Móvil NRioPay

Gráfico 1-4. Logotipo NRioPay – NFC Mobile Payment
Elaborado por: Castro Cristhian, 2017

Para la validación del modelo de seguridad NRioSec, se implementó un prototipo de pago móvil basado en NFC denominado NRioPay, que incluye una aplicación para dispositivos móviles con sistema operativo Android (4.4 o superior) y que dispongan de un chip NFC. Adicionalmente contempla una aplicación web que funciona como back-end en el lado del servidor.

Este prototipo contempla todos los actores y elementos que participan en un proceso de pago móvil con NFC. La simulación realiza un pago de un boleto de tren a través de un POS que soporta NFC. El valor de la compra es debitado del saldo de la tarjeta que previamente registró el usuario en la aplicación.

La aplicación para dispositivos móviles permite el registro de información del usuario y de la forma de pago, que se detallan a continuación:

- Nombre, teléfono, dirección, email
- Contraseña, pin
- Número tarjeta de crédito, fecha vencimiento, código cvv

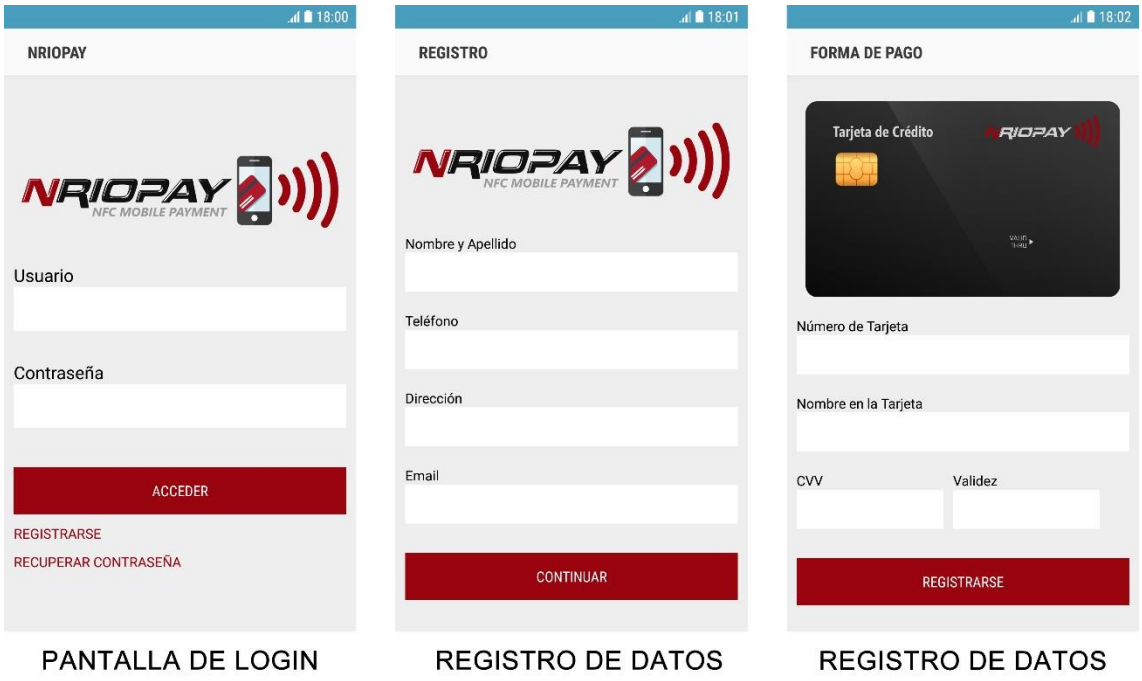


Gráfico 2-4. Pantallas de login y registro de datos de la app móvil NRioPay
Elaborado por: Castro Cristhian, 2017

Cuando el dispositivo móvil con el prototipo NRioPay activo se acerca al POS, se despliega la información a detalle de la compra en la pantalla. El usuario puede rechazar o aceptar el pago desde la misma pantalla.

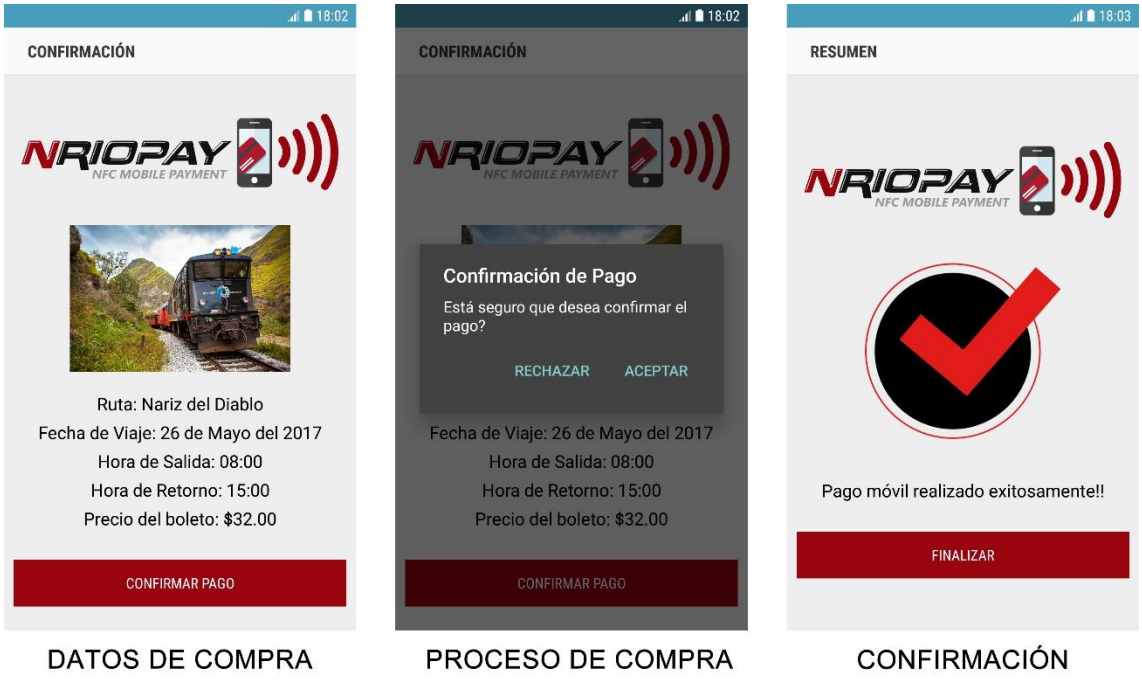


Gráfico 3-4. Pantallas de compra y confirmación de pago de la app móvil NRioPay
Elaborado por: Castro Cristhian, 2017

En el sistema de back-end del prototipo NRioPay, permite al usuario (comerciante), acceder a la configuración de productos y al historial de compras realizadas mediante la aplicación móvil.

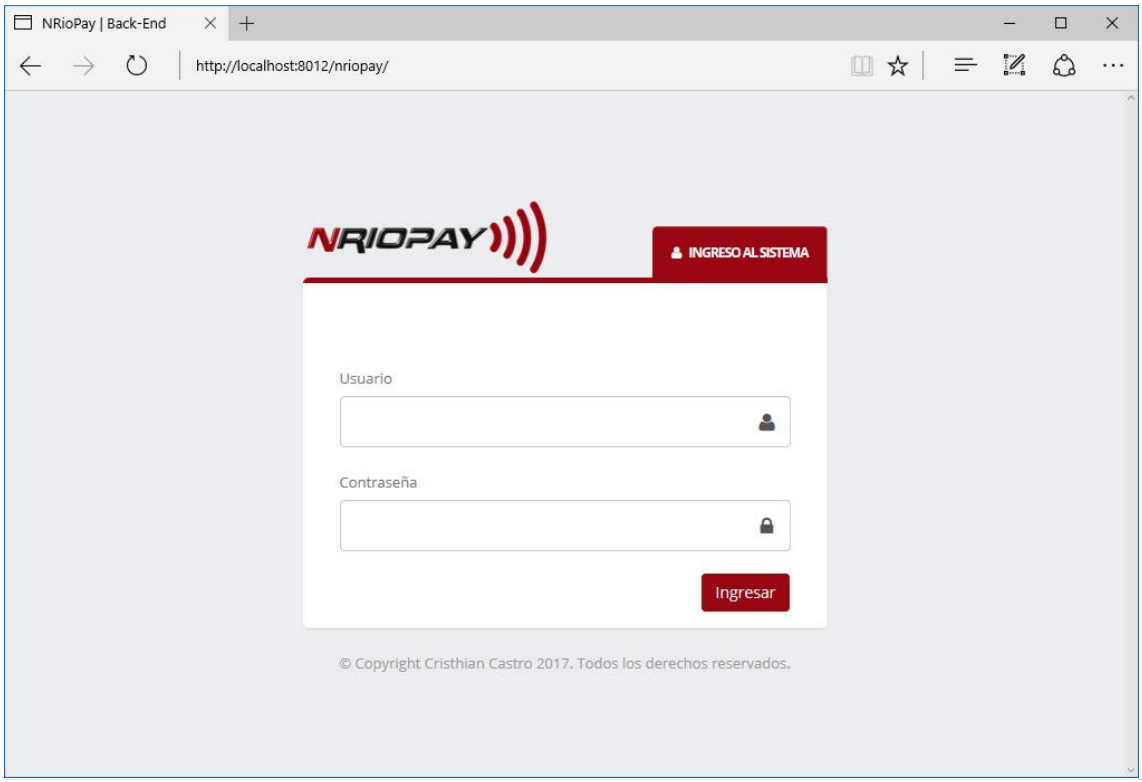


Gráfico 4-4. Pantalla de login del sistema de back-end de NRioPay
Elaborado por: Castro Cristhian, 2017

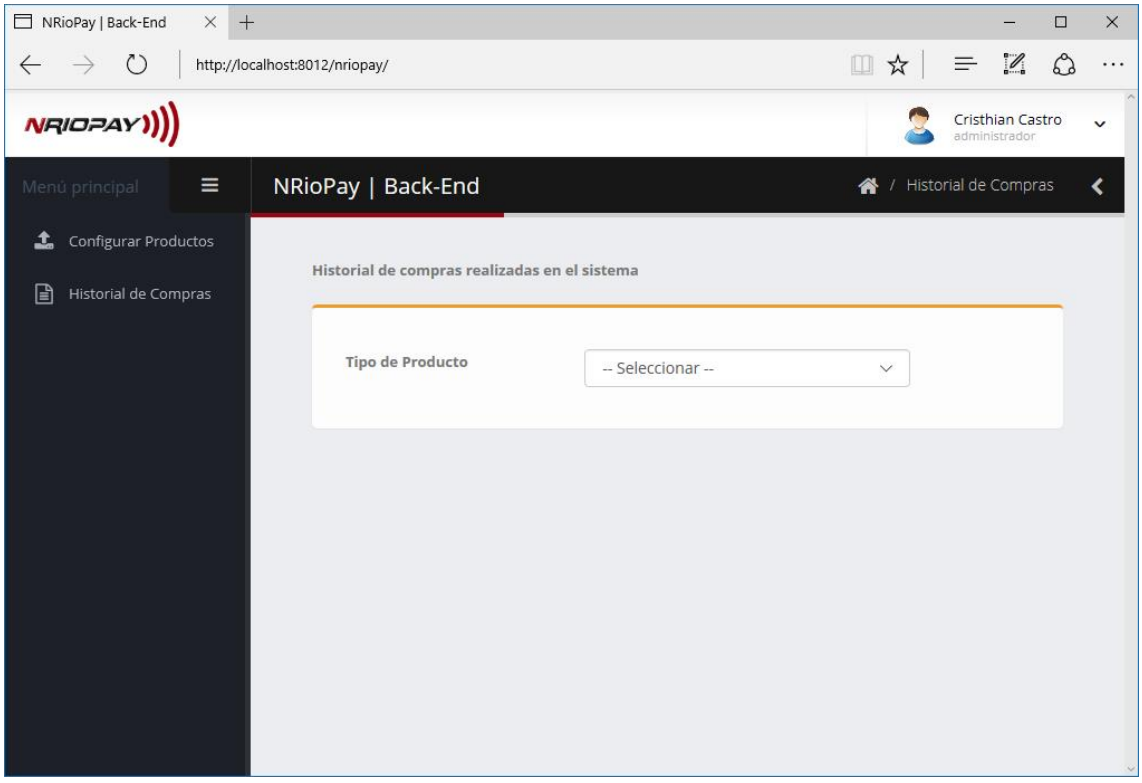


Gráfico 5-4. Pantalla de historial de compras del sistema de back-end de NRioPay
Elaborado por: Castro Cristhian, 2017

A continuación de detalla el flujo de procesos de una transacción de pago móvil con NRioPay:

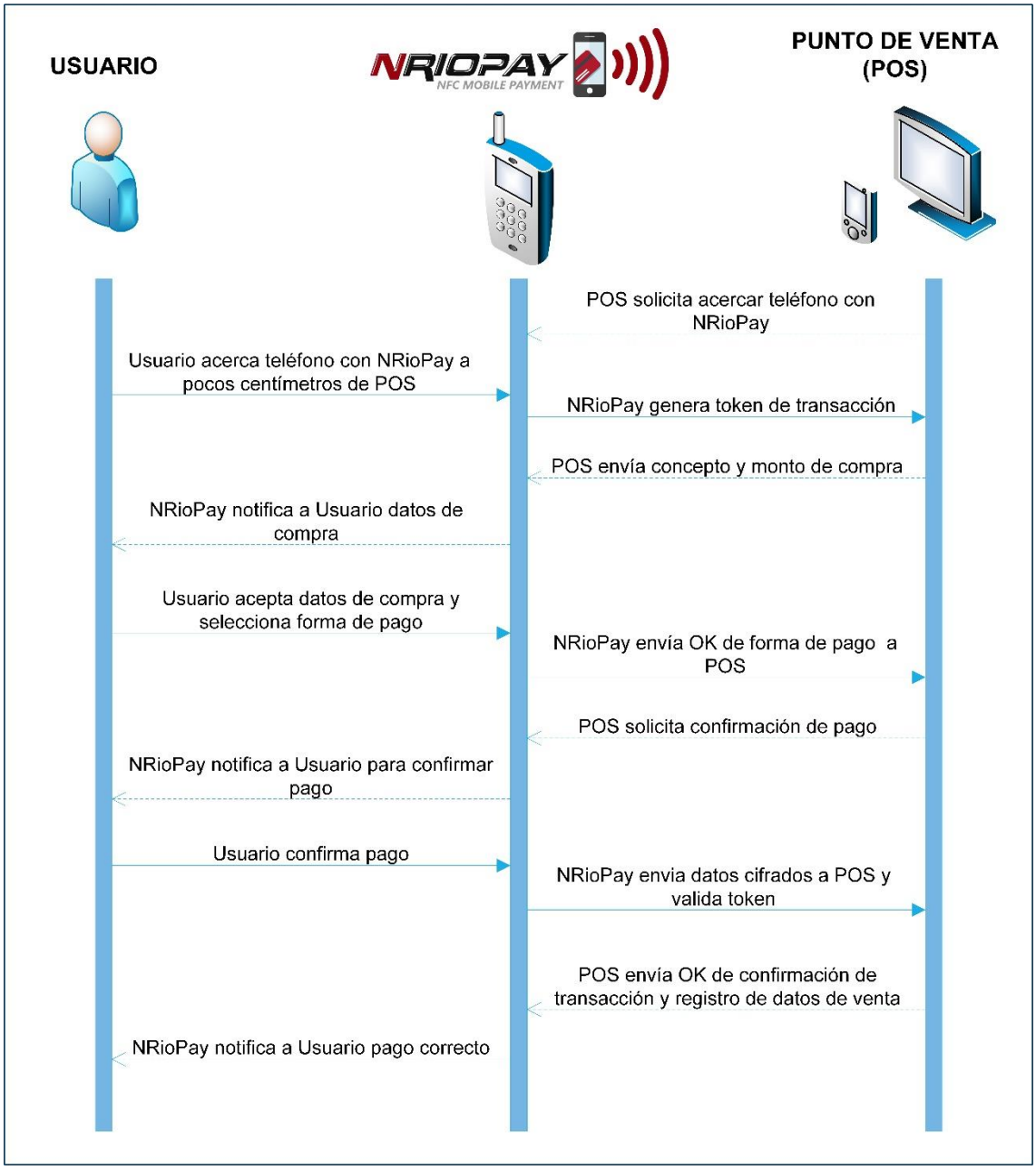


Gráfico 6-4. Flujo de procesos de transacción de pago móvil con NRioPay
Elaborado por: Castro Cristhian, 2017

4.2 Procesamiento de la Información

Para el procesamiento y manejo de la información en las tablas, se utilizará la siguiente abreviatura:

- **Indicador:** Indicadores planteados en la Operacionalización de las Variables.
- **Escenario:** Escenario sin/con modelo de seguridad aplicado.
- **Información expuesta:** Tipo de vulnerabilidad.

- **AppVulnerable:** Aplicación vulnerable sin el modelo de seguridad.
- **AppSegura:** Aplicación con modelo de seguridad implementado.
- **Número:** Número de vulnerabilidades encontradas.
- **Nivel de Integridad:** Nivel de integridad de los datos obtenidos tras el ataque, en base a la tabla 2-4.

La tabla 1-4 permitirá la recolección de datos de los resultados obtenidos en los escenarios de prueba, la cual posee la siguiente estructura:

Tabla 1-4. Tabla para recolección de datos

Indicador:					
Escenario	Información expuesta	AppVulnerable		AppSegura	
		Número	Nivel	Número	Nivel
----------	----------	X	X	X	X

Elaborado por: Castro Cristhian, 2017

Para establecer los tipos de vulnerabilidades aplicables al análisis estadístico, el prototipo de pago móvil basado en NFC denominado NRioPay, desarrollado durante el presente proceso de investigación, contiene la siguiente información que puede o no ser expuesta durante el ataque en los escenarios de prueba:

Tabla 2-4. Información del prototipo NRioPay

Información	Tipo de Información	Cantidad
Datos básicos de usuario	Nombre, teléfono, dirección, email	4
Datos básicos del pago	Valor a pagar, forma de pago, moneda	3
Datos sensibles del usuario	Contraseña, pin	2
Datos sensibles del pago	Número tarjeta de crédito, fecha vencimiento, código cvv	3
Datos sensibles de la aplicación	Datos del algoritmo de cifrado, clave del certificado .p12	2

Elaborado por: Castro Cristhian, 2017

Para establecer el nivel de exposición de la información en los escenarios de prueba, se ha elaborado la tabla 3-4 para ponderar cada uno de los niveles.

Tabla 3-4. Nivel de integridad de los datos

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

Elaborado por: Castro Cristhian, 2017

Donde:

- **Nivel 1:** Los datos son expuestos en su totalidad y son vulnerables.
- **Nivel 2:** Los datos sensibles son expuestos tras el ataque.
- **Nivel 3:** Únicamente datos no relevantes son expuestos tras el ataque.
- **Nivel 4:** Integridad garantizada.

4.3 Escenario de prueba 1

El escenario de prueba 1 basado en el indicador "*Captura de información (data sniffing)"* se utilizará el prototipo de pago móvil basado en NFC denominado NRioPay, el mismo que fue desarrollado durante el proceso de investigación.

4.3.1 Escenario de prueba 1 vulnerable

A continuación, se muestran los resultados obtenidos en el escenario vulnerable.

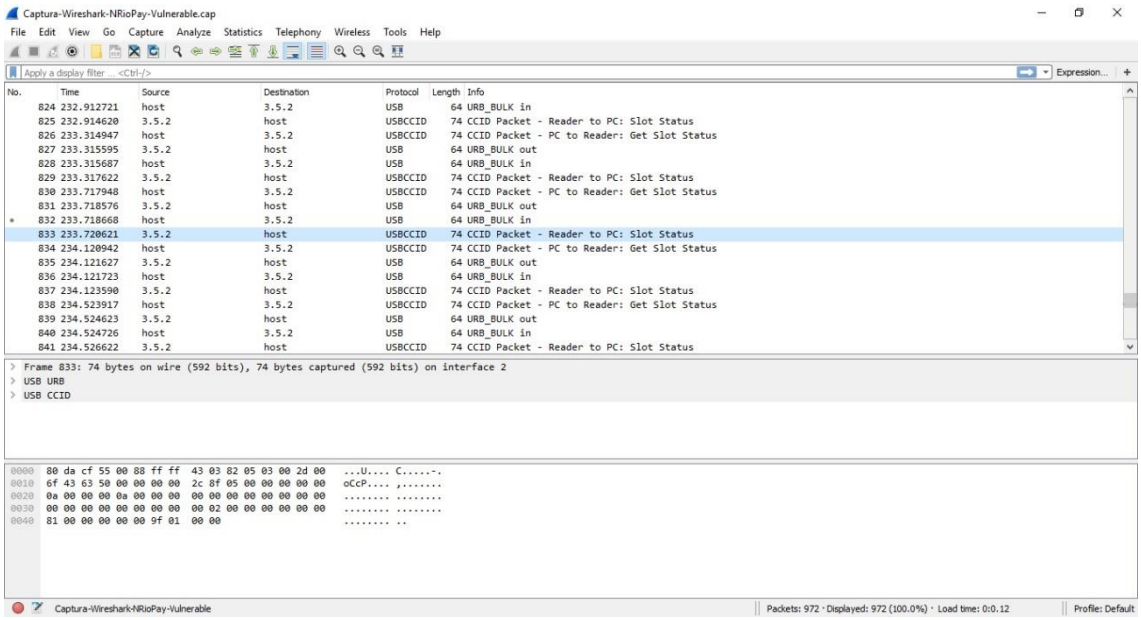


Gráfico 7-4. Captura Wireshark aplicación vulnerable

Elaborado por: Castro Cristhian, 2017

Tabla 4-4. Datos escenario 1 aplicación vulnerable

Escenario	Información expuesta	AppVulnerable	
		Número	Nivel
Escenario 1 Vulnerable	Datos básicos de usuario	4	3
	Datos básicos del pago	3	3
	Datos sensibles del usuario	0	4
	Datos sensibles del pago	1	2
	Datos sensibles de la aplicación	0	4

Elaborado por: Castro Cristhian, 2017

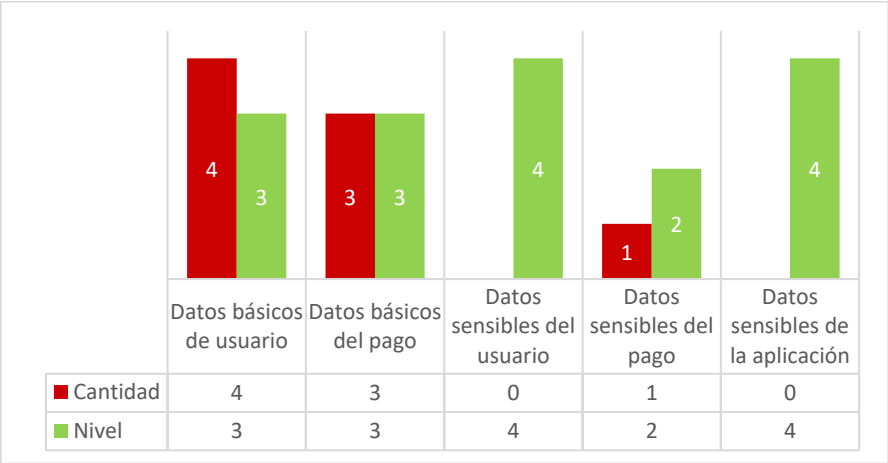


Gráfico 8-4. Datos escenario1 aplicación vulnerable

Elaborado por: Castro Cristhian, 2017

4.3.2 Escenario de prueba 1 seguro

A continuación, se muestran los resultados obtenidos en el escenario seguro.

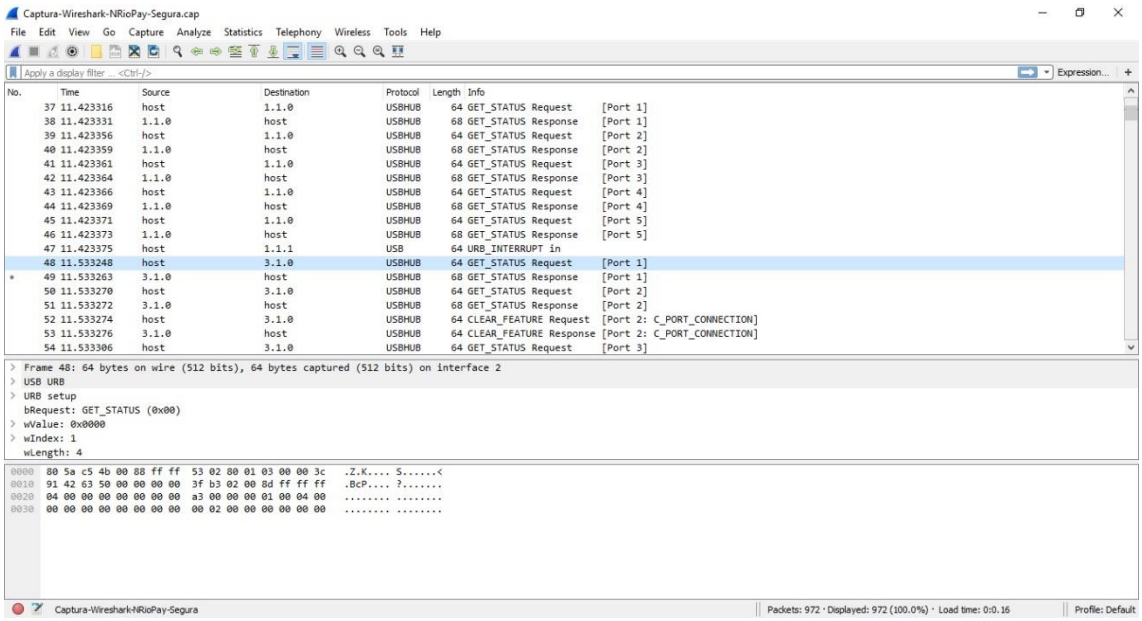


Gráfico 9-4. Captura Wireshark aplicación segura

Elaborado por: Castro Cristhian, 2017

Tabla 5-4. Datos escenario 1 aplicación segura

Escenario	Información expuesta	AppSegura	
		Número	Nivel
Escenario 1 Seguro	Datos básicos de usuario	1	3
	Datos básicos del pago	0	4
	Datos sensibles del usuario	0	4
	Datos sensibles del pago	0	4
	Datos sensibles de la aplicación	0	4

Elaborado por: Castro Cristhian, 2017

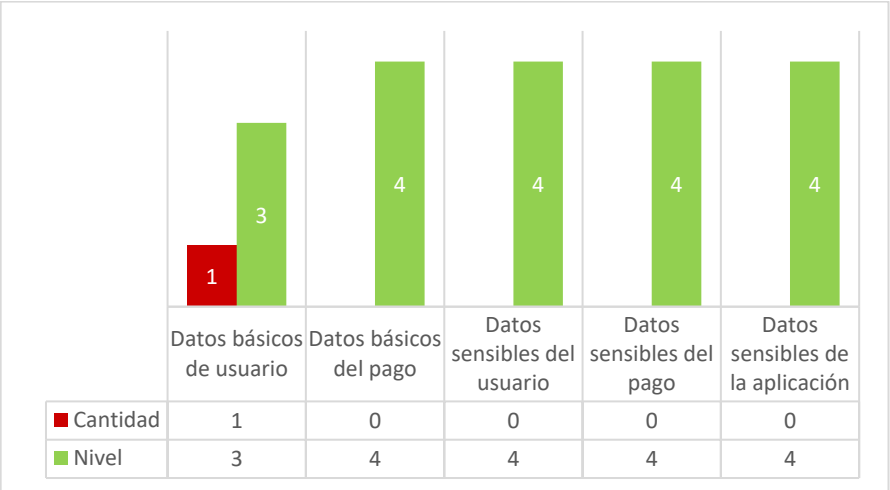


Gráfico 10-4. Datos escenario 1 aplicación segura

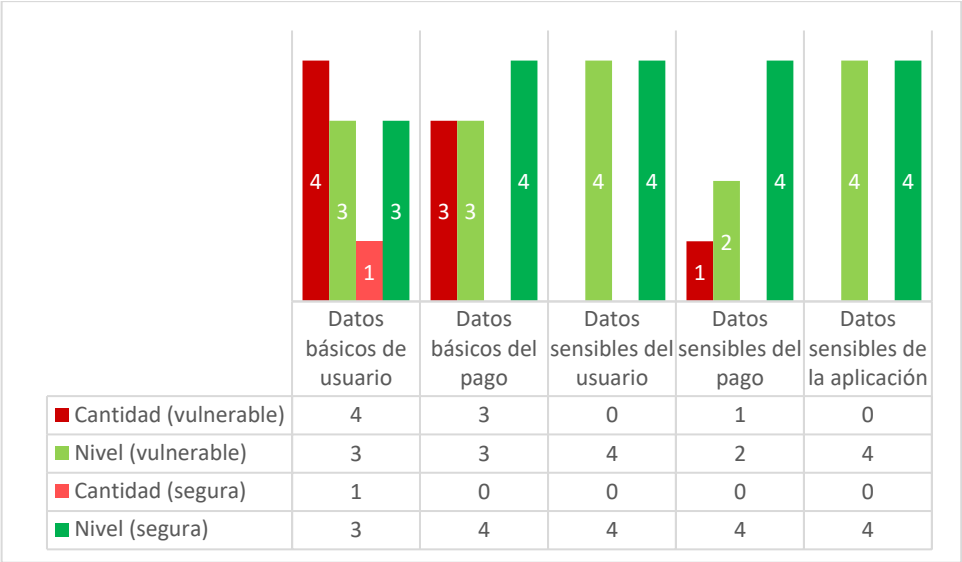
Elaborado por: Castro Cristhian, 2017

De acuerdo a los resultados obtenidos en el Escenario 1 con la aplicación del modelo de seguridad NRioSec, es notoria la disminución de la información expuesta con respecto al mismo escenario sin la aplicación del modelo. A continuación, se muestra un consolidado de las pruebas realizadas.

Tabla 6-4. Datos consolidados escenario 1

Escenario	Información expuesta	AppVulnerable		AppSegura	
		Número	Nivel	Número	Nivel
Escenario 1	Datos básicos de usuario	4	3	1	3
	Datos básicos del pago	3	3	0	4
	Datos sensibles del usuario	0	4	0	4
	Datos sensibles del pago	1	2	0	4
	Datos sensibles de la aplicación	0	4	0	4

Elaborado por: Castro Cristhian, 2017



	Datos básicos de usuario	Datos básicos del pago	Datos sensibles del usuario	Datos sensibles del pago	Datos sensibles de la aplicación
Cantidad (vulnerable)	4	3	0	1	0
Nivel (vulnerable)	3	3	4	2	4
Cantidad (segura)	1	0	0	0	0
Nivel (segura)	3	4	4	4	4

Gráfico 11-4. Datos consolidados escenario 1
Elaborado por: Castro Cristhian, 2017

4.4 Escenario de prueba 2

El escenario de prueba 2 basado en el indicador "*Alteración de información (data modification)"* utilizará el prototipo de pago móvil basado en NFC denominado NRioPay, el mismo que fue desarrollado durante el proceso de investigación.

4.4.1 Escenario de prueba 2 vulnerable

A continuación, se muestran los resultados obtenidos en el escenario vulnerable.

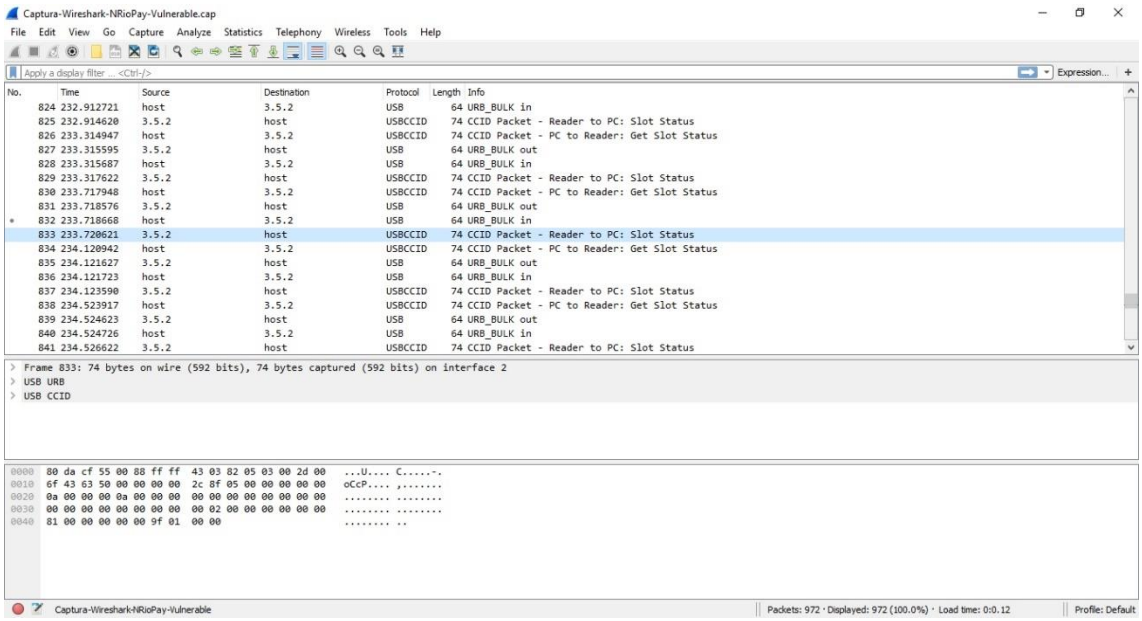


Gráfico 12-4. Captura NRioPay aplicación vulnerable
Elaborado por: Castro Cristhian, 2017

Tabla 7-4. Datos escenario 2 aplicación vulnerable

Escenario	Información expuesta	AppVulnerable	
		Número	Nivel
Escenario 2 Vulnerable	Datos básicos de usuario	4	3
	Datos básicos del pago	3	3
	Datos sensibles del usuario	2	2
	Datos sensibles del pago	3	2
	Datos sensibles de la aplicación	2	1

Elaborado por: Castro Cristhian, 2017

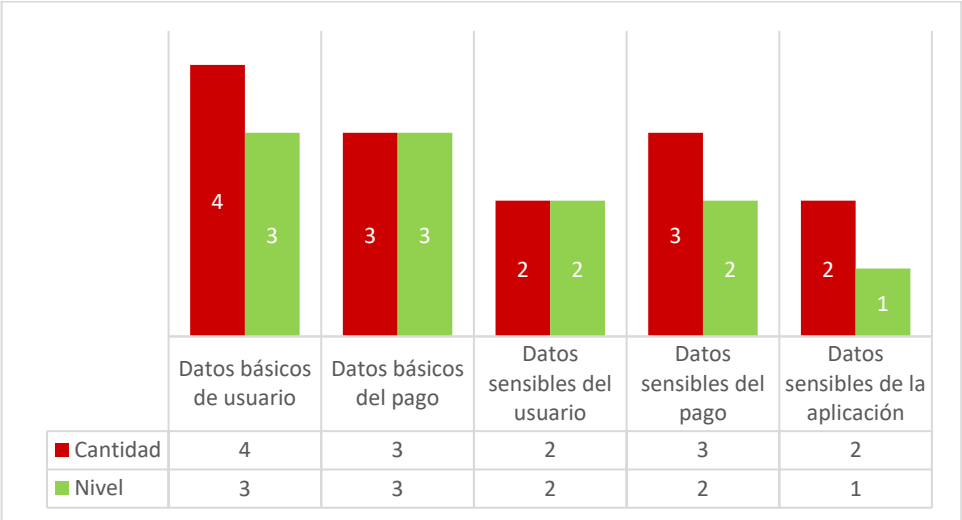


Gráfico 13-4. Datos escenario 2 aplicación vulnerable

Elaborado por: Castro Cristhian, 2017

4.4.2 Escenario de prueba 2 seguro

A continuación, se muestran los resultados obtenidos en el escenario seguro.

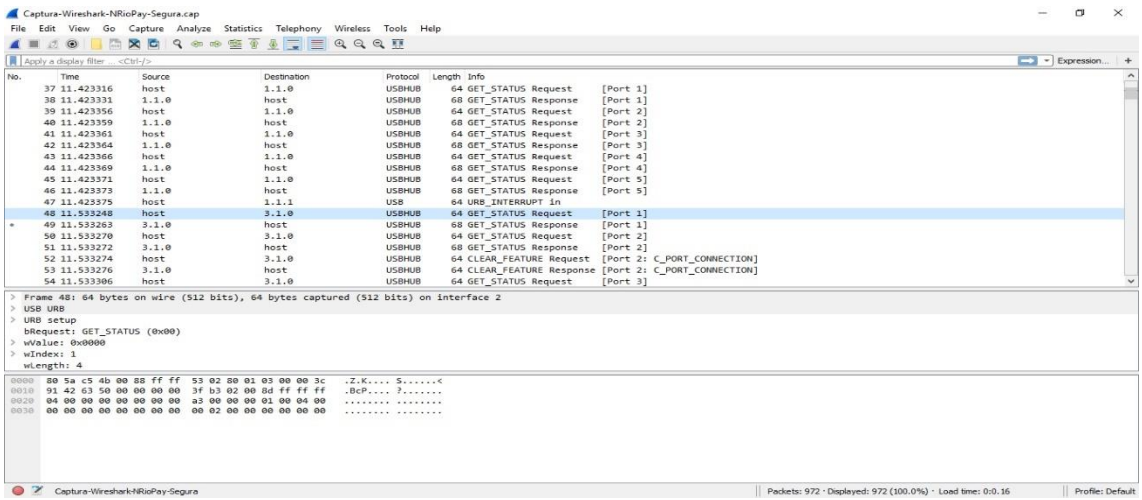


Gráfico 14-4. Captura NRioPay aplicación segura

Elaborado por: Castro Cristhian, 2017

Tabla 8-4. Datos escenario 2 aplicación segura

Escenario	Información expuesta	AppSegura	
		Número	Nivel
Escenario 2 Seguro	Datos básicos de usuario	0	4
	Datos básicos del pago	1	3
	Datos sensibles del usuario	0	4
	Datos sensibles del pago	0	4
	Datos sensibles de la aplicación	0	4

Elaborado por: Castro Cristhian, 2017

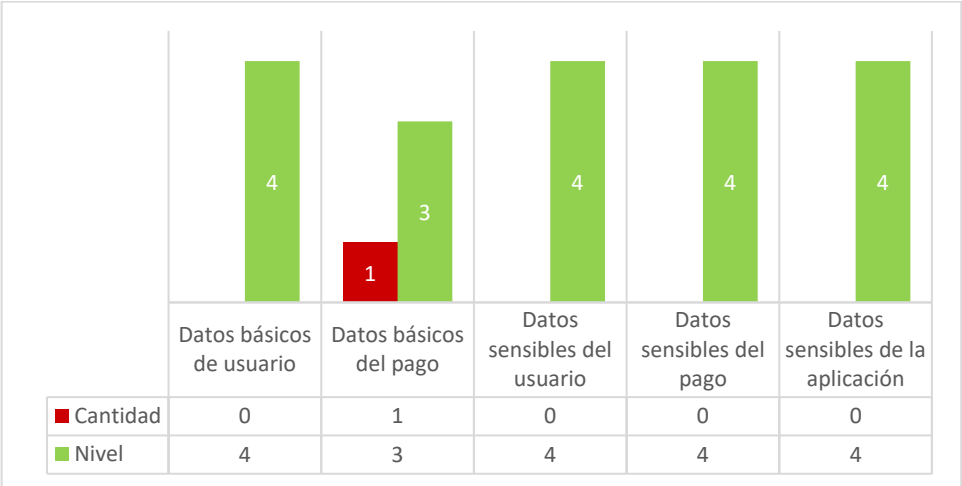


Gráfico 15-4. Datos escenario 2 aplicación segura

Elaborado por: Castro Cristhian, 2017

De acuerdo a los resultados obtenidos en el Escenario 2 con la aplicación del Modelo de Seguridad NRioSec, es notoria la disminución de la información expuesta con respecto al mismo escenario sin la aplicación del modelo. A continuación, se muestra un consolidado de las pruebas realizadas.

Tabla 9-4. Datos consolidados escenario 2

Escenario	Información expuesta	AppVulnerable		AppSegura	
		Número	Nivel	Número	Nivel
Escenario 2	Datos básicos de usuario	4	3	0	4
	Datos básicos del pago	3	3	1	3
	Datos sensibles del usuario	2	2	0	4
	Datos sensibles del pago	3	2	0	4
	Datos sensibles de la aplicación	2	1	0	4

Elaborado por: Castro Cristhian, 2017

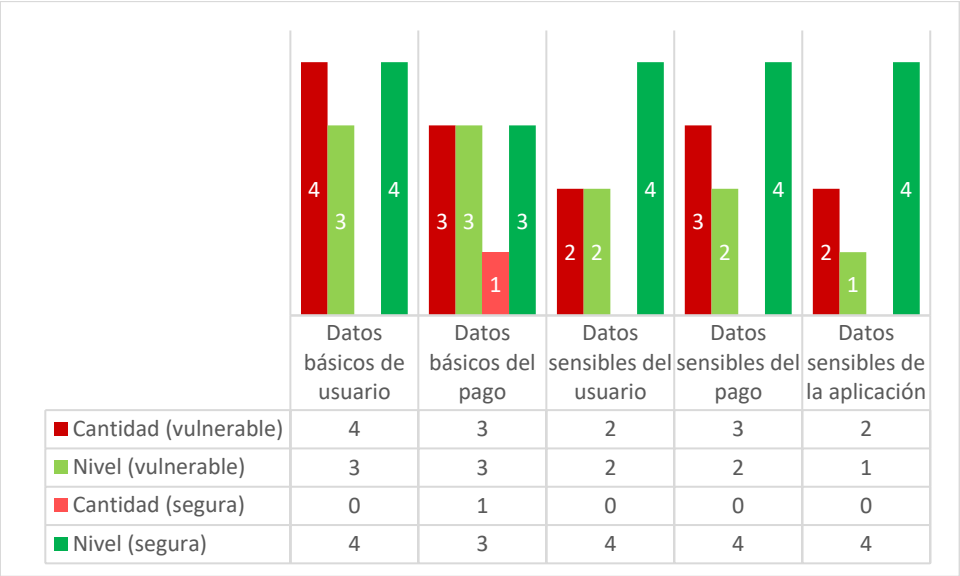


Gráfico 16-4. Datos consolidados escenario 2
Elaborado por: Castro Cristhian, 2017

4.5 Prueba de hipótesis

La hipótesis definida en el presente trabajo de investigación es *"El Modelo de Seguridad NRioSec incrementará el nivel de integridad de los pagos móviles basados en NFC".*

La estadística descriptiva será el punto de partida de la investigación para la demostración de la hipótesis, en la que se cuantifican los resultados de las pruebas realizadas en los escenarios planteados para cada uno de los indicadores definidos, y posteriormente realizar el proceso de la estadística inferencial.

Tras la obtención de los resultados en los escenarios de prueba, se realiza el cálculo del promedio de los valores resultantes de los indicadores, tal como como se muestra en la tabla 10-4.

Tabla 10-4. Valores promedios de indicadores

Promedio	Escenario 1		Escenario 2	
	Vulnerable	Seguro	Vulnerable	Seguro
Cantidad de información expuesta	1,6	0,2	2,8	2,2
Nivel de integridad	3,2	3,8	0,2	3,8

Elaborado por: Castro Cristhian, 2017

En los gráficos se aprecian los resultados realizados tras las comparaciones de cada indicador.

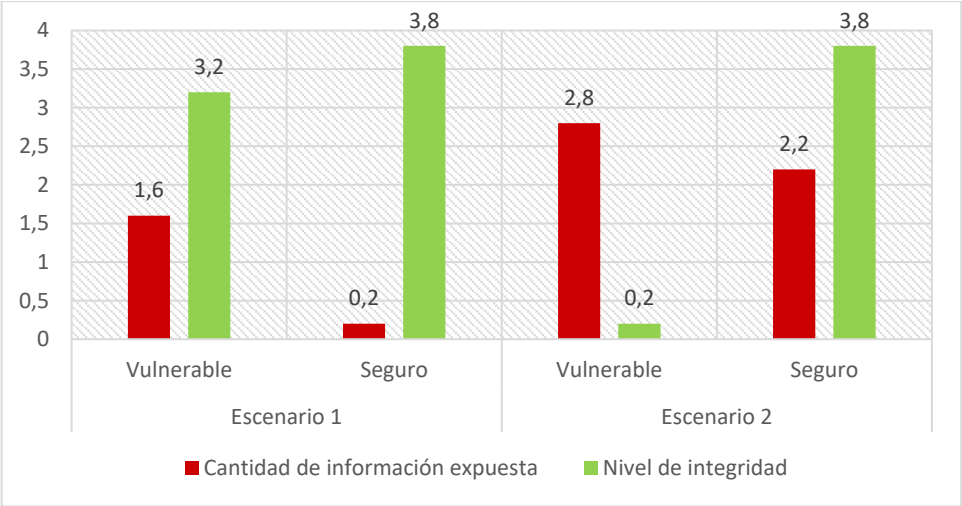


Gráfico 17-4. Valores promedios de indicadores
Elaborado por: Castro Cristhian, 2017

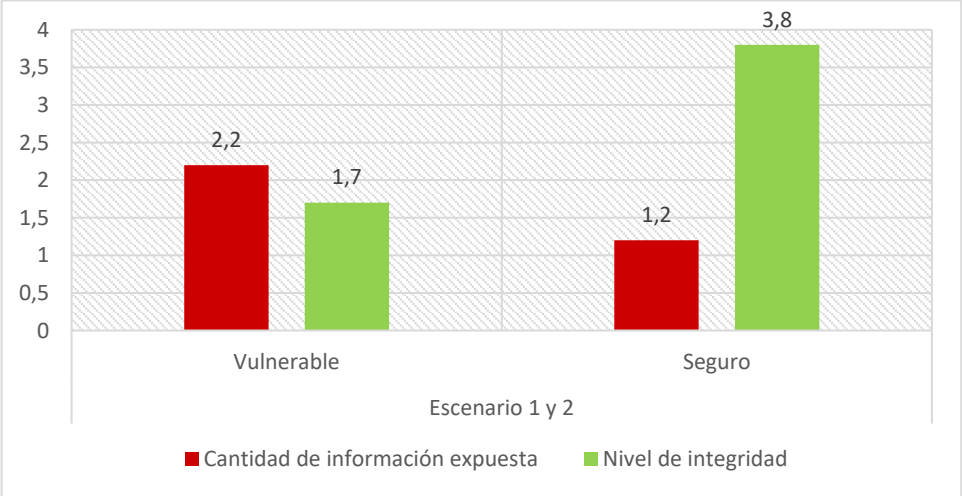


Gráfico 18-4. Promedios totales de indicadores de los escenarios
Elaborado por: Castro Cristhian, 2017

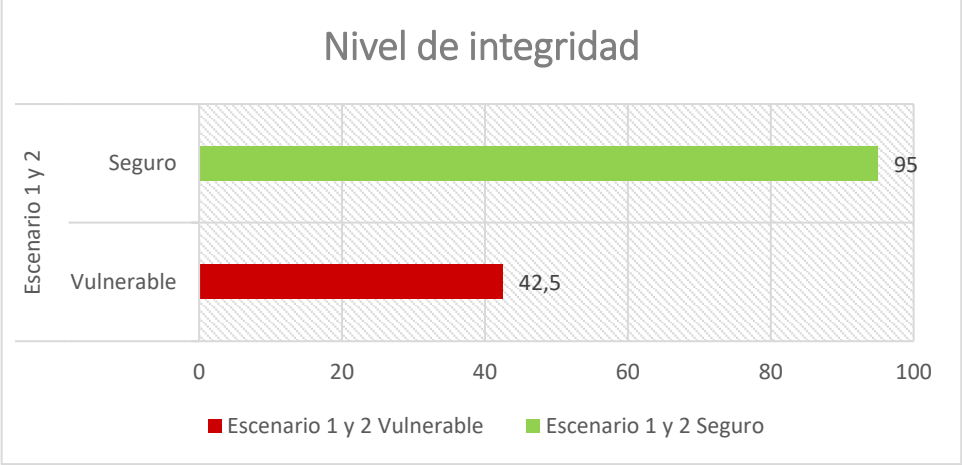


Gráfico 19-4. Porcentaje total de integridad de los escenarios
Elaborado por: Castro Cristhian, 2017

De esta manera se concluye que al utilizar el Modelo de Seguridad NRioSec mejora en un 52,5% la integridad en el prototipo de pago móvil basado en NFC. En el proceso de la estadística inferencial, se asigna los siguientes valores a la variable independiente X, para la comprobación de la hipótesis de investigación:

X = Modelo de Seguridad
$\mathbf{X_1}$ = Garantiza la integridad
$\mathbf{X_2}$ = No garantiza la integridad

En estos valores se comprobará su impacto en relación con la variable dependiente que hace referencia a la integridad de los pagos móviles y que fue implementada en el prototipo NRioPay en los escenarios 1 y 2.

Para la comprobación estadística de la hipótesis se utilizó Chi-cuadrado (X^2), que es una prueba de hipótesis no paramétrica que compara la distribución observada de los datos con una distribución esperada.

Adicionalmente, se establece la hipótesis de investigación *Hi* y la hipótesis nula *Ho* a ser consideradas.

- **Hi:** El modelo de seguridad incrementará el nivel de integridad de los pagos móviles basados en NFC.
- **Ho:** El modelo de seguridad no incrementará el nivel de integridad de los pagos móviles basados en NFC.

La tabla de contingencia 11-4 contienen las frecuencias observadas de cada indicador, las mismas que serán utilizadas para el cálculo de chi-cuadrado.

Tabla 11-4. Tabla de contingencia para chi-cuadrado

V. Independiente / V. Dependiente	Prototipo	Escenario 1 Vul.	Escenario 1 Seg.	Escenario 2 Vul.	Escenario 2 Seg.	Total
Mejora la integridad (No vulnerable)	NRioPay	0	12	0	14	26
No mejora la integridad (Vulnerable)	NRioPay	7	0	14	0	21
TOTAL		**7**	**12**	**14**	**14**	**47**

Elaborado por: Castro Cristhian, 2017

La tabla de contingencia de frecuencias esperadas son aquellos valores que se espera encontrar bajo el supuesto de independencia de las variables, el mismo que es usado por Chi-cuadrado para evaluar si es verdadero o falso, analizando si las frecuencias observadas difieren de lo esperado, en caso de no existir correlación.

La frecuencia esperada, se calcula mediante la siguiente fórmula:

- $Frec = \frac{(filas_{total}) * (columnas_{total})}{T}$

Donde:

- *T*: Total de frecuencias observadas

Tras su aplicación en los valores de la tabla 11-4 se obtiene la tabla 12-4 de contingencia de valores esperados.

Tabla 12-4. Tabla de frecuencias esperadas

V. Independiente / V. Dependiente	Prototipo	Escenario 1 Vul.	Escenario 1 Seg.	Escenario 2 Vul.	Escenario 2 Seg.	Total
Mejora la integridad (No vulnerable)	NRioPay	3,87	6,63	7,74	7,74	26
No mejora la integridad (Vulnerable)	NRioPay	3,12	5,36	6,26	6,26	21
TOTAL		**7**	**12**	**14**	**14**	**47**

Elaborado por: Castro Cristhian, 2017

A continuación, se aplica chi-cuadrado a las frecuencias esperadas calculadas, mediante la fórmula:

- $X^2 = \sum \frac{(FO-FE)2}{FE}$

Donde:

- *FO:* Frecuencia observada por celda
- *FE:* Frecuencia esperada por celda

Tabla 13-4. Tabla de cálculo de chi-cuadrado

	Indicador	*FO*	*FE*	*FO - FE*	$(FO - FE)^2$	$\frac{(FO - FE)^2}{FE}$
Escenario 1 Seguro	Mejora	12	6,63	5,37	28,84	4,35
Escenario 2 Seguro	Mejora	14	7,74	6,26	39,19	5,06
Escenario 1 Vulnerable	No mejora	7	3,12	3,88	15,05	4,83
Escenario 1 Seguro	No mejora	14	7,74	6,26	39,19	5,06
X^2						**19.30**

Elaborado por: Castro Cristhian, 2017

Análisis

El valor de chi-cuadrado puede ser o no ser significativo, y para ello se deben establecer los grados de libertad mediante la siguiente fórmula.

- $GradLiber = (fil - 1)(col - 1)$

Donde:

- *fil:* Total de filas de la tabla de continencia
- *col:* Total de columnas de la tabla de contingencia

Por lo tanto:

- $GradLiber = (2-1)(4-1) = 6$

En base a la tabla de distribución de chi-cuadrado, donde se selecciona el nivel de significancia de

- α=5% = 0.05

para disponer de un nivel de confianza del 95%, se obtiene que para 6 grados de libertad el punto crítico de chi-cuadrado es

- $X^2_{Crítico} = 12.5916$

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

Gráfico 20-4. Distribución Chi-cuadrado
Fuente: http://upla.edu.pe/portal/wp-content/uploads/2017/01/Tabla-del-chi-cuadrado.pdf

El valor chi-cuadrado calculado es de 19.30, que a su vez es superior al valor de la tabla de distribución de 12.5916.

- $X^2_{\text{Crítico}}$ (12.5916) < $X^2_{Calculado}$ (19.30)

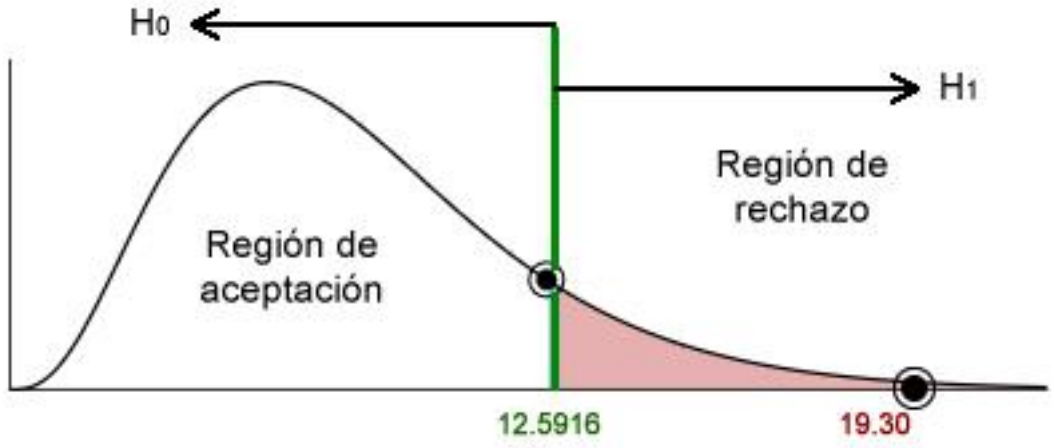


Gráfico 21-4. Curva de Chi-cuadrado
Elaborado por: Castro Cristhian, 2017

Por tanto, se valida que el valor calculado de chi-cuadrado se localiza en la región de rechazo de la hipótesis nula H_0 y se acepta la hipótesis de investigación H_i que es significativa, con un nivel de significancia de α=5% = 0.05 para obtener un nivel de confianza del 95%.

CONCLUSIONES

Las pruebas realizadas en esta investigación ponen en evidencia que la tecnología NFC puede resultar vulnerable a la alteración de información (data modification) y al acceso no permitido de información (data sniffing) si no se implementan mecanismos de seguridad adecuados. Si el rango de interceptación de un atacante se encuentra dentro de los 10cm, la vulneración puede resultar más efectiva.

El mercado de los pagos móviles se está convirtiendo en un elemento primordial para satisfacer las necesidades cotidianas de los usuarios que buscan alternativas fáciles e innovadoras de pago mediante dispositivos móviles. Se establecen perspectivas prometedoras tanto para los consumidores como para los proveedores, teniendo en cuenta que el uso de servicios móviles basados en la tecnología NFC se está expandiendo en todo el mundo. Esto ha despertado puntos clave de especial interés para los profesionales a cargo de la seguridad y el aseguramiento, sobre el futuro de los pagos mediante dispositivos móviles.

El modelo de seguridad NRioSec establece tres niveles de protección con un alto grado de compatibilidad y fácil integración en el desarrollo de aplicaciones de pago móviles. Sus componentes permiten controlar la autenticación con certificados digitales, la unicidad de transacciones mediante la tokenización y el cifrado de datos mediante algoritmos robustos, y que sumados a las normas de seguridad de aceptación de pagos móviles del PCI SSC, determinan la eficacia de su aplicación para mitigar las vulnerabilidades analizadas.

Con la implementación del prototipo de pago móvil NRioPay, se logró comprobar que el modelo de seguridad NRioSec incrementa el nivel de integridad de los pagos móviles basados en NFC porque mediante cifrado protege la información sensible que se transmite durante una transacción; al ser transmitida la información únicamente entre el emisor y el receptor se protege la información confidencial de los atacantes o de las entidades participantes, pues éstas no tienen necesidad de acceder a dicha información; el modelo proporciona cifrado y autenticación de origen para que el receptor los pueda validar y, se asegura al receptor que los detalles del pago son correctos y corresponden a los datos proporcionados por el emisor mediante una pantalla donde se confirme que los datos son correctos.

RECOMENDACIONES

En cualquier parte donde se realice una transferencia de datos, siempre existirá el riesgo de que estos sean interceptados y manipulados. De hecho, a medida que la adopción de la tecnología NFC siga en aumento, los atacantes se enfocarán en obtener los datos compartidos entre los dispositivos que intervienen en el proceso de pagos móviles.

Los delincuentes informáticos pueden desarrollar aplicaciones similares infectadas con malware para comprometer los dispositivos móviles de los usuarios y tener acceso a su información sensible, por lo que es necesario tomar las medidas de seguridad al tratarse de una forma de pago adicional a las tradicionales.

La adopción de la tecnología NFC en Ecuador podría revolucionar el mercado en los próximos 2 o 3 años, brindando un ecosistema de pago móvil moderno, que ofrezca comodidad y seguridad a los usuarios al efectuar transacciones financieras o de servicios, en establecimientos que cuenten con sistemas basados en esta tecnología. Sin embargo, está claro que la seguridad en NFC puede ser susceptible de vulnerabilidades, por lo que la aplicación del modelo de seguridad NRioSec propuesto en esta investigación, ayudará en la mitigación y control oportuno.

El prototipo NRioPay pone en evidencia la aplicabilidad de esta forma de pago móvil en una transacción habitual que se realiza en el Ecuador, como es la compra de boletos de tren. Pero podría ser utilizado en un sinnúmero de escenarios donde exista un pago de un usuario por un servicio que recibió. Esta afirmación invita a que los resultados obtenidos en esta investigación puedan ser tomados como referencia y punto de partida para futuros estudios de pagos móviles donde la tecnología NFC sea la principal protagonista.

BIBLIOGRAFIA

1) **AbdAllah, M. M.** (2011). Strengths and Weaknesses of Near Field Communication (NFC) Technology. *Global Journal of Computer Science and Technology*, *11*(2).

2) **Abu-Saymeh et al.** (2013). An Application Security Framework for Near Field Communication. En *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 396–403). https://doi.org/10.1109/TrustCom.2013.50

3) **Apple.** (2014). Apple Pay. Recuperado el 5 de enero de 2017, a partir de https://www.apple.com/es/pr/library/2014/10/16Apple-Pay-Set-to-Transform-Mobile-Payments-Starting-October-20.html

4) **Argentina. Samsung.** (2015). Samsung Pay, un Innovador Servicio de Pagos Móviles. Recuperado el 5 de enero de 2017, a partir de http://fb.ar.samsung.com/news/local/samsung-samsung-announces-pay-an-innovative-mobile-payment-service/

5) **Attard, A., & Leung, A.** (2012). *Novel Card-present Payment Scheme Using Nfc Technology*. Lap Lambert Academic Publ. Recuperado a partir de https://pdfs.semanticscholar.org/c27c/c6f5fe80e657cb3660708269c793252ad37e.pdf

6) **BBVA.** (2015). Pagos móviles con NFC - Infografía. Recuperado el 5 de abril de 2017, a partir de http://www.centrodeinnovacionbbva.com/infografia/infografia-pagos-moviles-sin-contacto-nfc

7) **Benavides, B.** (2016). *Diseño e implementación de un módelo de entrenamiento para deres inalámbricas utilizando tecnología Wimax.* Universidad Estatal Península de Santa Elena. UPSE, La Libertad. Recuperado a partir de http://bibliotecas.upse.edu.ec/opac_css/index.php?lvl=notice_display&id=9839

8) **Cha, B., & Kim, J.** (2013). Design of NFC Based Micro-payment to Support MD Authentication and Privacy for Trade Safety in NFC Applications. En *2013 Seventh International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)* (pp. 710–713). https://doi.org/10.1109/CISIS.2013.127

9) **Cha, S.-C. et al.** (2014). Ensuring the integrity and non-repudiation of remitting e-invoices in conventional channels with commercially available NFC devices. En *2014 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)* (pp. 1–6). https://doi.org/10.1109/SNPD.2014.6888705

10) **Chen et al.** (2014). NFC Attacks Analysis and Survey. En *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)* (pp. 458–462). https://doi.org/10.1109/IMIS.2014.66

11) **Coskun et al.** (2012). A Survey on Near Field Communication (NFC) Technology. Wireless Personal Communications, 71(3), 2259–2294. https://doi.org/10.1007/s11277-012-0935-5

12) **Dell EMC.** (2014). PKCS #12: Personal Information Exchange Syntax Standard. Recuperado el 17 de marzo de 2017, a partir de https://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs12-personal-information-exchange-syntax-standard.htm

13) **Ecuador. Diners Club.** (2015). PayClub. Recuperado el 22 de enero de 2017, a partir de https://www.payclub.com.ec/

14) **Ecuador. El Telégrafo.** (2016). El dinero electrónico. Recuperado el 9 de enero de 2017, a partir de http://www.eltelegrafo.com.ec/noticias/economia/8/el-dinero-electronico-se-activa-al-marcar-153

15) **Ecuador. Grupo El Comercio.** (2015). PayPhone - Historia. Recuperado el 7 de enero de 2017, a partir de http://www.revistalideres.ec/lideres/industria-financiera-app-galardon-payphone.html

16) **Ecuador. Instituto Nacional de Estadística y Censos.** (2017). Número de usuarios de smartphones. Recuperado el 10 de febrero de 2017, a partir de https://twitter.com/Ecuadorencifras/status/829688887102566402/photo/1

17) **Ecuador. Junta de Regulación Monetaria Financiera.** (2014). Resolución No. 005-2014-M. Recuperado el 7 de abril de 2017, a partir de

http://www.juntamonetariafinanciera.gob.ec/PDF/Resolucion%20No.%20005-2014-M.pdf?dl=0

18) **Ecuador. Superintendencia de control del Poder de Mercado.** (2014). Sistema de Dinero Electrónico en beneficio de la economía popular y solidaria. Recuperado el 7 de enero de 2017, a partir de http://www.scpm.gob.ec/wp-content/uploads/2014/01/2.6-Fausto-Valencia-BCE-Sistema-de-dinero-electr%C3%B3nico.pdf

19) **Exxon and Mobil.** (2014). History. Recuperado el 5 de enero de 2017, a partir de https://www.exxon.com/en/history

20) **Garfinkel et al.** (2005). RFID privacy: an overview of problems and proposed solutions. IEEE Security Privacy, 3(3), 34–43. https://doi.org/10.1109/MSP.2005.78

21) **Google.** (2011). Google Wallet: make your phone your wallet. Recuperado el 5 de enero de 2017, a partir de https://googleblog.blogspot.com/2011/05/coming-soon-make-your-phone-your-wallet.html

22) **Google.** (2015). Android Pay - Official Android Blog. Recuperado el 5 de enero de 2017, a partir de https://android.googleblog.com/2015/09/tap-pay-done.html

23) **Günther, M., & Borchert, B.** (2013). Online Banking with NFC-Enabled Bank Card and NFC-Enabled Smartphone. En L. Cavallaro & D. Gollmann (Eds.), *Information Security Theory and Practice. Security of Mobile and Cyber-Physical Systems* (pp. 66–81). Springer Berlin Heidelberg. Recuperado a partir de http://link.springer.com/chapter/10.1007/978-3-642-38530-8_5

24) **Halgaonkar et al.** (2013). NFC: A review of technology, tags, applications and security. IJRCCT, 2(10), 979–987.

25) **Hong et al.** (2014). LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. En *Y. Kim, H. Lee, & A. Perrig (Eds.), Information Security Applications* (pp. 3–27). Springer International Publishing. Recuperado a partir de http://link.springer.com/chapter/10.1007/978-3-319-05149-9_1

26) **ISO/IEC 18092.** (2013). Near Field Communication - Interface and Protocol.

27) **Kerem Ok, M. N. A.** (2011). Exploring Underlying Values of NFC Applications. *International Proceedings of Economics Development & Research*, *12*, 290.

28) **Liu et al.** (2010). A Survey of Payment Card Industry Data Security Standard. IEEE Communications Surveys Tutorials, 12(3), 287–303. https://doi.org/10.1109/SURV.2010.031810.00083

29) **Mantoro et al.** (2014). Securing the authentication and message integrity for Smart Home using smart phone. En *2014 International Conference on Multimedia Computing and Systems (ICMCS)* (pp. 985–989). https://doi.org/10.1109/ICMCS.2014.6911150

30) **MasterCard.** (2015). MasterCard lleva el pago móvil a Android a través de Android Pay. Recuperado el 9 de enero de 2017, a partir de http://newsroom.mastercard.com/latin-america/es/press-releases/mastercard-y-android-pay-ofreceran-pagos-moviles-a-usuarios-de-dispositivos-android/

31) **Media Telecom.** (2016). Evolución de pagos móviles. Recuperado el 4 de enero de 2017, a partir de http://mediatelecom.com.mx/index.php/agencia-informativa/agencia-tecnologia/item/110672-evolución-de-pagos-móviles

32) **NFC Forum.** (2016a). NFC in Action. Recuperado el 2 de abril de 2016, a partir de http://nfc-forum.org/what-is-nfc/nfc-in-action/

33) **NFC Forum.** (2016b). The Near Field Communication (NFC) Forum. Recuperado el 3 de abril de 2015, a partir de http://nfc-forum.org/

34) **Nguyen et al.** (2014). Prospective Cryptography in NFC with the Lightweight Block Encryption Algorithm LEA. En *T. K. Dang, R. Wagner, E. Neuhold, M. Takizawa, J. Küng, & N. Thoai (Eds.), Future Data and Security Engineering* (pp. 191–203). Springer International Publishing. Recuperado a partir de http://link.springer.com/chapter/10.1007/978-3-319-12778-1_15

35) **Nikitin et al.** (2007). An Overview of Near Field UHF RFID. En IEEE International Conference on RFID, 2007 (pp. 167–174). https://doi.org/10.1109/RFID.2007.346165

36) **Nokia.** (2005). Nokia announces the world's first NFC enabled mobile product for contactless payment and ticketing. Recuperado el 5 de enero de 2017, a partir de http://www.nokia.com/en_int/news/releases/2005/02/09/nokia-announces-the-worlds-first-nfc-enabled-mobile-product-for-contactless-payment-and-ticketing

37) **Ok et al.** (2011). A Role-Based Service Level NFC Ecosystem Model. Wireless Personal Communications, 68(3), 811–841. https://doi.org/10.1007/s11277-011-0484-3

38) **Ottoy, G. et al.** (2011). A Modular Test Platform for Evaluation of Security Protocols in NFC Applications. En *B. D. Decker, J. Lapon, V. Naessens, & A. Uhl (Eds.), Communications and Multimedia Security* (pp. 171–177). Springer Berlin Heidelberg. Recuperado a partir de http://link.springer.com/chapter/10.1007/978-3-642-24712-5_15

39) **Payment Card Industry Security Standards Council.** (2014). PCI Mobile Payment Acceptance Security Guidelines for Developers. Recuperado el 16 de abril de 2017, a partir de https://www.pcisecuritystandards.org/documents/Mobile_Payment_Acceptance_Security_Guidelines_for_Developers_v1-1.pdf

40) **Pedreño, A.** (2013). Bancos del futuro y pagos móviles: ¿innovaciones o cambios disruptivos? Recuperado el 3 de agosto de 2015, a partir de http://www.finanzasparamortales.es/a-fondo/bancos-del-futuro-y-pagos-moviles-innovaciones-o-cambios-disruptivos

41) **Prieto, J., Ramírez, R., Morillo, J., & Domingo, M.** (2011). Tecnología y desarrollo en dispositivos móviles. Recuperado el 3 de agosto de 2015, a partir de http://materials.cv.uoc.edu/continguts/PID_00176756/index.html

42) **Produbanco - Grupo Promerica. (2016).** Payphone. Recuperado el 22 de enero de 2017, a partir de https://livepayphone.com/

43) **Roland, M., & Langer, J.** (2010). Digital Signature Records for the NFC Data Exchange Format. En *2010 Second International Workshop on Near Field Communication (NFC)* (pp. 71–76). https://doi.org/10.1109/NFC.2010.10

44) **Samsung Electronics Co.** (2015). Samsung Pay. Recuperado el 5 de enero de 2017, a partir de http://www.samsungmobilepress.com:80/press/Samsung-Announces-Samsung-Pay,-A-Groundbreaking-Mobile-Payment-Service?2015-03-02

45) **Samsung Electronics Co.** (2015). LoopPay. Recuperado el 9 de enero de 2017, a partir de https://www.looppay.com/faqs/

46) **SecTor.** (2012). *Charlie Miller - Exploring the NFC attack surface*. Recuperado a partir de http://2012.video.sector.ca/video/51115364

47) **Square Inc.** (2012). History of Near Field Communication. Recuperado el 5 de enero de 2017, a partir de http://nearfieldcommunication.org/history-nfc.html

48) **Urien, P.** (2015). Towards token-requestor for epayment based on cloud of secure elements and HCE mobiles. En *2015 First Conference on Mobile and Secure Services (MOBISECSERV)* (pp. 1–2). https://doi.org/10.1109/MOBISECSERV.2015.7072876

49) **Yinghui, P.** (2009). The Application of PKCS#12 Digital Certificate in User Identity Authentication System. En *2009 WRI World Congress on Software Engineering* (Vol. 4, pp. 351–355). https://doi.org/10.1109/WCSE.2009.202