ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES A LOS AUTORES

Vol. 39 (Nº 19) Año 2018 • Pág. 16

Modelo de Seguridad para Garantizar la Integridad de Pagos Móviles sobre *Near Field Communication* (NFC)

Security Model to Guarantee the Integrity of Mobile Payments on Near Field Communication (NFC)

Andrés Santiago CISNEROS Barahona 1; Cristhian Fernando CASTRO Ortiz 2; María Isabel UVIDIA Fassler 3; Gonzalo Nicolay SAMANIEGO Erazo 4; Ciro Diego RADICELLI García 5; Diego Guillermo BARBA Maggi 6

Recibido: 12/01/2018 • Aprobado: 10/02/2018

Contenido

RESUMEN:
Este artículo presenta un modelo de seguridad telemática sobre NFC, que establece tres niveles de protección, con compatibilidad e 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, 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.
Palabras-Clave: Pagos Móviles, Pagos sin Contacto, Modelo de Seguridad, Integridad.

ABSTRACT:
This article presents the security telematic model that establishes three levels of protection with a high degree of compatibility and easy integration in the development of mobile payment applications. Its components allow the control of authentication with digital certificates, uniqueness of transactions through tokenization and data encryption using robust algorithms, which, together with PCI SSC mobile payment acceptance security standards, determine the effectiveness of its application for mitigate the analyzed vulnerabilities.
Keywords: Mobile Payments, Contactless Payments, Security Model, Integrity.

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 (smartpones) que procesan información y datos en tiempo real, facilitando las actividades de las personas (Harnisch & Uitz, 2013).

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, y posteriormente se activaron varias funcionalidades adicionales tales como los SMS (Short Messaging Service), MMS (Multimedia Messaging Service) e incluso el acceso a Internet (Coskun, Ozdenizci, & Ok, 2012).

Al día de hoy 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 (HALGAONKAR, Jain, & Wadhai, 2013). 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, Rao, & Lazar, 2007).

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 (Sun-Kuk Noh et al., 2013).

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 (Ali & Awal, 2012).

Si bien existen modelos de seguridad para NFC (Abu-Saymeh, Abou-Tair, & Zmily, 2013), estos se enfocan

únicamente a entornos específicos, limitando así su aplicación para escenarios de aplicación más comunes. Por ello, el presente trabajo de investigación, aporta con el modelo de seguridad NRioSec, que puede 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.

2. Metodología

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. Se aplica 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. Finalmente se utiliza también la investigación experimental pues se desarrollan procesos, como 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.

La población está constituida por todas las vulnerabilidades que se presentan en distintos sistemas y equipos basados en tecnología NFC. Y a su vez 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 data sniffing y data modification (Si-Jung Kim & Bong-Han Kim, 2013).

El 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 (Chen & Lee, 2014).

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

Planteamiento del problema

Formulación de hipótesis

Levantamiento de información

Análisis e interpretación de resultados

Comprobación de la hipótesis

Difusión de resultados.

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

Observación

Experimentación

Comparación de escenarios

Análisis

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, donde se establecen lineamientos y pasos que otorgarán una secuencia lógica de cada uno de los procesos y que podrá ser tomada como guía de referencia:

Configuración de los instrumentos hardware.

Configuración de los instrumentos software.

Configuración del escenario de prueba 1.

Captura de información (data sniffing) de un pago móvil basado en NFC con el sniffer Wireshark.

Observación y análisis de vulnerabilidades.

Aplicación del modelo de seguridad NRioSec al escenario de prueba 1.

Configuración del escenario de prueba 2.

Alteración de información (data modification) durante el proceso de intercambio de datos en un pago móvil basado en NFC.

Observación y análisis de vulnerabilidades.

Aplicación del modelo de seguridad NRioSec al escenario de prueba 2.

Observación y análisis de resultados mediante la tabulación de toma de muestras y generación de datos estadísticos.

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:

Generación de ataques.

Análisis de los ataques NFC.

Aplicación del modelo de seguridad NRioSec.

Análisis comparativo de los resultados de los escenarios de prueba.

2.1. Near Field Communication (NFC)

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 - Charlie Miller - Exploring the NFC attack surface - SecTor 2012, 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
Vulnerabilidades de seguridad NFC y posibles soluciones

Vulnerabilidades y ataques	Posibles soluciones
Manipulación de etiquetas NFC URI/URL spoofing	Etiquetas con firmas basadas en técnicas de cifrado
Clonación, suplantación y reemplazo de etiquetas NFC	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 (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
Skimming y ataques de clonación de tokens	Enlaces cifrados con identificadores únicos

Fuente: Elaboración propia

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.

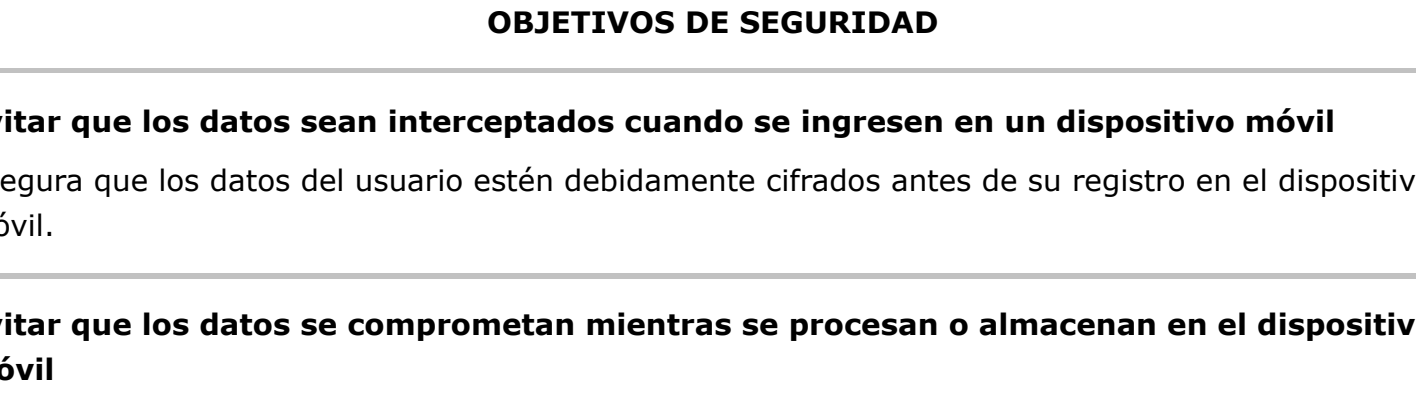
A su vez, (Nguyen, Seo, & Kim, 2014) proponen un modelo de seguridad basado en LEA, Lightweight Encryption Algorithm (Hong et al., 2014), que permite aplicar un bloque cifrado con LEA para proteger la comunicación entre dispositivos NFC y el sistema de base de datos, asegurando alta disponibilidad y 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 artículo, 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.

3. Resultados

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)

Figura 1
Logotipo NRioSec – NFC Security Model



Fuente: Elaboración propia

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 (“PCI Mobile Payment Acceptance Security Guidelines for Developers”, 2014).

3.1. Objetivos del Modelo

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 2
Objetivos de Seguridad del Modelo NRioSec

#	OBJETIVOS DE SEGURIDAD	
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.	•
	Evitar que los datos se comprometan mientras se procesan o almacenan en el dispositivo móvil	

2	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.	•
3	**Evitar que los datos sean interceptados tras la transmisión del dispositivo móvil** Los datos de la cuenta son cifrados (simétricamente o asimétricamente) antes que la transmisión se realice fuera del entorno de ejecución de confianza del dispositivo móvil.	•
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.	•
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.	•
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.	•
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.	•
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.	•
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.	•
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.	•
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.	•
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.	•
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.	•
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.	•
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.	
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.	•
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.	•
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.	•

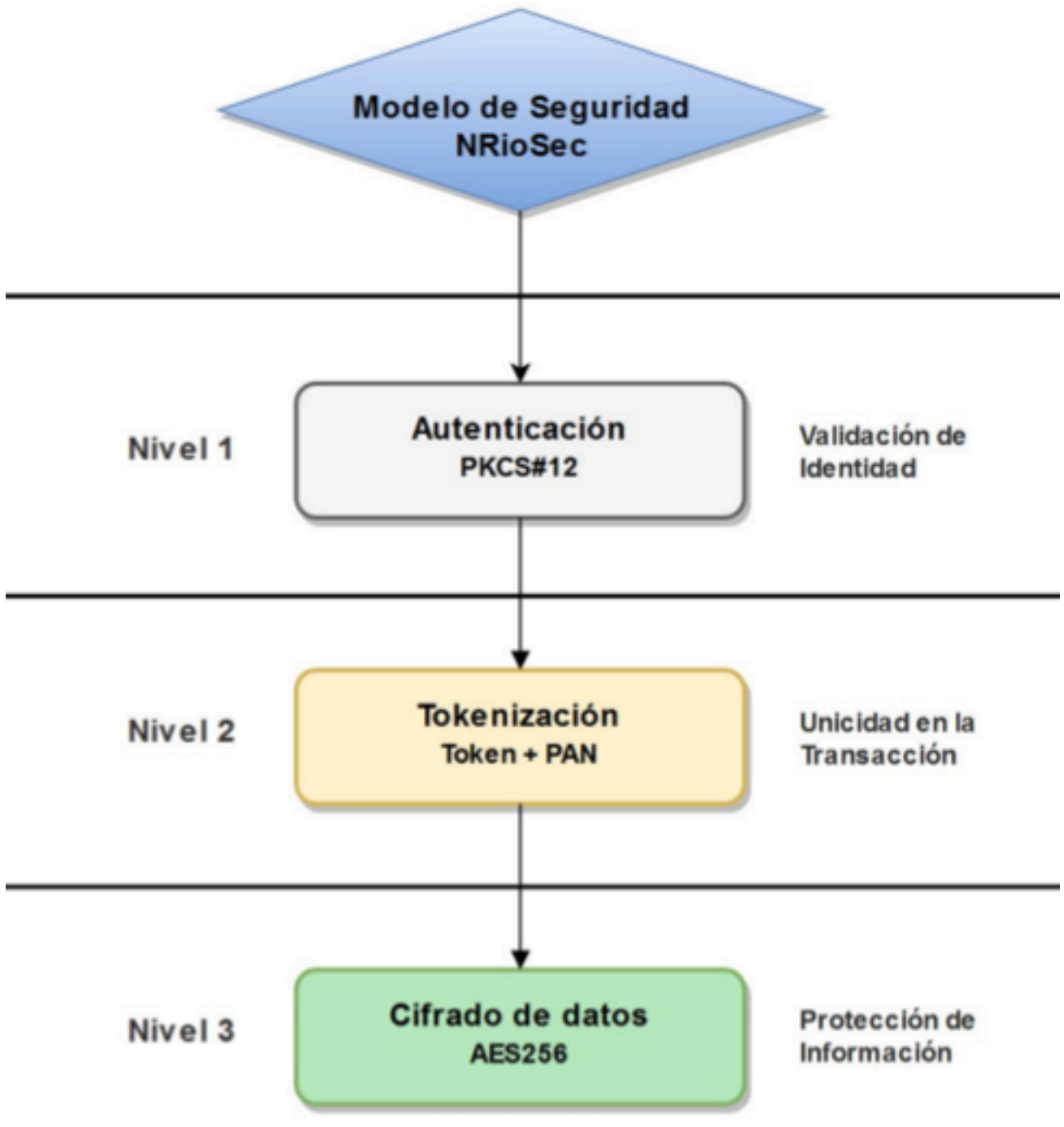
Fuente: Elaboración propia

3.2. 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.

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.

Figura 2
Componentes del modelo de seguridad NRioSec



Fuente: Elaboración propia

3.2.1. 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 (“PKCS #12: Personal Information Exchange Syntax Standard”, 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)

Figura 3
Nivel de Seguridad 1 – Autenticación

Fuente: Elaboración propia

3.2.2. 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 (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 (Cha & Kim, 2013):

Cumple con las especificaciones de PCI-DSS.

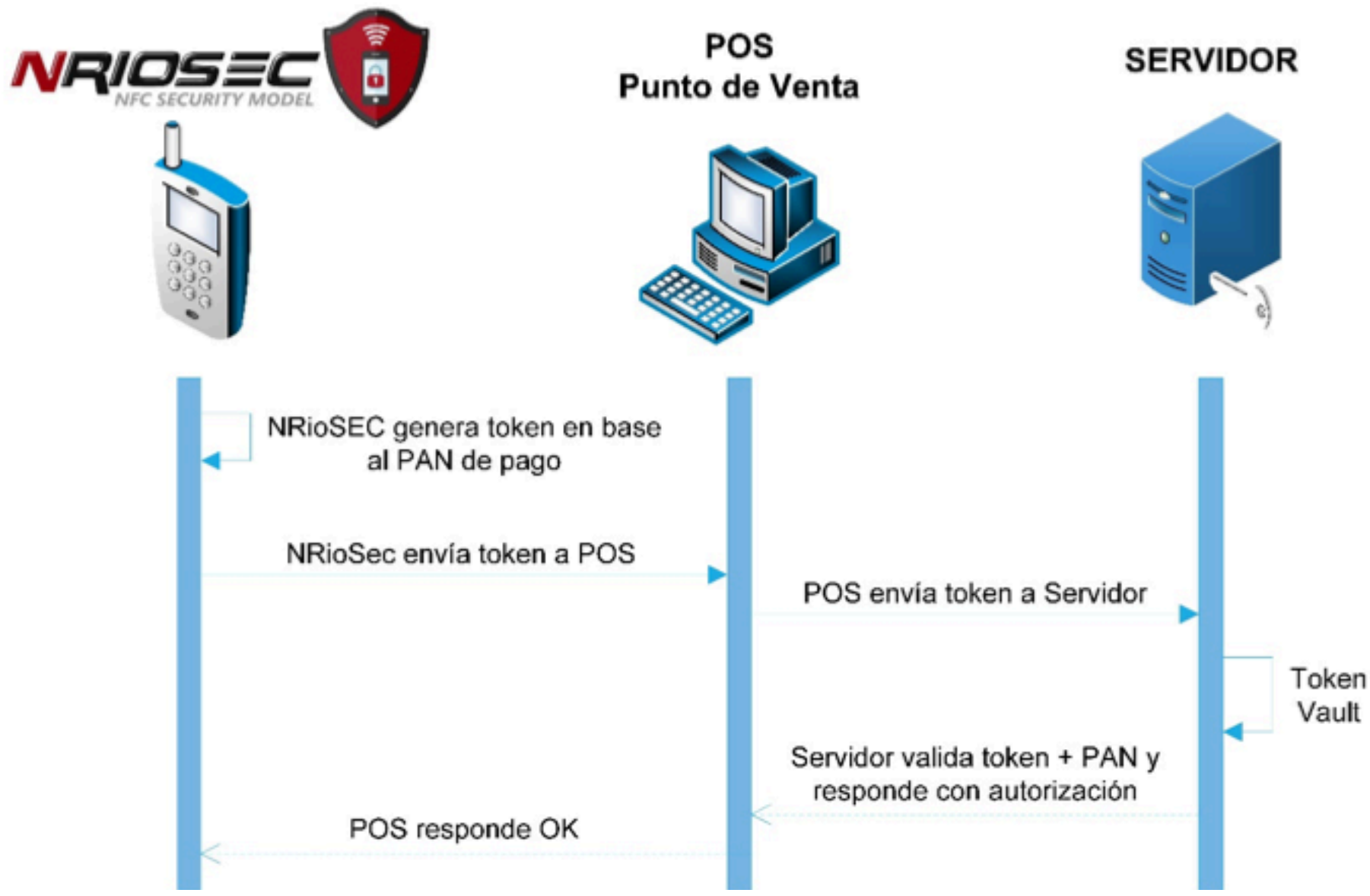
La privacidad se almacena y gestiona con seguridad en el servidor de tokens.

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).

Figura 4

Nivel de Seguridad 2 – Tokenización



Fuente: Elaboración propia

3.2.3. Nivel de Seguridad 3 – Cifrado de

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.

Figura 5
Nivel de Seguridad 3 – Cifrado de datos

Fuente: Elaboración propia

3.3. Implementación del modelo

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.

3.3.1. Prototipo de Pago Móvil NRioPay

Figura 6
Logotipo NRioPay – NFC Mobile Payment

Fuente: Elaboración propia

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

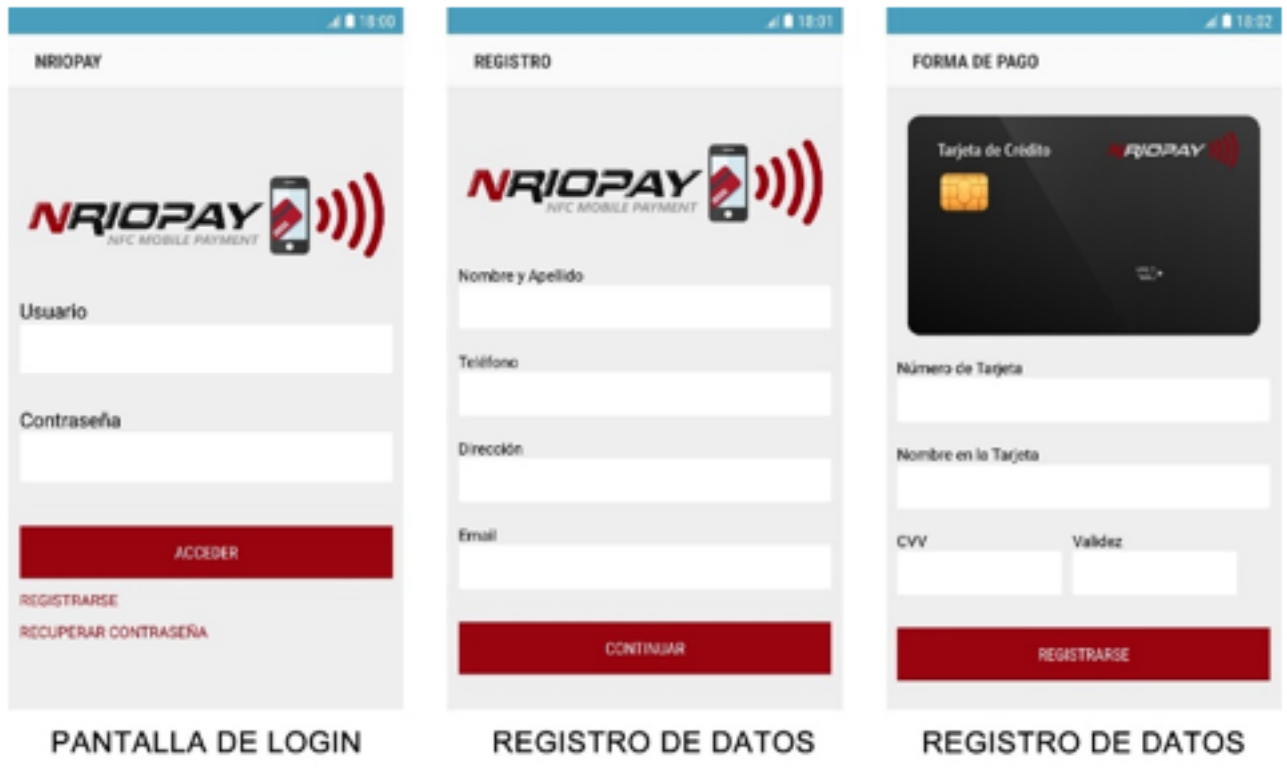
Número tarjeta de crédito, fecha vencimiento, código cvv

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.

En el sistema de back-end del prototipo NRioPay, permite al usuario (comerciante), acceder a la configuración de

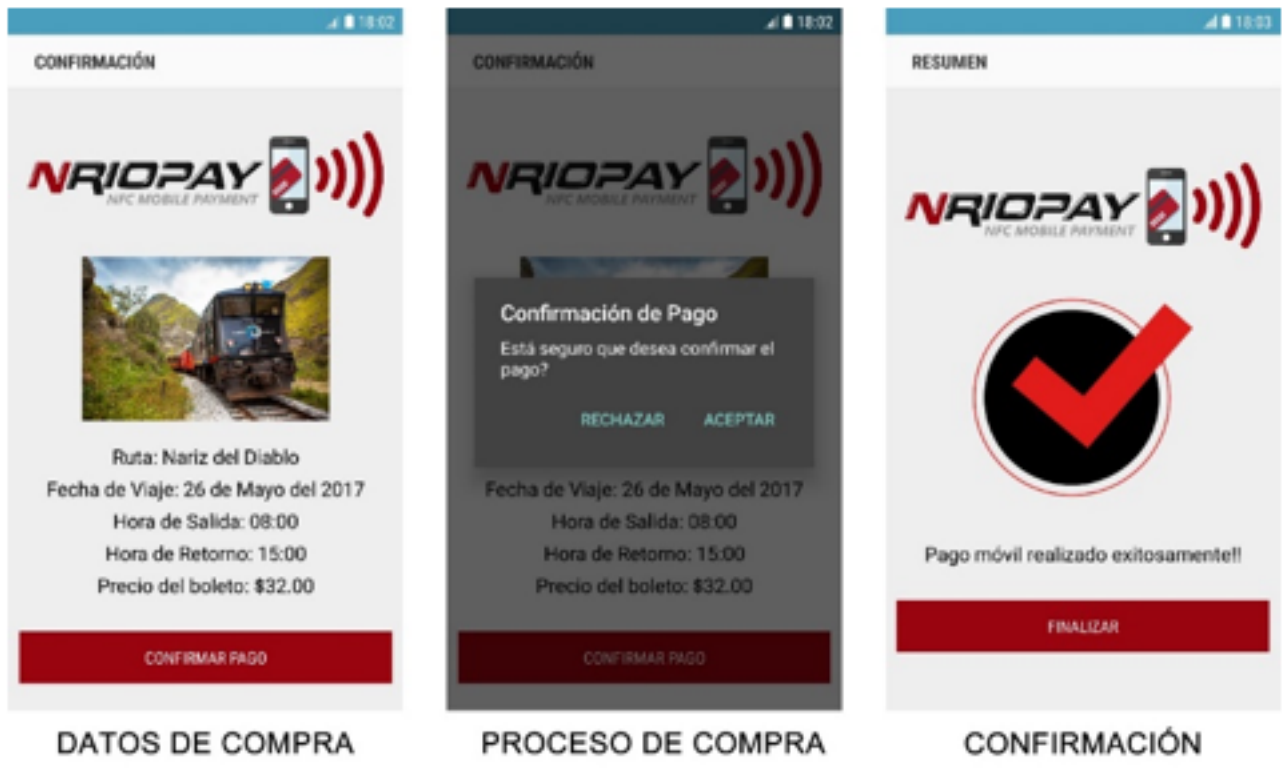
productos y al historial de compras realizadas mediante la aplicación móvil.

Figura 7
Pantallas de login y registro de datos de la app móvil NRioPay



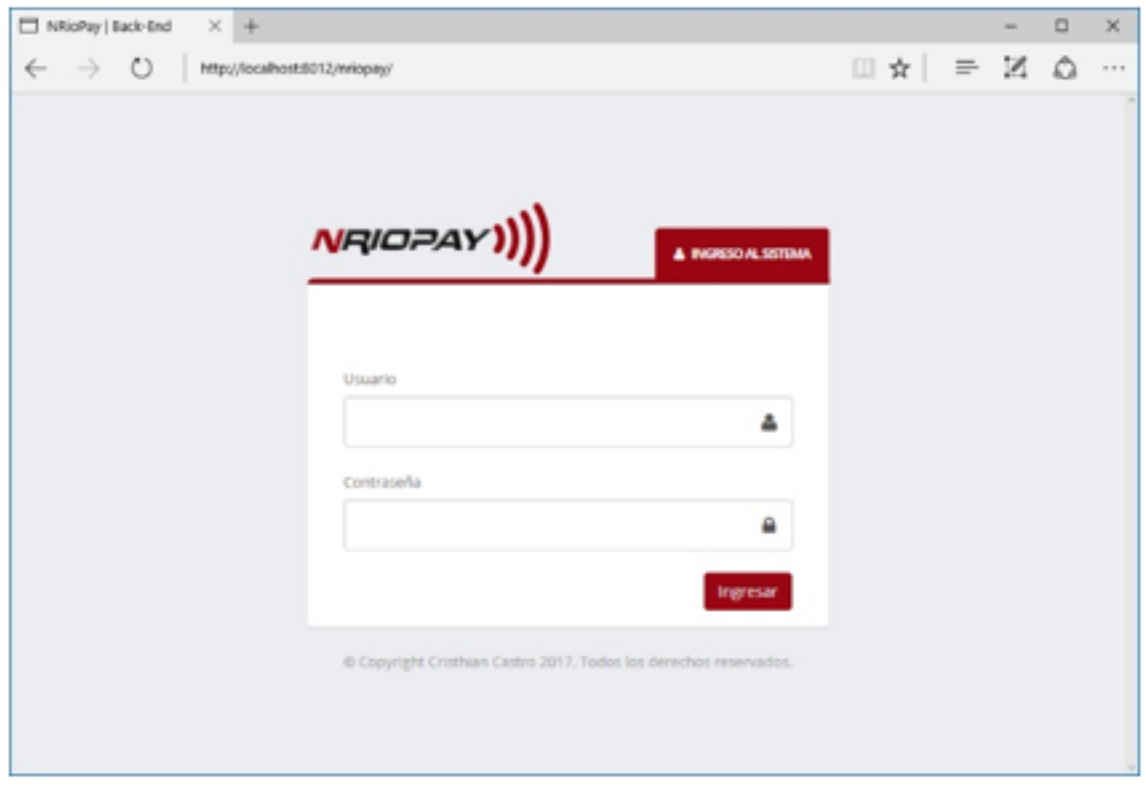
Fuente: Elaboración propia

Figura 8
Pantallas de compra y confirmación de pago de la app móvil NRioPay



Fuente: Elaboración propia

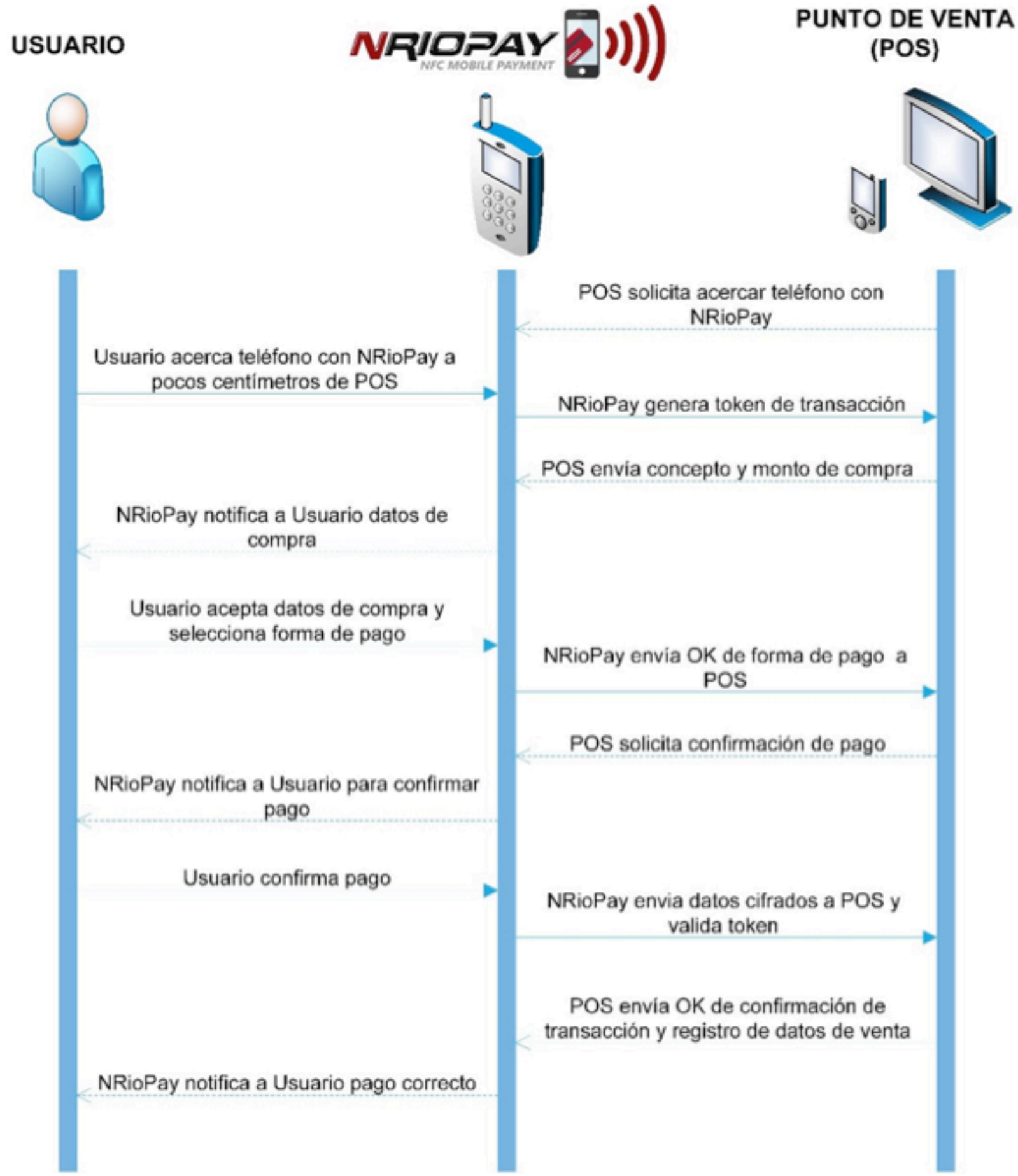
Figura 9
Pantalla de login del sistema de back-end de NRioPay



Fuente: Elaboración propia

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

Figura 10
Flujo de procesos de transacción de pago móvil con NRioPay



Fuente: Elaboración propia

3.3.2. 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, en base a la tabla 4.

AppVulnerable: Aplicación vulnerable sin el modelo de seguridad.

AppSegura: Aplicación con modelo de seguridad implementado.

Número: Número de vulnerabilidades encontradas.

Nivel de Integridad: integridad de los datos obtenidos tras el ataque, en base a la tabla 4.

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

Tabla 3
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

Fuente: Elaboración propia

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

Tabla 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

Fuente: Elaboración propia

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.

3.3.3. Escenario de Prueba 1

De acuerdo a los resultados obtenidos en el Escenario de prueba 1 basado en el indicador *"Captura de información (data sniffing)"* 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.

Tabla 5
Datos consolidados del 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

Fuente: Elaboración propia

3.3.4. Escenario de Prueba 2

De acuerdo a los resultados obtenidos en el Escenario de Prueba 2 basado en el indicador *"Alteración de información (data modification)"* 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.

Tabla 6
Datos consolidados del 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

Fuente: Elaboración propia

3.3.5. Prueba de Hipótesis

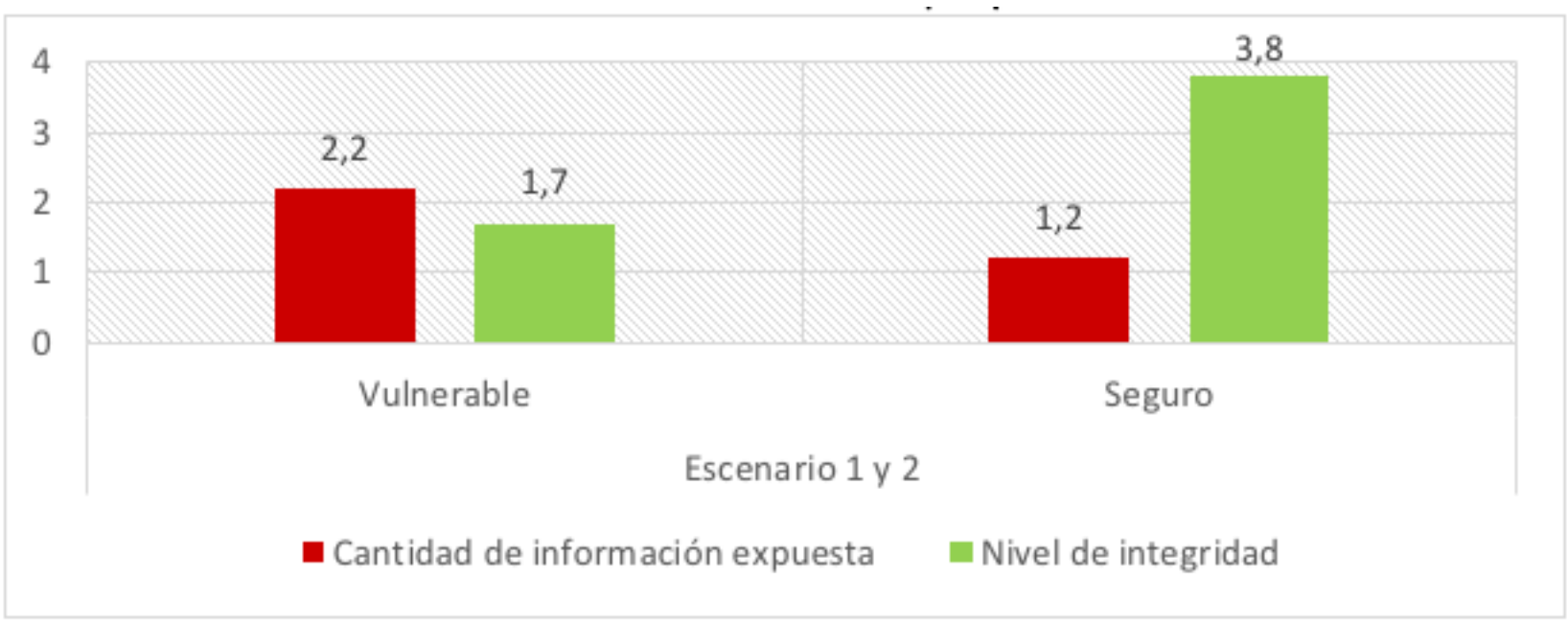
Tras la obtención de los resultados en los escenarios de prueba, se realiza el cálculo del promedio de los valores resultantes de los indicadores, tal como como se muestra en la tabla 7 y en el Figura 15.

Tabla 7
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

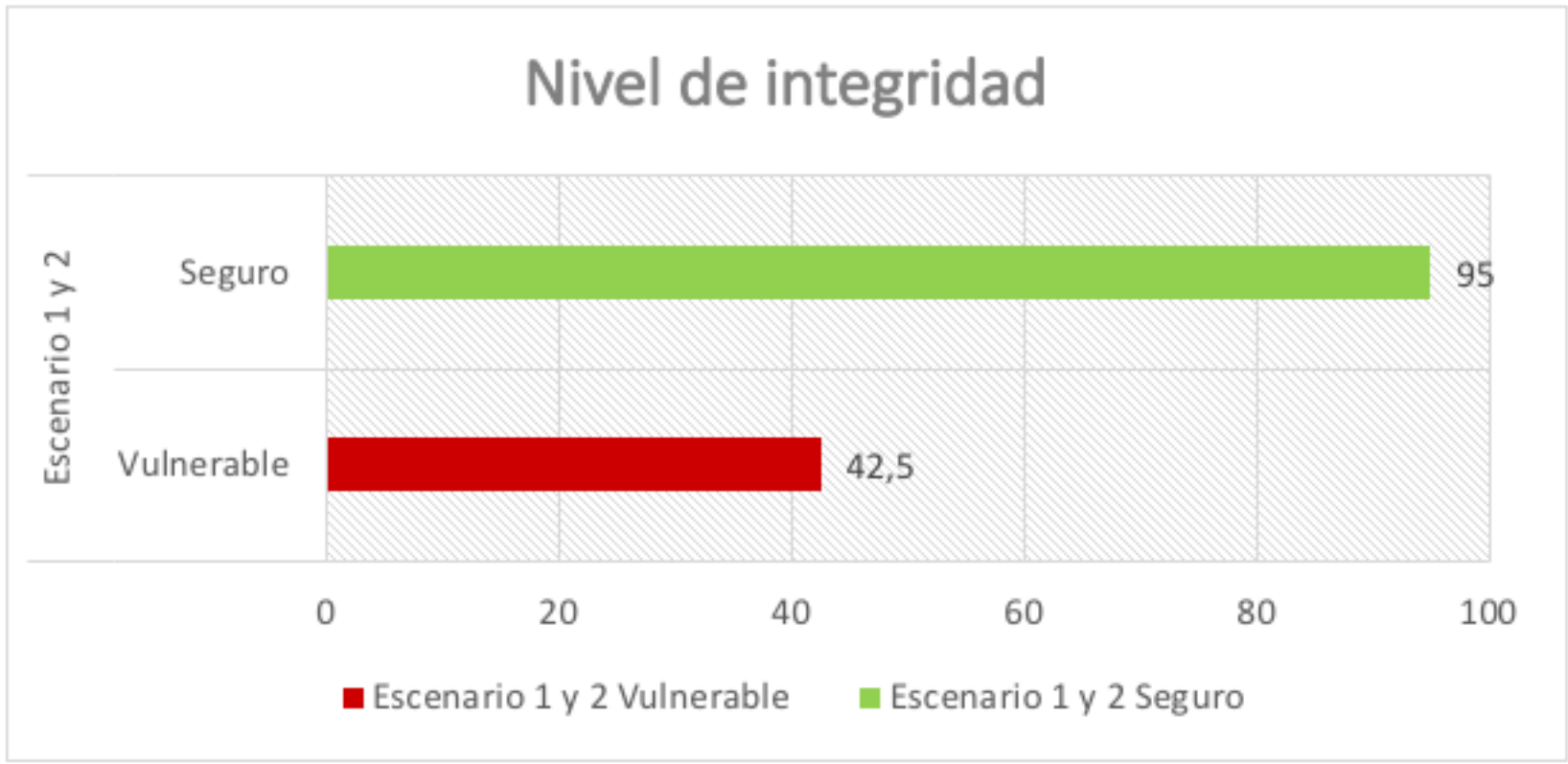
Fuente: Elaboración propia

Figura 11
Promedios totales de indicadores de los escenarios



Fuente: Elaboración propia

Figura 12
Porcentaje total de integridad de los escenarios



Fuente: Elaboración propia

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 y se comprueba la hipótesis de investigación.

4. 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.

Referencias bibliográficas

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

Abu-Saymeh, D., Abou-Tair, D. E.-D. I., & Zmily, A. (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

Ali, T., & Awal, M. A. (2012). Secure mobile communication in m-payment system using NFC technology. En *2012 International Conference on Informatics, Electronics Vision (ICIEV)* (pp. 133–136). https://doi.org/10.1109/ICIEV.2012.6317453

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

Chen, H. C. H., & Lee, P. P. C. (2014). Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation. *IEEE Transactions on Parallel and Distributed Systems*, *25*(2), 407–416. https://doi.org/10.1109/TPDS.2013.164

Coskun, V., Ozdenizci, B., & Ok, K. (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

Garfinkel, S. L., Juels, A., & Pappu, R. (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

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

Halgaonkar, P. S., Jain, S., & Wadhai, V. M. (2013). NFC: A review of technology, tags, applications and security. *IJRCCT*, *2*(10), 979–987.

Harnisch, M. J., & Uitz, I. (2013). Near Field Communication (NFC). *Informatik-Spektrum*, *36*(1), 99–103. https://doi.org/10.1007/s00287-012-0672-x

Hong, D., Lee, J.-K., Kim, D.-C., Kwon, D., Ryu, K. H., & Lee, D.-G. (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

Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S., & Singh, V. (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

Mantoro, T., Ayu, M. A., & Mahmod, S. M. binti. (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

Nguyen, H. V., Seo, H., & Kim, H. (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

Nikitin, P. V., Rao, K. V. S., & Lazar, S. (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

Ottoy, G., Martens, J., Saeys, N., Preneel, B., Strycker, L. D., Goemaere, J.-P., & Hamelinckx, T. (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

PCI Mobile Payment Acceptance Security Guidelines for Developers. (2014). 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

PKCS #12: Personal Information Exchange Syntax Standard. (2014). 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.html

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

Si-Jung Kim, & Bong-Han Kim. (2013). Vulnerability Analysis for Privacy Protection in Secure-NFC service. *International Journal of Advancements in Computing Technology*, *5*(13), 257.

Sun-Kuk Noh, Dong-You Choi, HyeongGyun Kim, DaeKyu Kim, JaeHyun Seo, JongWon Kim, & ByungRae Cha. (2013). Proposal of Micropayment and Credit Card Model using NFC Technology in Mobile Environments. *International Journal of Multimedia & Ubiquitous Engineering*, *8*(3), 295–305.

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

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

---

1. Profesor y profesional orientado a las telecomunicaciones y redes. Director Departamento de Evaluación y Acreditación. Universidad Nacional de Chimborazo. Ecuador. Investigador CIMOGSYS - Escuela Superior Politécnica de Chimborazo. Ecuador. Ingeniero en Electrónica y Computación. Magíster en Interconectividad y Redes. ascisneros@unach.edu.ec

2. Profesional orientado al desarrollo de aplicaciones informáticas, software y aplicaciones móviles. Empleado Privado. Ecuador. E-solutions. Ingeniero en Sistemas Informáticos. Magíster en Seguridad Telemática. ccastro@e-solutions.ec

3. Coordinadora Nivelación y Admisión. Universidad Nacional de Chimborazo. Ecuador. Investigador CIMOGSYS - Escuela Superior Politécnica de Chimborazo. Ecuador. Ingeniero en Sistemas Informáticos. Magíster en Gerencia Informática. Ecuador. muvidia@unach.edu.ec

4. Rector Universidad Nacional de Chimborazo. Ecuador. Presidente CEDIA. Ecuador. Doctor en Tecnología Educativa: E-Learning y Gestión del Conocimiento. nsamaniego@unach.edu.ec

5. Profesional orientado a la Telecomunicaciones. Ecuador. Docente investigador Universidad Nacional de Chimborazo. Ingeniero en Sistemas Informáticos. Ph.D. en Telecomunicación. cradicelli@unach.edu.ec

6. Aspirante al Doctorado en Ingeniería de la Universidad de Buenos Aires. Argentina. Docente Investigador Escuela Superior Politécnica de Chimborazo. Ecuador. Ingeniero Mecánico. Magister en Docencia y Currículo para la Educación Superior. dbarba@espoch.edu.ec

---