SISTEMA DE CONTROL DE ACCESO DEL PERSONAL DE LA CLÍNICA DE TRAUMAS Y FRACTURAS EN LA CIUDAD DE MONTERÍA

Trabajo de Grado de Maestría en Software Libre

CHRISTIAN CAMILO COGOLLO LOPEZ

Director: Ing. Freddy Méndez Ortiz

Universidad Autónoma de Bucaramanga

Facultad de Ingeniería

Grupo Prisma

Línea de Tecnología y Sociedad

Bucaramanga, enero de 2015

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del director

_____
Firma del jurado

_____
Firma del jurado

Bucaramanga, 15 de enero de 2015

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

LISTA DE ANEXOS

GLOSARIO

API (Application Programming Interface)

Interfaz de Programación de Aplicaciones) Grupo de rutinas (conformando una interfaz) que provee un sistema operativo, una aplicación o una biblioteca, que definen cómo invocar desde un programa un servicio que éstos prestan. En otras palabras, una API representa un interfaz de comunicación entre componentes software.

SDK (Software development kit - Kit de desarrollo de software) Es un conjunto de herramientas y programas de desarrollo que permite al programador crear aplicaciones para un determinado paquete de software, estructura de software, plataforma de hardware, sistema de computadora, consulta de videojuego, sistema operativo o similar.

XML (Extensible Markup Language) Lenguaje de marcado ampliable o extensible): es una especificación/lenguaje de programación desarrollada por el W3C. XML es una versión de SGML, diseñado especialmente para los documentos de la web. Permite que los diseñadores creen sus propias etiquetas.

RFID. Tecnología de intercambio inalámbrico de datos. La lectura y grabación de los datos se ejecuta a partir de un chip conectado a una antena que recibe señales de radiofrecuencia desde un dispositivo de lectura y grabación.

4G. Está basado en el protocolo IP, siendo un sistema de sistemas y una red de redes, que se alcanza gracias a la convergencia entre las redes de cables e inalámbricas.

SDK. Kit de herramientas estándar de desarrollo de software, como su nombre lo implica, es para desarrollo de software.

SQlite. Sistema de gestión de bases de datos relacional compatible con ACID, y que está contenida en una relativamente pequeña biblioteca en C.

ISO. Organización Internacional para la estandarización es una federación de alcance mundial integrada por cuerpos de estandarización nacionales de 130 países.

GHz. Es la unión del sufijo Giga, que añade el valor de 10^9 (mil millones), y de la palabra herzio, que es una medida de frecuencia creada por el físico H.R. Hertz.

SD. La memoria SD está específicamente desarrollada para cumplir con los requisitos de seguridad en el campo de los dispositivos electrónicos de video y audio.

TI. (Tecnología de la Información) Son aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información.

RESUMEN

Este trabajo presenta los resultados de la investigación “Sistema de Control de Acceso del Personal de la Clínica de Traumas en la Ciudad de Montería” desarrollado en el año 2014 en la “Universidad Autónoma de Bucaramanga”, sobre el uso de la identidad digital como medio control acceso e identificación y/o autenticación con tecnología NFC (Near Field Communication). Se establece una investigación cuantitativa y descriptiva. El proyecto tiene el planteamiento del problema definido al igual que los objetivos, se considera descriptiva porque pretende describir el estado y las características de las tecnologías NFC, se describe la elaboración de un prototipo de sistema validador de usuarios utilizando tecnología NFC. El propósito final planteado es obtener la caracterización de la tecnología NFC en dispositivos móviles para la autenticación de usuarios, determinar las principales normas existentes sobre control para el ingreso físico, realizar pruebas de validación del funcionamiento del prototipo con la implementación de un tester. Se crea documentación de la caracterización de la tecnología NFC en dispositivos móviles y la arquitectura y plataforma necesaria para su implementación, se realizan pruebas de funcionamiento con los usuarios de una institución de salud en la ciudad de Montería departamento de Córdoba. Con el desarrollo del prototipo de la aplicación se logró verificar la viabilidad de usar el dispositivo móvil para ser usado como credencial de identidad digital, y remplazar las tarjetas plásticas.

ABSTRACT

This paper presents the results of the investigation "System Access Control Staff Clinic Traumas in the city of Monteria" developed in 2014 in the "Autonomous University of Bucaramanga" on the use of digital identity as a means access control and identification and / or authentication with NFC (Near Field Communication). a quantitative and descriptive research is established. The project has defined the approach to the problem as well as the objectives, it is considered descriptive because it seeks to describe the status and characteristics of NFC technologies, the development of a prototype system users Validator using NFC technology is described. The ultimate purpose is to obtain raised characterization of NFC technology in mobile devices for user authentication, identify the main existing control standards for physical entry, validation testing operation of the prototype implementation of a tester. documentation characterization of NFC technology in mobile devices and architecture and platform necessary for its implementation is created, performance tests are conducted with users of a health institution in the city of Monteria, Cordoba department. With the development of the prototype implementation was achieved verify the feasibility of using the mobile device to be used as digital identity credentials and replace plastic cards.

INTRODUCCIÓN

Con la creciente tendencia global al uso de las comunicaciones con dispositivos móviles podemos disfrutar de una gran gama de aplicaciones y funciones integradas a estos dispositivos con los que podemos realizar diversas tareas.

Entre las nuevas funciones que nos ofrecen los nuevos diseños se encuentra el intercambio de datos utilizando la tecnología Near Field Communication (NFC).

Con esta tecnología combinada con aplicaciones seguras y tarjetas inteligentes se pretende asegurar y proteger las transacciones de identidad digital las cuales aprovechan las funciones de seguridad integrada a estos dispositivos.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. ANTECEDENTES

Los avances tecnológicos con los que se relaciona la persona hoy en día están sujetos a cambios constantes, por tal razón motivan a las diferentes entidades o personas a estar a la vanguardia y resulta importante que una institución este consiente de este avance, compare en qué nivel tecnológico está ubicada y esté dispuesta a realizar los cambios necesarios.

Enfocado con respecto a la identificación y acceso de personal, las empresas están implementando sistemas que facilitan el acceso con información propia de cada usuario, dentro de este campo existen varias alternativas que brindan soluciones para cada una de las necesidades, cabe mencionar métodos como fingerprint (escaneo de la huella digital), escaneo del iris, reconocimiento de voz y reconocimiento a través de tarjetas magnéticas.

Los avances tecnológicos abren nuevas oportunidades en los diferentes entornos en los que se aplica, adaptándose a las necesidades de cada momento y de cada persona. En algunos lugares se utiliza infraestructura costosa y/o de manejo delicado; material informático de alto valor, tanto en equipos como en información; que en caso de pérdida o daño ocasiona un grave problema para la institución.

Debido a lo anterior, surge la necesidad de desarrollar alternativas que permitan resolver el problema de control de acceso, haciendo uso de la tecnología actual, para así explotar al máximo sus capacidades; como es el caso de la tecnología NFC que permite el intercambio de datos entre dispositivos, y no está dirigida a la transmisión masiva de datos, ni al estilo de tecnologías WLAN (Wi-Fi) o Bluetooth, sino a la comunicación entre dispositivos con capacidad de proceso como teléfonos móviles, PDAs, o PCs por lo que es una tecnología complementaria y no sustitutiva.

1.2. DESCRIPCIÓN DEL PROBLEMA

El sistema de control de acceso propuesto en esta investigación surge a partir de la idea de realizar un sistema económico con tecnología de punta, que su tiempo de vida sea escalable, confiable, seguro y con interfaces amigables.

La tecnología propuesta es NFC, debido a la seguridad que presenta actualmente, la adaptabilidad que posee para este proyecto, además de ser una innovación tecnológica que poco a poco va tomando fuerza. Una ventaja de este sistema es que no necesitan contacto físico, como introducir la tarjeta en una ranura o esperar a que sea reconocido ópticamente, sólo con aproximarla a cierta distancia del lector, el dispositivo con NFC será validado.

El sistema validará la identidad del usuario dando respuesta según las necesidades de seguridad: aceptado, para usuarios autorizados y denegado, para usuarios que en determinado acceso no están autorizados para ingresar.

Algunas de las ventajas de la aplicación propuesta en este estudio son:

- Tecnología fácil de configurar y capaz de adaptarse a distintas situaciones que tenga la posibilidad de aumentar el número de dispositivos o accesos que controla.

- Tecnología que le permita a una PC tener comunicación bidireccional con múltiples dispositivos lectores y actuadores (tarjeta controladora de cerradura) a distancias de hasta 1km.
- Registro de la hora y fecha en cada entrada y salida de la persona, al momento de ingresar con su dispositivo móvil. Esto proporciona un registro de las personas que acceden al inmueble.
- Los reportes de asistencia y retardos, generados por el sistema, serán enviados por correo electrónico, para facilitar el control de asistencia del personal.
- El software permite el registro de visitantes con fotografía, así como modificaciones, altas y bajas de usuarios en el sistema.
- Se definió una arquitectura orientada a servicios cuyo objetivo es tener la posibilidad de crear procesos que integren diversas aplicaciones o tecnologías heterogéneas, y así poder llevar la información generada a otro nivel.

1.3. DELIMITACIÓN DEL PROBLEMA

Near Field Communication (NFC) utiliza como base la tecnología de comunicación RFID, como medio de enlace presenta corto alcance, lo cual limita la utilización de dispositivos que sean compatibles con este contorno.

El estudio realizado está dirigido básicamente para dispositivos móviles con la tecnología de comunicación NFC, que tengan el sistema operativo de celulares reconocido en el mercado como Android, con las versiones de software Gingerbread 2.3, Honeycomb 3.0, Ice Cream 4.0, JellyBeam 4.1, 4.2, 4.3.

1.4. ALCANCES

Simular el proceso de autenticación de usuarios a través de dos dispositivos móviles con posean tecnología de comunicación Near Field Communication (NFC), el cual nos garantizará que la información se transmita con seguridad.

1.4.1. Aplicación Demostrativa

Se utilizaron dos dispositivos móviles, el primero se utilizó la aplicación que se desarrolló para registrar la identidad digital del usuario y segundo dispositivo móvil realizo las funciones de dispositivo Lector para el cual se desarrolló otra aplicación la cual maneja los controles de seguridad y la gestión de datos que se utilizan para otorgar los controles de entrada y salida de usuarios.

Para la gestión de datos, validación y control de credenciales de autenticación de usuario se utilizó SGBD SQlite (MySQL).

1.5. JUSTIFICACIÓN

El sistema de comunicación de campo cercano NFC permitirá que procesos que actualmente se realizan de una manera propensa a errores, con largos tiempos de respuesta en la adquisición de información y con poca capacidad de gestionar y manipular la información del entorno para la ayuda en la toma de decisiones, sean realizados de forma que se eviten estas situaciones. El sistema permitirá tener mayor disponibilidad y movilidad a la hora de verificar la información de los usuarios.

La identificación de los usuarios se realizará por medio de un dispositivo móvil con NFC que posee un CUID (‘código único de identificación') que será el encargado de identificar de manera exclusiva y única a los usuarios y lo relacionará con un sistema de información.

Con el sistema NFC en el teléfono móvil se reducirá el costo del proyecto y se realizará la identificación y toma de información de los usuarios con esta tecnología.

1.5.1. Enunciado del Problema

¿El control de acceso de usuarios a través de Smartphone con NFC es más seguro y eficiente que las tarjetas de Plásticos?

1.6. OBJETIVOS

1.6.1. Objetivo General

- Evaluar la factibilidad de implementar un sistema de autenticación de usuarios para el ingreso físico de los empleados de la Clínica de Traumas y Fracturas en la ciudad de Montería.

1.6.2. Objetivos Específicos

- Identificar mediante revisión de literatura técnica la caracterización de la tecnología NFC en dispositivos móviles para la autenticación de usuarios.
- Determinar las principales normas existentes sobre el ingreso físico de los empleados de la Clínica de Traumas y Fracturas en la ciudad de Montería.
- Implementar un prototipo de sistema validador de usuarios utilizando tecnología NFC.
- Validar el funcionamiento del prototipo implementando un tester en la Clínica de Traumas y Fracturas en la ciudad de Montería.

2. MARCO TEÓRICO

2.1. ESTADO DEL ARTE

En la ciudad de Montería aunque gran número de habitantes cuentan con celulares de alta gama los cuales cuentan con la tecnología NFC[1] esta es poco usada y no existe ningún tipo de proyecto conocido en estos momentos en curso con esta tecnología.

En términos generales, en Colombia son pocos los proyectos que utilizan esta tecnología, solo en algunas universidades como la UNAB cuentan con grupos de investigación, entre ellos se destaca Prisma[2] que se dedica a su estudio y aplicación. También encontramos empresas privadas como es el caso de "NFC COLOMBIA SAS" que brindan soluciones como NFC PAY para ofrecer tarjetas de fidelidad recargables y NFC CREDIT para ofrecer tarjetas con cupos de crédito aplicando esta tecnología.

En algunos países de Latinoamérica como Costa Rica y Ecuador encontramos algunos proyectos que estudian la fundamentación y aplicabilidad de esta tecnología, en Europa el desarrollo de esta tecnología tiene más fuerza y encontramos un gran número de proyectos en España.

[1] **Near field communication (NFC)** es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos. http://es.wikipedia.org/wiki/Near_field_communication

[2] Universidad Autónoma de Bucaramanga. http://www.unab.edu.co/portal/page/portal/UNAB/investigacion/investigacion-en-sentido-estricto/inicio/grupo/descripcion?idgrupo=21 .

El número de estudios referidos en Colombia es mucho menor que en algunos países como Corea del Sur, Japón, España, Francia, Estados Unidos la cual se encuentra con mucho retraso respecto estos en la aplicación de esta tecnología.

Los usos más comunes de esta tecnología son pequeñas aplicaciones de pago como el transporte urbano, el aparcamiento público o para acceder a información. La utilización y aplicación de esta tecnología se reconoce en diferentes estudios, como es el caso de:

- En Japón, la operadora de telefonía móvil NTT DoCoMo ya probó el año pasado esta tecnología en el pago a través del móvil. Recientemente NTT DoCoMo ha lanzado el nuevo servicio "DCMX mini" que permitirá a los usuarios comprar pasando su teléfono móvil NFC por lectores. La transacción se añadirá a la factura mensual del usuario. En Estados Unidos las estaciones de servicio de Exxon Mobile ofrecen ya este tipo de pagos.

- Motorola ya ha anunciado que sus terminales incorporarán un chip NFC con funcionalidad de pago. Además, los teléfonos incorporarán una serie de características de seguridad para proteger los datos financieros y garantizar la seguridad de las transacciones financieras.

- La industria de la música tampoco es ajena a esta tecnología. Philips, Visa y Universal Music Francia están trabajando en desarrollar un producto denominado “Smart Poster” que permitirá el pago de canciones desde

cualquier lugar y dispositivo: desde un anuncio en una marquesina a una tienda de música. Posteriormente los usuarios podrán descargarse a través de Internet la canción comprada mediante este sistema.

- En España, existen diferentes iniciativas piloto en la utilización de esta tecnología. La empresa Mobilpay, en colaboración con Indra, la Empresa Malagueña de Transportes, Oberthur y Orange, inauguraba en 2008 un sistema de pago mediante el móvil. Para ello, los dispositivos deben tener el chip NFC integrado en la SIM.

2.1.1. Estudios Centrados en el Ámbito de Países Hispanoamericanos

De acuerdo a dicha evidencia, se estructura el estado del arte dedicado al caso de los estudios relativos al ámbito de España, Costa Rica y Ecuador. La revisión se organizará ordenando cronológicamente los estudios, y clasificándolos por separado según los indicadores de la eficiencia de aplicaciones de autenticación con tecnología NFC.

2.1.1.1. Aplicaciones De La Tecnología NFC

Los primeros usos de la tecnología NFC están estrechamente ligados a los teléfonos móviles debido a su ubicuidad y al hecho de que sea el único dispositivo que todos necesitamos llevar a todas partes. Se espera que, en un periodo de tres a cinco años, un tercio de los teléfonos móviles a nivel mundial estén equipados con tecnología NFC.

Las aplicaciones para la tecnología NFC, Daniel Chavaría; 2011 [1], en su obra la cual está enfocado en conocer los fundamentos de esta tecnología de Comunicación de Campo Cercano NFC en la cual describe las aplicaciones más importantes:

- Efectuar pagos con un toque en cualquier lugar los lectores de tarjetas sin contacto se han desplegado, aunque a la fecha no se ha podido implementar con éxito este método.
- Obtener información y "recoger" ofertas especiales y descuentos de carteles o vallas publicitarias inteligentes.
- Tiquetes o Ticket para acceder a las puertas o billete en servicios de transporte público, aparcamientos o entrar en los eventos deportivos, cines, museos, aparcamientos.
- Almacenar información personal que permita el acceso al edificio seguro.
- Tomar una imagen y la transfiere a una Conferencia Nacional, impresora habilitada o monitor.

Otras aplicaciones importantes, Fermín Gallego de la Sacristana [2], en el proyecto de investigación en la aplicación de inicio de sesión mediante autenticación con NFC:

- Identificación el DNI electrónico ha permitido la posibilidad de realizar todo tipo de trámites vía web con un lector.

- Fidelización y cupones descuento (loyalty&cuponing) la sustitución de los cupones descuento de papel, por nuevas formas de enviar y aceptar ofertas de forma digital. Las tarjetas de fidelización integradas en el teléfono móvil permiten premiar al consumidor de una forma más personalizada (teniendo en cuenta sus preferencias y hábitos de compra) e instantánea.
- Control de acceso, la idea principal es el uso de tarjetas o teléfonos NFC como llaves electrónicas. Implementado en un edificio, se puede saber quién y cuando accedió una persona, los lugares a los que accedió, así como tener diferentes permisos para diferentes usuarios. Estos permisos son fácilmente modificables en caso de tenerlos de forma centralizada.
- Conexiones de red, iniciar conexiones con otro tipo de comunicaciones, que requieren algún tipo de autorización o información previa: emparejamiento entre dispositivos con Bluetooth, o acceso a una red Wi-Fi protegida.
- Tarjetas de presentación, en una etiqueta NFC es fácil compartir información de contacto (nombre, e-mail, número de teléfono,). En este aspecto tiene como competencia los códigos QR.
- Inventariado, las etiquetas NFC permiten realizar una identificación y clasificación de productos, de igual manera que un código de barras. Para este tipo de aplicaciones es más frecuente utilizar RFID, ya que, al funcionar a una distancia mayor, es más cómodo de utilizar.
- Check-in, confirmar que realmente se está en un determinado lugar o establecimiento y poder compartirlo.

2.1.1.2. Aplicaciones Diseñadas para la NFC

En diseño de aplicación con NFC, Natalia Sánchez [3], en su proyecto diseña una aplicación para evaluación/calificación el cual los estudiantes no usan papel sino su dispositivo móvil con tecnología NFC.

En esta obra se estudia nuevas aplicaciones puedan ser implementadas en entornos universitarios con la finalidad de ofrecer a estudiantes y profesores información que puedan ser utilizadas en los nuevos modelos de educativos.

2.1.1.3. Aplicaciones de Autenticación Aplicando NFC

En relación al diseño de aplicaciones de autenticación, Diego Veloz; 2010 [4], en su tesis diseña e implementa un sistema de control de acceso de personas utilizando la tecnología NFC, el cual tiene la finalidad de realizar un control automático en el acceso de personas utilizando un teléfono celular, este sistema se opera por si solo y permite el ingreso o restricción de personas autorizadas a aún determinado lugar.

Una de las conclusiones más significativas fue que el sistema control de acceso con NFC es más seguro que, por ejemplo con tecnologías RFID[3] porque con el uso del celular se pueden crear aplicaciones que permitan mayor seguridad a través de autenticación antes de establecer comunicación NFC.

[3] **RFID** (siglas de ***R**adio **F**requency **ID**entification*, en español **identificación por radiofrecuencia**) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados **etiquetas**, **tarjetas**, **transpondedores** o **Tags RFID.** http://es.wikipedia.org/wiki/RFID

Beatriz Juárez; 2011 [5], en su tesis desarrolla una aplicación para obtener información en cualquier lugar de la universidad (despachos, laboratorios, aulas, biblioteca, etc.), la cual emplea un lector NFC y es accesible para cualquier usuario que posea un móvil con esta tecnología, el usuario tan sólo necesitará tener en el elemento seguro de su móvil su identificador (NIA) y una clave que le será solicitada cuando consulte cierta información restringida (reserva de libros, solicitación de tutoría, etc.). La conclusión más importante de este proyecto es que existe mayor utilidad al complementar NFC con Bluetooth y no mirarlas como diferentes tecnologías con sus ventajas y desventajas, si no aprovechar las estudiantes ventajas que nos ofrecen las dos.

Fermín Gallego [6], realiza un proyecto en el cual diseña una librería suficientemente completa, estable y funcional, que permita ser utilizada y/o adaptada en diferentes casos de usos para la tecnología NFC y desarrollando una aplicación de autenticación e inicio de sesión. El autor considera que actualmente resulta bastante interesante realizar un proyecto que permitiera realizar comunicaciones NFC entre móviles y PC de tal forma que sirviera como referencia para futuras aplicaciones de diversa índole.

2.2. MARCO CONCEPTUAL

La tecnología NFC es un sistema de comunicación inalámbrico de corto alcance con el cual podemos realizar intercambio de datos entre dispositivos en sentido bidireccional a una distancia entre 10 y 20 centímetros, este funciona en la banda de los 13.56 MHz cuya utilización no necesita licencia o permiso para su uso. Esta plataforma es abierta y diseñada para dispositivos móviles, tiene una tasa de transferencia que puede alcanzar hasta los 424 kilobytes, por esto es muy eficaz y rápida en la comunicación por esto se aplicabilidad en la autenticación de usuarios.

Su fortaleza es la rapidez en la comunicación, lo que la hace casi instantánea sin necesidad de realizar emparejamiento, además, es transparente para el usuario y los dispositivos que poseen esta tecnología siendo capaces de enviar y recibir datos al mismo tiempo, sin perder información en la trasferencia. La desventaja principal está dada por su alcance, el cual es muy pequeño y oscila entre 10 y 15 centímetros.

Esta tecnología surge en el año 2002, desarrollada por Philips y Sony los cuales buscaban desarrollar un protocolo que fuera compatible con sus tecnologías de tarjetas sin contactos Mifare de Philips y FeliCa de Sony. El estándar con el que fue aprobado es ISO 18092 en el año 2003; para 2004 Philips, Sony y Nokia crearon NFC Forum logrando integra empresas como Google, Visa, At&t, PayPal, etc.

NFC es compatible con toda la infraestructura de pago sin contactos y de transporte que existe en la actualidad ya que fue basada el estándar ISO/IEC-14443 para tarjetas de proximidad sin contactos. Funciona bajo el estándar RFID, de hecho, puede decirse que NFC es la unión de RFID y de tecnologías interconectadas.

2.2.1. Fases de la comunicación en NFC

La comunicación NFC consta de cinco fases las cuales describe Chavarría (2011) y son importantes para la comunicación entre dispositivos ya que tienen una función específica y siempre están presentes en el establecimiento de esta.

Estas etapas son:

Descubrimiento: En esta fase los dispositivos inician la etapa de rastrearse el uno al otro y posteriormente su reconocimiento.

Autenticación: En esta parte los dispositivos verifican si el otro dispositivo está autorizado o si deben establecer algún tipo de cifrado para la comunicación.

Negociación: En esta parte del establecimiento, los dispositivos definen parámetros como la velocidad de transmisión, la identificación del dispositivo, el tipo de aplicación, su tamaño, y si es el caso también definen la acción a ser solicitada.

Transferencia: Una vez negociados los parámetros para la comunicación, se puede decir que ya está realizada exitosamente la comunicación y ya se puede realizar el intercambio de datos.

Confirmación: El dispositivo receptor confirma el establecimiento de la comunicación y la transferencia de datos.

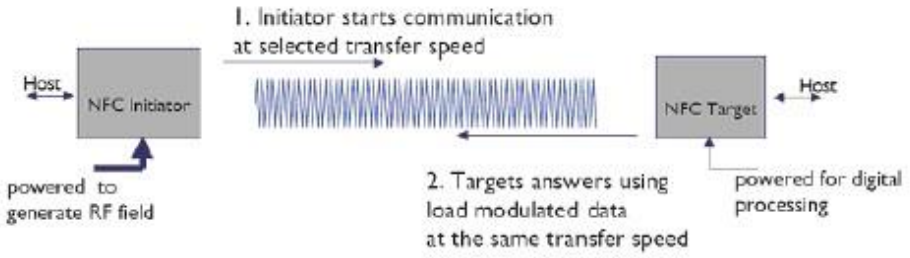
2.2.2. Modos de Funcionamiento

La tecnología NFC puede operaras de dos modos distintos: **Pasivo y Activo.**

2.2.2.1 Modo Pasivo

El dispositivo Iniciador genera el campo electromagnético y el dispositivo destino se comunica con éste modulando la señal recibida. En este modo, el dispositivo destino obtiene la energía necesaria para funcionar del campo electromagnético generado por el Iniciador" (Chavarría, 2011, p. 39).

Ilustración 1. Esquema del modo de funcionamiento pasivo NFC

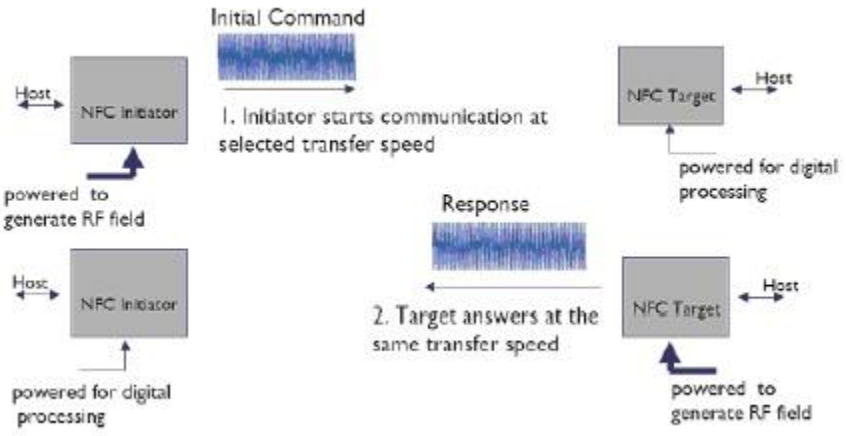


Fuente: http://blog.kuapay.com/es/tag/nfc/pasivo

2.2.2.2. Modo Activo

En la definición de modo activo Chavarría (2011) describe que el dispositivo Iniciador como el destino se comunica generando su propio campo electromagnético. En este modo, ambos dispositivos requieren de una fuente de alimentación para funcionar. Cuando el dispositivo funciona en modo pasivo, el receptor sólo se utiliza para establecer la comunicación y confirmar la recepción de los datos. Sin embargo, en modo, se requiere que ambos nodos negocien el intercambio de datos. (p. 40)

Ilustración 2. Esquema del modo de funcionamiento activo NFC



Fuente: http://blog.kuapay.com/es/tag/nfc/activo

2.2.2.3. Funcionamiento Técnico de NFC

Morales, V.S. & Ramírez, J.C. (2008). Definen que dentro de la tecnología NFC se deben analizar algunos términos, definiciones y componentes, que son necesarios para que el funcionamiento de esta tecnología sea lo más claro posible.

NFC trabaja bajo lo que se conoce como el acoplamiento magnético inductivo, lo cual es una técnica sencilla y fácil de aplicar sobre el silicio, lo que permite una integración más sencilla y eficaz de las antenas del sistema NFC (para el envío y recepción de señales) y diferentes circuitos digitales en un solo chip para un dispositivo móvil.

El módulo de transmisión NFC de un semiconductor PN511 diseñado por la empresa Philips, en donde se logra ilustrar cómo los elementos de un sistema NFC se pueden integrar en un solo chip dentro de un dispositivo. Este circuito análogo procesa las señales que se reciben o se envían desde otro dispositivo. El elemento UART maneja toda la parte tecnológica detrás de la comunicación NFC entre dispositivos. El buffer FIFO permite la transferencia de datos entre el host y el UART Otros componentes del chip se refieren a un detector de nivel de radio frecuencia que se sintoniza para reconocer señales de 13.56 MHz y poder así también identificar la presencia de otro dispositivo NFC cerca.

El “cardmode detector” reconoce qué tipo de tecnología (Ejemplo: MIFARE de Philips o FeliCade Sony) es la que envía la señal y prepara el “Receiver” para desmodular la misma (p 9 -10).

2.2.2.4. NFC Protocol-1 (NFCIP-1)

En la investigación realizada por Veloz (2010) nos explica que el protocolo NFCIP-1 está definido en el ECMA-340 y en ISO-IEC 18092. Los estándares definen la modulación y esquemas de codificación de bits y la arquitectura para las tasas de transferencia de datos de 106, 212 y 424 kbits/s. Además, estandarizan la interfaz de señal de comunicación y el flujo general del protocolo. En los sistemas NFC, máximo dos dispositivos se pueden comunicar simultáneamente. Estos intercambian datos usando acoplamiento inductivo y señales de radio.

Uno de los pares en la comunicación se llama iniciador y tiene un rol activo, mientras que el par pasivo se llama target. Ambos roles son siempre asignados, incluso si dos dispositivos NFC con carga de baterías se comunican.

El chip NFC que está integrado en el dispositivo móvil puede leer la información de un tag (a), emular una smart card para que un reader pueda acceder a sus datos (b), o comunicarse directamente con otro dispositivo NFC (c). NFCIP- 1 define modelos de comunicación activa y pasiva.

En modo activo, tanto el iniciador como el target generan un campo de frecuencia de radio. El iniciador empieza la comunicación usando el protocolo NFCIP-1 Una vez se completa la configuración y el handshake, comienza la transmisión de datos. En modo pasivo, solo el iniciador genera un campo de radio frecuencia. El target obtiene energía a través del acoplamiento inductivo y es capaz de enviar o recibir datos.

Este modo permite el ahorro significativo de energía. Además, NFCIP-1 define el protocolo de transporte, métodos de anti-colisión para el modo activo, y selección de target e inicialización para el modo pasivo. (Veloz, 2010, p.35)

2.2.2.5. NFC Interface Protocol-2 (NFCIP-2)

En la investigación realizada por Veloz (2010) nos explica que el protocolo NFCIP-2 está definido en el CMA-352 y en ISO-IEC 21481. Este estándar especifica un método para escoger uno de los tres posibles modos de comunicación definidos en el ECMA-340 (NFCIP-1), ISO/IEC 14443 (MIFARE de Philips) e ISO/IEC 15693 (tags RFID).

Por esta razón, NFCIP-2 provee una puerta de entrada entre diferentes estándares de interfaz existentes. Los dispositivos que implementan NFCIP-2 necesitan implementar funciones de dispositivo de acoplamiento de proximidad (ISO/IEC 14443), dispositivo de acoplamiento de vecindad (ISO/IEC 15693) y las funciones de iniciador y target definidas en ECMA-340.

Esto hace que los dispositivos NFC sean compatibles con sistemas existentes de FeliCa, MIFARE y otros. Sin embargo, no se logra compatibilidad en la emulación de smart cards para los estándares ISO/IEC 14443B e ISO/IEC 15936, aunque es posible la lectura y edición. Otro enfoque del protocolo es no perturbar cualquier comunicación saliente en la frecuencia de 13.56 MHz. Esto se alcanza usando CSMA (Carrier Sense with Multiple Access), por tanto, un dispositivo NFCIP-2 no activará su campo de radio frecuencia cuando detecta un campo de radio que excede un umbral específico.

2.2.3. Android

Este Sistema Operativo se encuentra basado en Linux y fue diseñado para funcionar en dispositivos móviles como Smartphone o Tablet. Google en la actualidad es quien lo desarrolla, pero fue comprado a Android Inc. quien lo creo.

La ventaja principal de Android es que es un SO común para los diferentes fabricantes de dispositivos móviles, gracias a estos se puede personalizar Android a su necesidad.

La estructura del sistema operativo Android se compone de aplicaciones que se ejecutan en un framework Java de aplicaciones orientadas a objetos sobre el núcleo de las bibliotecas de Java en una máquina virtual Dalvik con compilación en tiempo de ejecución. El sistema operativo está compuesto por 12 millones de líneas de código, incluyendo 3 millones de líneas de XML, 2,8 millones de líneas de lenguaje C, 2,1 millones de líneas de Java y 1,75 millones de líneas de C++.

2.2.3.1. Características y Arquitectura

Las principales características de Android son:

- Es in SO libre distribuido bajo licencia Apache: Con esta licencia se encuentra disponible el código fuente para su uso libre, y cada fabricante puede modificarlo el SO a sus requerimientos o necesidades, sin estar obligado a publicar el código fuente con los cambios (a diferencia de lo que ocurriría con una licencia GPL). Además, ha permitido que se crearan diferentes comunidades que han modificado Android con sus preferencias y modificaciones particulares.

- El lenguaje en que fue desarrollado es Java y C. Para programar en esta plataforma se usa principalmente Java. Para casos excepcionales (tareas de rendimiento) es posible programarlo en C gracias al SDK Bionic. Actualmente hay iniciativas para el uso de nuevos lenguajes (c#) pero el recomendado es java.
- Soporte para un gran número de comunicaciones: 3G, Wi-Fi, Bluetooth, Wimax, NFC y más.
- Navegador web basado en Webkit: Otros navegadores como Chrome o Safari están basados también en este, lo que facilita la compatibilidad y futuras correcciones de vulnerabilidades y errores.
- Soporte para Flash: Aunque no es recomendable en dispositivos móviles, debido entre otras cosas al gasto de batería que supone, para una navegación web completa a día de hoy sigue siendo importante la posibilidad de instalar flash en Android, hasta que termine de implantarse HTML5.
- Soporte para compartir la red (tethering): Es posible compartir la conexión de datos contratada con un PC u otros móviles a través del USB o creando una red Wi-Fi.
- La arquitectura está planificada para simplificar la reutilización de componentes: cualquier aplicación puede publicar sus propias funciones para que otras aplicaciones hagan uso de estas. A través del framework el desarrollador puede acceder a la información de ubicación, estado de la

red, información del teléfono y de la SIM, cámara y el resto de dispositivos de hardware, a alto nivel.

- Aplicaciones: En esta última capa se encuentra las aplicaciones de las que hará uso el usuario, tanto pre-instaladas como las desarrolladas y posteriormente instaladas. Correo electrónico, agenda, calendario, gestor de mensajes (SMS), AndroidMarket.

2.2.3.2. Android Incorpora Soporte Para NFC

Gingerbread es la versión 2.3 de Android con la cual comienza el soporte para NFC. Android 2.3.3 API (GINGERBREAD_MR1) es una pequeña versión de funciones que añade varias mejoras y las API de la plataforma Android 2.3 la cual proporciona un mejor y ampliado apoyo a NFC, para que las aplicaciones puedan interactuar con más tipos de etiquetas de nuevas maneras.

Un nuevo y completo conjunto de APIs busca brindar a las aplicaciones acceso de lectura y escritura una gama más amplia de tecnologías de etiquetas estándar, incluyendo:

- NFC-A (ISO 14443-3A)
- NFC-B (ISO 14443-3B)
- NFC-F (JIS 6319-4)
- NFC-V (ISO 15693)
- ISO-DEP (ISO 14443-4)
- MIFARE Classic
- MIFARE Ultralight
- Etiquetas NFC Fórum NDEF

La plataforma también proporciona un protocolo limitado peer-to-peer de comunicación y API. Primer plano Las actividades pueden utilizar la API para registrar un mensaje de NDEF que quedarse relegados a otros dispositivos NFC cuando se conecten.

Tag avanzada despachando ahora ofrece a las aplicaciones más control sobre cómo y cuándo se ponen en marcha, cuando se descubre una etiqueta NFC. Anteriormente, la plataforma utiliza un despacho intención de un solo paso para notificar a las aplicaciones interesadas de que se descubrió una etiqueta. La plataforma utiliza ahora un proceso de cuatro pasos que permite a la aplicación en primer plano para tomar el control de un evento de etiqueta antes de pasar a otras aplicaciones. El nuevo proceso de despacho también permite aplicaciones escuchan contenidos etiqueta específica y las tecnologías de la etiqueta, basado en dos nuevas acciones de intención:

- android.nfc.action.NDEF_DISCOVERED.
- android.nfc.action.TECH_DISCOVERED.

La API de NFC está disponible en los android.nfc y android.nfc.tech paquetes.

2.2.3.3. Las clases principales son

- NfcAdapter , que representa el hardware NFC en el dispositivo.
- NdefMessage, lo que representa un mensaje de datos NDEF, el formato estándar en el que "registros" que transportan datos se transmiten entre los dispositivos y las etiquetas. Un mensaje NDEF ciertas muchos registros NDEF de diferentes tipos. Las aplicaciones pueden recibir estos mensajes
  de NDEF_DISCOVERED , TECH_DISCOVERED oTAG_DISCOVERED I ntenciones.

- NdefRecord, entregado en un NdefMessage, que describe el tipo de datos que se comparten y se lleva los datos en sí.
- Tag, lo que representa una etiqueta escaneado por el dispositivo. Pueden varios tipos de etiquetas, basado en la tecnología de etiqueta subyacente.
- TagTechnology, una interfaz que da a las aplicaciones acceder a etiquetar las propiedades y las operaciones de E / S basada en las tecnologías presentes en la etiqueta.
- Comunicación NFC se basa en la tecnología inalámbrica en el hardware del dispositivo, y no está presente en todos los dispositivos Android. Los dispositivos Android que no admiten NFC devolverá un objeto nulo cuando getDefaultAdapter (Context) se llama, y context.getPackageManager().hasSystemFeature(PackageManager.FEATURE_NFC) volverán false . La API de NFC está siempre presente, sin embargo, independientemente de soporte de hardware subyacente.

Para utilizar la API de NFC, las aplicaciones deben solicitar permiso al usuario al declarar <uses-permission android: name = "android.permission.NFC"> en sus archivos de manifiesto.

2.2.3.4. Interfaces

NfcAdapter.CreateBeamUrisCallback

- *NfcAdapter.CreateNdefMessageCallback* Una devolución de llamada que se invoca cuando otro dispositivo NFC capaz de NDEF push (Android Beam) está dentro del rango.

- *NfcAdapter.OnNdefPushCompleteCallback* Una devolución de llamada que se invoca cuando el sistema se entrega con éxito su NdefMessage a otro dispositivo.

2.2.3.5. Clases

- *NdefMessage* Representa un mensaje inmutable NDEF.
- *NdefRecord* Representa un registro inmutable NDEF.
- *NfcAdapter* Representa el adaptador NFC local.
- *NfcEvent* Envuelve la información asociada a cualquier evento NFC.
- *NfcManager* gestor de alto nivel para obtener una instancia de un NfcAdapter.
- *Tag* Representa una etiqueta NFC que se ha descubierto.

2.2.3.6. Principales Librerías de Android

El sistema operativo Android fue orientado para uso de dispositivos móviles. Las principales librerías que se utiliza al desarrollar una aplicación son:

- java.lang: Clases fundamentales para el diseño del lenguaje de programación Java.
- java.io: Capacidades de entrada y salida.
- java.net: Conexiones de red.
- java.util: Utilidades.
- java.text: Utilidades para el manejo de texto.
- java.math: Clases matemáticas y de manipulación de números.

- javax.net: Clases para el manejo de red.
- javax.security: Clases relacionadas a la seguridad.
- javax.xml: Clases para manejo de XML basado en DOM.
- org.apache: Clases relacionadas con HTTP.
- org.xml: Clases para el manejo de XML basado en SAX.

2.2.3.7. Herramientas para el Desarrollo de Aplicaciones

Tabla 1. Herramientas Para el Desarrollo de Aplicaciones

Herramienta	URL
Eclipse (Juno)	**http://www.eclipse.org/downloads**
Java Development Kit (JDK)	**http://java.sun.com/javase/downloads/index.jsp**
Android Software Developer Kit (SDK)	**http://developer.android.com/sdk/index.html**
Android Developer Tool (ADT)	**http://developer.android.com/sdk/eclipse-adt.html**

2.2.4. Java

Es un lenguaje de programación de propósito general, concurrente, orientado a objetos y basado en clases que fue diseñado específicamente para tener tan pocas dependencias de implementación como fuera posible. Su intención es permitir que los desarrolladores de aplicaciones escriban el programa una vez y lo ejecuten en cualquier dispositivo (conocido en inglés como *WORA*, o "*write once, run anywhere*"), lo que quiere decir que el código que es ejecutado en una plataforma no tiene que ser recompilado para correr en otra. Java es, a partir de 2012, uno de los lenguajes de programación más populares en uso,

particularmente para aplicaciones de cliente-servidor de web, con unos 10 millones de usuarios reportados.

Desde la creación de la especificación J2ME (Java 2 Platform, Micro Edition), una versión del entorno de ejecución Java reducido y altamente optimizado, especialmente desarrollado para el mercado de dispositivos electrónicos de consumo se ha producido toda una revolución en lo que a la extensión de Java se refiere.

2.2.4.1. En dispositivos móviles y sistemas empotrados

Es posible encontrar microprocesadores diseñados para ejecutar bytecode Java y software Java para tarjetas inteligentes (JavaCard), teléfonos móviles, buscapersonas, set-top-boxes, sintonizadores de TV y otros pequeños electrodomésticos.

El modelo de desarrollo de estas aplicaciones es muy semejante a las *applets* de los navegadores salvo que en este caso se denominan MIDlets.

2.2.4.2. APIs

Sun define tres plataformas en un intento por cubrir distintos entornos de aplicación. Así, ha distribuido muchas de sus APIs (Application Program Interface) de forma que pertenezcan a cada una de las plataformas:

- Java ME (Java Platform, Micro Edition) o J2ME - orientada a entornos de limitados recursos, como teléfonos móviles, PDAs (Personal Digital Assistant), etc.

- Java SE (Java Platform, Standard Edition) o J2SE - Para entornos de gama media y estaciones de trabajo. Aquí se sitúa al usuario medio en un PC de escritorio.
- Java EE (Java Platform, Enterprise Edition) o J2E - orientada a entornos distribuidos empresariales o de Internet.

Las clases en las APIs de Java se organizan en grupos disjuntos llamados paquetes. Cada paquete contiene un conjunto de interfaces, clases y excepciones relacionadas. La información sobre los paquetes que ofrece cada plataforma puede encontrarse en la documentación de ésta.

El conjunto de las APIs es controlado por Sun Microsystems junto con otras entidades o personas a través del programa JCP (Java Community Process). Las compañías o individuos participantes del JCP pueden influir de forma activa en el diseño y desarrollo de las APIs, algo que ha sido motivo de controversia.

2.2.5. Android SDK

El SDK (Software Development Kit) de Android, incluye un conjunto de herramientas de desarrollo. Comprende un depurador de código, biblioteca, un simulador de teléfono basado en QEMU, documentación, ejemplos de código y tutoriales. Las plataformas de desarrollo soportadas incluyen Linux (cualquier distribución moderna), Mac OS X 10.4.9 o posterior, y Windows XP o posterior. La plataforma integral de desarrollo (IDE, Integrated Development Environment) soportada oficialmente es Eclipse junto con el complemento ADT (Android Development Tools plugin), aunque también puede utilizarse un editor de texto

para escribir ficheros Java y XML y utilizar comandos en un terminal (se necesitan los paquetes JDK, Java Development Kit y Apache Ant) para crear y depurar aplicaciones. Además, pueden controlarse dispositivos Android que estén conectados (es decir, reiniciarlos, instalar aplicaciones en remoto, etc.).

Las actualizaciones del SDK están coordinadas con el desarrollo general de Android. El SDK soporta también versiones antiguas de Android, por si los programadores necesitan instalar aplicaciones en dispositivos ya obsoletos o más antiguos.

Las herramientas de desarrollo son componentes descargables, de modo que una vez instalada la última versión, pueden instalarse versiones anteriores y hacer pruebas de compatibilidad. Una aplicación Android está compuesta por un conjunto de ficheros empaquetados en formato. apk y guardada en el directorio /data/app del sistema operativo Android (este directorio necesita permisos de súper usuario, root, por razones de seguridad). Un paquete APK incluye ficheros. dex (ejecutables Dalvik, un código intermedio compilado), recursos, etc.

2.2.6. Eclipse

Es un entorno de desarrollo integrado (IDE). Contiene una base de espacio de trabajo y una extensible plug-in de sistema para personalizar el entorno. Escrito principalmente en Java, Eclipse se puede utilizar para desarrollar aplicaciones. Por medio de varios plug-ins, Eclipse también se puede utilizar para desarrollar aplicaciones en otra programación lenguajes: Ada, ABAP, C, C++, COBOL,

Fortran, Haskell, JavaScript, Lasso, Natural, Perl, PHP, Prolog, Python, R, Ruby (including Ruby on Rails marco), Scala, Clojure, Groovy, Esquema y Erlang. También se puede utilizar para desarrollar paquetes para el software Matemática. Entornos de desarrollo incluyen las herramientas de desarrollo Eclipse Java (JDT) para Java y Scala, Eclipse CDT para C / C ++ y Eclipse PDT para PHP, entre otros.

2.2.6.1. Arquitectura

Eclipse utiliza plug-ins para proporcionar toda la funcionalidad dentro y en la parte superior del sistema de ejecución. Su sistema de ejecución se basa en Equinox, una implementación de la OSGi especificación marco básico.

Además de permitir la Plataforma Eclipse se extienda el uso de otros lenguajes de programación, como C y Python, el marco de plug-in permite la Plataforma Eclipse para trabajar con lenguajes de composición tipográfica como LaTeX y de las aplicaciones de red, tales como Telnet y sistemas de gestión de base de datos. La arquitectura plug-in admite escribir cualquier extensión deseada con el medio ambiente, como para la gestión de configuración. Java y CVS apoyo se proporciona en el Eclipse SDK, con soporte para otros sistemas de control de versiones proporcionadas por terceros plug-ins.

Con la excepción de un pequeño núcleo en tiempo de ejecución, todo en Eclipse es un plug-in. Esto significa que cada plug-in se integra desarrollado con Eclipse exactamente de la misma manera que otros plug-ins; en este sentido, todas las características son "creados iguales". Eclipse ofrece complementos para una

amplia variedad de características, algunas de las cuales son a través de terceros que utilizan modelos tanto gratuitos como comerciales. Ejemplos de los plug-ins incluyen por UML, para la secuencia y otros diagramas UML, un plug-in para DB Explorer, y muchos otros.

El SDK de Eclipse incluye las herramientas de desarrollo Eclipse Java (JDT), que ofrece un IDE con un built-in incremental compilador Java y un modelo completo de los archivos fuente de Java. Esto permite una avanzada de refactorización técnicas y análisis de código. El IDE también hace uso de un espacio de trabajo, en este caso un conjunto de metadatos en un espacio de archivos plana permitiendo modificaciones de archivos externos, siempre que el correspondiente "recurso" espacio de trabajo se actualiza después.

Eclipse implementos utiliza los elementos de control gráficos del conjunto de herramientas Java llamada SWT, mientras que la mayoría de las aplicaciones Java utilizan el estándar de Java Toolkit Abstract Window (AWT) o swing. Interfaz de usuario de Eclipse también utiliza un compuesto intermedio de interfaz gráfica de usuario de capa llamada JFace, lo que simplifica la construcción de aplicaciones basadas en SWT. Eclipse fue hecho para funcionar en Wayland durante una GSoC -Proyecto en 2014.

Los paquetes de idioma que está desarrollando el proyecto "Babel" proporcionar traducciones en más de una docena de lenguas naturales.

2.2.7. Etiquetas NFC

También conocidas como *Tags* o *transpondedores,* estos dispositivos constan de tres componentes principales, antena, circuito integrado y elemento almacenador de energía. La antena se usa para realizar la comunicación entre la etiqueta y el lector, y se debe tener en cuenta que su tamaño limitará la distancia máxima de lectura.

2.2.7.1. Etiquetas activas

Una etiqueta activa necesita de una pequeña batería que le proporcione alimentación para poder generar y transmitir continuamente la señal de radiofrecuencia donde van codificados y modulados los datos. Pueden ser leídas por lectores que se encuentren a grandes distancias, llegando incluso a los 30 metros, y su capacidad de memoria le permite almacenar Kilobytes de información.

Entre los inconvenientes nos encontramos con las interferencias que se producen con móviles y otros aparatos, su precio que es elevado al requerir la batería y la vida útil de la batería que depende de muchos factores, lo que hace muy difícil prever cuándo ocurrirá un fallo. Otro inconveniente es que su batería en ocasiones se descarga y como consecuencia se produce una pérdida total de la señal.

2.2.7.2. Etiquetas pasivas

No contienen batería, utiliza campos electromagnéticos creados por los lectores que tienen un doble propósito, ya que a la vez obtienen información de ellas. La distancia de lectura de una etiqueta pasiva puede llegar hasta los 5 y 7 metros. Al

trabajar con pequeños niveles de energía, tienen una capacidad de memoria relativamente baja.

Presentan una gran ventaja sobre las etiquetas activas en cuanto a precio por unidad, por lo que se usan en más aplicaciones. De una manera gradual, a medida que el precio disminuye, entran en competencia con los códigos de barras.

2.3. HIPÓTESIS A CONTESTARSE

¿El uso de dispositivos móviles con NFC crea una plataforma ideal para llevar credenciales de identidad para autenticar al titular del dispositivo?

¿Se podrá consolidar este sistema en el mercado como mecanismo de validación de identidad a través de NFC?

¿Proporciona más ventajas a los empleados autenticar su identidad a través del teléfono móvil?

2.4. VARIABLES DE INVESTIGACIÓN

Con la tecnología NFC se puede interactuar con dispositivos móviles, a través de interfaces que hacen posible enlazar las aplicaciones con el usuario.

Tabla 2. Variables de La Investigación

Variables De La Investigación	
VARIABLES	**COMPONENTES**
Control de acceso de operaciones relacionadas con la identidad.	% Control de identidad.
Alternativa tecnológica de autenticación.	Avance tecnológico de los dispositivos móviles.
Uso de tecnología NFC.	Tecnología de comunicación Inalámbrica.

Elaboración: Christian Cogollo
Fuente: Christian Cogollo

3. MARCO METODOLÓGICO

3.1. BREVE DESCRIPCIÓN DEL MÉTODO

El proyecto propone una solución usando tecnología NFC en una solución móvil para la identificación y control de tiempo de entrada y salida de los usuarios. Para esto primero se realiza un proceso de investigación y estado del arte de esta tecnología para proponer la solución del prototipo del sistema final a desarrollar.

El tipo de investigación que se desarrollara es una investigación cuantitativa y descriptiva. El proyecto tiene el planteamiento del problema definido al igual que los objetivos, y se considera descriptiva porque pretende describir el estado y las características de las tecnologías NFC.

3.2. RELACIÓN DE SUS CARACTERÍSTICAS CON LAS NECESIDADES PARTICULARES DEL PROYECTO

La finalidad del método consiste en obtener información sobre las ventajas de utilizar dispositivos móviles con tecnología NFC como mecanismo de control de usuarios para el acceso al sitio de trabajo, cumplimiento de horarios, acceso digital.

Para el cumplimiento de los objetivos y resultados de la investigación se realizará en varias fases, inicialmente al estudio de cómo funciona y como se usa, que problemas se encuentra, ventajas y desventajas de esta tecnología, luego se

aplicará el conocimiento al problema planteado y se usará una metodología de desarrollo de software para la creación del prototipo funcional. Finalmente se pasará a la fase de pruebas y documentación de los resultados obtenidos en la investigación y se socializará el proyecto ante la comunidad académica.

3.3. TÉCNICA DE MUESTREO

Como parte del estudio se realizará una encuesta dirigida a empleados de la Clínica de Traumas y Fracturas de la ciudad de Montería. El objetivo de la encuesta es evaluar la confiabilidad de los usuarios sobre el concepto de la tecnología de comunicación NFC, además si conocen las características y beneficios que les brindan los dispositivos inteligentes.

La población de estudio son empleados de la clínica de traumas y fracturas de la ciudad de Montería.

Fórmula Utilizada: $n = m / (e^2 (m-1) +1)$

m= tamaño de la población 50 de empleados de la clínica de traumas y fracturas de la ciudad de montería.

E= error de estimación 5%

$n = m / (e^2 (m-1) +1)$
$n = 50 / 0.05^2(50-1) +1$
$n = 44,54$

Para el cálculo de la fracción de la muestra, se utilizará:

$$f = n / N = 44,54 / 500 = 0.8908$$

Tabla 3. Población y Muestra

	Población	**Muestra**
Usuarios con móvil	292	78%
Usuarios con Smartphone con NFC	83	22%
Total	**375**	**100%**

Elaboración: Christian Cogollo
Fuente: Christian Cogollo

3.4. OPERACIONALIZACIÓN DE VARIABLES

Tabla 4. Matriz Operacionalización de variables

Matriz Operacionalización De Variables			
Variables	**Dimensiones**	**Indicadores**	**Técnicas y/o Instrumentos**
Control de acceso de operaciones relacionadas con la identidad.	Población de empleados de clínica de traumas y fracturas.	Porcentaje de empleados que utilizan celulares con NFC.	Encuesta. Resúmenes de Textos seleccionados.
	Controles de acceso de los empleados de la Clínica de traumas y Fracturas.	Porcentaje de empleados que se registran el acceso con biometría en la Cínica de Traumas y Fracturas.	Texto seleccionado. Bibliografía especializada.
	Controles de horarios de los empleados de la Clínica de traumas y Fracturas.	Porcentaje de empleados que cumplen con los horarios establecidos.	Encuesta Gráficas.
Alternativa tecnológica de autenticación.	La tendencia de utilizar el dispositivo móvil para la actividad cotidiana y como nueva forma control de acceso.	Porcentaje de satisfacción sobre las ventajas de utilizar dispositivos móviles con tecnología NFC.	Bibliografía Especializadas
	Uso de la tecnología de comunicación inalámbrica NFC.	Distancia de enlace de conexión entre los dispositivo.	Texto Seleccionado
	La aceptación del S/O en el mercado mundial con NFC.	de Tecnología Android con NFC en el Mercado Mundial.	Gráficas, Texto Seleccionado.
Uso de tecnología NFC.	Manejo de Estándares de Seguridad	% Fiabilidad y seguridad mediante códigos de Acceso.	Gráficas, Texto Seleccionado
	Manejo de Normas Internacionales de Calidad.	Las Principales características de los Estándares y normas ISO /IEC 14443 e ISO/IEC 18092.	Bibliografía Especializadas
	Reglamentos y referentes a la utilización de tarjetas de crédito que dispone el proveedor.	Numero de Acuerdos que tienen el proveedor y el usuario acerca del uso de tarjeta de crédito.	Bibliografía seleccionada. Encuesta.

Elaboración: Christian Cogollo
Fuente: Christian Cogollo

3.5. SECUENCIA DESCRIPTIVA DE PASOS

La secuencia para aplicar el método es la siguiente:

1. Recolección de bibliografía necesaria para la investigación.
2. Diseño de la encuestas y entrevistas.
3. Recolección de datos.
4. Análisis de resultados.
5. Desarrollo de prototipo para el cliente y para el servidor.
6. Realizar pruebas de funcionamiento y comportamiento del servidor en función de validación de usuarios, el almacenamiento correcto de la información de control en la base de datos SQlite.
7. Análisis de los datos de laboratorio.
8. Generación de las gráficas.

3.6. DISEÑO DE INSTRUMENTOS

Las técnicas de recolección de datos que se aplicaran en la investigación de este proyecto son:

Documentales

- Lectura científica para formar conocimientos relativos al tema de estudio se utilizarán como instrumentos para obtener información la Internet, además de la extensa bibliografía que se detalla más adelante en este documento.

De campo

- La indagación directa: técnica que fue utilizada para comprobar a través del desarrollo de aplicaciones el funcionamiento y las características de los componentes que nos brinda la tecnología NFC.
- Encuesta: esta técnica se utilizó para tener principalmente una perspectiva sobre las plataformas que utilizan los desarrolladores, lo que conlleva a conocer la apertura que tienen en nuestro mercado. Como instrumento se desarrollará un pequeño cuestionario de preguntas.

3.7. TÉCNICA POR USAR PARA LA RECOPILACIÓN DE DATOS

Las técnicas principales que ayudarán a culminar con éxito la investigación será la recolección de información bibliográfica. Se hace necesario acudir al Internet para buscar, recopilar la información necesaria acerca de la Tecnología NFC, para poder cumplir con los objetivos planteados. La investigación bibliográfica servirá para proporcionar conocimientos de investigaciones ya existentes acerca de la tecnología NFC y pueden servir para realizar el análisis de factibilidad sobre la misma.

3.8. PROCESAMIENTO Y ANÁLISIS

Después de haber recolectado toda la información esta será procesada para su posterior análisis y los resultados obtenidos serán presentados de forma tabulada y graficada.

3.9. CRITERIOS PARA LA ELABORACIÓN DE LA PROPUESTA

Las elaboraciones de la propuesta para la construcción del prototipo fueron considerados varios puntos importantes, los cueles fueron tema de estudio, entre los que se pueden citar el tema de la seguridad que utiliza la tecnología, el radio de alcance de la comunicación, la tasa trasferencia de datos, la infraestructura necesaria y el margen de adquisición de dispositivos de alta gama.

3.10. CRITERIOS PARA LA VALIDACIÓN DE LA PROPUESTA

La propuesta será aprobada por el personal idóneo quien a su juicio evaluará y dará las recomendaciones necesarias, se realizará un análisis respectivo teniendo en cuenta lo sugerido y por último se realiza el diseño del prototipo.

3.11. RESULTADOS DEL CUESTIONARIO

Pregunta 1.

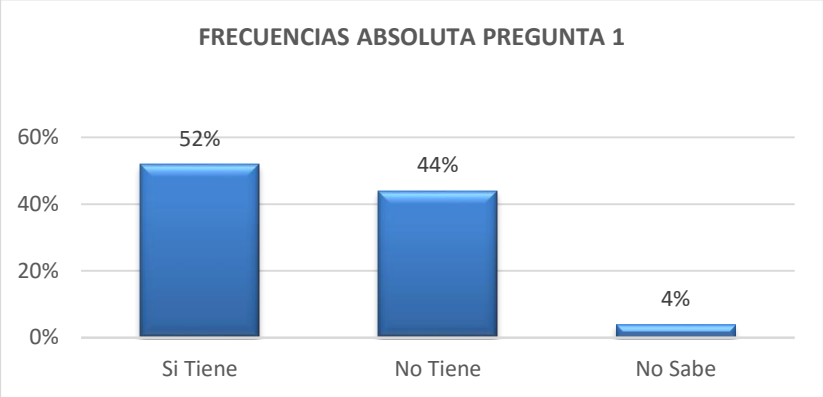
¿Usted tiene teléfono celular de tipo Smartphone?

Tabla 5. Frecuencia Absoluta Pregunta 1

Frecuencias Absoluta Pregunta 1			
Variable	**Fr. Absoluta**	**Fr. Relativa**	**Porcentaje**
A	26	0,52	52%
B	22	0,44	44%
C	2	0,04	4%
TOTAL	**50**	**1**	**100%**

Elaboración: Christian Cogollo
Fuente: Investigación

Ilustración 3. Frecuencias Absoluta Pregunta 1



Elaboración: Christian Cogollo
Fuente: Investigación

Análisis. Según el resultado de la encuesta, entre los empleados de la clínica de traumas y fracturas, el 52% posee un Smartphone. Es un índice alto que se tiene ya que por los costó de estos dispositivos hace que las muchas personas opten por comprar equipos de gama baja que los cuales no cuentan con esta tecnología.

Pregunta 2.

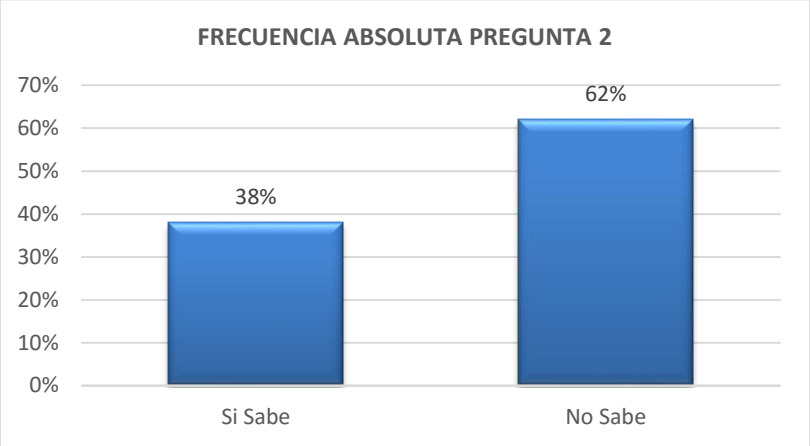
¿Sabe que es tecnología NFC y que utilidad tiene?

Tabla 6. Frecuencia Absoluta Pregunta 2

Frecuencia Absoluta Pregunta 2			
Variable	**Fr. Absoluta**	**Fr. Relativa**	**Porcentaje**
A	19	0,38	38%
B	31	0,62	62%
TOTAL	**50**	**1**	**100%**

Elaboración: Christian Cogollo
Fuente: Investigación

Ilustración 4. Frecuencia Absoluta Pregunta 2



Elaboración: Christian Cogollo
Fuente: Investigación

Análisis. Según, el resultado de la encuesta, el 38% de los empleados de la clínica de traumas y fracturas, no saben que es ni para que se usa, esto se debe básicamente a que el 62% de los encuestados no poseen Smartphone o no están relacionados con toda la tecnología que posee su teléfono.

Pregunta 3.

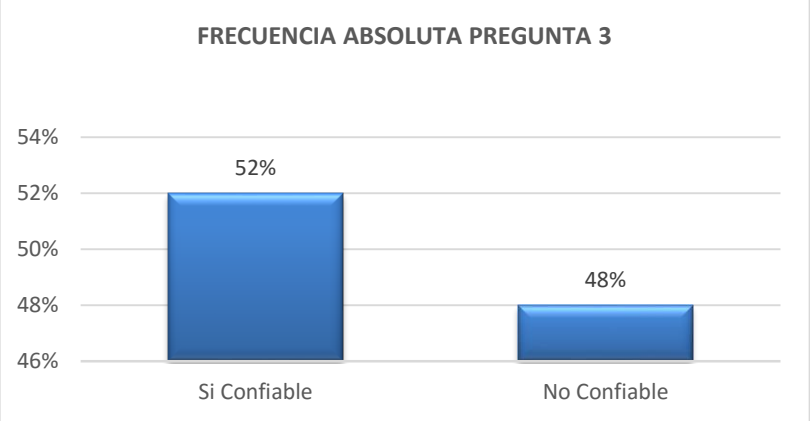
¿Considera confiable los medios de control de acceso utilizados en su lugar de trabajo?

Tabla 7. Frecuencia Absoluta Pregunta 3

Frecuencia Absoluta Pregunta 3			
Variable	**Fr. Absoluta**	**Fr. Relativa**	**Porcentaje**
A	26	0,52	52%
B	24	0,48	48%
TOTAL	**50**	**1**	**100%**

Elaboración: Christian Cogollo
Fuente: Investigación

Ilustración 5. Frecuencia Absoluta Pregunta 3



Elaboración: Christian Cogollo
Fuente: Investigación

Análisis. Según, el resultado de la encuesta, el 52% de los empleados de la clínica de traumas y fracturas, considera que los controles empleados en la seguridad actual son confiables, mientras el 48% restantes lo considera no confiables esto se debe a las limitantes que perciben en los controles actuales.

Pregunta 4

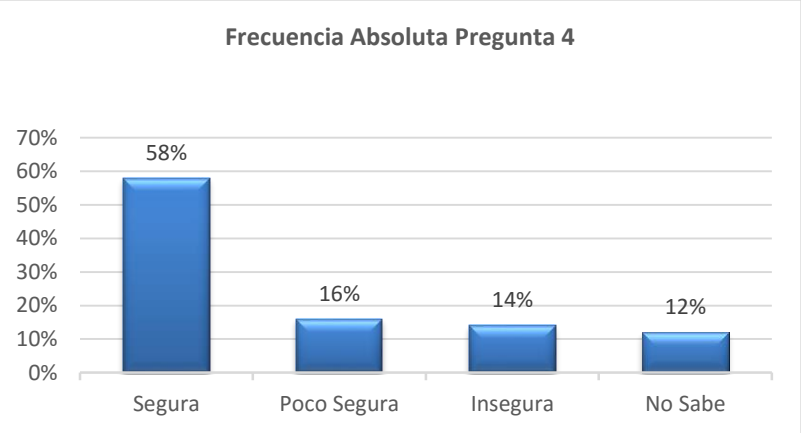
¿Cree que un Smartphone es una plataforma segura para llevar credenciales de identidad y utilizarlas como medio de autenticación?

Tabla 8. Frecuencia Absoluta Pregunta 4

Frecuencia Absoluta Pregunta 4			
Variable	**Fr. Absoluta**	**Fr. Relativa**	**Porcentaje**
A	29	0,58	58%
B	8	0,16	16%
C	7	0,14	14%
D	6	0,12	12%
TOTAL	**50**	**1**	**100%**

Elaboración: Christian Cogollo
Fuente: Investigación

Ilustración 6. Frecuencia Absoluta Pregunta 4



Elaboración: Christian Cogollo
Fuente: Investigación

Análisis. Según, el resultado de la encuesta, el 58% de los empleados de la clínica de traumas y fracturas, considera que es confiable el uso del teléfono celular como herramienta de autenticación, mientras que el porcentaje restante tiene cierta resistencia a confiar en este tipo de tecnología para este uso.

Pregunta 5.

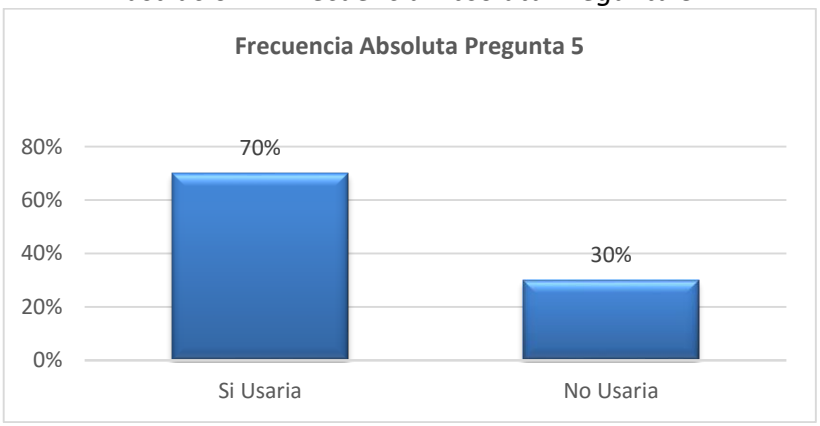
¿Estaría dispuesto a usar un Smartphone como medio de autenticación en su lugar de trabajo?

Tabla 9. Frecuencia Absoluta Pregunta 5

Frecuencia Absoluta Pregunta 5			
Variable	**Fr. Absoluta**	**Fr. Relativa**	**Porcentaje**
Si	35	0,70	70%
No	15	0,30	30%
TOTAL	**50**	**1**	**100%**

Elaboración: Christian Cogollo
Fuente: Investigación

Ilustración 7. Frecuencia Absoluta Pregunta 5



Elaboración: Christian Cogollo
Fuente: Investigación

Análisis. Según, el resultado de la encuesta, el 70% de los empleados de la clínica de traumas y fracturas estarían dispuesto a usar su teléfono como medio de autenticación, mientras el 30% restante no lo haría debido a que no consideran que es seguro este medio.

3.12. RESULTADOS ESPERADOS

Con este proyecto se espera llegar a obtener los siguientes resultados.

1. Documento resumen de la caracterización de la tecnología NFC en dispositivos móviles para la autenticación de usuarios.
2. Documento explicativo de la arquitectura y plataforma necesarias para la implementación.
3. Prototipo de sistema validador de usuarios utilizando tecnología NFC.

4. Resultado de la evaluación de funcionalidad del prototipo.
5. Artículo que describa el resultado de la experiencia del proyecto.

4. MARCO ADMINISTRATIVO

4.1. ACTIVIDADES Y CRONOGRAMA

A continuación, se describen las diferentes actividades descritas por fases necesarias para cumplir con los objetivos propuestos.

4.1.1 Fase de Planeación

- Investigación y formulación del problema.
- Definir marco teórico.
- Formular objetivos.
- Investigación del estado de arte.
- Creación del documento del Proyecto.

4.1.2. Fase de Recolección de Información

- Investigación y documentación de tecnología NFC y Android.
- Investigación y documentación de arquitecturas para desarrollo en móviles.
- Investigación de implementaciones de sistemas de control de usuarios.

4.1.3. Fase de Documentación en NFC

- Definir funcionamiento de la tecnología NFC.
- Documentar dicho funcionamiento.
- Investigar y documentar aplicaciones realizadas con estas dos tecnologías a nivel mundial.
- Documentar ventajas del uso de la tecnología NFC.

- Definir las problemáticas encontradas.
- Definir las ventajas de esta tecnología.
- Listar posibles aplicaciones a desarrollar.

4.1.4. Fase de Desarrollo

Para el desarrollo del prototipo usaremos una metodología de desarrollo de software que nos permita hacer un desarrollo ágil, ligero, basándonos en buenas prácticas para cumplir los objetivos y aumentar la productividad a la hora de desarrollar.

Se basa en una serie de metodologías de desarrollo de software en la que se da prioridad a los trabajos que dan un resultado directo y que reducen la burocracia que hay alrededor de la programación. EXtremeProgramming, puede dividirse en cuatro principios sobre los que se va iterando hasta que el proyecto ha finalizado (el cliente aprueba el proyecto). Estas fases o principios son planificación, diseño, desarrollo y pruebas.

4.1.5. Fase de instalación de Software

- Configuración de servidor de base de datos.
- Instalación del aplicativo en los celulares.
- Fase de Pruebas.
- Pruebas del aplicativo en el celular.
- Pruebas de los servicios.
- Pruebas del aplicativo en terreno de campo.

4.1.6. Fase de documentación

- Elaboración de documento final.
- Revisión de objetivos cumplidos.
- Conclusiones finales.
- Socialización del proyecto y demostración del aplicativo.

4.2. CRONOGRAMA DE ACTIVIDADES

El tiempo estimado para realizar cada tarea se estipula en semanas; se presentan algunas tareas que se solapan ya que se pueden trabar en paralelo, en la siguiente tabla se muestra la planificación planteada.

Mes / Semanas	Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre			
Actividad	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Fase 6.1																																				
Fase 6.2																																				
Fase 6.3																																				
Fase 6.4																																				
Fase 6.5																																				
Fase 6.6																																				

4.3. PRESUPUESTO Y RECURSOS NECESARIOS

El coste todos los componentes necesarios, ordenadores, teléfonos móviles documentación se ve reflejado en la siguiente tabla:

Tabla 10. Presupuesto y Recursos Necesarios

Material	Cantidad	Costo	Valor Total
Ordenador	1	$1.500.000	1.500.000
Dispositivo móvil con tecnología NFC	1	$700.000	$700.000
Papelería (resma tamaño carta)	1	$7.000	$7.000
Materiales e Insumos	1	$170.000	170.000
Transporte	1	$200.000	$200.000
Imprevistos	1	$300.000	$300.000
Total		**$2'887.000**	**$2'887.000**

Como el proyecto es basado en software libre se utilizarán entornos de desarrollo libre, gracias a esto podemos reducir costos

4.3.1. Recursos Tecnológicos

Tabla 11. Recursos Tecnológicos

Recursos	Cant	Costo	Total
Ordenador	1	$1.500.000	$1.500.000
Dispositivo móvil con tecnología NFC	1	$700.000	$700.000
Api Desarrollo Android	1	0	0
S.O. Android	1	0	0
Total Recursos			**$2'200.000**

4.3.2. Recursos Académicos

Tabla 12. Recursos Académicos

LIBRO	Valor
Communications Handbook (Internet and Communications) [Hardcover] Syed A. Ahson (Editor), Mohammad Ilyas (Editor)	$ 250.000
Professional Android 4 Application Development (Wrox Professional Guides) by Reto Meier (May 1, 2012)	$ 120.000
Total	**$370.000**

4.3.3 Recursos Humanos

Tabla 13. Recursos Humanos

Investigador	Formación Académica	Función	Horas semana	Financiación Entidad	Financiación Otras fuentes
Freddy Méndez Ortiz	Maestría/ Docente	Director	--	UNAB	$1’000.000 *9meses
Christian Cogollo López	Estudiante Postgrado	Investigador/ Desarrollador	10	--	Propios 450.000 * 9meses
Total					**$14’500.000**

4.4.4 Total de Recursos

Tabla 14. Total de Recursos

Recurso	Valor
Recursos Tecnológicos	$2’200.000
Recursos Académicos	$370.000
Recursos Humanos	$14’500.000
TOTAL	**$16’620.000**

5. RESULTADOS DEL PROTOTIPO

5.1. DISEÑO DE LA APLICACIÓN MÓVIL

Este capítulo trata de la elección de la tecnología requerida para la construcción de la aplicación, diseño de base de datos, sistema operativo móvil y herramientas de trabajo.

5.1.1. Elección de las Herramientas de Trabajo

La intención de la aplicación es poder validar las credenciales de identidad de los empleados la cual está contenida en una base de datos, valiéndonos de las terminales móviles de los usuarios y el dispositivo lector NFC.

El dispositivo lector es encargado de enviar los datos al servidor de base de datos, en donde se validad la identidad y retorna la confirmación de autenticación o denegando la identidad, para este caso como es un prototipo el lector y servidor de bases están integrados en un mismo dispositivo.

A continuación, se hará el análisis y justificación de tecnología y herramientas requeridas para conseguir los objetivos.

Entre las características de NFC podemos destacar

- Mejora de la experiencia de usuario
- Paradigma “ABC” (Always Best Connected)
- Añade múltiples facilidades a la vida diaria

  - Interacción con el medio
  - Notificación de ofertas
  - Pago con móvil
  - Identificación
- NFC: tecnología en crecimiento
  - Grandes compañías
  - Comunidad científica
- Compatibilidad de NFC con tecnologías equivalentes: RFID
- Bridging the physical and the virtual worlds.

5.1.1. Sistema operativo para móvil, entorno de desarrollo y base de datos

En el apartado anterior se explicó las razones por la cuales se escogió la tecnología NFC como tecnología de comunicación para acceder a los datos de autenticación.

Ahora apuntamos a la escogencia del sistema operativo para móviles que usaremos como plataforma principal, recordemos que al usar Java como lenguaje de programación para el desarrollo, se tiene la ventaja que la aplicación es multiplataforma y al realizar un análisis comparativo los sistemas operativos más destacados para móvil, se puede decir que iOS no soporta la tecnología NFC y solo tiene un 13% del mercado en comparación que Android, Windows Phone y BlackBerry OS que si soportan NFC y con un mercado de 86%, pero sin ninguna

duda que Android es el más distribuido, el solo cuenta con un 81%, también se tuvo en cuenta que está basado en Linux y es libre.

Como ya se mencionaba el lenguaje de desarrollo es Java con el cual se puede desarrollar aplicaciones nativas para Android y como entorno de desarrollo usaremos Eclipse Juno y Android SDK, en cual podemos desarrollar la aplicación multiplataforma.

Para la gestión de datos se utilizó SQLite que es un sistema de gestión de base de datos relacional de código abierto, gratuito y gran rendimiento para transacciones y consultas.

5.1.2. Estructuración de la Aplicación Móvil

La aplicación o prototipo desarrollado tiene como función de consultar las credenciales de identidad de los usuarios en base a lectura del dispositivo lector el cual consultara en la base de datos.

El comportamiento del sistema enfocado desde el punto de vista de usuario, la función principal es obtener las características generales del sistema y conseguir la totalidad de funciones que el sistema puede ejecutar.

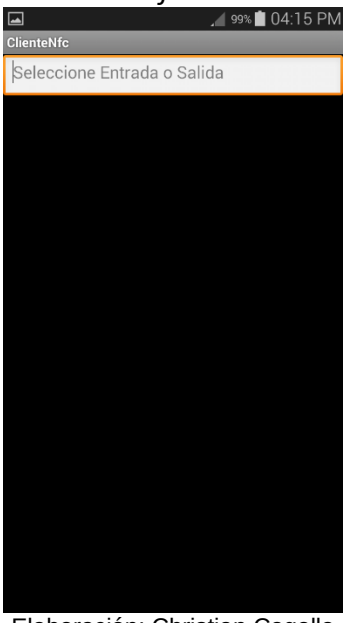
Los mockups que son las representaciones gráficas de la planificación de las vistas de una aplicación q e ayudan a tener un marco de referencia al momento de programar las interfaces y darles funcionalidad y las especificaciones de la aplicación.

5.1.3. Aplicación de Cliente

Esta es la aplicación cliente la cual se encuentra instalada en el dispositivo móvil y es aquella que se muestra cuando iniciamos la aplicación y realiza la consulta a la base de datos, para realizar la búsqueda en la base de datos se necesita un dato importante, el cual es único para cada usuario.

En las siguientes imágenes observamos la interfaz de inicio donde se solicita al usuario que marque entre entrada y salida, seguidamente las imágenes donde el usuario escoge entre entrada salida, para hacerlo más ilustrativo se visualiza la identificación del usuario acompañado del evento escogido por el usuario.

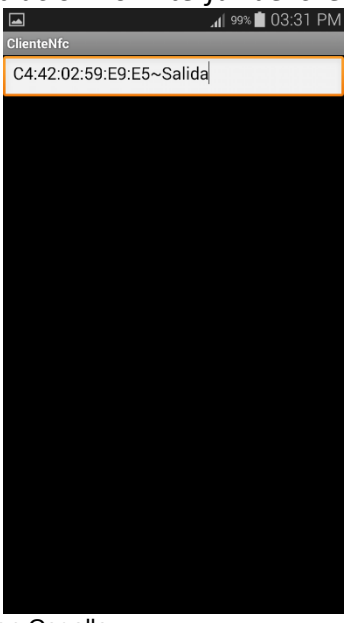
Ilustración 8. Interfaz inicial del cliente



Elaboración: Christian Cogollo
Fuente: Christian Cogollo

Ilustración 9. Interfaz del cliente.

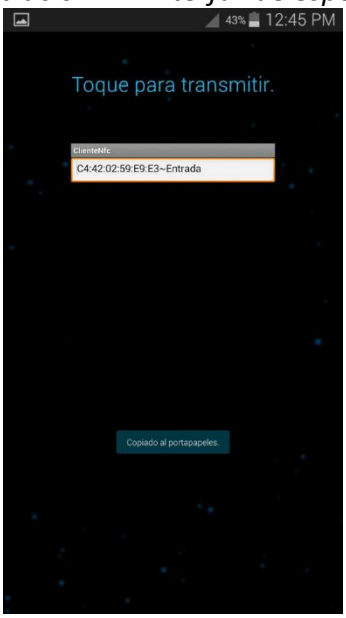
Ilustración 10. Interfaz del cliente.



Elaboración: Christian Cogollo
Fuente: Christian Cogollo

La interfaz de espera es aquella que se genera cuando la aplicación a través del terminal móvil ha tenido contacto con el lector NFC. Se obtienen los datos del cliente y se realiza la consulta a la base de datos para validar la identidad. En caso sea positivo, se devuelve la información al móvil, caso contrario, de lanza la interfaz de error y se pone a la aplicación en estado de espera para la siguiente lectura.

Ilustración 11. Interfaz de espera.



Elaboración: Christian Cogollo
Fuente: Christian Cogollo

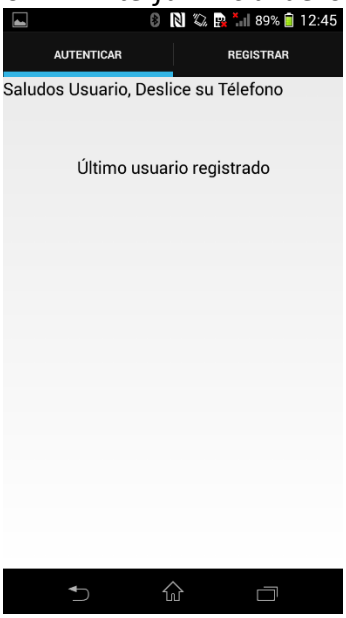
5.1.4. Aplicación Servidor

La aplicación servidor se encuentra instalado en el dispositivo lector es la encargada de validar las credenciales enviadas por el cliente y constatarla con la almacenada en la base de datos, si la validación es correcta realiza los registros de entrada o salida correspondientes al usuario y se es erróneo invalidando al usuario.

Se utiliza en la base de datos un campo para almacenar la identidad que identifica a cada usuario de forma única.

A continuación, las gráficas muestran la interfaz inicial de la aplicación.

Ilustración 12. Interfaz inicial del servidor.



Elaboración: Christian Cogollo
Fuente: Christian Cogollo

Interfaz de validación y confirmación, esta se muestra al usuario registrado, así como la fecha y hora del registro.

Ilustración 13. Interfaz de validación y confirmación de usuario a la entrada.

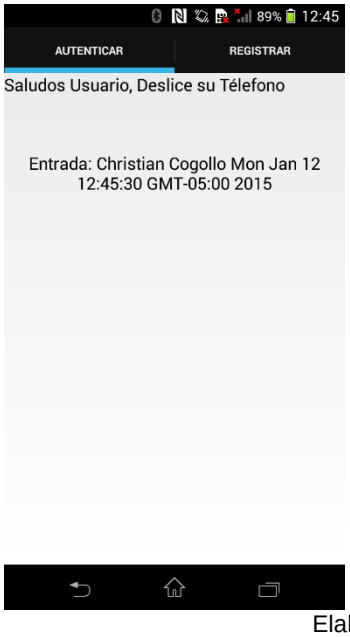
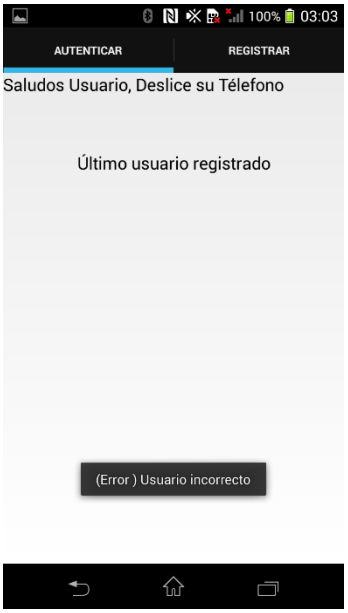


Ilustración 14. Interfaz de validación y confirmación de usuario a la salida.

Elaboración: Christian Cogollo
Fuente: Christian Cogollo

La interfaz de error, esta interfaz es generada ante una consulta fallida a la base de datos ya sea porque esta no se encuentra habilitada o porque la información obtenida del cliente NFC no está existe en la base de datos. En esta interfaz podemos volver a escanear el cliente NFC para una segunda consulta de información.

Ilustración 15. Interfaz del error al validad un usuario no registrado.



Elaboración: Christian Cogollo
Fuente: Christian Cogollo

Ilustración 16. Interfaz de registro de usuario.

Elaboración: Christian Cogollo
Fuente: Christian Cogollo

5.1.5. Funcionamiento de la Aplicación

En este punto ya está realizada la aplicación cliente que permite trabajar con las funcionalidades del lector. Ahora ya se puede pasar a tratar de conseguir los objetivos propuestos: Realizar una aplicación de autentificación.

Cuando la aplicación solicita información restringida, el servidor le responde que la autenticación es necesaria y al recibir esta respuesta, la aplicación abre una conexión ISO14443 al elemento seguro para solicitarle la contraseña y este la devuelve correctamente demostrando así el correcto funcionamiento de las conexiones al elemento seguro.

5.1.6. Funcionamiento de la Base de Datos

Las conexiones a la Base de Datos se realizan para autenticar al usuario y/o registro de información de usuario. Cuando un usuario envía la contraseña cifrada obtenida de su elemento seguro, es enviada a la Base de Datos para comprobar si es válida o no en función de la respuesta de la Base de Datos. La conexión entre la Base de Datos y el aplicativo cliente funciona correctamente, verificando así la funcionalidad de ambos.

El dispositivo móvil que tiene la aplicación servidor y la base de datos local que contienen los datos de usuario y la comprobación están en la misma máquina. Los datos del usuario están en el dispositivo cliente, pero la base de datos donde se realiza la autentificación está en el dispositivo servidor.

5.1.7. Modo de uso

Para ello la aplicación en el terminal móvil dispondrá de 2 modos de funcionamiento: Registro y login. El primero de ellos se encarga la primera vez de que el móvil sea registrado en el sistema. Posteriormente, la aplicación de cliente permitirá a todo el usuario con su terminal registrado acceder a su cuenta de usuario.

5.1.8. Protocolo de autentificación

Se definen los siguientes protocolos de funcionamiento de la aplicación. En el caso de registro:

En el primer intercambio se envían los identificadores de la conexión que se envía desde el móvil para señalar que se trata de un teléfono móvil con la aplicación de registro preparada. En el otro extremo, el dispositivo lector envía para indicar que se trata del dispositivo lector con la aplicación de registro. Ambos elementos deben comprobar que se trata de la aplicación correcta. Una vez comprobado, el dispositivo cliente envía la clave correspondiente que serán utilizadas en la aplicación del cliente. Serán guardadas en la memoria del dispositivo. Desde el móvil se envía la mac como identificador del móvil. En este punto el dispositivo guarda en su base de datos la mac que le corresponde y que sirven para autenticarse. Finalmente, si todo ha ido bien se envía un mensaje de confirmación para finalizar la comunicación.

5.2. PROYECTOS Y CLASES DESARROLLADAS

Proyecto Cliente

Clase ClienteNfc

android.app.Activity

android.app.AlertDialog

android.app.PendingIntent

android.content.Context

android.content.DialogInterface

android.content.Intent

android.content.IntentFilter

android.content.IntentFilter.MalformedMimeTypeException

android.net.wifi.WifiInfo

android.net.wifi.WifiManager

android.nfc.NdefMessage

android.nfc.NdefRecord

android.nfc.NfcAdapter

android.nfc.Tag

android.nfc.tech.Ndef

android.nfc.tech.NdefFormatable

android.os.Bundle

android.os.Parcelable

android.text.Editable

android.text.TextWatcher

android.util.Log

android.view.KeyEvent

android.view.View

android.widget.EditText

android.widget.Toast

Proyecto Servidor

Para el servidor se implementaron 3 clases principales clase Autenticar_Empleado, class Registro_empleado, clase ServidorNf.

Clase ServidorNfc

android.app.Activity

android.os.Bundle

android.view.Menu

android.view.MenuItem

android.support.v4.app.Fragment

android.support.v4.app.FragmentManager

android.support.v4.app.FragmentTransaction

android.support.v7.app.ActionBar

android.support.v7.app.ActionBar. Tab

android.support.v7.app.ActionBar. TabListener

android.support.v7.app.ActionBarActivity

Clase Registro Empleado

Componentes.Persistencia.UsuarioAsistencia

android.content.ContentValues

android.database.Cursor

android.database.sqlite.SQLiteDatabase

android.os.Bundle

android.support.v4.app.Fragment

android.view.LayoutInflater

android.view.View

android.view.ViewGroup

android.widget.Button

android.widget.EditText

android.widget.Toast

Autenticar Empleado

Componentes.Persistencia.UsuarioAsistencia

android.annotation.SuppressLint

android.app.Activity

android.app.PendingIntent

android.content.ContentValues

android.content.Intent

android.content.IntentFilter

android.content.IntentFilter.MalformedMimeTypeException

android.database.Cursor

android.database.sqlite.SQLiteDatabase

android.nfc.NdefMessage

android.nfc.NdefRecord;

android.nfc.NfcAdapter

android.nfc.Tag

android.os.Bundle

android.os.Parcelable

android.support.v4.app.Fragment

android.util.Log

android.view.LayoutInflater

android.view.View

android.view.ViewGroup

android.widget.TextView

android.widget.Toast

5.3. RESULTADOS DE EVALUACION DE FUNCIONAMIENTO

Para el aplicativo móvil las pruebas en este caso se enfocaron en veinte empleados. Se evaluará que el aplicativo sea de uso sencillo e intuitivo, y cumpla con la autenticación de manera inmediata. Los resultados se muestran a continuación.

Tabla 15. Resultado de pruebas

Muestra	Éxito	Fracaso	Tiempo Promedio (Seg)	Porcentaje de éxito
375	285	90	3	76%

Elaboración: Christian Cogollo
Fuente: Investigación

Los resultados respecto a la aplicación móvil fueron que de las veinte personas que probaron la aplicación, quince tuvieron éxito en lograr escanear con el cliente NFC y desplegar la información en el celular rápidamente, el tiempo aproximado

entre todo el proceso fue 60 segundos. Aquellos que no pudieron lograr el objetivo fueron adultos mayores que no tienen mucha experiencia con Smartphone.

6. CONCLUSIONES

Con el desarrollo de este proyecto se evaluó la viabilidad de implementar un sistema de control para la autenticación de usuarios, desarrollando un prototipo para este proceso el cual implica utilizar teléfonos móviles con la aplicación de tecnologías de comunicación de campo cercano NFC la cual trae consigo muchos beneficios.

La aplicación móvil desarrollada cuenta con dos módulos uno cliente o aplicación de cliente y otra para servidor que se instaló en el dispositivo recetor, esto nos ha permitido evidenciar todo el potencial y alcance que podemos obtener con la tecnología NFC, además nos ha permitido proyectar nuevas posibilidades como utilizar este mismo mecanismo para obtener acceso a cuentas de usuarios y sirva de login en computadora; gracias al uso de base de datos donde se almacenan todos los registros podemos contar con una mejor administración de los datos y no tendremos el problema de capacidad en espacio en los sistemas de reconocimiento de huella actuales con que cuenta la compañía.

Otras características que podemos citar:

Es multiplataforma, gracias a que fue desarrollado con java.

Tiene la posibilidad a llegar a integrase en aplicaciones web.

El uso de esta tecnología es un poco costoso ya que los dispositivos móviles que la traen son de gama alta, se espera que con el tiempo y la difusión de la tecnología su coste baje.

La ventaja de utilizar Java para el desarrollo es que nos permite crear aplicaciones nativas para Android, por lo que son mucho más rápidas de ejecutar en los dispositivos, que las desarrolladas con otras tecnologías como por ejemplo PhoneGap; a su vez fue uno de los

mayores inconvenientes para el desarrollo ya que para esto se debe contar con un conocimiento previo del lenguaje y del entorno de desarrollo Eclipse o Android estudio.

El uso de esta tecnología nos brinda mucha seguridad gracias al corto alcance al campo de operación.

Tecnología más segura que RFID.

- NFC se desactiva al bloquear la pantalla.

NFC no sustituye a otras tecnologías, es complementaria:

- Bluetooth Secure Simple Pairing Using NFC.
- Autenticación a una red WiFi

Mejora de la experiencia de usuario.

Todas las plataformas móviles comienzan a integrarlo

- Nokia, Android, Windows Phone, iOS?

Tecnología en constante crecimiento

- Periodo de adaptación largo: educar al usuario.

7. RECOMENDACIONES Y TRABAJOS FUTUROS

7.1. Recomendaciones

Basados en el presente documento se proponen las siguientes recomendaciones.

- Realizar una búsqueda exhaustiva con proveedores sobre los dispositivos requeridos para la comunicación vía NFC para poder tener un manejo apropiado de los costos que beneficie tanto a la compañía como empleados.
- Impulsar implementación en otras organizaciones que quiera modernizar sus sistemas de control para la autenticación de usuarios, se pueden aprovechar ciertos puntos los cuales podrán ayudar en el desarrollo de este tema.
- Se puede citar la necesidad de indagar en el uso de nuevas metodologías de control y seguridad con el uso de la tecnología NFC y adaptarlas al entorno requerido.

7.2. Trabajos futuros

Sobre la aplicación de servidor aún existe trabajo por hacer, ya que solo se desarrolló el prototipo para la evaluación de llevar a cabo la implementación, entre los puntos desarrollar se encuentran los siguientes.

- Ampliar el desarrollo de base de datos donde se utilizaría un motor más robusto que SQlite en un servidor de datos, en el cual se conectaría la aplicación del dispositivo lector NFC el cual autenticaría las credenciales con la información almacenada y guardaría los registros de los usuarios.

- También se puede ampliar el sistema para aplicaciones como validación electrónica de visitantes y familiares de pacientes.
- Desarrollar una aplicación web para la administración sistema de una forma más amigable.

BIBLIOGRAFÍA

(1) Chavarría Daniel Antonio. (2011). *Tecnología de comunicación de campo cercano (NFC) y sus aplicaciones*. Universidad de Costa Rica, Facultad de Ingeniería, Escuela de Ingeniería Eléctrica, Costa Rica. http://eie.ucr.ac.cr/uploads/file/proybach/pb2011/pb2011_012.pdf

(2) Gallego de la Sacristana Fermín. Aplicación de inicio de sesión mediante autenticación con NFC. Universidad Carlos III de Madrid, España.

http://orff.uc3m.es/bitstream/handle/10016/13738/PFC_Fermin_GallgoSacristana_LopezPablo.pdf?sequence=1

(3) Juárez Gutiérrez Beatriz. (2011). Desarrollo de una aplicación NFC en un entorno universitario con autenticación basada en el Elemento Seguro. Universidad Carlos III de Madrid, Ingeniería Técnica De Telecomunicación Telemática, España.

http://e-archivo.uc3m.es/bitstream/handle/10016/11932/PFC_BEATRIZ_JUAREZ_GUTIERREZ.pdf?sequence=1

(4) Juan Mir, Nuevos retos de seguridad en dispositivos NFC. Obtenido de: http://recsi2012.mondragon.edu/es/programa/recsi2012_submission_52.pdf

(5) Javier Areitio Bertolin (2011). Análisis de los riesgos y contramedidas en seguridad-privacidad de la tecnología NFC en móviles. http://www.redeweb.com/_txt/684/42.pdf

(6) Ortiz Aguirre, Sergio Fabián. Near Field Communication Universidad Católica “Nuestra Señora de la Asunción" Campus Santa Librada, Asunción-Paraguay. http://www.jeuazarru.com/docs/NFC.pdf

(7) Sánchez Moreno Natalia (2009). Aplicación de evaluación basada en NFC (Near Field Communication). Universidad Carlos III de Madrid, Departamento de Telemática de Madrid. http://orff.uc3m.es/bitstream/handle/10016/7487/PFC_Natalia_Sanchez_Moreno.pdf?sequence=1

(8) Veloz Chérrez, Diego Fernando (2010). Diseño e implementación de un prototipo para control de acceso de personas aplicando la tecnología NFC por

medio del uso de teléfonos celulares compatibles con esta tecnología, Escuela Politécnica Nacional, Facultad de ingeniería Electrónica, Quito. http://bibdigital.epn.edu.ec/bitstream/15000/2227/1/CD-2970.pdf

Otras Referencias

(9) http://www.computerworld.es/archive/los-dispositivos-hablan-entre-si-gracias-a-nfc

(10) http://www.consultec.es/DocInformes/Servicios%20de%20Proximidad.pdf

(11) http://www.consumer.es/web/es/tecnologia/internet/2008/08/26/179004.php

(12) http://www.taringa.net/posts/info/4612231/Tecnologia-NFC-no-sabes-para-que-sirve-entra.html

(13) http://los40.com/los40/2004/01/09/actualidad/1073602800_274342.html

(14) http://pegasus.javeriana.edu.co/~mad/J2ME.pdf

(15) http://es.wikipedia.org/wiki/Java_%28lenguaje_de_programaci%C3%B3n%29

(16) http://en.wikipedia.org/wiki/Eclipse_(software)

(17) www.nfc-forum.org

(18) www.nfc.cc

(19) www.google.com/events/io/2011/sessions/how-to-nfc.html

(20) www.google.com/events/io/2011/sessions/how-to-nfc.html

(21) https://developers.google.com/android/

(22) www.gsma.com/mobilenfc/

(23) http://nfctimes.com

ANEXOS

Anexo 1. FORMULARIO DE LA ENCUESTA

ENCUESTA PARA EL ESTABLECIMIENTO DE LINEA BASE PARA EL PROYECTO DE SISTEMA DE CONTROL DE ACCESO DEL PERSONAL DE LA CLÍNICA DE TRAUMAS Y FRACTURAS EN LA CIUDAD DE MONTERÍA

Nombre

Cargo

Responda
Si/No/No Sabe Preguntas #1
Si/No Preguntas #2, #3, #5
[1] Segura. [2]. Poco Segura. [3]. Insegura. [4]. No Sabe. Preguntas #4

1. ¿Usted tiene teléfono celular de tipo Smartphone?

   a. Si ◯

   b. No ◯

   c. No Sabe ◯

2. ¿Sabe que es tecnología NFC y que utilidad tiene?

   a. Si ◯

   b. No ◯

3. ¿Considera confiable los medios de control de acceso utilizados en su lugar de trabajo?

   a) Si ◯

   b) No ◯

4. ¿Cree que un Smartphone es una plataforma segura para llevar credenciales de identidad y utilizarlas como medio de autenticación?

1	2	3	4

5. ¿Estaría dispuesto a usar un Smartphone como medio de autenticación en su lugar de trabajo?

   a. Si ◯

   b. No ◯

Anexo 2. Caracterización de NFC

Introducción

- Tecnología inalámbrica de muy corto alcance
- Estándar ISO 18092 (aprobado en 2003)
- Tecnología basada en RFID y compatible en la banda de 13,56MHz.
- Orientado a la comunicación entre dispositivos iguales.
- Tecnología desarrollada por el NFC Forum, formado en 2004.
- Cuenta con más de 160 miembros de todos los sectores.
- Han publicado 16 especificaciones.
- Aún continúan generando especificaciones.
    - Bluetooth Secure Simple Pairing using NFC [01/11/2011]

Características técnicas

- Opera en la banda de 13.56MHz (banda ISM)
- Velocidad: 106Kbit/s, 212Kbit/s y 424Kbit/s.
- Alcance: 10 cm
- Compatible con RFID
- No soporta detección ni corrección de errores
- Comunicación punto a punto entre dos dispositivos
- Sin descubrimiento ni *pairing*
- Permite establecer dos tipos de comunicación:
    - Orientado a la conexión, como TCP

– No orientado a la conexión como UDP

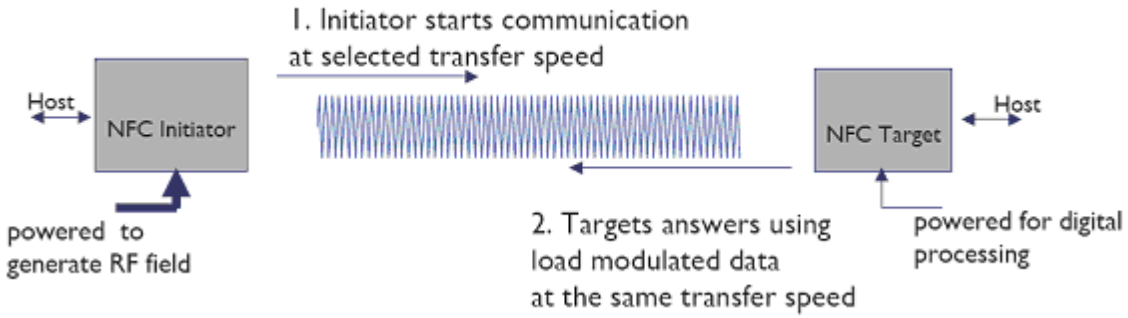
Tipos de dispositivos

Dos tipos de dispositivos:

- **Pasivo**

El dispositivo Iniciador genera el campo electromagnético y el dispositivo destino se comunica con éste modulando la señal recibida. En este modo, el dispositivo destino obtiene la energía necesaria para funcionar del campo electromagnético generado por el Iniciador.

Ilustración 17. Pasivo

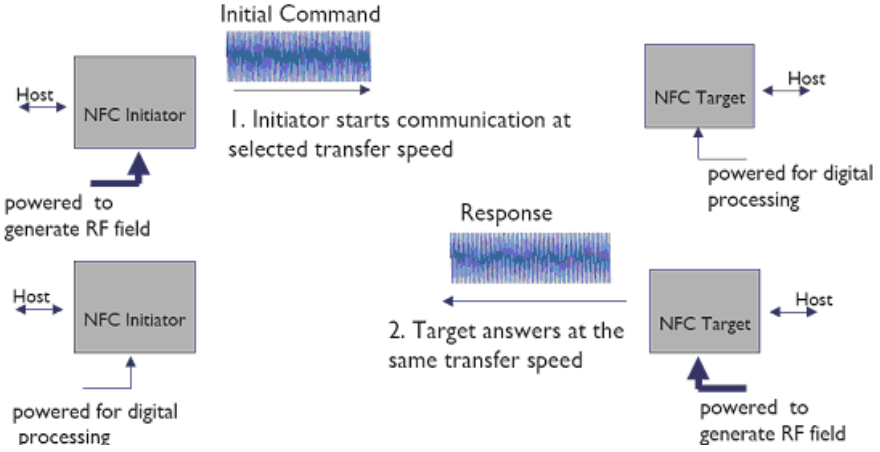


Fuente: http://blog.kuapay.com/es/tag/nfc/pasivo

- **Activo**

El dispositivo Iniciador como el destino se comunica generando su propio campo electromagnético. En este modo, ambos dispositivos requieren de una fuente de alimentación para funcionar. Cuando el dispositivo funciona en modo pasivo, el receptor sólo se utiliza para establecer la comunicación y confirmar la recepción de los datos. Sin embargo, en modo activo, se requiere que ambos nodos negocien el intercambio de datos.

Ilustración 18. Pasivo



Fuente: http://blog.kuapay.com/es/tag/nfc/activo

Fases de la comunicación en NFC

La comunicación NFC consta de cinco fases las cuales son importantes para la comunicación entre dispositivos ya que tienen una función específica y siempre están presentes en el establecimiento de esta.

Estas etapas son:

Descubrimiento: En esta fase los dispositivos inician la etapa de rastrearse el uno al otro y posteriormente su reconocimiento.

Autenticación: En esta parte los dispositivos verifican si el otro dispositivo está autorizado o si deben establecer algún tipo de cifrado para la comunicación.

Negociación: En esta parte del establecimiento, los dispositivos definen parámetros como la velocidad de transmisión, la identificación del dispositivo, el tipo de aplicación, su tamaño, y si es el caso también definen la acción a ser solicitada.

Transferencia: Una vez negociados los parámetros para la comunicación, se puede decir que ya está realizada exitosamente la comunicación y ya se puede realizar el intercambio de datos.

Confirmación: El dispositivo receptor confirma el establecimiento de la comunicación y la transferencia de datos.

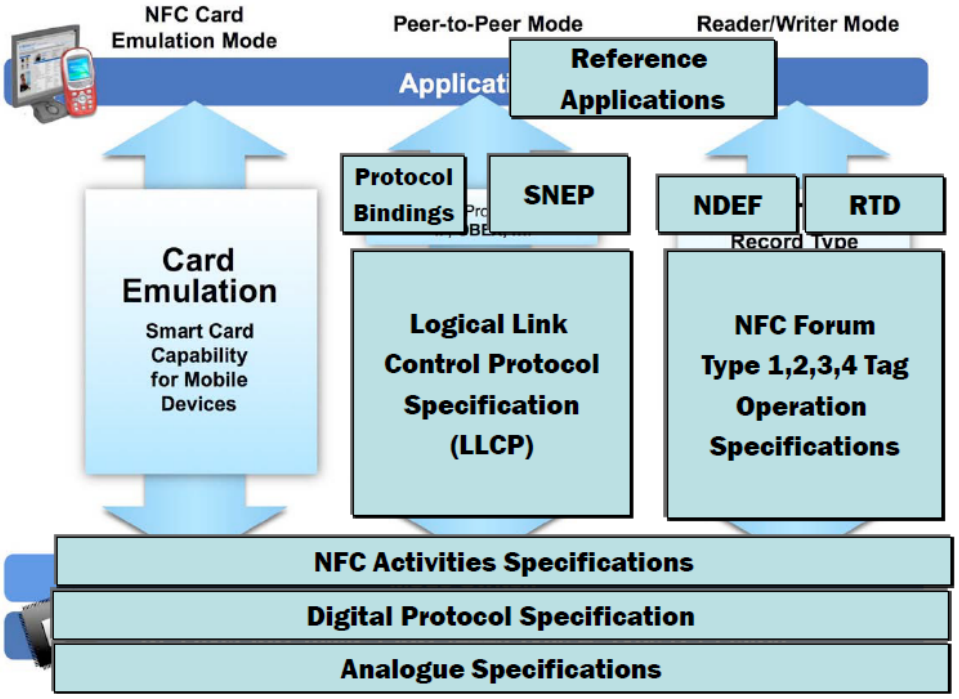
Modos de comunicación

- Lectura/escritura: un dispositivo es activo (lector/escritor) y el otro pasivo (tarjetas RFID).
- *Peer to Peer (P2P)*: dos dispositivos activos comunicándose
- *Card Emulation:* un dispositivo activo actúa como pasivo.

  ¿Ventajas?
  - Puede emular varias tarjetas
    - Mejora la experiencia del usuario
    - Servicio más personalizado al cliente
- Utiliza un elemento de seguridad *(secure element)*
  - Chip integrado.
  - SIM.
- ¿Qué tecnología emulamos?
- Recursos limitados en el SE.
- Elemento seguro basado en chip integrado:
  - Fabricante NXP, principal impulsor

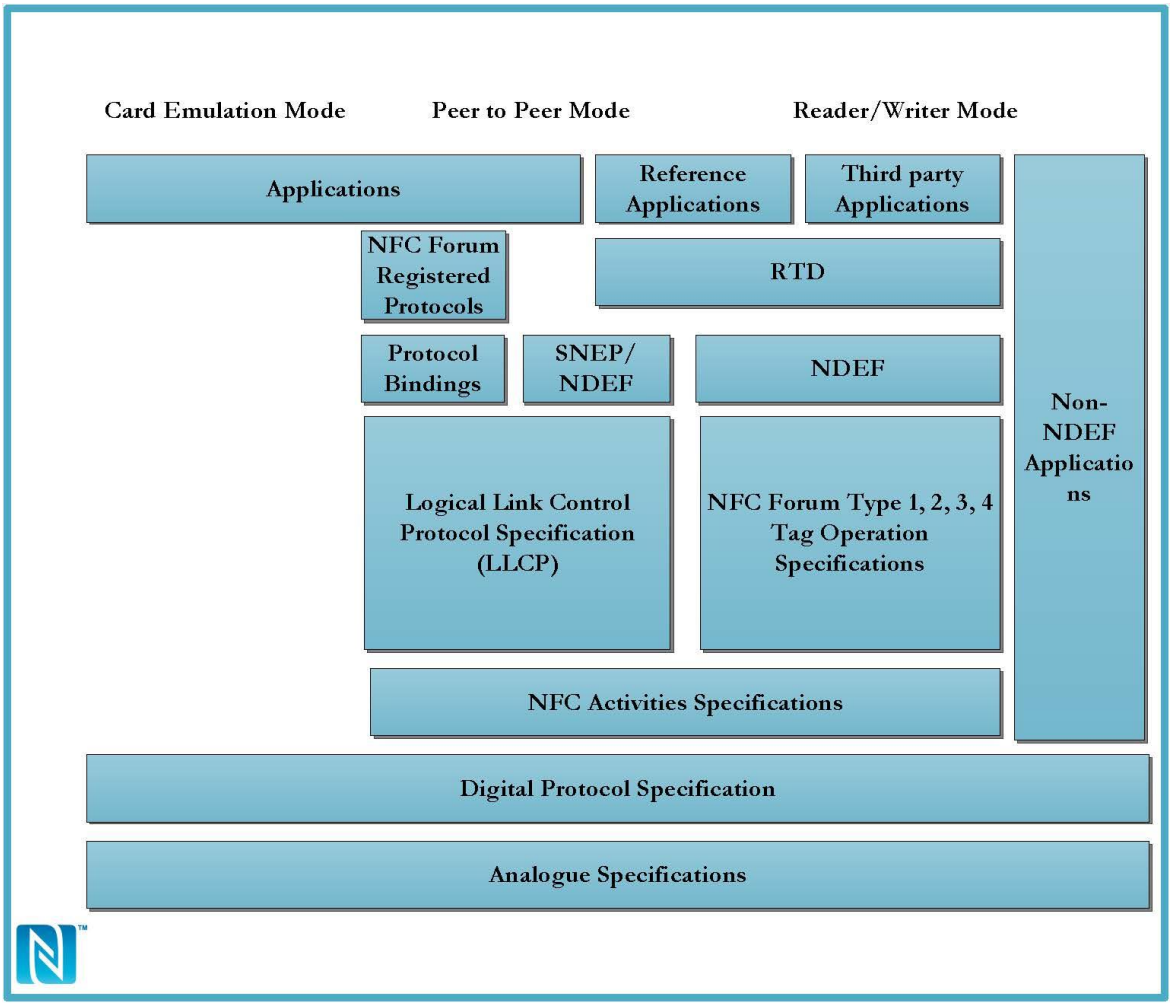
    - Chip integrado con Java Card OS
    - Solución implementada por Google y Samsung
- Elemento seguro basado en SIM:
    - Inicialmente acceso por RIL *(Radio Interface Layer)*
    - Propietaria
    - GSMA impulsa SWP *(Single Wire Protocol)*
    - Chip para comunicarse con la SIM (también debe soportarlo)
    - Telefónica y RIM implementan esta solución
- En cualquier caso:
    - Sólo aplicaciones confiables (TTP) tendrán acceso
    - No tendrán acceso a todos los recursos.

Ilustración 19. Capas de NFC



Fuente: http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/

Ilustración 20. Capas de NFC



Fuente: http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/

RTD *(Record Type Definition)*

- Los tipos de datos que permite enviar NFC son:
  - MIME
  - URI
  - RTD
- 2 tipos de RTDs:

  - *Well-Known types:* se utilizan cuando no hay MIME o URI equivalente. Hay varios:
    - *Text*
    - *Generic Control*
    - *Smart Poster*
    - *Signature*
  - *External types:* utilizado por las empresas para definir su propio espacio de nombres

RTD: *text*

- No pretende sustituir al objeto MIME *text/plain*
- Puede tener varios usos:
  - Añadir información de algún servicio
  - Si aparece en un único registro entonces la aplicación de usuario lo interpreta
- Buenas prácticas: no interpretar este campo, considerarle únicamente como campo de información.

RTD: *text* (estructura)

Offset (bytes)	Length (bytes)	Content
0	1	Status byte.
1	<n>	ISO/IANA language code. Examples: “fi”, “en-US”, “fr-CA”, “jp”. The encoding is US-ASCII.
n+1	<m>	The actual text. Encoding is either UTF-8 or UTF-16, depending on the status bit.

Bit number (0 is LSB)	Content
7	0: The text is encoded in UTF-8 1: The text is encoded in UTF16
6	RFU (MUST be set to zero)
5..0	The length of the IANA language code.

NDEF (*NFC Data Echange Format*)

- Define el intercambio de información entre dos dispositivos
  - P2P
  - *Reader/Writer*
- La información viaja en mensajes
- Cada mensaje se compone de varios registros
- Cada registro se compone de varios campos
  - Longitud
  - Tipo

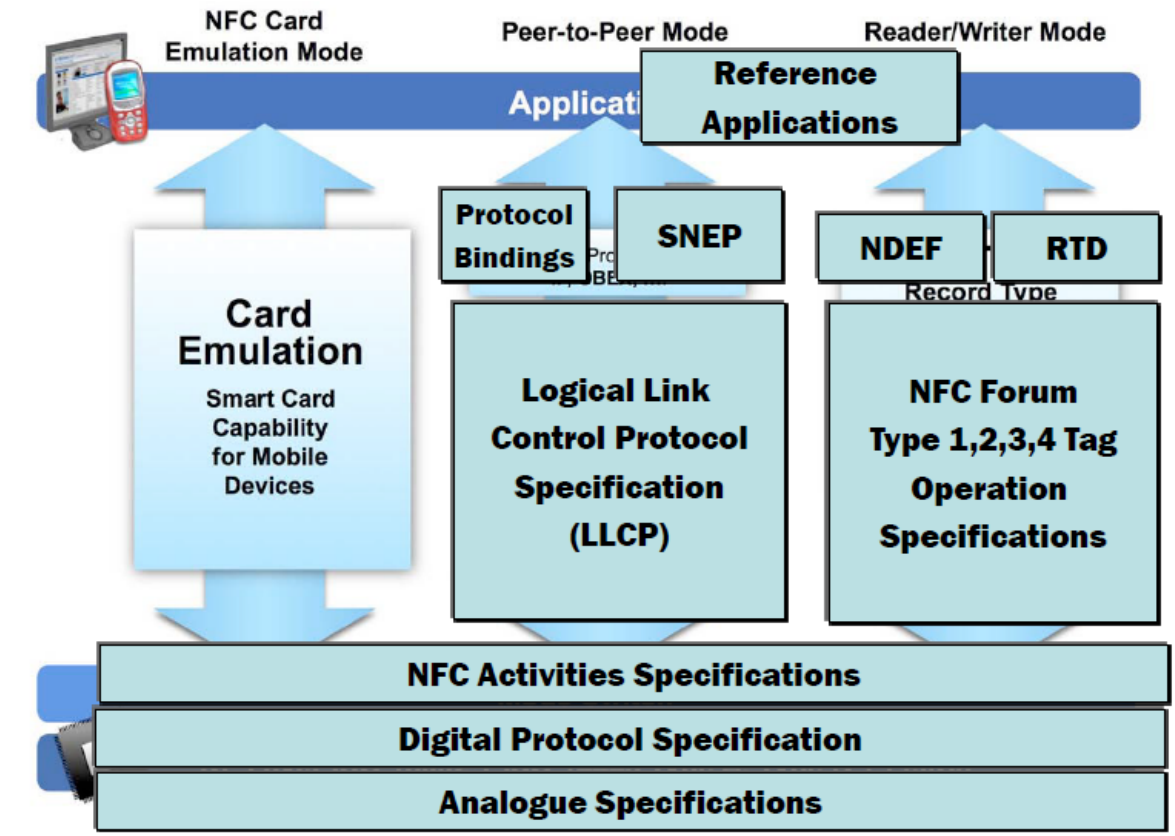
- Identificador
- *Payload*

NDEF (*NFC Data Echange Format*)

Registro de un mensaje NDEF

- Header
  - MB
  - ME
  - CF
  - SR
  - IL
  - TNF
- Tipo
  - Longitud
  - Valor
- ID
  - Longitud
  - Valor
- Payload
  - Longitud
  - Valor

Ilustración 21. SNEP (Simple NDEF Exchange Protocol)



Fuente: http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/protocol-technical-specifications**/**

SNEP (*Simple NDEF Exchange Protocol*)

- Protocolo de petición/respuesta
- Define como se realiza el intercambio de mensajes NDEF
- Fue aprobado a finales de 2011. Implementa
- Procedimiento:
  - Cliente envía petición
  - Servidor responde
  - Admite fragmentación.

NFC Tag Types

- ***Tag 1 Type***
  - Basado en ISO-14443A
  - Escritura/lectura (se pueden configurar de sólo lectura)
  - Tamaño memoria: 96bytes-2Kbytes
  - Velocidad: 106kbits/s
  - No soporta anticolisión
  - Ejemplo: topaz
- ***Tag 2 Type* (similares a las anteriores)**
  - Basado en ISO-14443A
  - Escritura/lectura (se pueden configurar de sólo lectura)
  - Tamaño memoria: 96bytes-2Kbytes
  - Velocidad: 106kbits/s
  - Soporta anticolisión
  - Ejemplo: NXP Mifare Ultralight
- ***Tag 3 Type***
  - Basado en X 6319-4 (estándar japonés)
  - Configurado de fábrica para escritura y/o lectura
  - Tamaño memoria: hasta 1MB
  - Velocidad: 212 o 424Kbits/s
  - Soporta anticolisión
  - Ejemplo: Sony-Felica

- ***Tag 4 Type***
  - Basado en ISO-14443A
  - Configurado de fábrica para escritura y/o lectura
  - Tamaño memoria: hasta 32KB
  - Velocidad: 106, 212 o 424Kbits/s
  - Soporta anticolisión
  - Ejemplo: NXP Desfire
- **Mifare Classic**
  - No son estándar
  - Soportados por móviles con chip de NXP
  - Basado en ISO-14443A
  - Escritura/lectura (se puede configurar de sólo lectura)
  - Tamaño memoria: 192, 768 o 3584Bytes
  - Velocidad: 106Kbits/s
  - Soporta anticolisión
  - Ejemplo: NXP Mifare Classic
- **Todos estos Tags se pueden leer/escribir mediante NDEF**

API NFC

- **Soporta dos modos de comunicación:**
  - Lectura/escritura de tags
  - *Android Beam*
  - *Card Emulation* no está abierto a desarrolladores
- **Soporta la mayoría de mensajes NDEF definidos en el estándar**

  - No soporta el modo *Generic*

- **Soporta mensajes propietarios, no NDEF**
  - Android.nfc.tech.package
- **Cada aplicación debe filtrar el tipo de información que desea recibir.**

Funcionamiento básico

1. Una aplicación de usuario envía varios documentos.
   - Por ejemplo: un contacto, una URL y/o una nota.
2. Cada documento es encapsulado en un registro (en el payload) distinto.
3. NDEF conforma el mensaje agrupando todos los registros.
4. Envía el mensaje a través del enlace establecido.
5. El mensaje es recibido y parseado por un dispositivo activo.
6. Se escribe el mensaje en un tag, que luego será leído por un dispositivo activo.
7. Finalmente, la aplicación de usuario recibe el mensaje.

Seguridad

- Seguridad en las comunicaciones *(Sniffing o eavesdropping):*
  - ✓ El alcance tan corto complica los ataques.
  - ✓ NFC está apagado si el móvil está bloqueado.
  - ✓ NFC no cifra.

- Seguridad en los dispositivos:

❖ Etiquetas

- ✗ *URL Spoofing.*
- ✗ Superposición de tags.

- ✓ Comprobar la URL antes de cargar

- ✓ Firmar mensaje (RTD Signature)

- ✗ *Record Composition Attack*
- ✗ *Record Hidden*

❖ Móviles

- ✗ Aplicaciones maliciosas del *market*
- ✗ *Secure element*

Aplicaciones

- Sistema de control de accesos
- Aplicación Android:
  - NFC.
  - Bluetooth.
- Terminal Bluetooth
  - Monitorización.
- Acceso web
  - Apertura.

Anexo 3. Arquitectura y Plataforma Necesarias Para la Implementación

Arquitectura de aplicación de NFC

Aplicación cliente:

Interface de usuario.

Interpretación del dispositivo lector.

Funcionalidad P2P entre dispositivos móviles.

Funcionalidad P2P entre móvil y pc, m. venta.

Comunicación con el servidor.

Seguridad (Secure Element).

Aplicación servidor:

Lógica de la aplicación.

Gestión de la base de datos.

Comunicación hacia el cliente.

Ilustración 22. Arquitectura Aplicación NFC

Fuente: Autor

Funcionalidades del servidor Requisitos de la aplicación.

Diseño del protocolo de comunicación entre el cliente y el servidor.

Diseño de la identificación de los clientes.

Diseño del concepto de la seguridad (encriptación).

Escalabilidad.

Diseño de la política de fallos de la red GSM.

Requisitos de una aplicación NFC

Desarrollo de un concepto de despliegue.

Desarrollo de una aplicación para el mantenimiento de los dispositivos (con control de versiones).

Desarrollo de una aplicación para el dispositivo móvil.

Gestión de usuarios, administradores, roles y permisos.

Asegurar que nuevas funcionalidades sean compatibles y coexistan en paralelo con la infraestructura existente.

Diseño de la actualización del servidor en ejecución.

NFC móvil. Funcionalidad

Resulta: El móvil NFC mobile es:

una tarjeta.

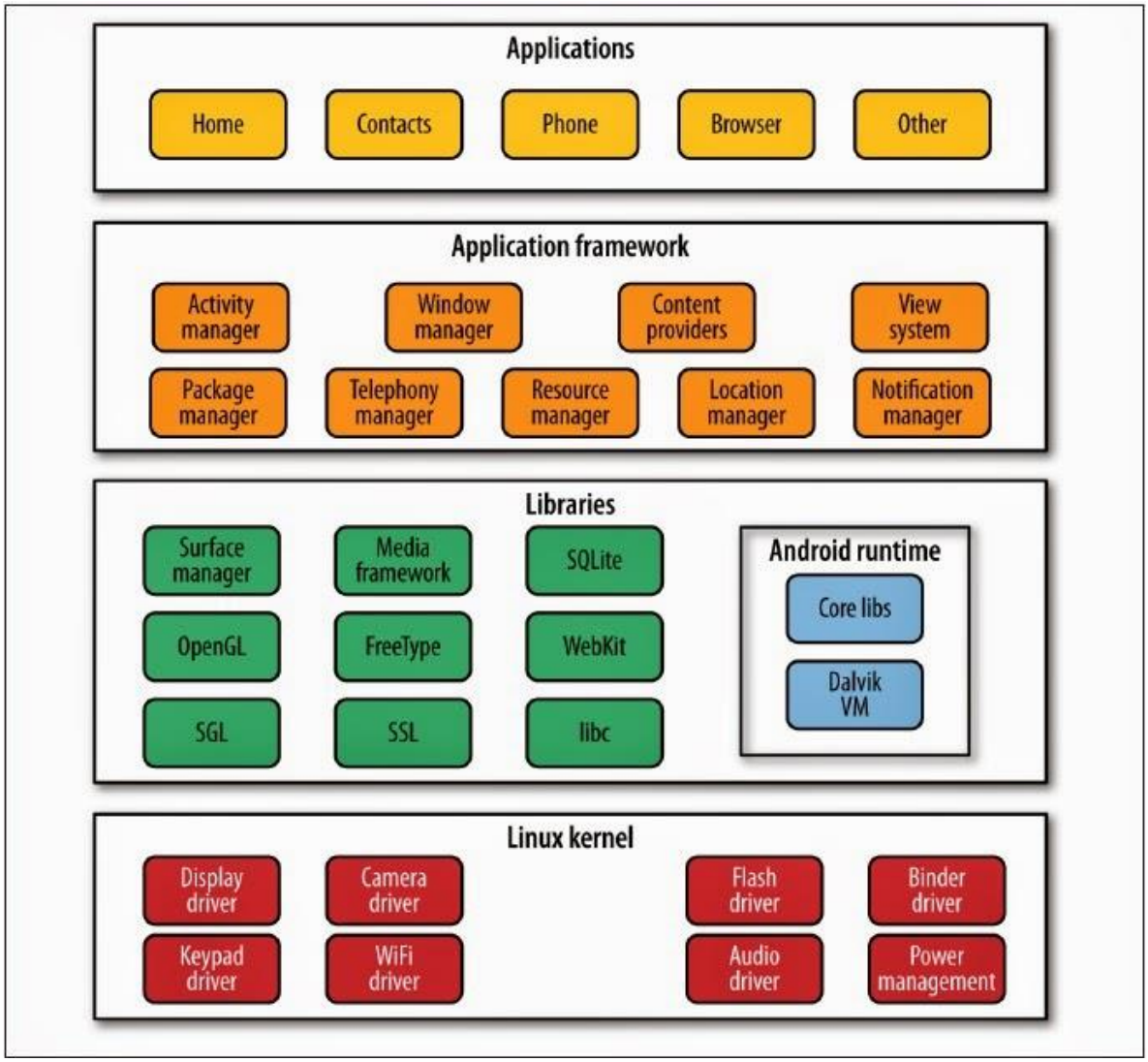
un lector.

un dispositivo peer-to-peer En un concepto.

Modelo De Capas En La Arquitectura De Android

Android está construido con una arquitectura de 4 capas o niveles relacionados entre sí. A continuación, veremos un diagrama ilustrativo extraído del libro Learning Android escrito por Marko Gargenta y Masumi Nakamura:

Ilustración 23. Arquitectura Android



Fuente:http://www.hermosaprogramacion.com/2014/08/aprendiendo-la-arquitectura-de-android/

El diagrama indica que la estructura de Android se encuentra construida sobre el Kernel de Linux. Luego hay una capa de Librerías relacionadas con una estructura administradora en tiempo de ejecución. En el siguiente nivel encontramos un Framework de apoyo para construcción de aplicaciones y posteriormente vemos a la capa de Aplicaciones.

Kernel De Linux

Android está construido sobre el núcleo de Linux, pero se ha modificado dramáticamente para adaptarse a dispositivos móviles. Esta elección está basada en la excelente potabilidad, flexibilidad y seguridad que Linux presenta. Recuerda que el Kernel de Linux está bajo la licencia GPL, así que en consecuencia Android también.

Capa De Librerías O Capa Nativa

En esta capa se encuentran partes como la HAL, librerías nativas, demonios, las herramientas de consola y manejadores en tiempo de ejecución. Veamos un poco el propósito de estos conceptos:

Hardware Abstraction Layer (HAL): Este componente es aquel que permite la independencia del hardware. Quiere decir que Android está construido para ejecutarse en cualquier dispositivo móvil sin importar su arquitectura física. El HAL

actúa como una arquitectura genérica que representa a todos los posibles tipos de hardware existentes en el mercado. Aunque por el momento no hay estándares de construcción en el hardware de dispositivos móviles, el HAL permite que cada fabricante ajuste sus preferencias para que Android sea funcional sobre su tecnología.

Librerías nativas: Aquí encontramos interfaces de código abierto como OpenGL para el renderizado de gráficos 3D, SQLite para la gestión de bases de datos, WebKit para el renderizado de los browsers, etc. También librerías para soportar los servicios del sistema como Wifi, posicionamiento, telefonía, y muchos más.

Demonios (Daemons): Los demonios son códigos que se ejecutan para ayudar a un servicio del sistema. Por ejemplo, cuando se requiere instalar o actualizar una aplicación, el demonio de instalación “installd” es ejecutado para administrar todo el proceso. O cuando los desarrolladores vamos a ejecutar en modo de depuración nuestro teléfono desde un PC, se ejecuta un demonio llamado adbd (Android Debug Bridge Daemon) para auxiliar a dicho proceso.

Consola: Al igual que otros sistemas operativos, Android permite que empleemos comandos de línea para la ejecución de procesos del sistema o explorar el sistema operativo.

Manejadores en tiempo de ejecución: Si bien las aplicaciones Android están escritas en lenguaje Java y son traducidas a bytecodes, estas no son interpretadas por la máquina virtual de Java. Android tiene su propia máquina virtual interpretadora de bytecodes llamada Dalvik. Esta herramienta fue diseñada

para ser flexible ante el diseño de hardware de un dispositivo móvil. Además, JVM no es de licencia GPL, así que Google decidió generar su propia herramienta.

Framework Para Aplicaciones

Esta es la capa que nos interesa a los desarrolladores, ya que en ella encontramos todas las librerías Java que necesitamos para programar nuestras aplicaciones. Los paquetes con más preponderancia son los android.*, en ellos se alojan todas las características necesarias para construir una aplicación Android.

No obstante, es posible acceder a clases como java.utils.*, java.net.* , etc. Aunque hay librerías Java excluidas como la java.awt.* y java.swing.*.

En esta capa también encontraremos manejadores, servicios y proveedores de contenido que soportaran la comunicación de nuestra aplicación con el ecosistema de Android.