



Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas y Telemática

“Near Field Communication-Teoría y Aplicaciones”

Tesis previa a la obtención del título de Ingeniero de Sistemas y Telemática

Autores:

Jorge Esteban Padilla Contreras

Wilber Adrián Iñiguez López

Director: Ing. Esteban Crespo Martinez, MBA

Cuenca, Ecuador

2014

DEDICATORIA

La elaboración de la presente tesis la dedicamos principalmente a nuestros padres: Wilber, Esperanza, Sara y Jorge. Ya que supieron siempre apoyarnos y brindarnos fortaleza a lo largo de nuestras vidas académicas, aconsejándonos y transmitiéndonos su sabiduría. De igual manera a nuestros familiares y amigos, que aportaron su granito de arena para que hoy podamos cumplir esta importante meta en nuestras vidas profesionales y personales.

AGRADECIMIENTOS

A los profesores de la Universidad del Azuay, por compartir con nosotros sus experiencias y conocimientos a lo largo de todos estos años de aprendizaje.

Al Ing. Esteban Crespo y al Ing. Marcos Orellana por brindarnos todo su respaldo en la realización del presente trabajo, ya que sin su ayuda no hubiéramos podido alcanzar las metas propuestas.

Y de manera muy especial a nuestros compañeros de clase, por brindarnos su ayuda, compartir sus conocimientos y por las innumerables experiencias de vida que compartimos durante estos cinco años. Han sido muchos momentos de alegría, tristeza, compañerismo, cariño y victoria, los cuales han contribuido a que seamos mejores personas para el mañana. Gracias infinitas compañeros.

ÍNDICE DE CONTENIDOS

DEDICATORIA	ii
AGRADECIMIENTOS	iii
ÍNDICE DE CONTENIDOS	iv
ÍNDICE DE ILUSTRACIONES Y CUADROS	vi
ÍNDICE DE ANEXOS.....	ix
RESUMEN.....	x
ABSTRACT.....	xi
CAPÍTULO 1	1
INTRODUCCIÓN A NFC.....	1
1.1 Fundamentos de NFC	1
1.2 Beneficios de la tecnología NFC	4
1.3 Evolución de NFC	10
CAPÍTULO 2	15
La Tecnología NFC.....	15
2.1 Especificaciones Técnicas	15
2.2 Electromagnetismo y Transferencia de datos	25
2.3 Modos de Comunicación	32
2.4 Modos de Operación.....	35
2.5 Comparación NFC con RFID	41
2.6 Comparación NFC con Bluetooth.....	45
2.7 Comparación NFC con Infrarrojo	47
CAPÍTULO 3	50
Áreas de Aplicación y Modelos de Negocio basados en NFC.....	50
3.1 Control de Acceso.....	50
3.2 Transacciones Financieras	56

3.3	Automatización de Tareas	61
3.4	Seguimiento y Control Médico.....	63
3.5	El futuro de NFC.....	65
CAPÍTULO 4		69
Seguridad y privacidad en NFC		69
4.1	Conceptos básicos sobre seguridad.....	69
4.2	Principales problemas de seguridad.....	74
4.3	Mecanismos y Herramientas.....	78
CAPÍTULO 5		85
Prototipo de una aplicación móvil con NFC		85
5.1	Pasos Iniciales.....	85
5.2	Preparación del entorno y herramientas.....	94
5.3	Programación para el modo de operación lectura/escritura.....	96
5.4	Programación para el modo de operación punto a punto.....	97
5.5	Programación para el modo de operación emulación de tarjeta	97
5.6	Análisis del prototipo.....	98
5.7	Diseño del prototipo.....	109
5.8	Desarrollo del prototipo	110
CONCLUSIONES y RECOMENDACIONES		121
GLOSARIO		124
BIBLIOGRAFÍA		128
ANEXOS		135

ÍNDICE DE ILUSTRACIONES Y CUADROS

Ilustración 1. Interacción entre dispositivos con NFC	2
Ilustración 2. Modos de Operación y Comunicación de NFC	4
Ilustración 3. Beneficios de NFC según el modo de operación	6
Ilustración 4. Arquitectura de un teléfono móvil con NFC.....	16
Ilustración 5. Modelos de Elementos Seguros (SE).....	18
Ilustración 6. Estructura de la Interfaz NFC	19
Ilustración 7. Arquitectura del protocolo NFC-WI.....	20
Ilustración 8. Transmisión de datos por SWP	21
Ilustración 9. Pronóstico Mundial de Teléfonos con NFC.....	22
Ilustración 10. Aplicaciones de los lectores NFC	22
Ilustración 11. Componentes de una etiqueta NFC.....	23
Ilustración 12. Tipos de Antenas NFC	24
Ilustración 13. Líneas de flujo magnético alrededor de un conductor y una bobina cilíndrica.....	26
Ilustración 14. Definición de Inductancia, L.....	29
Ilustración 15. Bobinas acopladas y diagrama del circuito equivalente para dos bobinas acopladas.....	31
Ilustración 16. Modos de Comunicación Activo o Pasivo.....	34
Ilustración 17. Rol iniciador o destino	34
Ilustración 18. Combinación de Rol iniciador o destino y modos activo o pasivo	35
Ilustración 19. Rol de cada tipo de dispositivo	35
Ilustración 20. Arquitectura de Comunicación del Modo Punto a Punto	36
Ilustración 21. Protocolos de la Arquitectura del Modo Punto a Punto.....	37
Ilustración 22. Arquitectura de Comunicación del Modo Escritura-Lectura.....	38
Ilustración 23. Protocolos de la Arquitectura del modo escritura-lectura.....	39
Ilustración 24. Arquitectura de Comunicación Emulación de Etiquetas	40
Ilustración 25. Protocolos de la Arquitectura del modo emulación de etiquetasEstándares y Protocolos	41
Ilustración 26. Arquitectura de un sistema RFID.....	42
Ilustración 27. Componentes de un Sistema RFID	42

Ilustración 28. Bandas de Frecuencia, Protocolos y distancias de operación de RFID	43
Ilustración 29. Tabla comparativa ente RFID y NFC	45
Ilustración 30. Tabla comparativa ente Bluetooth y NFC	47
Ilustración 31. Tabla comparativa ente Infrarrojo y NFC	48
Ilustración 32. Ejemplo Sistema en línea: Legic-Installation Kaba Security Locking Systems	52
Ilustración 33. Sistema fuera de línea integrado en una cerradura de puerta: Häfele GmbH, D-Nagold.....	53
Ilustración 34. Pago del sistema de transporte público en Alemania con un teléfono Nokia 3220.....	55
Ilustración 35. Ecosistema NFC.....	58
Ilustración 36. Comparación de los métodos de pago móviles alternativos	60
Ilustración 37. Herramientas utilizadas en la elaboración de muebles: EUCHNER & Co., Leinfelden-Echterdingen	62
Ilustración 38. Ejemplo de los datos de configuración almacenados en una etiqueta NFC.....	62
Ilustración 39. Conjunto de Acciones disponibles en la aplicación NFC Task Launcher.....	63
Ilustración 40. Toshiba Satellite U925T- Primera ultrabook con NFC	65
Ilustración 41. Patente de Apple: Ejemplo de Control de Dispositivos con NFC	66
Ilustración 42. Patente de Apple: Aplicaciones NFC del Iphone para Televisores y Juegos.....	67
Ilustración 43. Pilares de la Seguridad de la Información	72
Ilustración 44. Análisis de las Amenazas.....	73
Ilustración 45. Esquemas de codificación.....	76
Ilustración 46. Esquema de ataque Hombre en medio.....	77
Ilustración 47. Proceso de Encriptación-Desencriptación	79
Ilustración 48. Esquema de algoritmo asimétrico de encriptación-RSA	81
Ilustración 49. Proceso de Autenticación utilizando una firma digital	83
Ilustración 50. Andy Rubin-Fundador de Android Inc.	86
Ilustración 51. Arquitectura del Sistema Operativo Android.....	87
Ilustración 52. Distribución de Versiones de Android al 4 de Septiembre del 2013.	88
Ilustración 53. Composición General de un mensaje Tipo NDEF.....	90

Ilustración 54. Código Hexadecimal de lectura de un mensaje NDEF.....	90
Ilustración 55. Formato del código binario contenido en un mensaje NDEF.....	90
Ilustración 56. Estructura detallada del contenido de un mensaje en formato NDEF	91
Ilustración 57. Flujo del sistema de ejecución de etiquetas	94
Ilustración 58. Emulación de tarjeta con un elemento seguro	97
Ilustración 59. Emulación de tarjeta sin un elemento seguro.....	98
Ilustración 60. Sistema de despacho de etiquetas.	112

ÍNDICE DE ANEXOS

6.1 Especificación de Requisitos del Sistema (ERS)

6.2 Manual de Usuario

6.3 Manual de Estilos

RESUMEN

Near Field Communication (NFC por sus siglas en inglés), o comunicación de campo cercano, es una tecnología inalámbrica para transmisión de datos, que opera en la frecuencia de los 13.56 MHz, por lo cual funciona en un rango máximo de distancia de 10 cm aproximadamente.

La importancia de la tecnología NFC recae en que, para la transmisión de datos no es necesario contar con dos objetos provistos de una fuente de alimentación, ya que gracias a la inducción de voltaje, que produce el objeto origen sobre el objeto destino, se energiza el receptor y permite una comunicación. Lo cual posibilita la fabricación de etiquetas muy económicas, de varios materiales, de tamaño muy pequeño y que a su vez puedan almacenar una pequeña cantidad de información.

La inclusión de chips NFC en los teléfonos inteligentes ha permitido, que el desarrollo de aplicativos que utilicen esta tecnología crezca exponencialmente, abriendo de esta manera un nuevo nicho de mercado, que puede ser aprovechado por los desarrolladores de tecnología para cubrir necesidades cotidianas de las personas de una manera intuitiva y fácil.

El presente trabajo describe los aspectos técnicos del funcionamiento de esta tecnología, sus posibles campos de aplicación, problemas de seguridad involucrados y su ejemplificación, por medio de la elaboración de un prototipo de aplicación móvil para el sistema operativo Android, que involucra la lectura y escritura de etiquetas NFC.

ABSTRACT

Near Field Communication (NFC), is a wireless technology for data transmission, which operates in the 13.56 MHz frequency, subsequently it works on a maximum range of approximately 10 cm.

The importance of the NFC technology lies on the fact that it is not necessary to have two objects provided with power supply for data transmission because, thanks to the induction of voltage that the source object produces on the target object, the receiver is energized, allowing communication. This makes it possible to manufacture very inexpensive labels of several materials, very small in size and which can in turn store a small amount of information.

The inclusion of NFC chips in smartphones has enabled an exponential growth of the development of applications that use this technology; which opens a new market niche that can be exploited by technology developers to meet the everyday needs of people in an intuitive and easy way.

This paper describes the technical aspects of how this technology works, its possible areas of application, related security issues, and their modeling by developing a prototype mobile application for the Android operating system which involves reading and writing NFC tags.



A handwritten signature in blue ink, which appears to read "Lourdes Crespo".

Translated by,
Lic. Lourdes Crespo

CAPÍTULO 1

INTRODUCCIÓN A NFC

En el presente capítulo se desarrolla los conceptos básicos necesarios para describir la tecnología, sus modos de comunicación, modos de operación, beneficios del uso de la tecnología tanto para las personas como para las empresas. Adicionalmente se realiza una reseña histórica de la evolución de los sistemas de identificación desde el código de barras, pasando por la identificación de radio frecuencia (RFID) hasta las tarjetas inteligentes.

1.1 Fundamentos de NFC

NFC (*Near Field Communication* o Comunicación de Campo Cercano por sus siglas en inglés) es una de las últimas tecnologías inalámbricas de comunicación, se trata de un estándar basado en un protocolo de transmisión de corto rango, que permite una interacción simple, intuitiva y bidireccional entre dispositivos electrónicos (Pankaj y Bhuraria). El objetivo de NFC es la comunicación entre terminales sin la necesidad de excesivos esfuerzos intelectuales en configurar una red, lo que hace que aplicaciones y el uso de datos sea fácil y conveniente. El concepto general es simple: “*quieres comunicar dos dispositivos, acércalos y listo*“. (International)

NFC trabaja en la radio frecuencia global y no licenciada de los 13.56 MHz, con un ancho de banda de al menos 2 MHz (Falke, Rukzio y Dietz, Mobile Services for Near Field Communication-Ludwig Maximilians University of Munich), permitiendo el intercambio de datos entre dispositivos a una distancia de 10cm (4 in) (Pankaj y Bhuraria). La tecnología está basada en la Identificación de Radio Frecuencia (RFID por sus siglas en inglés) que inicialmente fue desarrollada para la implementación y comunicación de sistemas de identificación automáticos (Bravo, Hervás and Chavira), tanto RFID como NFC emplean la inducción de campo

magnético como medio de comunicación entre dos dispositivos electrónicos. La disponibilidad de chips NFC en los teléfonos móviles modernos ha permitido que se desarrollen un gran número de aplicaciones, que ofrecen grandes oportunidades y soluciones en diversas áreas de la vida cotidiana.



Ilustración 1. Interacción entre dispositivos con NFC

(Fuente: Autoría Propia)

Modos de comunicación

Existen dos modos de comunicación NFC:

Modo de comunicación pasiva: en este caso el dispositivo emisor proporciona un campo portador y el dispositivo receptor responde modulando el campo existente. En este modo el receptor obtiene el poder de operación por el campo electromagnético proporcionado por el emisor. Un ejemplo de este modo es la comunicación entre un teléfono móvil y una etiqueta NFC, es decir una conexión entre un dispositivo activado por energía y una etiqueta pasiva.

Modo de comunicación activa: tanto el emisor como el dispositivo receptor se comunican por la generación alternada de sus propios campos. Uno de los dispositivos debe desactivar su campo de radio frecuencia mientras espera la llegada de datos. Para este modo ambos dispositivos deben contar con una fuente de poder o energía. Un claro ejemplo de este tipo de comunicación es la realizada entre dos teléfonos móviles, es decir la comunicación entre 2 dispositivos que tengan una fuente de poder activa y capacidades computacionales.

Modos de operación

Los dispositivos son capaces de operar en tres modos distintos:

Modo punto a punto: este es el modo clásico de operación de *Near Field Communication*, permite una conexión de datos a una velocidad aproximada de 424 kBit/seg. Las propiedades de electromagnetismo y el protocolo usado se encuentran estandarizadas en la ISO 18092 y ECMA 320/340 (ISO/IEC 18092 (ECMA-340)).

Modo escritura / lectura: una funcionalidad adicional de los dispositivos NFC es la habilidad de leer y escribir etiquetas y tarjetas inteligentes. Como ya se indicó en el modo de comunicación pasiva, el dispositivo puede actuar como un emisor y la etiqueta como un receptor pasivo. En este modo de operación la velocidad de transmisión de datos se aproxima a los 106 Kbit/seg. (Coskun, Ok y Ozdenizci)

Modo de emulación de etiquetas: en este modo los dispositivos NFC pueden emular el comportamiento y propiedades de una tarjeta inteligente con el estándar ISO 14443. Un lector no tiene la capacidad de distinguir entre un dispositivo operando en modo de emulación o una tarjeta inteligente ordinaria. Esto implica una gran ventaja, puesto que actualmente existe una infraestructura de lectura desarrollada para tarjetas inteligentes, estas no tienen que ser reemplazadas y se las puede aprovechar con tecnología NFC. (Coskun, Ok y Ozdenizci)

En resumen, NFC, en su operación básica, está estandarizada en la norma ISO/IEC 18092 (Falke, Rukzio y Dietz, Mobile Services for Near Field Communication-Ludwig Maximilians University of Munich), la que al ser una norma abierta ha permitido el avance de la tecnología en aspectos importantes como la eliminación de problemas de la configuración de la comunicación, larga duración, establecimiento de conexión y alto consumo de energía.

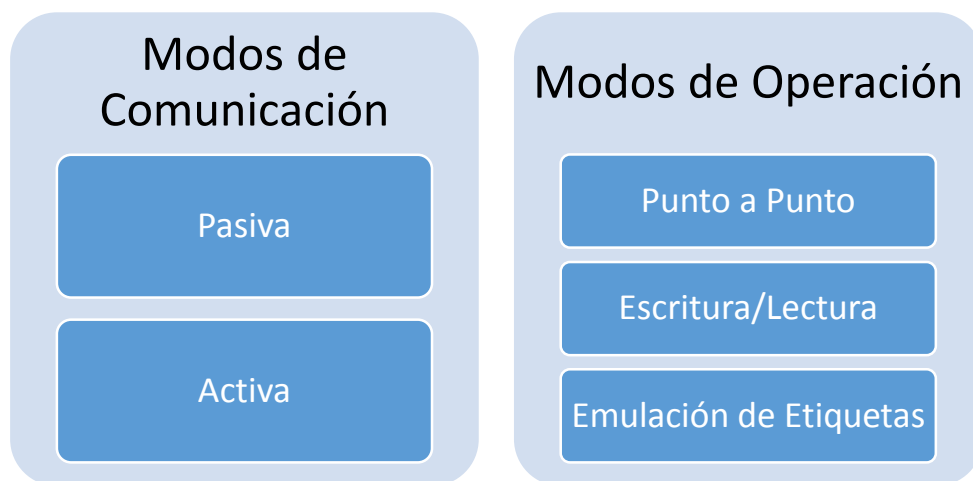


Ilustración 2. Modos de Operación y Comunicación de NFC

(Fuente: Autoría Propia)

1.2 Beneficios de la tecnología NFC

Si bien es cierto, esta tecnología presenta beneficios generales como:

- ❖ **Intuitiva:** puesto que para una interacción no se requiere nada más que un pequeño acercamiento entre los dispositivos.
- ❖ **Versátil:** La tecnología NFC se adapta a una amplia gama de entornos, industrias y usos.
- ❖ **Basada en estándares:** el funcionamiento de la tecnología sigue los estándares ISO, ECMA y ETSI. (ECMA International)
- ❖ **Brinda Tecnología:** facilita y acelera la configuración de tecnologías inalámbricas como: Bluetooth, Wi-Fi, etc.

- ❖ **Seguridad Inherente:** las transmisiones NFC son de corto alcance (es necesario un acercamiento a unos pocos centímetros), reduciendo la posibilidad que otras personas puedan capturar información si no están cerca del lugar.
- ❖ **Interoperabilidad:** mediante el modo de emulación de tarjetas, la tecnología NFC puede comunicarse con tarjetas RFID inteligentes de contacto corto.
- ❖ **Seguridad lista:** NFC posee capacidades incorporadas que soportan aplicaciones seguras. (Prakash Sharma)

Es preciso especificar que cada **modo de operación** provee diferentes beneficios para los usuarios.

En el **modo de lectura/escritura**, los datos se almacenan en una etiqueta NFC, la cual es leída por un dispositivo móvil con NFC, y dicho dato es usado para procesar futuras transacciones (Coskun, Ok y Ozdenizci). La información que se transfiere es un texto: que puede ser una dirección web, una dirección de correo electrónico, fecha de un evento o cualquier otro dato. El objetivo de este modo es proveer movilidad y disminuir el esfuerzo físico (Coskun, Ok y Ozdenizci). La mayoría de aplicaciones son desarrolladas en el modo lectura/escritura, debido a los escenarios de uso que provee y que es más fácil de implementar que los otros modos. (Coskun, Ok y Ozdenizci)

Por otro lado, el **modo punto a punto** es el más usado para los casos de emparejamiento de dispositivos (proceso en el cual 2 dispositivos provistos de la tecnología Bluetooth agregan a su lista de elementos sincronizados, un nuevo dispositivo, este proceso es requerido, previo a la conexión de dichos equipos), redes sociales, y transferencia de archivos (Coskun, Ok y Ozdenizci). De esta manera se puede evitar las molestas configuraciones al momento de parear dos dispositivos para realizar una comunicación Bluetooth, o configurar la clave de acceso a un punto Wi-Fi sin tener que revelarla a nadie, de la misma forma permite actualizar o realizar un check-in en un lugar y publicarlo en el muro de un perfil de usuario de una red social, o simplemente transferir una fotografía, un contacto, una canción; todo esto es posible simplemente acercando los dispositivos móviles.

Finalmente, el **modo de emulación de tarjeta/etiqueta** está destinado a eliminar la necesidad de llevar un objeto físico, como por ejemplo una tarjeta de crédito o tarjeta de débito, en lugar de esto se habilita la posibilidad de realizar pagos con un teléfono inteligente, de forma similar se puede reemplazar las tarjetas de acceso a una habitación, tickets, entradas de papel, cupones, etc. La mayoría de las aplicaciones con fines comerciales son desarrolladas utilizando este modo. (Coskun, Ok y Ozdenizci)



Ilustración 3. Beneficios de NFC según el modo de operación

(Fuente: Autoría Propia)

Una vez analizados los beneficios generales por cada modo de operación, es momento de clasificar los **beneficios según su beneficiario**: personas o negocios.

Beneficios para personas

Pagos sin contacto

Es posiblemente el uso más conocido para la tecnología NFC, con esta funcionalidad los clientes simplemente acercan su teléfono inteligente sobre un lector y pueden pagar una cuenta, eliminando la necesidad de portar tarjetas de crédito, débito o dinero en efectivo. Las aplicaciones denominadas billeteras virtuales, permiten incluso al usuario escoger la tarjeta con la que desea pagar cada transacción, acumular cupones, etc. De esta manera se centraliza todos los pagos de un cliente empleando su teléfono inteligente, reemplazando de esta manera el tener que portar una billetera con efectivo y con todas las tarjetas que un usuario posea. (NFC Organization)

Compartición de Información

El pequeño tamaño de las etiquetas NFC en conjunto con su no necesidad de batería, ha permitido que las etiquetas puedan incluirse en cualquier lugar, desde un poster, pantallas de un museo, librerías, galerías, escuelas, estantes, vitrinas, anuncios impresos, etc. Una etiqueta puede contener información importante como los detalles de un evento, y al acercar un teléfono con NFC a la etiqueta, el usuario puede agregar automáticamente dicho evento a su calendario personal. Esta portabilidad se debe en gran medida al reemplazo de la batería por señales de radio frecuencia enviadas desde un dispositivo con capacidad NFC hacia la etiqueta. (NFC Organization)

Transportación

Países pioneros en tecnología como Japón ya ofrecen la emisión de tickets para metro, tren o bus vía NFC, este servicio elimina la necesidad de una persona que recoja los tickets o perfore una tarjeta para varios viajes, permitiendo que los usuarios puedan circular más rápido al momento del

ingreso a la estación y eliminan las molestas congestiones y colas para ingresar. (NFC Organization)

Cuidado de la Salud

El beneficio en esta área radica en los sistemas de seguimiento de la información de los pacientes, permitiendo a los doctores anotaciones en tiempo real, cada vez que una enfermera o doctor visita un paciente, puede realizar notas, cambiar recomendaciones o grabar las medicinas que deben ser administradas. Evitando de esta forma utilizar una ficha impresa de papel, la cual se puede reemplazar por una pulsera que contenga incrustada una etiqueta NFC. (NFC Organization)

Redes Sociales

Sin lugar a duda las redes sociales están actualmente en auge, lo cual quiere ser aprovechado por la tecnología NFC, ya sea acercando nuestro teléfono para realizar un check-in en un restaurante, o intercambiar contactos con otro teléfono, la idea es evita el realizar engorrosos inicios de sesión o acceder a pantallas de menú para interactuar con nuestro amigos. Algunas compañías como Foursquare (1) están ya probando servicios basados en etiquetas NFC para evitar que el usuario tenga que realizar un inicio de sesión, buscar un sitio, o activar el GPS para actualizar su ubicación, de la misma forma se desea buscar formas para que el usuario comparta un link, poste una reseña o haga una recomendación, tan solo acercando su dispositivo NFC y escribiendo su opinión. (NFC Organization)

(1) Foursquare: es un servicio basado en la localización web aplicada a las redes sociales, que permite a un usuario registrar su ubicación, buscar lugares de interés y recomendarlos a sus contactos.

Beneficios para los negocios

Los beneficios de NFC no son exclusivos para los clientes, las empresas y negocios también pueden beneficiarse de esta tecnología. Los administradores pueden comunicarse rápidamente con los empleados y con otros negocios, de la misma forma incrementar la satisfacción del cliente a través de sistemas de pago sin contacto y proveyendo sistemas de información. (NFC Organization)

Comunicación con el personal

Las etiquetas NFC permiten a los empleados registrar su ubicación y tiempo empleado en las labores, incluso su tiempo de descanso. El saber donde está un empleado es de vital importancia para los administradores para mantener el negocio trabajando correctamente. Según como ellos terminen tareas o comiencen nuevas, pueden actualizar su agenda de tareas diarias y en donde las realizan. (NFC Organization)

Actualizaciones en tiempo real

Las actualizaciones son muy importantes en el rápido mundo de los negocios, rastrear a los empleados o leer actualizaciones del personal, permite a los administradores manejar eficientemente la calendarización y planificación del día a día. Si un cliente necesita ayuda, el administrador lo único que hace es acercar su dispositivo NFC y puede observar quien está libre en el departamento para que acuda a ayudar al cliente. (NFC Organization)

Mejoramiento de Servicio al cliente

Adicionalmente al sistema de pago sin contacto, NFC permite a los clientes buscar información, simplemente acercando su dispositivo a un producto, el cliente puede observar el detalle del producto, observar artículos similares,

del mismo fabricante, relacionados, complementarios, especificaciones técnicas, etc. También permite ahorrar tiempo permitiendo al cliente cargar previamente en su teléfono cupones o recolectar puntos automáticamente por sus compras, eliminando la necesidad que la cajera escanee cupones por separado y aplicar complejos sistemas de descuentos. (NFC Organization)

Sea cual fuera el ámbito, el modo de comunicación o el beneficiario, la tecnología NFC busca incluirse en nuestra vida cotidiana y ofrecer numerosas funcionalidades que nos ayuden a realizar nuestra tareas diarias y nuestras vidas más simples.

Una descripción más a profundidad sobre las áreas de aplicación será detallada en el capítulo 3: Áreas de Aplicación y Modelos de Negocio basados en NFC.

1.3 Evolución de NFC

Para poder comprender el funcionamiento de la tecnología NFC y hacer un pronóstico de la futura aplicación de la misma, se tiene que viajar algunos años atrás hacia los inicios de la tecnología RFID. Se puede decir que NFC es una extensión de RFID que también hace uso de interfaces tecnológicas por medio de tarjetas inteligentes. (Coskun, Ok y Ozdenizci)

Para lograr dicho entendimiento es necesario comprender los pasos evolutivos de las tecnologías predecesoras a NFC:

Tecnología de código de barras

La tecnología de código de barras, aún utilizada en la actualidad, tiene una larga historia. La primera patente fue registrada en octubre de 1952 por los inventores Joseph Woodland, Jordin Johanson y Bernard Silver en Estados Unidos (Wikipedia), llegando a tener gran impacto comercial en la década de 1980.

El principio de funcionamiento es bastante sencillo: un código de barras es una representación visual que almacena datos relacionados a un cierto objeto o producto. Estas representaciones visuales son escaneadas por un lector de código de barras y los datos se transfieren a un sistema computacional conectado al lector. Después de este proceso de lectura, el computador es capaz de procesar estos datos para obtener la información que se necesite.

La representación visual de los códigos de barras también ha sufrido una evolución a lo largo de este tiempo para ajustarse a requerimientos relacionados principalmente con el máximo número de códigos disponibles en cada versión. Las primeras aplicaciones consistían en imágenes que representaban datos por medio líneas paralelas que variaban en ancho y espacio, a esta primera representación se la conoce como Una-dimensión (1D). La siguiente versión conocida como Dos-dimensiones (2D) insertó información de identificación adicional para cada representación.

Entre los ejemplos más representativos de códigos de barras lineales se encuentran: EAN13, Code 128, Code 39, Code 93, UPC. Respecto a los códigos de barras bidimensionales se tiene: PDF417, Datamatrix y Código QR.

Tecnología RFID

RFID (Radio Frequency Identification o Identificación por Radiofrecuencia) es una tecnología que proporciona almacenamiento y recuperación de datos mediante el uso de ciertos dispositivos conocidos como etiquetas (*tags* en inglés), o tarjetas RFID. La comunicación se da mediante el intercambio de datos a través de ondas de radio y usa un esquema de funcionamiento similar al de los códigos de barra, es decir se emplea un lector RFID y las mencionadas etiquetas electrónicas.

Las etiquetas electrónicas son circuitos integrados que pueden almacenar una pequeña cantidad de datos. Existen dos tipos de etiquetas, las etiquetas pasivas y las etiquetas activas. Las etiquetas de modo pasivo no poseen alimentación electrónica,

su funcionamiento se resume a que un lector RFID introduce una pequeña corriente eléctrica para que el circuito integrado en la etiqueta puede operar y de esta manera transmitir los datos requeridos. Por otro lado, las etiquetas activas cuentan con su propia fuente de alimentación capaz de hacer funcionar el circuito integrado para lograr la transferencia de datos. Las etiquetas activas son más confiables ya que tienen menos errores de operación por lo que se consideran eficientes en ambientes un tanto caóticos para radiofrecuencia como la implementación en grandes distancias o entornos con metal o agua.

La mayor diferencia que se puede notar entre RFID y la tecnología de código de barras está en su precio, RFID requiere de mayores inversiones ya que las etiquetas RFID son circuitos integrados a comparación de un código de barras que es únicamente una representación visual que incluso puede ser distribuida digitalmente. Sin embargo, RFID ha permitido que una cantidad interesante de aplicaciones se lleguen a desarrollar, como control de inventarios, control de acceso, seguimiento de artículos y personas, sistemas de transporte, peajes, entre otros.

Tecnología de tarjetas inteligentes

Una tarjeta inteligente es un ítem que contiene un circuito integrado que posee memoria, y en la mayoría de los casos involucra un microcontrolador seguro. (Coskun, Ok y Ozdenizci). Las tarjetas inteligentes no poseen fuente de alimentación, la energía es proporcionada por un lector o un dispositivo externo. De acuerdo a su interfaz, las tarjetas inteligentes se dividen en tres grupos; tarjetas inteligentes de contacto, tarjetas inteligentes sin contacto y tarjetas híbridas.

Las tarjetas inteligentes de contacto requieren de una unión directa con un lector para su funcionamiento, para ello poseen contactos metálicos que deben ser insertados en una ranura, alimentando de esta manera a la tarjeta y logrando la transferencia de datos. Todo esto se encuentra normalizado bajo el estándar ISO/IEC 7816 e ISO/IEC 7810.

Las tarjetas inteligentes sin contacto realizan la transferencia de datos solo cuando los dispositivos se encuentran a una distancia cercana de proximidad, es por ello que la comunicación entre lector y tarjeta se da por medio de inducción, en donde el lector propaga una señal electromagnética y la tarjeta es alimentada por la señal. Entre los estándares utilizados en este modo de operación se tiene ISO/IEC 10536, ISO/IEC 14443 e ISO/IEC 15693.

Finalmente una tarjeta híbrida es una tarjeta sin contacto a la cual se le adiciona un circuito de contacto. De esta manera se puede usar la tarjeta en diferentes situaciones, por ejemplo en entornos que requieren mayor seguridad se puede usar el circuito de contacto y en situaciones que requiere transacciones rápidas se puede usar el circuito sin contacto.

La tecnología NFC

Esta tecnología ofrece una forma simple e intuitiva de comunicar dos dispositivos compatibles con NFC, simplemente al acercarlos, se genera un campo magnético el cual hace posible la comunicación entre los dispositivos. (123seminaronly).

NFC es uno de los términos de moda en estos días, sin embargo, es una tecnología aún en desarrollo que ha dado lugar a un número interesante de aplicaciones en diferentes áreas de la vida cotidiana. La tecnología NFC está enfocada principalmente a ser empleada en teléfonos inteligentes donde las aplicaciones van desde transmisión de contenidos pasando por la interacción con electrónicos del hogar como cines en casa hasta el pago móvil.

Conclusión del Capítulo

Durante el desarrollo de este capítulo se pudo conocer los datos básicos de la tecnología como su rango de alcance, frecuencia utilizada, modos de comunicación y operación, así como los beneficios que pueden representar su uso en la vida cotidiana; ya sea facilitando nuestros pagos o reemplazando los tickets de transportación con la ayuda de un teléfono inteligente, inclusive mejorando el rastreo de una evolución médica o simplemente para compartir nuestras visitas a lugares en las redes sociales. De igual manera se citó los beneficios que pueden percibir las empresas al utilizar NFC, tales como: el mejoramiento de la comunicación con su personal, rastreo de localización, identificación de acceso hasta el mejoramiento del servicio al cliente brindando información por medio de etiquetas NFC.

Finalmente se observó la evolución de la tecnología, partiendo de una representación gráfica de líneas como el código de barras, pasando por las tarjetas inteligentes que incluyeron por primera vez un microcontrolador para realizar operaciones computacionales y llegando a RFID que se constituyó como la primera tecnología inalámbrica de identificación y formó la base del funcionamiento de lo que luego llegaría a ser la tecnología NFC.

CAPÍTULO 2

LA TECNOLOGÍA NFC

En este segundo capítulo se detalla las especificaciones técnicas de la tecnología NFC, tales como: interfaces de comunicación, protocolos, estructura interna y componentes de los lectores, etiquetas y telefono móviles con NFC. De la misma forma se define los conceptos físicos que hacen posible la comunicación: electromagnetismo, campo magnético, inductancia, etc. Finalmente se incluye una comparación con otras tecnologías de comunicación inalámbricas como Bluetooth, RFID e Infrarrojo.

2.1 Especificaciones Técnicas

Una vez que se han explicado los conceptos esenciales sobre la tecnología NFC en el capítulo 1, es momento de especificar los detalles técnicos de esta tecnología inalámbrica. Para lo cual es necesario ampliar a fondo la estructura de NFC y de los dispositivos NFC (lectores, etiquetas y teléfonos móviles), puesto que estos componentes deben apegarse a los estándares para ofrecer una correcta comunicación. (Coskun, Ok y Ozdenizci)

Dispositivos Inteligentes con NFC

Los dispositivos NFC está disponibles en tres presentaciones: teléfonos móviles, lectores y etiquetas.

Teléfonos Móviles

Un dispositivo móvil con NFC está compuesto por varios circuitos integrados, elementos de seguridad y una interfaz NFC, dicha interfaz está constituida por un contacto frontal analógico/digital, una antena NFC y por un circuito integrado

controlador que permite realizar las transacciones (Coskun, Ok y Ozdenizci). Adicionalmente cada teléfono tiene por lo menos un elemento de seguridad, el cual provee un entorno seguro y dinámico para los programas y sus datos, protegiendo el almacenamiento de datos confidenciales e importantes como información de tarjetas de crédito las cuales permiten realizar pagos sin contacto. Las interfaces más comunes entre los elementos seguros y el controlador NFC son: El protocolo de cable sencillo (*Single Wire Protocol SWP*) y la interfaz cableada NFC (NFC Wired Interface NFC-WI), el elemento seguro puede ser accedido tanto del controlador interno como desde el campo de radio frecuencia externo. (Coskun, Ok y Ozdenizci)

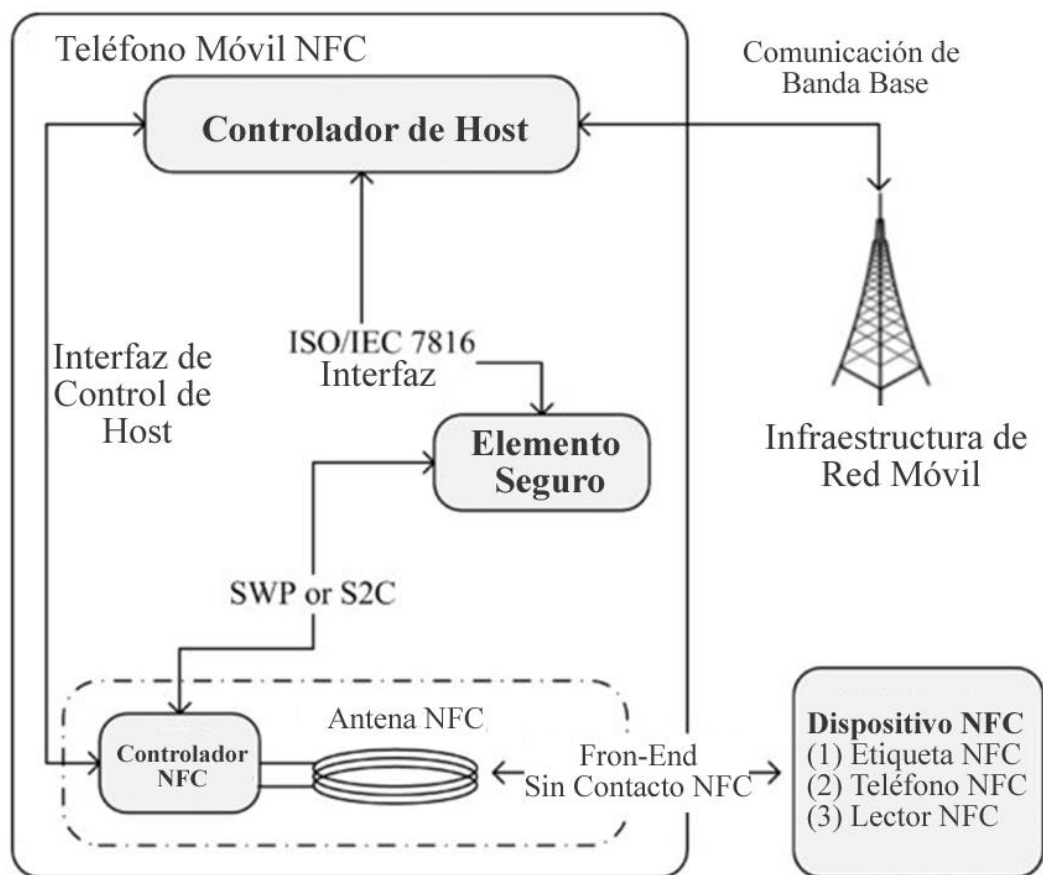


Ilustración 4. Arquitectura de un teléfono móvil con NFC

(Coskun, Ok y Ozdenizci)

EL controlador del equipo anfitrión (*Host Controller*) es el corazón del teléfono móvil, la interfaz del controlador (*Host Controller Interface-HCI*) constituye un puente entre el controlador NFC y el controlador del equipo anfitrión. La interfaz

ISO/IEC 7816 soporta la conexión del elemento seguro con el controlador del anfitrión, el cual configura el modo de operación a través de la interfaz del controlador, procesa los datos que son enviados o recibidos y establece la conexión entre el controlador NFC y el elemento seguro. (Coskun, Ok y Ozdenizci)

Elemento Seguro (SE)

Está formado por una combinación de hardware, software, interfaces y protocolos embebidos en un aparato móvil que garantiza un almacenamiento seguro. Dicho componente también necesita de un sistema operativo para funcionar, el cual puede ser: MULTOS o JavaCard OS, etc. (Coskun, Ok y Ozdenizci) Todo esto es necesario para crear un ambiente seguro puesto que ciertas transacciones poseen datos valiosos o información privada como puede ser el realizar pagos, información de tarjetas de crédito, datos personales, etc. Si no existiera este elemento, el teléfono simplemente recibiría o transmitiría información, dejando la puerta abierta para que la información del teléfono y la memoria interna pueda ser capturada, manipulada e incluso eliminada.

Las aplicaciones que requieren de confidencialidad de los datos necesitan ejecutarse y almacenarse en la memoria de un elemento seguro de un teléfono móvil. Varios módulos pueden servir como elementos seguros: Tarjetas de Memoria seguras (*Secure Memory Card- SMC*), hardware embebido y tarjetas universales de circuitos integrados (*Universal Integrated Circuit Cards*) como la sim del mismo teléfono, etc. (Coskun, Ok y Ozdenizci)

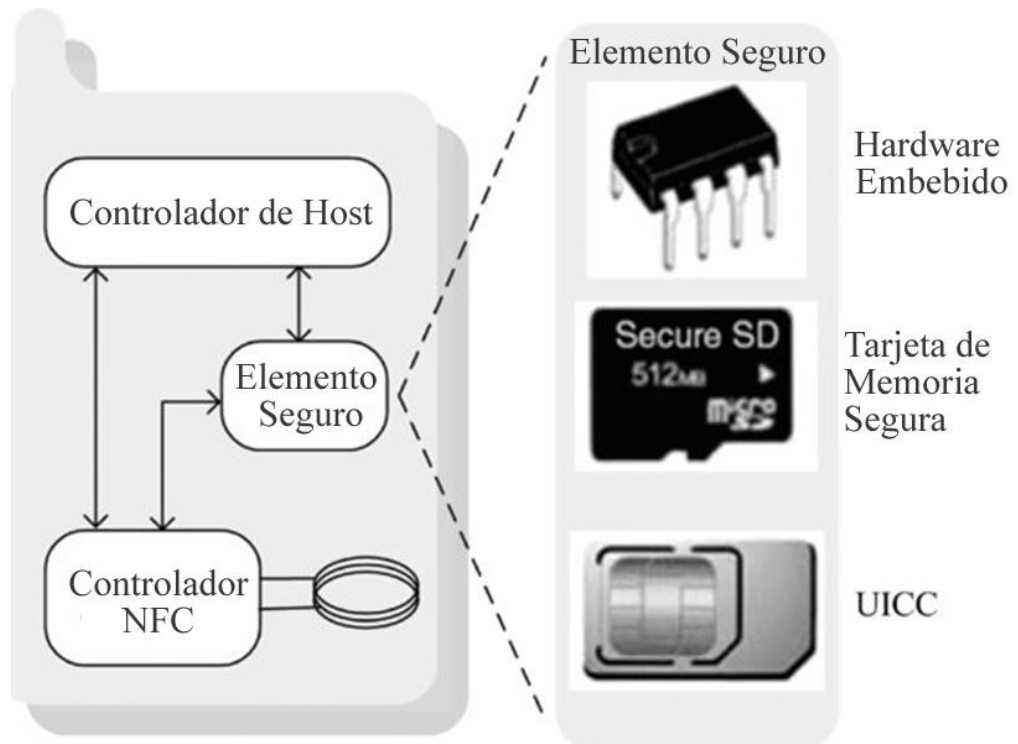


Ilustración 5. Modelos de Elementos Seguros (SE)

(Coskun, Ok y Ozdenizci)

Hardware Embebido: es una tarjeta soldada al teléfono que no puede ser removida, lo que garantiza que no pueda ser transferida a otro teléfono. Este chip es colocado durante la fabricación del teléfono y deberá ser personalizada después que el dispositivo es entregado al usuario, y hacerlo de nuevo en caso que el teléfono pase a un nuevo dueño. A pesar que este hardware cumple todos los estándares para las tarjetas inteligentes, su comunicación con el teléfono aún no ha sido estandarizada. (Coskun, Ok y Ozdenizci)

Tarjetas de Memoria Segura (SMC): están compuestas de una memoria, una tarjeta segura embebida y un controlador inteligente de tarjetas. Ofrece el mismo grado de seguridad que una tarjeta de memoria y cumple con todos los estándares, interfaces y entornos para tarjetas inteligentes como: EMV, *GlobalPlatform*, ISO/IEC 7816 y JavaCard. (Coskun, Ok y Ozdenizci) Al ser una tarjeta removible y de gran capacidad, permite almacenar gran

cantidad de aplicaciones y no necesita reeditarse cada vez que el usuario adquiere un nuevo teléfono, puesto que se puede transferir a otro dispositivo fácilmente.

Tarjetas universales de circuitos integrados (UICC): es una tarjeta inteligente que se implementa en la SIM del dispositivo. De igual manera que el tipo anterior, esta cumple con todos los estándares para tarjetas inteligentes, adicionalmente puede almacenar varias aplicaciones de distintos fabricantes, este tipo de elemento seguro, protege la integridad y seguridad de todo tipo de información personal y es ideal para aplicaciones de: pago, venta de tickets, pasaportes electrónicos y similares. (Coskun, Ok y Ozdenizci)

Interfaz NFC

Está compuesto de un contacto analógico/digital de entrada (*NFC Contactless Front-end NFC CLF*), una antena NFC y el circuito integrado controlador de NFC. El controlador NFC permite la conexión en el teléfono, funcionando como modulador-demodulador entre la señal análoga de radio frecuencia y la antena NFC. El controlador NFC soporta tanto comunicación activa como pasiva, de igual forma los modos de operación punto a punto, lectura/escritura y emulación de etiquetas, incluso suele ser compatible con el estándar RFID ISO/IEC 15693. La interfaz lógica del NFC CLF define el protocolo de la capa de datos más alto, así como la forma en la que los mensajes son transmitidos entre el elemento seguro y el NFC CLF. (Coskun, Ok y Ozdenizci)

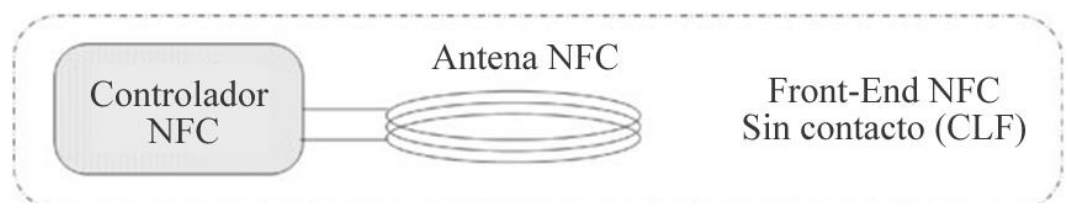


Ilustración 6. Estructura de la Interfaz NFC

Fuente: (Coskun, Ok y Ozdenizci)

Interfaz entre el SE y el controlador NFC

Para el diseño de esta interfaz se suele utilizar dos protocolos principalmente NFC-WI y SWP. La diferencia principal entre estos 2 protocolos, es que mientras SWP emplea una línea física, NFC-WI utiliza 2 líneas.

NFC-WI

También denominado S2C, es una interfaz de cable digital estandarizado por las normas ECMA 373, ISO/IEC 28361 y ETSI TS 102 541. En este modelo de protocolo, el elemento seguro es un transductor y el controlador NFC es el Font-end del mismo. El elemento seguro está conectado al controlador NFC por medio de 2 cables, el uno utilizado como señal de entrada y el otro como señal de salida. (Coskun, Ok y Ozdenizci)

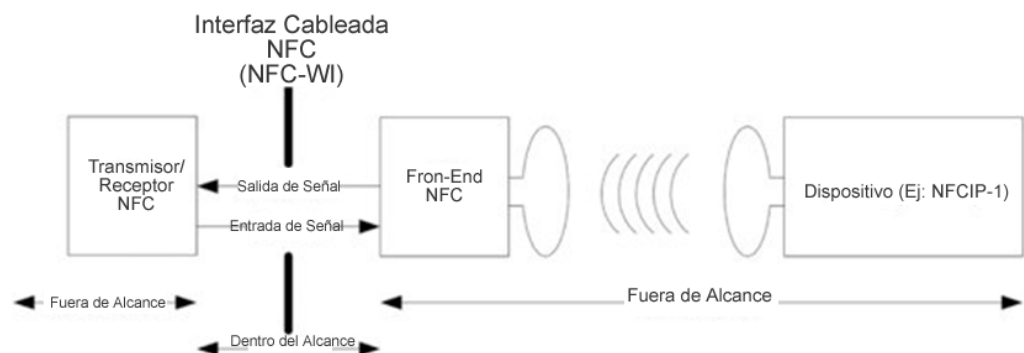


Ilustración 7. Arquitectura del protocolo NFC-WI

Fuente: (Coskun, Ok y Ozdenizci)

El transductor maneja el cable de la señal de entrada y recibe datos a través de la señal de salida. En el front-end maneja el cable de la señal de salida y recibe datos a través de la señal de entrada. La interfaz digital cableada lleva 2 señales binarias las cuales son definidas como alta (HIGH) y baja (LOW), ambas transmiten señales moduladas entre el controlador NFC y el elemento seguro, para luego ser digitalmente recibidas o enviadas por la interfaz de

radio frecuencia. .El protocolo NFC-WI maneja 3 velocidades: 106, 212 y 424 kbps. (Coskun, Ok y Ozdenizci)

SWP

Este protocolo está estandarizado por la norma ETSI TS 102 613, es un protocolo digital full dúplex. La velocidad de transmisión de los datos puede oscilar entre 212 kbps hasta 1.6 Mbps para una distancia menor a 10cm. Este es un protocolo orientado a bits para una comunicación punto a punto entre el elemento seguro y el controlador NFC. Su principio de funcionamiento es similar al de maestro-esclavo, el controlador NFC sería el maestro mientras que el elemento seguro sería el esclavo. El protocolo SWP es principalmente utilizado para ser empleado con tarjetas UICC en los teléfonos móviles. (Coskun, Ok y Ozdenizci)

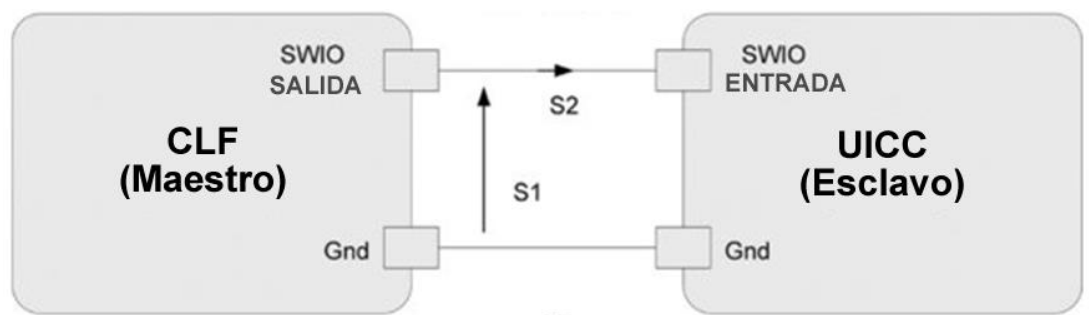


Ilustración 8. Transmisión de datos por SWP

Fuente: (Coskun, Ok y Ozdenizci)

Los teléfonos inteligentes son los dispositivos NFC más importantes, ya que la incorporación de NFC en los mismos, ha permitido una gran oportunidad para su facilidad de uso y aceptación del ecosistema por parte del usuario. (Coskun, Ok y Ozdenizci) Esto se debe en gran medida al incremento en la producción de teléfonos con NFC y a su distribución por todo el globo, en la siguiente figura se puede apreciar un pronóstico (Rebello):

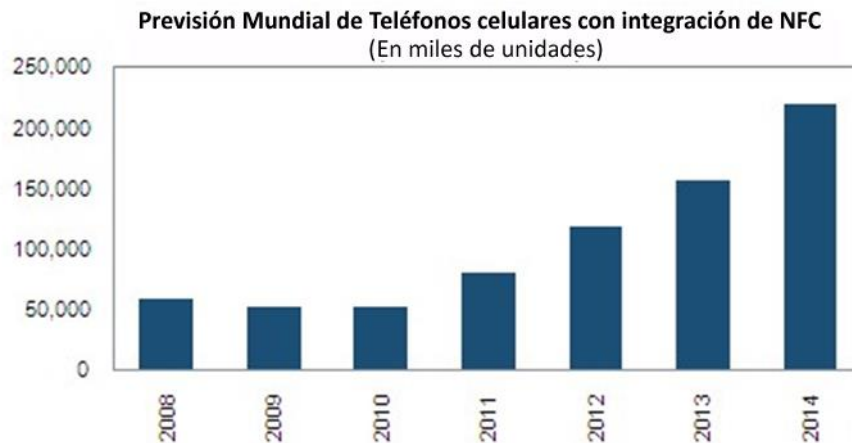


Ilustración 9. Pronóstico Mundial de Teléfonos con NFC

Fuente: (Rebello)

Actualmente existen 104 modelos distintos de teléfonos inteligentes con tecnología NFC embebida. (RapidNFC)

Lectores

Es un dispositivo capaz de transferir datos a otro dispositivo con NFC. Tal vez el ejemplo más conocido de este tipo de dispositivo sean los puntos de venta ubicados en muchas tiendas, dichos terminales permiten realizar pagos sin contacto al acercar un teléfono móvil a un lector. De la misma forma se pueden encontrar lectores en estaciones de tren o metro, máquinas expendedoras, etc.



Ilustración 10. Aplicaciones de los lectores NFC

(Fuente: Autoría Propia)

Etiquetas

Las etiquetas NFC trabajan a través de un dispositivo activo, el cual genera un campo magnético el cual induce una corriente eléctrica en la antena del dispositivo pasivo y de esta forma enciende el chip NFC de la etiqueta. Entonces la etiqueta NFC crea un campo magnético adicional el cual puede ser leído por el dispositivo activo permitiendo de esta forma la transmisión de datos. (RapidNFC)

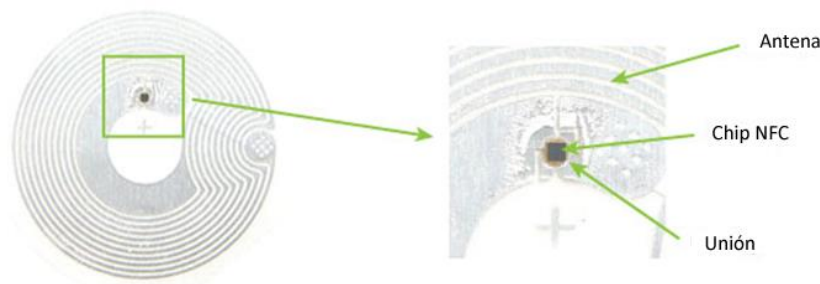


Ilustración 11. Componentes de una etiqueta NFC

Fuente: (RapidNFC)

La Antena

Está fabricada usualmente de aluminio, pero también existen de cobre, este último elemento es más costoso para utilizar que el aluminio pero su desempeño es superior. Técnicamente hablando no son antenas del todo, en realidad son solo inductores diseñados para convertir el campo magnético cercano en energía. La antena está diseñada cuidadosamente para operar a la frecuencia deseada de 13.56 MHz de la forma más eficiente y efectiva posible. El grosor de la antena no afecta el rendimiento de la misma, razón por la cual las etiquetas pueden ser tan delgadas como un adhesivo. En tanto que el largo si afecta el funcionamiento, mientras más larga la antena tendrá un mejor desempeño, como los teléfonos móviles no producen demasiada energía el tamaño de la antena se ve limitado.

Dada la variedad de presentaciones (brazaletes, adhesivos, llaveros,) de las etiquetas NFC, su construcción puede ser de dos tipos. Una bobina de cobre que se denomina “*E-Unit*” o la presentación de circuito impreso “*Printed Circuit Board-PCB*”, esta

última es más resistente y permite su encapsulación en módulos plásticos. (RapidNFC)



Ilustración 12. Tipos de Antenas NFC

Fuente: (RapidNFC)

El punto de Unión (*Bonding*)

Este componente es considerado el talón de Aquiles de las etiquetas NFC, puesto que este se rompe cuando la etiqueta se dobla demasiado. Es el punto de unión es la conexión entre el chip NFC y la antena. Debido a su fragilidad muchas empresas están desarrollando puntos de unión flexibles, pero estos prototipos aún no han presentado resultados confiables como para utilizarlos. (RapidNFC)

La tecnología NFC brinda un soporte y apoyo muy importante para la computación ubicua, es decir colabora a la realización de tareas cotidianas del usuario, sin complicadas interacciones y configuraciones. (Bonalde) En este sentido la tecnología NFC trabaja de una forma muy intuitiva, dos dispositivos inician inmediatamente su comunicación tan pronto como entran en contacto; este acercamiento ejecuta el disparador condicional para la comunicación NFC. (Coskun, Ok y Ozdenizci)

Conexión

En cada sesión de comunicación NFC, el dispositivo que inicializa la comunicación es denominado “Iniciador”, en tanto que el dispositivo que responde la solicitud del iniciador se denomina “destino”, esta tipo de conexión es una analogía de la

arquitectura cliente-servidor, en la cual un cliente inicializaba la comunicación y el servidor contestaba dicha solicitud. (Coskun, Ok y Ozdenizci)

Si se habla de un modo de comunicación activo/pasivo, este ocurre cuando un componente NFC tiene incorporado su propia fuente de poder y puede generar su propio campo de radio frecuencia, este será el dispositivo que inicializa y guía la comunicación, por lo tanto se denomina “dispositivo activo”. Por otro lado si el componente no posee una fuente de poder incorporada, se lo conoce como “dispositivo pasivo” y su función será únicamente responder al dispositivo activo. (Coskun, Ok y Ozdenizci)

El “iniciador” siempre necesitará ser un dispositivo activo, puesto que necesita una fuente de poder para inicializar la comunicación, en tanto que el “destino” puede ser un dispositivo activo o un pasivo. Si el dispositivo destino es un componente activo, este usa su propia fuente de poder para responder, pero si es un componente pasivo, usará la energía creada por el campo electromagnético que generó el dispositivo iniciador que es un componente activo. (Coskun, Ok y Ozdenizci) Una vez dicho esto, se puede afirmar que las etiquetas NFC son siempre componentes pasivos, puesto que no disponen de una fuente de poder incorporada, lo que les hace artículos de bajo costo y poca capacidad, únicamente están destinados para almacenar datos que puedan ser leídos por un dispositivo activo.

2.2 Electromagnetismo y Transferencia de datos

Los sistemas NFC y RFID operan de acuerdo al principio de acoplamiento inductivo (Bilginer y Ljunggren), por lo tanto, para entender los procedimientos de potencia y transferencia de datos es necesario una base teórica de los principios del fenómeno magnético. A continuación se desarrolla una descripción de los principales conceptos de electromagnetismo.

Campo Magnético

a) Intensidad de Campo Magnético

Las cargas eléctricas en movimiento (Flujo de Corriente) generan un campo magnético, la magnitud de dicho campo está descrito por la intensidad de campo magnético H . En forma general se puede decir que, la integral de contorno de la intensidad de campo magnético a lo largo de una curva cerrada, es igual a la sumatoria de las intensidades de corriente dentro de ella. (Bilginer y Ljunggren)

Como se describe en la ecuación siguiente:

$$\sum I = \oint \vec{H} \cdot \vec{ds}$$

Si el conductor es recto, la intensidad de campo H a lo largo de una línea de flujo circular a una distancia r es constante. (Bilginer y Ljunggren)

Y puede ser expresada como:

$$H = \frac{1}{2\pi r}$$

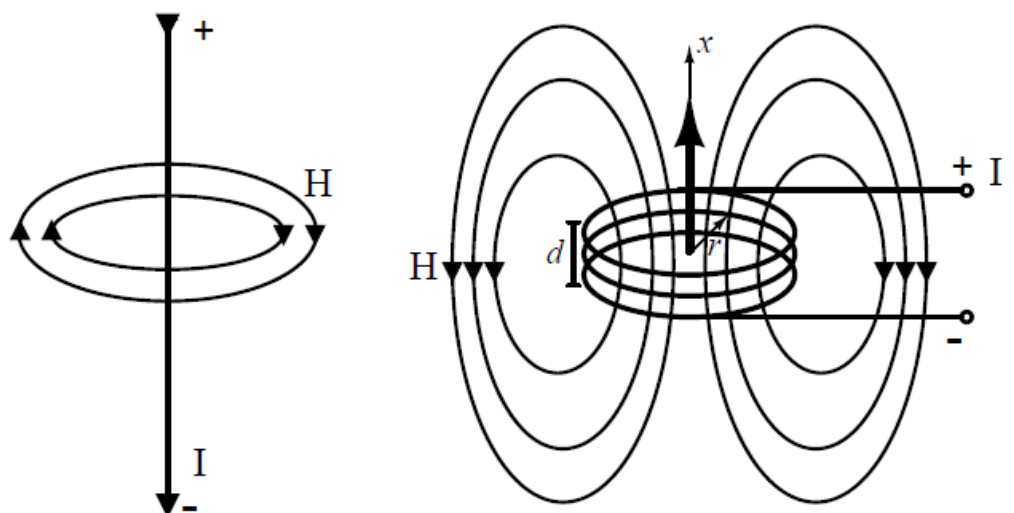


Ilustración 13. Líneas de flujo magnético alrededor de un conductor y una bobina cilíndrica

Fuente: (Bilginer y Ljunggren)

Los anillos hechos de un material conductor son utilizados como antenas magnéticas, para generar el campo magnético alterno en los dispositivos de acoplamiento inductivo de sistemas RFID o NFC (Bilginer y Ljunggren).

La intensidad de campo magnético H , tiende a disminuir a medida que el punto de medición es alejado del eje de la bobina (Ilustración 13). La intensidad de campo magnético a lo largo del eje x de una bobina puede ser calculada mediante la fórmula:

$$H = \frac{I \cdot N \cdot r^2}{2\sqrt{(r^2 + x^2)^3}}$$

En donde: N es el número de vueltas, r es la radio de los círculos de las vueltas, x es la distancia del centro de la bobina en la dirección x . (Bilginer y Ljunggren)

b) Flujo Magnético y Densidad de Flujo Magnético

El flujo magnético es una medida de la cantidad de campo magnético que pasa a través de una determinada superficie, y es simbolizada como ϕ_m . (Bilginer y Ljunggren)

La densidad de flujo magnético es la medida de la cantidad de flujo magnético por unidad de área de una sección, perpendicular a la dirección del flujo. Su representación magnética es:

$$B = \frac{\phi_m}{A}$$

En donde: B es la densidad de flujo magnético medida en teslas (T), ϕ_m es el flujo magnético medido en weberios (Wb) y A es el área en metros cuadrados (m^2).

La relación entre la densidad de flujo magnético B y la intensidad de campo magnético H es:

$$B = \mu_0 \cdot \mu_r \cdot H = \mu \cdot H$$

En donde: μ_0 es la constante de campo magnético ($\mu_0 = 4\pi \cdot 10^{-7} \frac{H}{m}$), la cual describe la permeabilidad del vacío. La variable μ_r es llamada la permeabilidad relativa, e indica que tan mayor o menor que μ_0 es la permeabilidad de un material. (Bilginer y Ljunggren)

c) Inductancia, L

Cuando la corriente circula en un conductor de cualquier forma, un campo magnético es generado a su alrededor. Este campo será más fuerte si el conductor tiene forma de bobina. Una bobina consiste en realizar N vueltas de la misma área A y a través de la cual fluye una corriente I . Cada vuelta contribuye en igual cantidad al flujo magnético. (Bilginer y Ljunggren)

Dicho flujo puede ser expresado como:

$$\psi = \sum_N \phi_N = N \cdot \phi = N \cdot \mu \cdot H \cdot A$$

La relación entre el flujo magnético y la intensidad se denomina inductancia y es simbolizada por L .

$$L = \frac{\psi}{I} = \frac{N \cdot \phi}{I} = \frac{N \cdot \mu \cdot H \cdot A}{I}$$

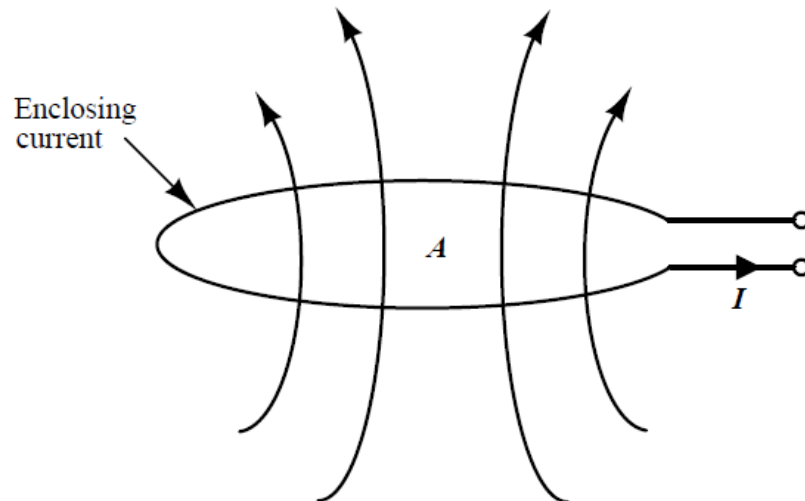


Ilustración 14. Definición de Inductancia, L

Fuente: (Bilginer y Ljunggren)

La inductancia de una vuelta de conductor depende de la geometría de la figura y de la permeabilidad del medio en el que el flujo circula.

d) Inductancia Mutua, M

La inductancia mutua describe el acoplamiento de 2 circuitos con un campo magnético y siempre existe entre 2 circuitos eléctricos. Su unidad de medida y dimensión son las mismas que para la inductancia. Este es el concepto físico en el cual basan su funcionamiento los sistemas RFID. (Bilginer y Ljunggren)

Si una segunda vuelta de conductor con un área A_2 , es colocada en la cercanía de la primera vuelta de conductor con un área A_1 por la cual una corriente está circulando, provocará que una porción del total de flujo magnético que circula por el área A_1 , sea desviada y fluya también por el área A_2 . Como resultado, las dos vueltas de conductor denominadas como bobinas, se conectan a través de este flujo. (Bilginer y Ljunggren)

La magnitud del flujo de acoplamiento ψ_{21} depende de la distancia de separamiento que tiene la una bobina de la otra, las propiedades magnéticas

del medio y de las dimensiones de las bobinas. El radio del flujo parcial ψ_{21} delimitado por la segunda bobina, a la corriente I_1 en la primera bobina, es igual a la inductancia mutua M_{21} de la segunda bobina en relación a la primera. (Bilginer y Ljunggren)

Como se describe en la siguiente ecuación:

$$M_{21} = \frac{\psi_{21}(I_1)}{I_1} = \oint_{A_2} \frac{B_2(I_1)}{I_1} \cdot dA_2$$

Para la inductancia M_{12} , el flujo de acoplamiento ψ_{12} en la primera bobina está determinado por la corriente I_2 que fluye a través de la segunda bobina.

$$M = M_{12} = M_{21}$$

e) Coeficiente de Acoplamiento

El coeficiente de acoplamiento es una forma conveniente de especificar el grado de acoplamiento eléctrico que existe entre dos circuitos. El coeficiente de acoplamiento κ se expresa como:

$$k = \frac{M}{\sqrt{L_1 \cdot L_2}}$$

En donde ($0 \leq k \leq 1$), un valor de κ cercano a 0 significa un alto desacoplamiento por ejemplo debido a la distancia, en tanto que, un valor de κ cercano a 1 significa un alto acoplamiento. Si $\kappa = 1$ entonces las bobinas están sujetas al mismo flujo magnético. (Bilginer y Ljunggren)

f) Ley de Faraday

Un cambio en el flujo magnético genera una intensidad de campo eléctrico E_i , la cual esta descrita por la ley de Faraday. El efecto del campo magnético depende del material de su recubrimiento. (Bilginer y Ljunggren)

La ley de Faraday en su forma general se describe como:

$$\mu_i = \oint E_i \cdot ds = - \frac{d\psi(t)}{dt}$$

Para el caso puntual de una bobina de N vueltas, dicha ecuación puede ser expresada como:

$$\mu_i = N \cdot \frac{d\psi}{dt}$$

Una variante de tiempo en la intensidad $i_1(t)$ en la primera bobina, genera una variante de tiempo del flujo magnético $\frac{d\phi(i_1)}{dt}$, la cual provoca que un voltaje sea inducido en ambas bobinas. Se debe diferenciar entre dos casos: la inductancia propia y la inductancia mutua.

En el caso de la inductancia propia, el cambio de flujo generado por el cambio de corriente, induce un voltaje en el mismo conductor del circuito. En tanto que, en la inductancia mutua el cambio de flujo generado por el cambio de corriente induce un voltaje en conductor del circuito adyacente. (Bilginer y Ljunggren)

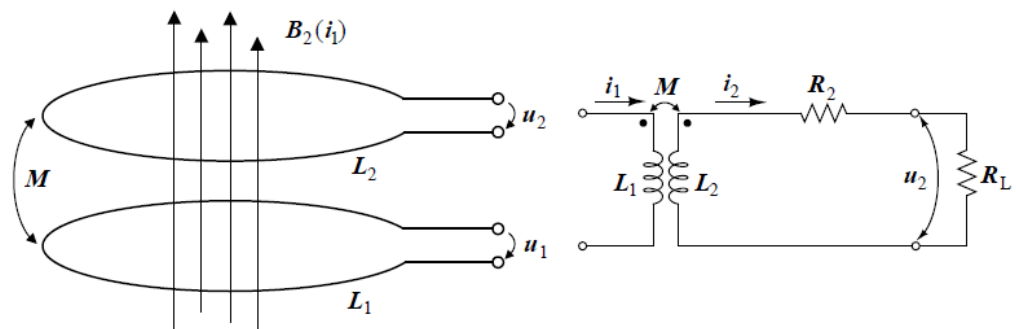


Ilustración 15. Bobinas acopladas y diagrama del circuito equivalente para dos bobinas acopladas

Fuente: (Bilginer y Ljunggren)

En un sistema RFID, L_1 representaría la antena del transmisor del lector, mientras que L_2 representaría la antena del objetivo.

El consumo de corriente del chip esta simbolizado por la resistencia de carga R_L . Una variación en el tiempo del flujo en la primera bobina L_1 inducirá un voltaje U_{2i} en la segunda bobina L_2 debido a la inductancia mutua M . Una caída de voltaje a través de la resistencia de la bobina R_2 será provocada por el flujo de corriente, lo que significará que el voltaje u_2 puede ser medido por medio de R_L . Se generará un flujo magnético opuesto al flujo magnético $\psi_1(i_1)$ debido al flujo de corriente que atraviesa L_2 . (Bilginer y Ljunggren)

Esto fenómeno puede ser descrito por medio de la ecuación:

$$u_2 = + \frac{d\psi_2}{dt} = M \frac{di_1}{dt} - L_2 \frac{di_2}{dt} - i_2 R_2$$

2.3 Modos de Comunicación

Como ya se indicó anteriormente la comunicación NFC ocurre entre dos dispositivos habilitados para poder gestionar la conexión y transferencia de datos en un rango de corto alcance. Dichos dispositivos pueden funcionar de diferentes maneras y es por ello que el estándar NFC hace una distinción en los modos de comunicación que se pueden llegar a tener.

La primera clasificación que se debe comprender es que existen dispositivos que cuentan con una fuente de poder embebida, por lo que son capaces de generar su propio campo de radio frecuencia, a estos dispositivos se los conoce como dispositivos activos. En el otro lado, existen dispositivos que únicamente se alimentan de la fuente de poder del campo de radio frecuencia generado por otro dispositivo, a estos se los conoce como dispositivos pasivos.

Una segunda clasificación a considerar, es que se puede distinguir a los dispositivos según un punto de vista algorítmico. Si un dispositivo es capaz de liderar el proceso de comunicación, ya sea solicitando o enviando datos hacia el receptor, se le conoce como un dispositivo activo. Al contrario si se trata de un dispositivo que únicamente

responde peticiones de otro, a este se lo conoce como dispositivo pasivo. Por lo general, la primera clasificación relacionada a la fuente de poder coincide con la clasificación desde un punto de vista algorítmico, ya que el escenario común es que el dispositivo que cuenta con la fuente de poder sea el encargado de iniciar el liderar una sesión de comunicación NFC.

Una vez detallados estos conceptos se puede entender como una interface NFC opera, para ello existen dos modos de comunicación diferentes:

Modo de comunicación pasiva

En este caso el dispositivo emisor proporciona un campo portador y el dispositivo receptor responde modulando el campo existente. Es decir únicamente un dispositivo genera un campo de radio frecuencia, mientras el otro usa modulación de carga para transferir los datos (Coskun, Ok y Ozdenizci). En este modo el receptor obtiene el poder de operación por el campo electromagnético proporcionado por el emisor. Un ejemplo de este modo es la comunicación entre un teléfono móvil y una etiqueta NFC, es decir conexión entre dispositivos activados por energía y etiquetas pasivas.

Modo de comunicación activa

Tanto el emisor como el dispositivo receptor se comunican por la generación alternada de sus propios campos. Uno de los dispositivos debe desactivar su campo de radio frecuencia mientras espera la llegada de datos. Para este modo ambos dispositivos deben contar un una fuente de poder o energía. Un claro ejemplo de este tipo de comunicación es la realizada entre dos teléfonos móviles, es decir la comunicación entre 2 dispositivos que tengan una fuente de poder activa y capacidades computacionales (Coskun, Ok y Ozdenizci).

En la siguiente tabla se puede apreciar las diferentes combinaciones de dispositivos que generan como resultados los modos de comunicación Activo o Pasivo.

Dispositivo A	Dispositivo B	Descripción	Modo de Comunicación
Activo	Activo	El campo RF es generado por los 2 dispositivos	Modo Activo
Activo	Pasivo	El campo RF es generado por el dispositivo A única	Modo Pasivo
Pasivo	Activo	El campo RF es generado por el dispositivo B única	Modo Pasivo

Ilustración 16. Modos de Comunicación Activo o Pasivo

Fuente: (Coskun, Ok y Ozdenizci)

Un concepto adicional que se debe considerar para la correcta armonía en la comunicación NFC, es el de iniciador y destino. El iniciador es aquel dispositivo que inicia una sesión de comunicación, esto lo hace mediante el envío de un mensaje de petición al destino, y obviamente el destino es aquel que recibe la petición de comunicación por parte del iniciador y envía un mensaje de retorno.

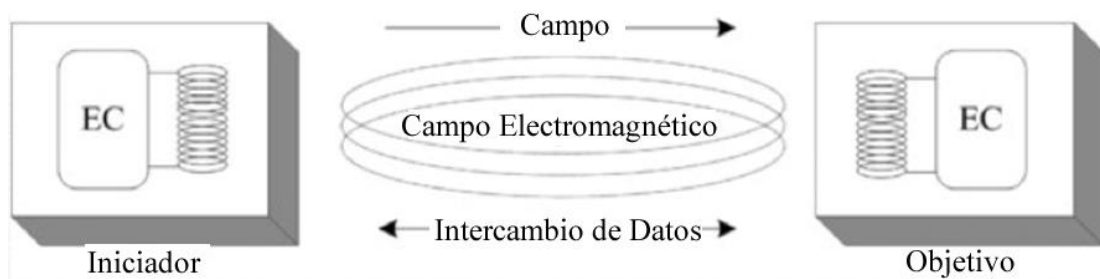


Ilustración 17. Rol iniciador o destino

Fuente: (Coskun, Ok y Ozdenizci)

La siguiente tabla muestra las posibles combinaciones de dispositivos activos/pasivos con relación al rol de iniciador/destino. Se puede apreciar que un dispositivo activo puede actuar tanto como iniciador o destino, mientras que un dispositivo pasivo se limita únicamente a ser un destino.

Rol	Disp. Activo	Disp. Pasivo
Iniciador	Es posible	No es posible
Objetivo	Es posible	Es posible

Fuente: (Coskun, Ok y Ozdenizci)

Ilustración 18. Combinación de Rol iniciador o destino y modos activo o pasivo

Como ya se indicó anteriormente, la comunicación NFC se da entre dos dispositivos habilitados, los mismos que pueden ser de tres tipos distintos: teléfonos móviles habilitados con NFC, etiquetas NFC o lectores NFC. La siguiente tabla resume el rol que puede tomar cada tipo de dispositivo.

Disp. Iniciador	Disp. Objetivo
Móvil NFC	Etiqueta NFC
Móvil NFC	Móvil NFC
Lector NFC	Móvil NFC

Ilustración 19. Rol de cada tipo de dispositivo

Fuente: (Coskun, Ok y Ozdenizci)

2.4 Modos de Operación

Los dispositivos habilitados con NFC son capaces de operar en tres modos distintos:

Modo punto a punto

Este es el modo clásico de operación de Near Field Communication, permite una conexión bidireccional de datos entre dos dispositivos con NFC, a una velocidad aproximada de 424 kBit/seg. Las propiedades de electromagnetismo y el protocolo

usado en este modo de operación se encuentran estandarizados en la ISO/IEC 18092 como NFCIP-1 y ECMA 320/340 (ISO/IEC 18092 (ECMA-340)).

En la siguiente imagen se puede observar la arquitectura de comunicación del modo de operación punto a punto.

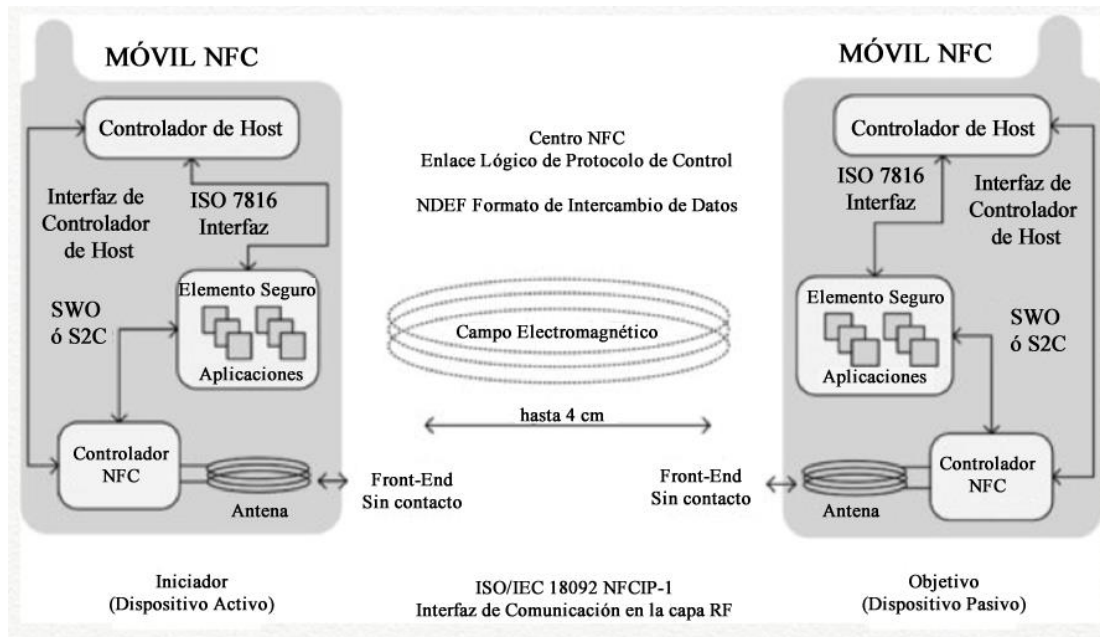


Ilustración 20. Arquitectura de Comunicación del Modo Punto a Punto

Fuente: (Coskun, Ok y Ozdenizci)

Protocolos de la arquitectura del modo punto a punto

Un dispositivo NFC que se encuentre operando en un modo punto a punto cuenta con la siguiente estructura de elementos de protocolos.

- Protocolos análogos y digitales estandarizados por NFCIP-1.
- LLCP permite la transferencia de información de capas superiores. Define un protocolo de enlace OSI y es esencial para la comunicación que involucra una transferencia bidireccional. LLCP proporciona cinco servicios:

- Transporte sin conexión: este modo de transporte puede ser usado si los protocolos de capas superiores implementan su propio flujo de control del mecanismo.
 - Transporte orientado a la conexión: ofrece un servicio de transmisión de datos secuenciado y garantizado.
 - Activación, supervisión y desactivación de enlace: LLPC indica como los dispositivos reconocen implementaciones LLCP compatibles, establecen un enlace, supervisan la conexión y desactivan el enlace.
 - Comunicación asíncrona balanceada: con el uso de un Modo Asíncrono Balanceado, cualquiera de los puntos de servicio son capaces de inicializar, supervisar, recuperarse de errores y enviar información en cualquier momento.
 - Protocolo de multiplexación: LLCP es capaz de habilitar varias instancias de protocolos de nivel superior al mismo tiempo.
- Enlaces de protocolo proporcionan un enlace estándar a los protocolos NFC Forum.
 - Protocolos NFC Forum son aquellos definidos por NFC Forum para enlazar a LLCP, como OBEX e IP.
 - Protocolo de intercambio NDEF permite el intercambio de NDEF mensajes.
 - Aplicaciones que corren sobre el protocolo de intercambio NDEF o sobre los protocolos de NFC Forum.

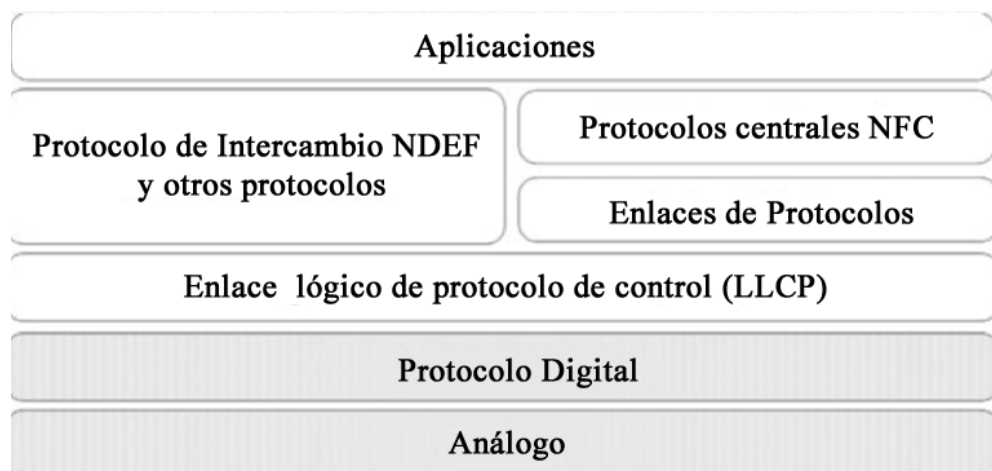


Ilustración 21. Protocolos de la Arquitectura del Modo Punto a Punto

Fuente: (Coskun, Ok y Ozdenizci)

Modo escritura / lectura

Una funcionalidad adicional de los dispositivos NFC es la habilidad de leer y escribir etiquetas y tarjetas inteligentes habilitadas con NFC. Como ya se indicó en el modo de comunicación pasiva, el dispositivo activo actúa como un emisor e inicia la comunicación inalámbrica y puede leer y escribir datos sobre una etiqueta NFC que actúa como un receptor pasivo. En este modo de operación la velocidad de transmisión de datos se aproxima a los 106 Kbit/seg. El modo de operación escritura / lectura está basado en la ISO/IEC 14443 Tipo A, Tipo B y el esquema FeliCa. (Coskun, Ok y Ozdenizci)

En la siguiente imagen se puede observar la arquitectura de comunicación del modo de operación escritura / lectura.

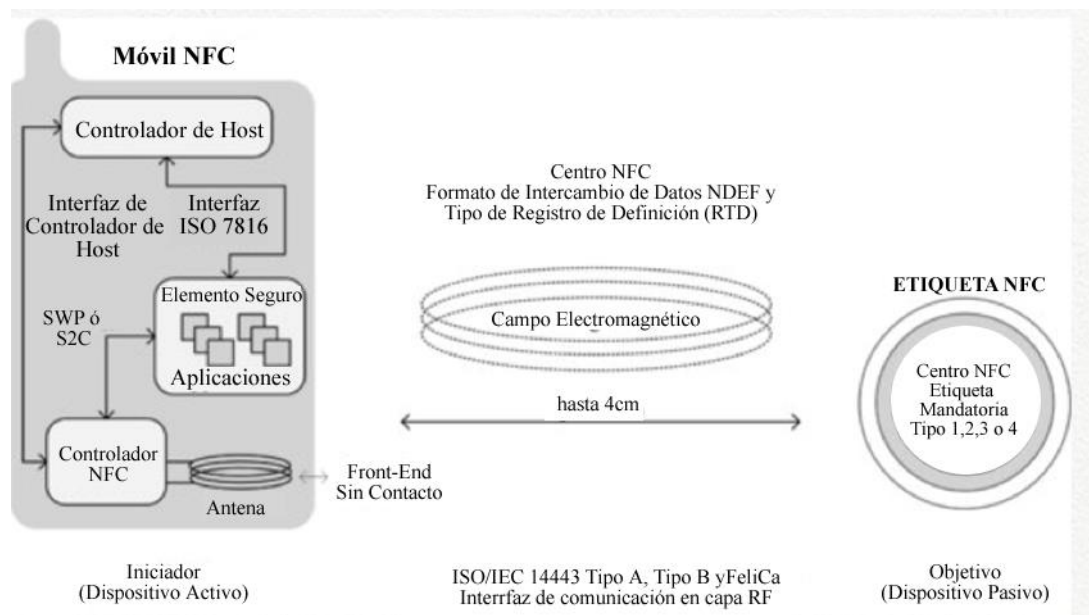


Ilustración 22. Arquitectura de Comunicación del Modo Escritura-Lectura

Fuente: (Coskun, Ok y Ozdenizci)

Protocolos de la arquitectura del modo escritura / lectura

Un dispositivo NFC que se encuentre operando en un modo escritura / lectura tiene la siguiente estructura de elementos de protocolos.

- Protocolos análogos y digitales en la capa inferior. Protocolo análogo hace referencia a las características de radio frecuencia de dispositivos NFC y determina el rango de operación de los mismos. Los protocolos digitales se refieren a los aspectos digitales establecidos en los estándares ISO/IEC 18092 e ISO/IEC 14443.
- Operaciones de etiqueta que indican los comandos e instrucciones que deben utilizar los dispositivos para manejar y habilitar operaciones de lectura y escritura sobre las etiquetas establecidas por el NFC Forum que pueden ser de Tipo 1, Tipo 2, Tipo 3 y Tipo 4. (Coskun, Ok y Ozdenizci)
- Aplicaciones NDEF son basadas en las especificaciones NDEF.
- Aplicaciones no NDEF son definidas por especificaciones propias de los vendedores y no están basadas en las especificaciones NDEF. (Coskun, Ok y Ozdenizci)

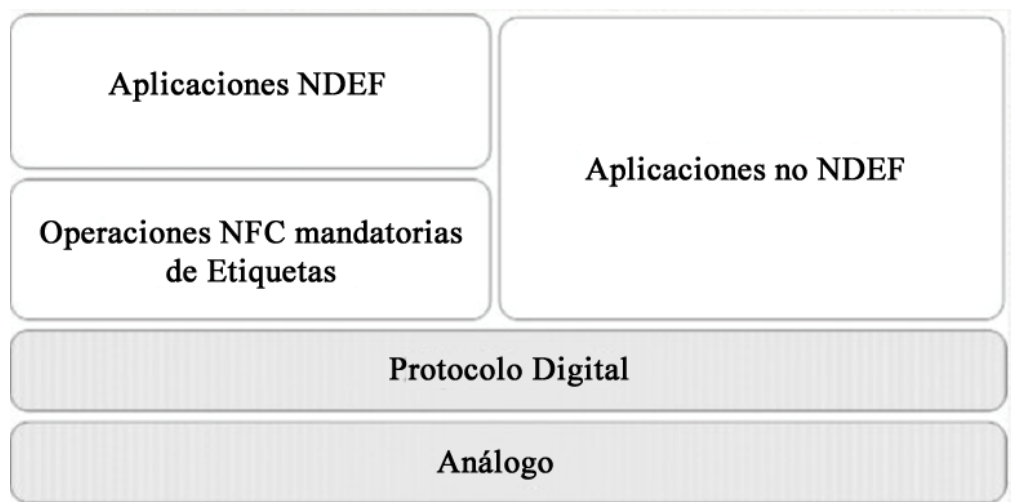


Ilustración 23. Protocolos de la Arquitectura del modo escritura-lectura

Fuente: (Coskun, Ok y Ozdenizci)

Modo de emulación de etiquetas

En este modo los dispositivos habilitados con NFC pueden emular el comportamiento y propiedades de una tarjeta inteligente con el estándar ISO/IEC 14443 Tipo A y Tipo B, y FeliCa. Un lector no tiene la capacidad de distinguir entre un dispositivo operando en modo de emulación o una tarjeta inteligente ordinaria. Esto implica una gran ventaja, puesto que actualmente existe una infraestructura de lectura desarrollada para tarjetas inteligentes, estas no tienen que ser reemplazadas y se las puede aprovechar con tecnología NFC.

En este modo de operación un dispositivo habilitado con NFC no genera su propio campo de radio frecuencia ya que el lector NFC es el encargado de crearlo, por lo que el dispositivo NFC se comporta como una tarjeta o etiqueta estándar. En la siguiente imagen se puede observar la arquitectura de comunicación del modo de operación emulación de etiquetas.

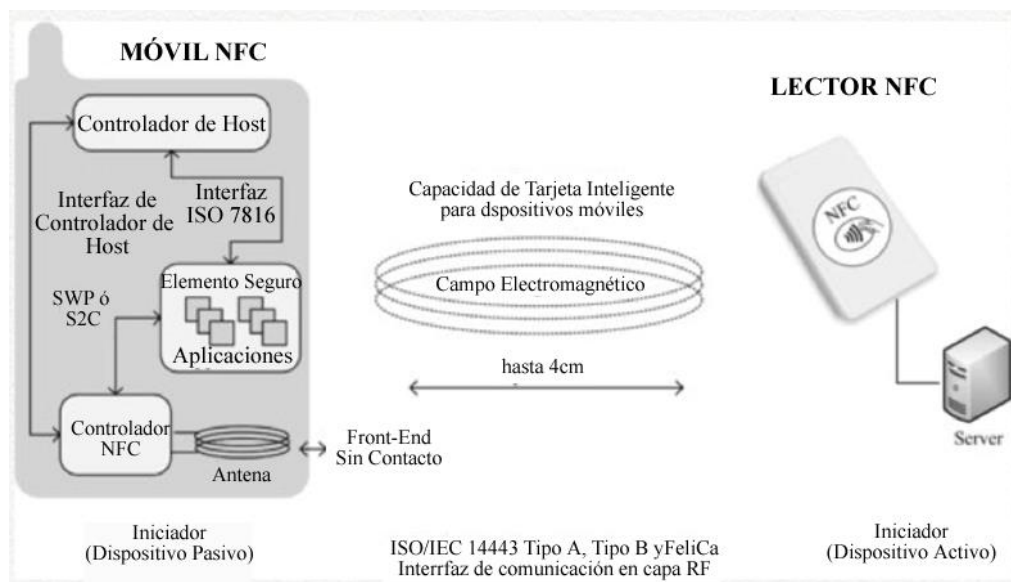


Ilustración 24. Arquitectura de Comunicación Emulación de Etiquetas

Fuente: (Coskun, Ok y Ozdenizci)

Protocolos de la arquitectura del modo emulación de etiquetas

Dispositivos que operan en el modo emulación de etiquetas usan protocolos análogos y digitales similares al de las tarjetas inteligentes ya que son compatibles con los mismos estándares.



Ilustración 25. Protocolos de la Arquitectura del modo emulación de etiquetas Estándares y Protocolos

Fuente: (Coskun, Ok y Ozdenizci)

2.5 Comparación NFC con RFID

Se comenzará definiendo la tecnología RFID, para posteriormente puntualizar sus diferencias frente a NFC.

Radio Frequency Identification (RFID), es una tecnología de comunicación para intercambiar datos entre un lector RFID y una etiqueta RFID mediante ondas de radio, esta tecnología fue patentada en 1983. (Rapid NFC)

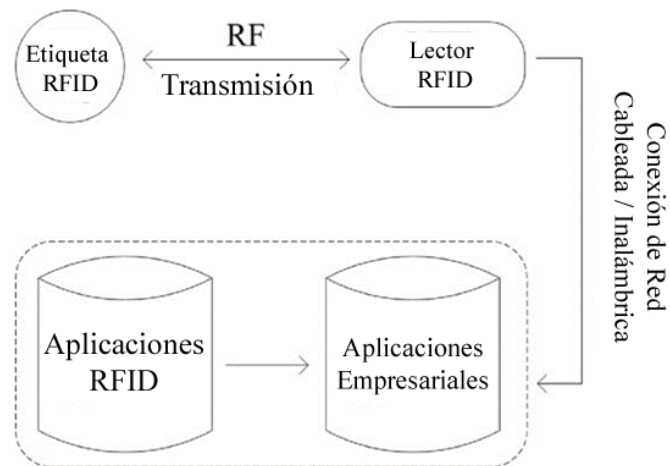


Ilustración 26. Arquitectura de un sistema RFID

Fuente: (Coskun, Ok y Ozdenizci)

Las etiquetas RFID generalmente están compuestas de un circuito integrado (IC) y una antena. El IC proporciona el almacenamiento de datos y su procesamiento, además de la modularización y de-modularización de la señal de radiofrecuencia. Por otro lado la antena permite que la señal sea recibida y transmitida. (Coskun, Ok y Ozdenizci)

Un sistema RFID está formado por 2 componentes, el transpondedor y el lector. El transpondedor es el componente el cual está localizado en un producto u objeto que va a ser identificado, y el lector es el componente que leerá o escribirá los datos del transpondedor. (Coskun, Ok y Ozdenizci)

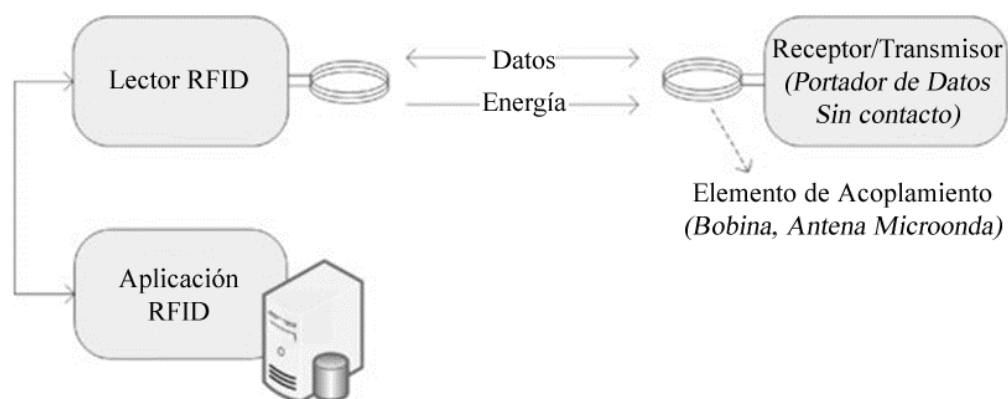


Ilustración 27. Componentes de un Sistema RFID

Fuente: (Coskun, Ok y Ozdenizci)

El transpondedor está compuesto de un elemento de unión y un IC el cual almacena los datos, en realidad el transpondedor es comúnmente llamado etiqueta RFID. Una vez que la etiqueta está en el rango del lector RFID, es activado por las señales de entrada. (Coskun, Ok y Ozdenizci)

El lector típicamente está conformado de un transceptor (o un módulo de lata frecuencia) con un decodificador, el cual interpreta los datos, además consta de una unidad de control y un antena. (Coskun, Ok y Ozdenizci)

RFID permite una comunicación inalámbrica en una sola vía, las etiquetas RFID pueden ser escaneadas a distancias de hasta 100 m sin la necesidad de una línea de vista hacia el lector, gracias a esta característica ha sido implementada en sistemas de seguimiento en bodegas, manejo de equipaje en aeropuertos, inventarios, etc. RFID opera en un rango de radio frecuencias, cada una de las cuales posee sus propios estándares y protocolos. (Rapid NFC)

Banda de Frecuencia RFID	Distancia de Escaneo
120-150 kHz (Baja Frecuencia, LF)	Hasta 10 cm
13.56 MHz (Alta Frecuencia, HF)	Hasta 1 m
433 MHz (Ultra Alta Frecuencia, UHF)	1-100 m
856-868 MHz & 902-928 MHz (Frecuencia Ultra Ligera Alta , UHF)	1-2 m
2450-5800 MHz (Microonda)	1-2 m
3.1-10 GHz (Microonda)	Hasta 200 m

Ilustración 28. Bandas de Frecuencia, Protocolos y distancias de operación de RFID

Fuente: (Rapid NFC)

Una vez que se ha definido la tecnología RFID, es momento de puntualizar sus diferencias y similitudes en comparación a la tecnología NFC.

Básicamente las tecnologías de RFID y NFC utilizan los mismos estándares para su funcionamiento. (123seminarsonly)

- NFC opera a 13.56 MHz y es una extensión de los estándares de Alta Frecuencia (HF) de RFID. (Rapid NFC)
- NFC posibilita una comunicación en dos vías, por lo tanto puede ser utilizado para interacciones más complejas como emulación de tarjetas y comunicación punto a punto (RapidNFC) , en tanto que RFID están diseñados para una comunicación de escritura/lectura simplemente. (Falke, Rukzio y Dietz, Mobile Services for Near Field Communication)
- La comunicación NFC está limitada a una distancia de 5cm o menos (Rapid NFC), lo cual es ideal para sistemas de pago, venta de tickets o pasaportes electrónicos, brindando una seguridad extra, en tanto que la tecnología RFID al brindar una distancia casi de 100m no brinda un entorno deseable puesto que cualquier persona malintencionada podría recibir la información de un usuario y clonarla en su dispositivo. (Mundo NFC)
- Solo es posible escanear una etiqueta NFC a la vez. (Rapid NFC)
- Gracias a la capacidad de NFC de operar en el modo emulación de etiquetas, es posible reemplazar tarjetas RFID con un teléfono inteligente con NFC por ejemplo. (123seminarsonly)
- Las etiquetas RFID también pueden funcionar en modos activos o pasivos. (Coskun, Ok y Ozdenizci)
- Tal vez la diferencia más importante entre estas tecnologías es, que NFC se incorporó a un teléfono inteligente, con el propósito de realizar de pagos a través de los móviles, aprovechando la limitación de interacciones de proximidad a una distancia pequeña. (Rapid NFC).

	HF RFID	NFC
Frecuencia de Operación	13.56 MHz	13.56 MHz
Comunicación	Una vía	Dos vías
Estándares	ISO 14443, 15693 18000	ISO 14443
Distancia de Escanéo	Hasta 1 m	Hasta 10 cm
Escaneo Simultáneo de Etiquetas	Sí	No

Ilustración 29. Tabla comparativa entre RFID y NFC

Fuente: (Rapid NFC)

2.6 Comparación NFC con Bluetooth

Bluetooth es una tecnología basada en un protocolo de comunicación, que permite la transmisión de datos y voz entre diferentes dispositivos de bajo consumo, dentro de una red inalámbrica de área personal (WPAN), para ello hace uso de un enlace por radiofrecuencia en la banda de los 2.4 GHz.

Los principales dispositivos que aprovechan las ventajas de esta tecnología son los teléfonos móviles, computadores personales, computadoras portátiles, impresoras, cámaras digitales, entre otros. Las principales aplicaciones están enfocadas hacia el remplazo del tradicional cable para permitir la transferencia de datos, como por ejemplo controles remotos, transferencia de tarjetas de contacto, conexión de periféricos como teclado o mouse, enlaces en sistemas de audio, etc.

Tanto NFC como Bluetooth son tecnologías de comunicación inalámbrica de corto alcance y comparten algunas características relacionadas a la transmisión de datos, sin embargo, cada una tiene sus ventajas y desventajas que pueden resultar eficientes en ciertos escenarios, dependiendo de la aplicación y especificaciones requeridas.

Si se compara NFC con otras tecnologías que se han implementado para permitir transferencia de datos de forma inalámbrica, en este caso Bluetooth, se puede decir que NFC mejora la forma en que los dispositivos interactúan unos con otros, ya que en general proporciona conexiones estables y rápidas. (Wozniaki)

A continuación se indican las principales diferencias y similitudes entre la tecnología NFC y Bluetooth:

- La principal ventaja de NFC en relación a Bluetooth, es el tiempo de configuración de la conexión. En NFC se requiere un menor esfuerzo para establecer una conexión, ya que no es necesaria una configuración manual para identificar otro dispositivo, con NFC el reconocimiento es inmediato y por lo tanto el tiempo requerido para el establecimiento de la conexión es mínimo, se puede decir que es menor a 0.1 segundos.
- Una ventaja que Bluetooth tiene sobre NFC es el soporte de conexiones punto a multipunto, es decir, se puede conectar un dispositivo con varios al mismo tiempo, situación que no ocurre con NFC en donde la conexión es únicamente entre dos dispositivos habilitados.
- NFC cuenta con un menor rango de alcance, sin embargo, este alcance limitado es una característica que lo hace novedoso al funcionar mejor en áreas saturadas, ya que al tener menor distancia las interferencias son menores. Por el otro lado Bluetooth ofrece mayor distancia pero la interferencias pueden hacer que la tecnología sea inutilizable.
- La velocidad de transmisión NFC es menor que Bluetooth, en NFC es de 424 kbps y Bluetooth de 721 kbps.
- NFC consume menos energía que Bluetooth cuando ambos dispositivos actúan como dispositivos activos con su propia fuente de energía, caso contrario si uno de los dispositivos actúa como pasivo y tiene que ser

alimentado por el otro dispositivo, entonces Bluetooth resulta más eficiente en cuanto a consumo de energía.

- NFC es compatible con RFID, mientras que Bluetooth no lo es.
- Algo adicional, es que la especificación Bluetooth v4.0 (2010) incluye Bluetooth de alta velocidad y protocolos de bajo consumo con *Bluetooth Low Energy* (BLE), lo que proporciona características mejoradas que reducen el tiempo de establecimiento de la conexión y trata de alcanzar ventajas que ofrecen tecnologías como NFC. (Aguirre)

	<u>NFC</u>	Bluetooth
Tipo de red	Punto a punto	Punto a multipunto
Rango	<0.1 m	10 m
Velocidad	424 kbps (1Mbps a futuro)	721 kbps
Tiempo de configuración	<0.1 s	6 s
Modos	Activo-activo, activo-pasivo	Activo-activo
Compatible con RF ID	Si	No
Costos	Bajo	Moderado

Ilustración 30. Tabla comparativa entre Bluetooth y NFC

Fuente: (Paus)

2.7 Comparación NFC con Infrarrojo

IrDA (Infrared Data Association) creada en 1993 por empresas como HP, IBM, Sharp, entre otras, se diseñó con el fin de definir un estándar que permita la transmisión y recepción de datos por medio de un canal de rayos infrarrojos, es decir la comunicación se da a través del movimiento de rayos luminosos dentro del espectro infrarrojo.

IrDA está compuesta por un conjunto de protocolos estructurados en capas que permiten una comunicación bidireccional entre dos dispositivos.

A continuación se indican las principales diferencias y similitudes entre la tecnología NFC y la tecnología infrarrojo:

- La principal desventaja de infrarrojo, es que se necesita una línea de visión directa para permitir la conexión y la transferencia de datos entre dos dispositivos.
- La comunicación entre dispositivos con tecnología infrarrojo tiene un mayor grado de sensibilidad a influencias externas como la luz o reflejos.
- Tanto NFC como infrarrojo permiten conexiones punto a punto.
- La velocidad de transmisión NFC es mayor que infrarrojo, en NFC es de 424 kbps e infrarrojo de 115 kbps.
- NFC es compatible con RFID, mientras que infrarrojo no. (Paus)

	<u>NFC</u>	IrDa
Tipo de red	Punto a punto	Punto a punto
Rango	<0.1 m	1 m
Velocidad	424 kbps (1Mbps a futuro)	115 kbps
Tiempo de configuración	<0.1 s	0.5 s
Modos	Activo-activo, activo-pasivo	Activo-activo
Compatible con RF ID	Si	No
Costos	Bajo	Bajo

Ilustración 31. Tabla comparativa ente Infrarrojo y NFC

Fuente: (Paus)

Conclusión del Capítulo

Una vez que se pudo detallar técnicamente el funcionamiento de la tecnología NFC (interfaz de conexión, componentes, modos de comunicación, modos de operación, protocolos). Así como los distintos componentes de los dispositivos de un entorno NFC, tales como etiquetas, lectores y dispositivos móviles. Se pudo establecer una comparación técnica con otras tecnologías de comunicación inalámbrica.

Para el caso de RFID, se puede destacar que es una tecnología con un alcance mayor (1m) y que brinda la oportunidad de un escaneo simultáneo de etiquetas, pero por otro lado NFC permite una comunicación bidireccional entre los dispositivos que se comunican.

Por otro lado la tecnología Bluetooth, al igual que RFID brinda un alcance mayor (10m aproximadamente) y de la misma forma posee una velocidad de transferencia superior (721Kbps vs 424 Kbps), como ventaja se destaca que la tecnología NFC representa un costo menor y funciona de manera intuitiva (acercar dos dispositivos).

Finalmente al analizar la tecnología de Infrarrojo, se destaca un alcance mayor (1m), en tanto que los beneficios de NFC recaen en su velocidad de transferencia (424Kbps vs 115Kbps) y mejora el tiempo de configuración entorno a su rival (0.1 segundos vs 0.5 segundos).

CAPÍTULO 3

ÁREAS DE APLICACIÓN Y MODELOS DE NEGOCIO BASADOS EN NFC

A pesar de que el enfoque de la tecnología NFC en la actualidad apunta hacia la estandarización de una estructura sólida y robusta para la realización de pagos electrónicos, existe una amplia variedad de campos en los que la tecnología se ha destacado y ha simplificado la realización de tareas cotidianas. En el mercado se pueden encontrar soluciones de control de acceso, pagos electrónicos, automatización de tareas, seguimiento y control médico, entre otras. En este capítulo se detallarán las características y ventajas de cada una de las áreas mencionadas, además de los posibles campos de aplicación de la tecnología en algunos años.

3.1 Control de Acceso

Antes de comenzar a describir los aspectos a tomar en cuenta en esta área de aplicación, es preciso diferenciar entre 2 posibles campos de aplicación: el primero es el control e identificación de personas u objetos, y el segundo es la emisión de entradas o tickets de acceso.

Identificación

Existen 2 sistemas principalmente utilizados para la identificación: Sistemas de Acoplamiento Cercano (*Close Coupled Systems*) y Sistemas de Acoplamiento Remoto (*Remote Coupled Systems*). (Rolf y Nilsson)

Sistemas de Acoplamiento Cercano

Se comenzará detallando los sistemas de emparejamiento cercano. Estos sistemas se basan en el estándar ISO 10536, estas tarjetas están diseñadas para trabajar con un

alto consumo de energía y a altas velocidades, su tasa de transferencia fluctúa entre (106-848 kbps), la transferencia de alto consumo facilita incluir un microprocesador junto con las tarjetas, pero al mismo tiempo su distancia de operación se ve limitada a (0.10 m). Un ejemplo de este tipo de tarjetas es el Sistema MIFARE desarrollado por Phillips, el cual ofrece memorias de distintos tamaños y con capacidades de procesamiento variadas, su memoria es segmentada para poder soportar un alto número de aplicaciones distintas. La memoria puede contener claves encriptadas u otros datos necesarios para realizar una autenticación segura, su ventaja en relación a los sistemas de acoplamiento remoto recae en que el objeto a ser identificado debe situarse cerca del lector lo cual disminuye la posibilidad de problemas de seguridad como el espionaje (*eavesdropping*), de la misma forma la tarjeta no debe ser insertada en el lector completamente, lo cual aumenta aún más la rapidez del tiempo de identificación, dicho proceso puede ser aplicado de la misma forma tanto para una persona, animal o cosa que se desee identificar. (Rolf y Nilsson)

Sistemas de Acoplamiento Remoto

Por otro lado, los sistemas de acoplamiento remoto contemplan 2 sub-estándares: tarjetas de aproximación (descritas en el estándar ISO 14443) y tarjetas de vecindad (detalladas en el estándar ISO 15693). A diferencia de las tarjetas de aproximación, las tarjetas de vecindad están diseñadas para trabajar con un consumo bajo de energía y a una velocidad lenta, usualmente a (26 Kbps), debido a la transferencia de energía baja, las tarjetas de memoria solo están disponibles en el formato de tarjetas de vecindad. Un ejemplo de su utilización es el sistema *I-CODE*, el cual fue diseñado para disminuir el precio por etiqueta lo más posible para competir contra el sistema de código de barras. Entre los beneficios que I-CODE ofrece están: manejar operaciones de lectura y escritura a distancias de hasta un metro, control anticolidión a través del uso de periodos de tiempo, cada etiqueta posee una memoria de 512 bits, la cual puede ser re-escrita 100.000 veces y posee una vida útil de 10 años. (Rolf y Nilsson)

También es importante citar que los sistemas destinados al control de acceso se pueden subdividir en: sistemas en línea (*Online Systems*) y sistemas fuera de línea (*Offline Systems*), a continuación se ampliará la información acerca de cada uno de estos tipos de sistemas. (Finkenzeller)

Sistemas en línea

Son utilizados en ambientes donde es necesaria la autorización de acceso para un gran número de personas pero con pocas entradas cada una, por ejemplo el acceso a edificios de oficinas o locales comerciales. En los sistemas de este tipo, todos los terminales están conectados a una computadora central por medio de una red. Esta computadora central ejecuta una base de datos, en la cual se encuentran todos los accesos autorizados para cada uno de los terminales, estos acceden a la base de datos por medio de la red para verificar cada petición de acceso, adicionalmente la bitácora de accesos es guardada en una tabla de la base. Los cambios de una autorización de acceso pueden ser hechos por medio de una sencilla entrada a la computadora del sistema de control de acceso, el soporte de datos no necesita estar presente, esto protege áreas importantes incluso en el caso que el soporte de datos haya sido extraviado. (Finkenzeller)



Ilustración 32. Ejemplo Sistema en línea: Legic-Installation Kaba Security Locking Systems

Fuente: (Finkenzeller)

Sistemas fuera de línea

Estos sistemas son principalmente utilizados en situaciones donde existen muchas habitaciones individuales a las cuales tienen acceso solo unas pocas personas. Cada terminal almacena una lista de identificación de claves (por ejemplo: clave genérica 3, habitación de invitados, cuarto de máquinas), no existe una red de conexión hacia otra terminal o hacia una computadora central. La información relacionada a las habitaciones a las cuales se puede dar acceso es almacenada en el soporte de datos en la forma de identificadores de claves. Cuando entra en funcionamiento la terminal compara el identificador de la clave almacenado en el soporte de datos con las claves almacenadas en su propia lista de permisos de acceso. En caso de visitas temporales se puede crear claves con tiempo de duración, por ejemplo para el caso de personas hospedadas en un hotel. Solo en el caso de que el soporte de datos no esté presente, es necesario eliminar los identificadores de las claves de la terminal. (Finkenzeller)



**Ilustración 33. Sistema fuera de línea integrado en una cerradura de puerta:
Häfele GmbH, D-Nagold**

Fuente: (Finkenzeller)

Al comparar los dos sistemas anteriormente citados se puede denotar que el sistema centralizado brinda una ventaja muy importante, en caso de requerirse cambios en los accesos, desde la computadora central se puede realizar dicho cambio, y las terminales automáticamente serán actualizadas con la nueva información, mientras que en los sistemas fuera de línea el cambio deberá ser ejecutado en cada una de las terminales que existan.

Ticketing

Esta aplicación de la tecnología NFC es un servicio del modo de operación de emulación de etiqueta (Coskun, Ok y Ozdenizci). Gracias a la alta eficiencia y bajo costo, numerosos sistemas para recolección automáticas de tarifas han sido implementados a nivel mundial (Rolf y Nilsson). En esta área los sistemas RFID han alcanzado una extraordinaria ventaja sobre los tickets comunes de papel o tarjetas magnéticas puesto que son menos sensibles al agua, al desgaste y a las fuerzas magnéticas o mecánicas. El proceso de validación es extremadamente rápido desde que las tarjetas ya no necesitan ser insertadas en una máquina sino solo se acercadas al frente de las mismas. La información y el saldo actual pueden ser almacenados en un pequeño chip de la tarjeta, de modo que no se recurra a una base de datos centralizada para consultar esta información, eliminando de esta manera la comunicación entre los lectores y el sistema centralizado de pagos, inclusive se puede encriptar la información para mantener su integridad y seguridad (Rolf y Nilsson), igualmente se evita la molestia de perder monedas, efectivo o tarjetas de crédito al pagar el ingreso a los medios de transporte. (Point About)

A pesar que muchas compañías de transportación utilizan la misma tecnología RFID, los sistemas MIFARE son muy populares en la transportación pública. El uso de RFID o teléfonos con NFC y adicionalmente la unificación de diferentes redes de transporte simplificaría la transportación pública para todos. Una de las empresas pionera en este ámbito es Nokia, la cual ha realizó muchos test utilizando el teléfono

Nokia 3220 con el sistema nacional de transportación pública en Alemania en 2005, gracias a su éxito, muchas alternativas de pago sin contacto están siendo desarrolladas a nivel mundial inclusive llegando a muchas tiendas para la realización de pagos.



Ilustración 34. Pago del sistema de transporte público en Alemania con un teléfono Nokia 3220

Fuente: (Point About)

Cabe recalcar que el servicio de *Ticketing* puede ser aplicado a medios de transporte como buses, trenes, metros, taxis, etc. Esta área constituye un importante nicho de mercado puesto que según la Asociación Americana de Transportación Pública, cerca de millones de personas dependen de los servicios de transporte masivo tan solo en Estados Unidos. (Point About)

De la misma forma el servicio de *Ticketing* puede ser empleado para pases de abordaje en aeropuertos, tickets electrónicos a eventos, conciertos, seminarios, convenciones, etc.

3.2 Transacciones Financieras

Actualmente existe una industria colaborando en el desarrollo e investigación de una infraestructura estandarizada y concisa para servicios de pagos electrónicos mediante NFC.

En general se puede identificar una serie de beneficios tanto para consumidores como para instituciones financieras o negocios que puedan hacer uso de NFC:

Consumidores:

- En cuanto a seguridad las credenciales de pago son almacenadas de forma segura en los dispositivos NFC, protegiendo dicha información de ataques o robos de datos.
- Los consumidores pueden efectuar diversas transacciones con una simple acción en sus teléfonos móviles habilitados con NFC, lo que permite ahorrar tiempo y evita que los usuarios tengan que usar varias veces la misma tarjeta de crédito física, además de que se puede dar soporte a pagos con múltiples marcas o cadenas financieras.
- Los teléfonos móviles proporcionan una interfaz intuitiva que permite a los consumidores usar la tecnología de forma rápida y segura.
- Se pueden aprovechar los diversos recursos de un teléfono inteligente habilitado con NFC como geo localización, lo que permite la realización de aplicaciones para brindar a los consumidores experiencias personalizadas, descuentos, ofertas, etc.
- Permitir a los consumidores contar con toda su información financiera centralizada dentro de un mismo dispositivo, son tener la preocupación de llevar múltiples tarjetas físicas para realizar sus transacciones.

- Existe una gran variedad de dispositivos que integran la tecnología NFC y hay muchos planes de fabricantes por incluirla en sus terminales, lo que permitirá a los usuarios tener diversas opciones de selección de un dispositivo NFC.

Instituciones financieras o negocios:

- Crear relaciones de fidelidad con los clientes al ofrecer servicios que combinen tecnología y contenidos mediante la ejecución y desarrollo de aplicaciones móviles habilitadas con NFC.
- Los lectores NFC requieren un menor mantenimiento lo que a la larga se refleja como ahorro.
- Reducir significativamente fraudes o problemas de seguridad que pueden degradar la reputación de las instituciones y representar gastos económicos.
- Máquinas habilitadas con NFC evitarían procesos de recolección de dinero por parte de las instituciones financieras, lo que facilitaría la implementación de las mismas generando estimulación en las ventas. (Smart Card Alliance)
- Los negocios o instituciones financieras se pueden enfocar en utilizar los terminales de pago con NFC como canales para publicidad y distribución de contenidos personalizados de ofertas y cupones para sus clientes. (Infocomm Development Authority of Singapore)

Ecosistema NFC

Aplicando la tecnología NFC se pueden crear sistemas móviles de pago sin contacto, en donde los dispositivos habilitados con NFC operan en el modo de emulación de tarjetas y se muestran ante los lectores como una tarjeta inteligente tradicional, de esta forma la información de pago es almacenada en el dispositivo móvil en un elemento seguro compuesto por un chip que protege los datos. Debido a que para los

pagos se usa el modo de emulación de tarjetas, se pueden habilitar los pagos con esta tecnología sin tener que realizar un cambio radical en la infraestructura actual.

Para implementar un entorno de pagos móviles sin contacto es necesario un ecosistema compuesto por varias entidades e interesados que aportan a que el proceso se cumpla satisfactoriamente:



Ilustración 35. Ecosistema NFC

Fuente: (RFID Point)

1. Elemento seguro: consiste de un microprocesador seguro compuesto por un procesador criptográfico que garantiza la seguridad en las transacciones y ofrece cierta capacidad de almacenamiento para guardar los datos de las aplicaciones de pago. Un elemento seguro puede ser implementado de tres formas diferentes: un elemento seguro MicroSD removible, en elemento seguro embebido, o un elemento seguro UICC removible.
2. Adquiridor: facilita la comunicación entre las transacciones de pago y la red de pago para la autorización y establecimiento.
3. Red de pago: facilita el proceso de autorización y el establecimiento de las transacciones de tarjetas bancarias.

4. Banco: lleva el control de la financiación de la cuenta del cliente entregando débitos y créditos según se requiera, pero además trabaja con terceros para proporcionar el sistema de pagos NFC en dispositivos móviles habilitados.
5. Expendedor: puede aceptar transacciones de pago NFC e implementar aplicaciones de pago NFC como tarjetas de regalo o una tarjeta de pago específica del expendedor.
6. Personalización Bureau: emisores de tarjetas y personalización bureau deben ser capaces de implementar aplicaciones para convertir la información de las tarjetas tradicionales en datos compatibles con la tecnología NFC que cuenta con chips que deben establecer procesos criptográficos y llaves de seguridad.
7. Set del fabricante: define cuáles serán los modelos de teléfonos inteligentes que contarán con la tecnología NFC de acuerdo a requerimientos y el nivel de demanda del mercado.
8. Operador red móvil: debe existir una configuración wireless para los dispositivos NFC y ciertas características y funciones que son proporcionadas por los operadores de dispositivos móviles.
9. Consumidor: es el consumidor de una aplicación de pago NFC.
10. Desarrollador Wallet: consiste en una interfaz que permite administrar múltiples aplicaciones de pago NFC, ofreciendo al consumidor varias opciones de pago que pueden ser proporcionadas por el proveedor de la solución de pago o algún otro proveedor o vendedor.
11. Proveedor del Sistema Operativo: mantiene el núcleo del sistema operativo para que pueda ser usado por varios desarrolladores y proporcionen aplicaciones compatibles y actualizaciones.
12. Proveedor de servicio de valor agregado: incluyen servicios adicionales como cupones, programas de fidelización, promociones, ofertas, servicios basados en localización, etc.
13. Administrador de servicio de confianza: facilita el manejo de las aplicaciones de pago NFC en los teléfonos de los consumidores. Algunas de las funciones proporcionadas por el administrador de servicios de confianza son: activación OTA (*over the air*), manejo del ciclo de vida de una transacción NFC en el teléfono del consumidor, servicios de transferencia de aplicaciones NFC a un nuevo dispositivo NFC cuando sea necesarios. (Smart Card Alliance)

Comparación de métodos de pago alternativos

A continuación se presenta una tabla que resume la comparación entre los pagos móviles usando NFC y otro tipo de servicios de pago, es importante indicar que estos valores y resultados cambian a lo largo del tiempo debido a varios factores como la madurez de las soluciones, aceptación del entorno y desarrollos técnicos:

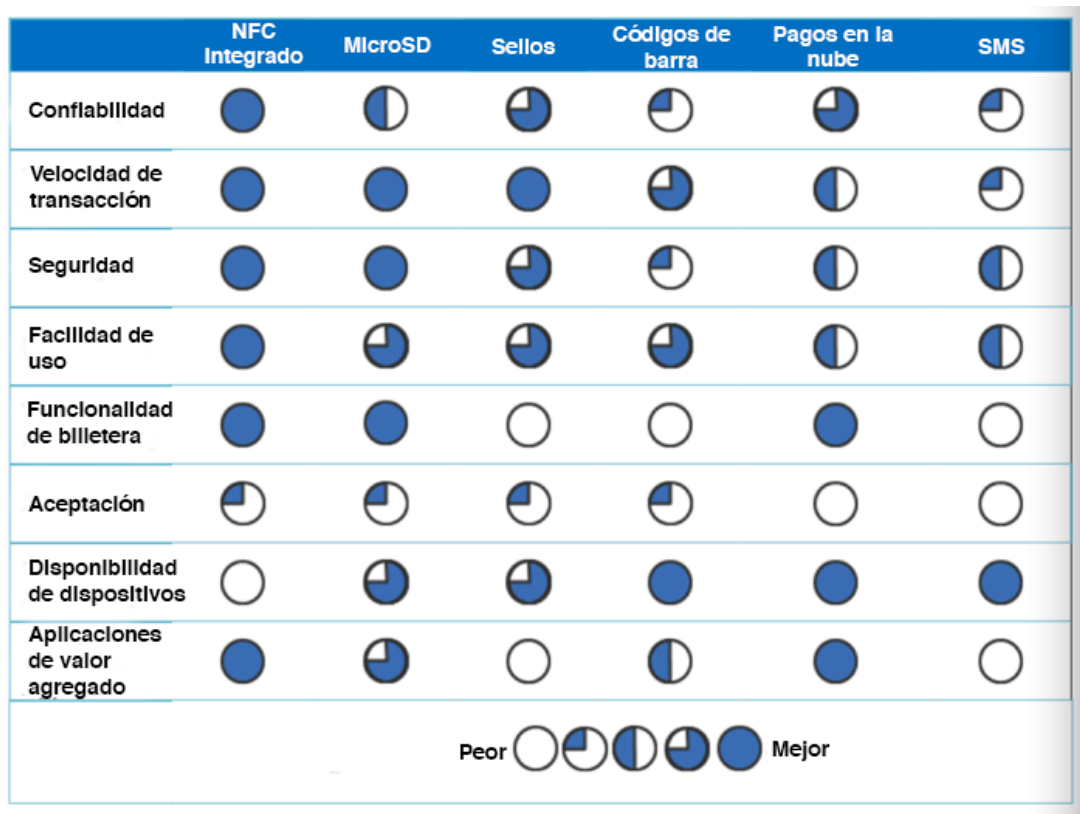


Ilustración 36. Comparación de los métodos de pago móviles alternativos

Fuente: (RFID Point)

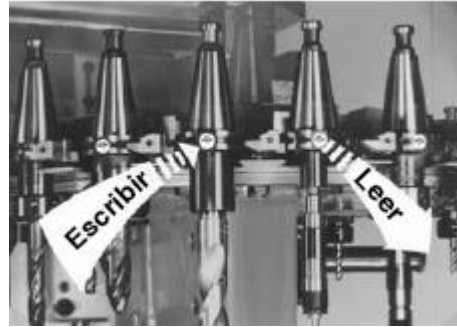
Al analizar el gráfico se puede deducir que existe una amplia variedad de soluciones de pago que crecerán a lo largo del tiempo, sin embargo, se puede notar que NFC se posiciona como la solución líder de pago móvil, gracias a ofrecer aspectos de

seguridad combinados con otras características como fidelidad y aplicaciones con valor agregado.

3.3 Automatización de Tareas

NFC está desempeñando un papel muy importante en el área de los negocios y la automatización de procesos de manufactura, puesto que los procesos pueden ser hechos de una forma más eficiente cuando el inventario o el proceso de control es realizado inalámbricamente y no necesita de un escaneo óptico o manual de números de partes por ejemplo. Los tamaños de los lotes pueden ser más pequeños cuando las funciones de ordenamiento de los ítems individuales pueden estar almacenados en un pequeño chip del artículo. (Rolf y Nilsson)

Se puede citar el ejemplo de la industria de elaboración de muebles, la cual si bien es cierto en muchos países se la sigue elaborando de forma manual y artesanal, en otras partes del mundo esta actividad ahora es totalmente realizada por máquinas (Finkenzeller). En estas fábricas existe una mínima participación humana, ya que las máquinas por lo general necesitan calibrarse y reconfigurarse dependiendo de la pieza que se necesite elaborar, es entonces donde entra en juego datos como: velocidad de rotación, ángulos, fuerza, presión, los mismos que deben ser ingresados manualmente a las computadoras que controlan la maquinaria, cada vez que se necesite una calibración. Esta interacción con la maquinaria muchas veces puede ser motivo de accidentes laborales e implica un riesgo constante para los trabajadores. En este sentido lo que se propone es que los datos de configuración que necesita el computador sean provistos por la lectura de etiquetas NFC, evitando de esta manera la intervención humana, minimizando el impacto de accidentes y de errores humanos al momento del ingreso de datos de configuración. Dichas etiquetas pueden estar adheridas a las mismas piezas en fabricación o en la maquinaria utilizada para su fabricación. (Finkenzeller)



**Ilustración 37. Herramientas utilizadas en la elaboración de muebles:
EUCHNER & Co., Leinfelden-Echterdingen**

Fuente: (Finkenzeller)

Cliente	Planta de producción de muebles XY
Número LEITZ ID	130004711 D25x60
Referencia de manufactura	Y21
Lugar de manufactura	UHE
Dirección de rotación	3
Velocidad máxima de rotación	24000
Velocidad mínima de rotación	18000
Velocidad ideal de rotación	20000
Corrección de radio	25011
Corrección longitudinal	145893
Mayor radio	25500
Mayor longitud	145893
Recorrido máximo	3000
Recorrido actual	875
Número de herramienta	14
Tipo de herramienta	1
Número de filos	2
Ángulo de holgura (grados)	20
Velocidad de corte (grados)	15
Texto libre	Corte final HM Z=3

Ilustración 38. Ejemplo de los datos de configuración almacenados en una etiqueta NFC

Fuente: (Finkenzeller)

Por otro lado si de automatizar tareas se habla, la tecnología NFC resulta ideal para ejecutar ciertas tareas en nuestro teléfono inteligentes. Acciones como configurar una red inalámbrica nueva, evitando de esta manera revelar la contraseña de la misma a un invitado, cambiar el perfil de sonido cuando se entra a un lugar más privado,

ejecutar una aplicación cualquiera de nuestro teléfono, realizar un check-in en foursquare, facebook o Google Plus, recibir una tarjeta de contacto (vCard), ir a un sitio web, etc. Una aplicación móvil en la cual se puede realizar todas estas tareas es NFC Task Launcher (NFC Task Launcher).

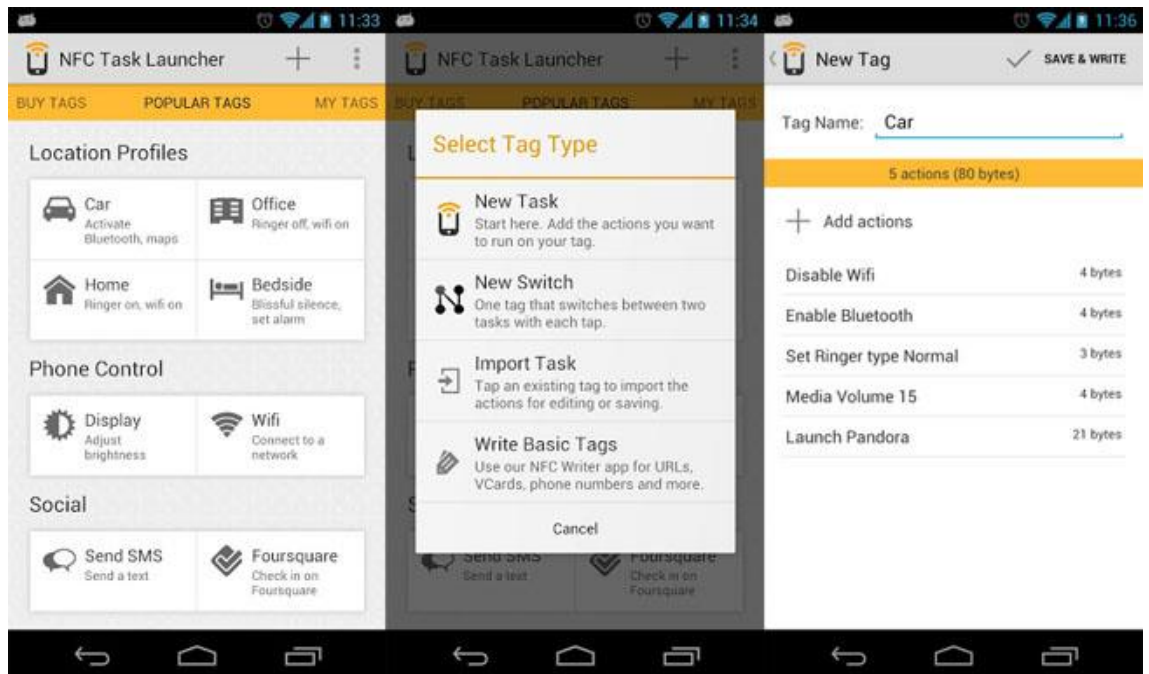


Ilustración 39. Conjunto de Acciones disponibles en la aplicación NFC Task Launcher

Fuente: (NFC Task Launcher)

Paralelamente a *NFC Task Launcher*, el número de aplicaciones para automatizar tareas ha ido incrementando en los últimos años, en la tienda de aplicaciones Google Play actualmente existen alrededor de 200 aplicaciones de automatización de tareas por medio de NFC. (Google Play)

3.4 Seguimiento y Control Médico

La evolución de la tecnología y su aplicación en el área del cuidado médico ha logrado mejorar la calidad de vida de las personas, más aún cuando se trata de soluciones con tecnología móvil, en donde los pacientes pueden usar sus dispositivos para obtener ayuda de manera inmediata, para contactarse con un profesional o para monitorizar su estado de salud.

Debido a la flexibilidad, costos y capacidad de adaptación de la tecnología NFC a diferentes entornos y situaciones, se ha logrado implementar o plantear su uso en centros de salud destinados a mejorar y facilitar el seguimiento y control médico. Por ejemplo gracias a esta nueva tecnología se pueden implementar etiquetas NFC en las bandas de los pacientes, en la medicación y en las tarjetas de identificación de los empleados de los centros médicos, de esta manera se puede lograr que la administración de medicinas sea fácil, segura, rápida y menos costosa. Otro ejemplo de aplicación es la creación de sistemas holísticos que almacenen toda la información de los pacientes en un lugar centralizado, y que permita consultar esta información desde cualquier lugar y en cualquier momento, incluyendo resultados de laboratorios, órdenes de prescripción, y todo el historial médico necesario.

Un caso existente de este tipo de aplicaciones fue desarrollado por la Escuela de Medicina de Harvard para el Hospital y Centro Médico de Boston “*Brigham and Women’s Hospital*”, quienes diseñaron y pusieron en práctica un proyecto cuyo objetivo era hacer más fácil la administración y seguimiento de la medicación de cada paciente, aplicando tecnología NFC. (Boden)

El sistema compuesto por un dispositivo móvil habilitado con NFC y etiquetas distribuidas entre los pacientes, medicinas y empleados del hospital, permite verificar que la medicación y las dosis sean las correctas para cada paciente y registra que medicación fue entregada a cada paciente y por quién en el centro médico.

En la actualidad es una tendencia dentro de los hospitales y centros médicos la aplicación de sistemas electrónicos móviles para la administración y registro de sus actividades, por lo que se verá una evolución grande en esta área en los próximos años.

3.5 El futuro de NFC

Como se ha citado en reiteradas ocasiones, actualmente el principal uso que se realiza de la tecnología NFC es el pago móvil, como apoyo a este y muchos más campos en los que se puede utilizar esta tecnología de corto alcance, Intel anunció en el *Intel Developer Forum* de 2012, la creación de la primera *Ultrabook* que incluiría un chip NFC (Oxford). Este producto no solo fortalecería el comercio electrónico al no tener que introducir nuestros datos de tarjetas de crédito en portales web, sino también una brindaría un soporte para serie de procesos de autenticación en línea.

Durante la presentación de su demo, se constató la realización de una compra y su pago a través del sistema *PayPass* de MasterCard (Parrish) que utiliza el portal web *TigerDirect.com*. Esta podría convertirse tal vez en la forma más segura de realizar pagos en línea, y ese así que tan solo unos meses después del anuncio de Intel, ya se puede adquirir esta *Ultrabook Toshiba Satellite U925T* por un precio de \$800 aproximadamente (Amazon), este avance brinda un nuevo abanico de oportunidades para la masificación y utilización de NFC.



Ilustración 40. Toshiba Satellite U925T- Primera ultrabook con NFC

Fuente: (Amazon)

A pesar que las predicciones afirman que para el 2014 los teléfonos con NFC llegarán a los 500 millones (RFID Point), muchos expertos en la materia tecnología piensan que mientras fabricantes como Apple esencialmente no incluya chips NFC, su masificación se ve limitada (Apple Weblog). A pesar de que reiteradamente antes de cada lanzamiento de un nuevo *iPhone* los rumores corren sobre la inclusión de NFC, y eso no se ha cristalizado hasta la fecha, lo que sí se puede afirmar es que a partir de 2009, Apple ya ha estado registrando muchas patentes con miras a una posible adopción de esta tecnología en sus diferentes dispositivos. (Apple Weblog)

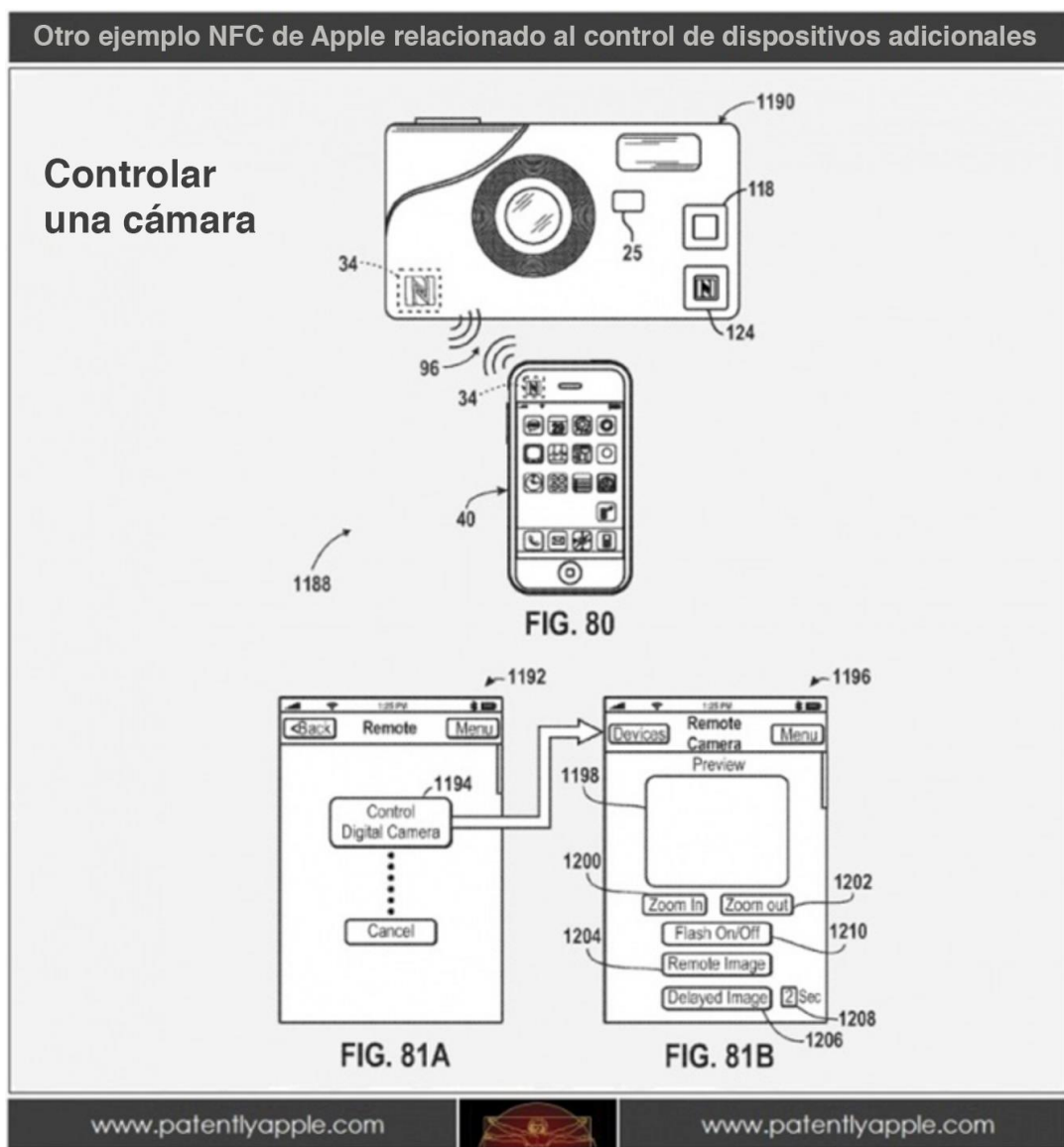


Ilustración 41. Patente de Apple: Ejemplo de Control de Dispositivos con NFC

Fuente: (Apple Weblog)

De esta forma Apple piensa revolucionar la domótica incluyendo un chip NFC en sus *iPhone* lo cual le permitiría: configurar termostatos, activar aspersores, abrir la puerta del garaje, manejar cámaras fotográficas de terceros, enlazar dispositivos a distancias cortas, etc. (Apple Weblog)



Ilustración 42. Patente de Apple: Aplicaciones NFC del iPhone para Televisores y Juegos

Fuente: (Apple Weblog)

Por otro lado, a pesar de que el mayor crecimiento de la industria NFC tiene un enfoque hacia un consumidor final, existe una gran expectativa de la aplicación de dicha tecnología en el mundo empresarial y las aplicaciones B2B (*business-to-business*).

Las aplicaciones NFC empresariales resultan atractivas, sobre todo para los desarrolladores, ya que actualmente pueden resolver dos de los conflictos principales con aplicaciones destinadas al consumidor: la falta de masificación de terminales NFC, y la falta de educación de los consumidores sobre el uso de la tecnología. (Shalaby)

Entre algunos ejemplos, de aplicación de la tecnología NFC en el campo empresarial, se puede mencionar el seguimiento y control de personal mediante la implementación de puntos NFC en donde los empleados pueden marcar la entrada y salida de sus estaciones de trabajo, control de pacientes y suministro de medicinas en clínicas y hospitales, control de inventarios y manejo de productos, entre otros.

Por estas razones las empresas están intentando migrar sus aplicaciones basadas en RFID hacia tecnología NFC con dispositivos móviles, ya que resultan económicas y proporcionan facilidad en su mantenimiento. En los próximos años se verá un crecimiento grande en esta área, por lo que resulta un buen momento para iniciar con la aplicación de soluciones empresariales que aprovechen todas las ventajas de la tecnología NFC.

Conclusión del Capítulo

Gracias a la gran industria dedicada al desarrollo e investigación de la tecnología NFC como una infraestructura sólida de comunicación inalámbrica, se ha conseguido ampliar el número de soluciones y el tamaño del mercado que puede explotar esta tecnología. Es importante mencionar que uno de los factores clave que han permitido el crecimiento de NFC ha sido la simplicidad en la unificación e integración con diferentes redes y estructuras ya conocidas, lo que ha facilitado la implementación de la tecnología sin tener que considerar cambios radicales en la infraestructura actual de muchos sistemas. Como ya se ha mencionado, el enfoque central de NFC apunta hacia el desarrollo de una alternativa robusta de pagos electrónicos, sin embargo, el objetivo debe fijarse en crear soluciones que puedan mejorar la calidad de vida de las personas, aprovechando la confiabilidad, velocidad, seguridad, facilidad de uso, y sobre todo la posibilidad de desarrollar aplicaciones de valor agregado con esta tecnología inalámbrica de comunicación.

CAPÍTULO 4

SEGURIDAD Y PRIVACIDAD EN NFC

Uno de los pilares de NFC es desarrollar una solución que pueda cumplir con los objetivos primarios de la seguridad de la información, sin embargo, existen varias amenazas que deben ser estudiadas y consideradas al momento de llevar a cabo cualquier tipo de implementación de la tecnología. Es importante conocer los conceptos básicos y los riesgos generales para proceder a comprender los principales problemas de seguridad que no llegan a ser amenazas exclusivas de NFC, si no, en algunos casos se comparten con otras tecnologías de comunicación inalámbrica.

4.1 Conceptos básicos sobre seguridad

Con el objetivo de entender los términos y conceptos involucrados en la seguridad de la información, se comenzará en esta sección detallando los más importantes, para luego describir los principales problemas de seguridad que pueden presentarse en una comunicación mediante NFC.

Objetivos Primarios de la Seguridad de la Información

Confidencialidad

Es el asegurar que la información sea accesible solo a las partes autorizadas, ya sean estas personas, procesos o dispositivos. Esto requiere esconder el contenido de la información usualmente mediante encriptación, de tal forma que se pueda acceder a la misma solo con la ayuda de una llave secreta (Coskun, Ok y Ozdenizci). La confidencialidad de flujo de tráfico protege la identidad tanto del origen y destino(s) del mensaje, su desventaja recae en que los métodos aplicados incrementan drásticamente el volumen de tráfico intercambiado. (Álvarez Marañón)

Autenticación

Es confirmar la identidad de una persona, proceso o dispositivo. Esto se puede conseguir mediante varias formas, por ejemplo: objetos (acercar una tarjeta RFID a un lector, código *token*, tarjeta inteligente, tarjeta de coordenadas), características físicas (huellas digitales, reconocimiento de voz, retina o iris), software (usuario y contraseña, firmas digitales, RSA) (Pintado) o comportamientos (caligrafía o ritmo de caminado) (Coskun, Ok y Ozdenizci). Para el caso de transacciones de alta criticidad como el manejo de dinero virtual, las entidades bancarias optan por un sistema de autenticación mutua, es decir no solo el portal web del banco pide la autenticación al usuario sino este a su vez, también solicita una identificación al portal web del banco para evitar que personas puedan suplantar la identidad del banco a través de un portal web falso.

Autorización

Una vez completada la autenticación, una autorización permitirá realizar diferentes acciones sobre un objeto (archivo, aplicación o máquina) por parte del usuario. Los privilegios de autorización se basan en una serie de condiciones como: tiempo, tipo de usuario, lugar en el que se realiza la acción, etc. Puesto que el hecho de que un usuario pasó correctamente el proceso de autenticación, no quiere decir que tengo un acceso total al sistema y pueda realizar cualquier acción (Coskun, Ok y Ozdenizci).

No Repudio

Hace referencia a una situación en la cual existe suficiente evidencia como para prevenir que un individuo niegue que otra persona ha realizado una declaración o tomado una acción (Andress). Es un requerimiento más fuerte que la autenticación en la seguridad de la información (Coskun, Ok y Ozdenizci). El No Repudio se puede realizar recolectando evidencia directamente del sistema, *logs* de la red o examinación forense de los equipos involucrados. También es posible implementarlo a través del uso de tecnologías de encriptación, como funciones hash específicamente para utilizarlas como una firma digital para cifrar un archivo o una comunicación. (Andress)

Disponibilidad

Es la capacidad de acceder a los datos cuando se los necesita. La falta de disponibilidad puede ocurrir por varios motivos, desde pérdida de energía, problemas del sistema operativo o de las aplicaciones hasta ataques provenientes de la red (Andress). De la misma forma conservar la disponibilidad también significa asegurar que el sistema responda correcta y completamente a los requerimientos de un usuario autorizado en un tiempo determinado (Coskun, Ok y Ozdenizci).

Integridad de los Datos

Es el asegurar que la información recibida sea exactamente igual a la información enviada. Es decir evitar que la información sea accidental o maliciosamente modificada o eliminada durante una operación como por ejemplo un almacenamiento o una transferencia (Coskun, Ok y Ozdenizci). Conservar la integridad significa no solo prevenir cambios no autorizados, sino también la capacidad de revertir dichos cambios en caso que se requiera. Particularmente la integridad es importante cuando está en juego información para toma de decisiones, si dicha información es alterada, por ejemplo resultados de pruebas médicas, se podría cometer errores al escoger un tipo de tratamiento y podría incluso desembocar en la muerte de un paciente. (Andress)

Si bien es cierto, todos los conceptos anteriormente citados son muy importantes para conseguir una seguridad adecuada en los sistemas de información, tres de ellos merecen un realce principal, estos componen el triángulo de la Seguridad de la Información.



Ilustración 43. Pilares de la Seguridad de la Información

Fuente: (Andress)

Vulnerabilidad

Es una debilidad la cual puede ser aprovechada por un atacante para realizar daño. Dicha debilidad puede ser un diseño, un error de implementación o una deficiencia en algún procedimiento. Una vulnerabilidad es la combinación de 3 elementos: una falla del sistema, capacidad de acceso por parte de un atacante para usar dicha falla, y la habilidad del atacante para explotar dicha falla (Coskun, Ok y Ozdenizci). Existen varios factores que contribuyen a la presencia de vulnerabilidades como: el sistema operativo o aplicación utilizada, la ubicación física del edificio de una oficina, un data center que está sobre poblado superando la capacidad del sistema de enfriamiento, carencia de generadores de respaldo, etc. (Andress)

Amenaza

Es un posible peligro que tiene el potencial para causar un beneficio injusto a una persona no autorizada o causar daño explotando una vulnerabilidad. Las amenazas pueden ser tanto intencionales como no intencionales. Las de naturaleza intencional tratan de obtener una ventaja injusta o de causar daño, en tanto que las no intencionales, generalmente ocurren accidentalmente y no buscan realizar un daño, como por ejemplo: errores humanos, errores técnicos o provenientes de la naturaleza (Coskun, Ok y Ozdenizci).

Según a que parte de la seguridad de la información ataquen, las amenazas se pueden categorizar de la siguiente forma:

Parámetros	Disponibilidad	Confidencialidad	Integridad
Hardware	No disponible cuando el hardware o sus componentes son robados o están rotos		
Software	No disponible cuando el software es modificado o borrado por lo tanto no funciona del todo	La confidencialidad es violada cuando el software es modificado para ayudar a los hackers	Funciones incorrectas generan resultados inesperados cuando el software es modificado
Datos	No disponible cuando los datos son borrados o modificados	La confidencialidad es violada cuando los datos son leídos por partes no autorizadas	Resultados falsos de datos cuando datos existentes son modificados, borrados o incluso se generan datos falsos
Paquetes	No disponible cuando los paquetes son modificados o borrados en el camino al receptor	La confidencialidad es violada cuando los paquetes son leídos por partes no autorizadas	Resultados falsos de datos cuando el contenido de un paquete es modificado, borrado o incluso un paquete falso es generado

Ilustración 44. Análisis de las Amenazas

Fuente: (Coskun, Ok y Ozdenizci)

Ataque

Es un intento intencional por parte de un intruso para leer, modificar, eliminar, desactivar o ganar acceso a información no autorizada. Ciertas acciones como intentos de leer información sin afectar al sistema fuente son llamados ataques pasivos en tanto que las acciones que alteran el sistema anfitrión son llamados ataques activos (Coskun, Ok y Ozdenizci).

Los ataques pasivos afectan la confidencialidad y son muy difíciles de detectar puesto que no existe cambio de la data durante el ataque, ejemplos de estos ataques son: *sniffing*, *eavesdropping*, *backdoor* y *key loggers*. En tanto que los ataques

activos buscan afectar la integridad, muchos de ellos son iniciados por un intruso el cual es un usuario no autorizado y consigue entrar al sistema. Ejemplos de estos ataques son: *spoofing*, negación de servicio (*DoS*), negación de servicio distribuida (*DDoS*) y hombre en el medio (*man in the middle*), etc (Coskun, Ok y Ozdenizci).

Riesgo

Es el potencial daño que puede surgir luego de la realización de una amenaza. A pesar que las amenazas tienen poca probabilidad de ocurrencia, en caso de cristalizarse dicha acción, puede ocasionar serias consecuencias. Por ejemplo el caso de terremotos en una fábrica, su probabilidad de ocurrencia es muy baja, pero en caso de ocurrir, puede dejar totalmente destrozada la fábrica y llevar a una inminente banca rota. No se puede aceptar un gran riesgo por más que su probabilidad de ocurrencia sea muy pequeña, lo que se debe realizar es asegurarnos hasta un punto en el que el riesgo ese bajo control y sea tolerable. (Coskun, Ok y Ozdenizci)

Para controlar estos problemas se debe implementar un proceso de gestión de riesgos. Por definición un riesgo involucra 2 posibles variables: el impacto o posible daño que cause (tiempo o dinero) y su probabilidad de ocurrencia.

4.2 Principales problemas de seguridad

Espionaje (*Eavesdropping*)

Actualmente NFC no ofrece protección contra el espionaje de datos, y al tratarse de una comunicación inalámbrica este es el modo de ataque más obvio y preferido por los atacantes. El atacante es capaz de colocar una antena intermedia que escuche y reciba la señal de radio frecuencia generada por la transferencia inalámbrica de mensajes entre dos dispositivos NFC habilitados. Como ya se ha indicado anteriormente, la distancia de transferencia entre emisor y receptor oscila entre los 10 centímetros, debido a este corto alcance de transferencia de datos de dicha tecnología se cree que un ataque de este tipo involucra mayor dificultad para capturar los datos,

sin embargo, la distancia que debe existir entre el atacante y el punto de ataque depende de algunos factores como:

- Características de radio frecuencia del emisor (antena, efecto de blindaje del protector, poder de la señal de envío, el ambiente).
- Características de la antena del atacante.
- Calidad del receptor del atacante.
- Calidad del decodificador de la señal de radio frecuencia del atacante.
- Infraestructura del ambiente y obstáculos como paredes. (Haselsteiner y Breitfuß)

Se puede mencionar que la distancia a la que debe estar colocado el atacante puede variar entre 1 metro y 10 metros según las consideraciones anteriores. Un último factor de gran importancia que influye en la distancia de espionaje es el modo de operación del emisor, ya que puede actuar en modo activo o pasivo, siendo el modo pasivo más difícil de interferir y capturar los datos.

Corrupción de datos (*Data Corruption*)

Es un tipo de ataque de denegación de servicio, en el cual el atacante bloquea o distorsiona la transmisión de datos entre dispositivos NFC habilitados, logrando que los datos o recursos enviados sean inaccesibles para los usuarios legítimos. En este tipo problema de seguridad, el atacante no se limita solo a escuchar la transmisión, sino la distorsiona. No es necesario que el atacante descifre los datos transmitidos, ya que su objetivo es únicamente destruir la información mediante el envío de señales de radio frecuencia que generan ruido e interferencia en la transmisión original. Para que el ataque sea efectivo, el atacante debe ser capaz de enviar frecuencias válidas del espectro de datos a tiempo correcto, esto solo lo conseguirá si tiene un entendimiento amplio del esquema de modulación y codificación.

Un aspecto importante a resaltar es que los dispositivos NFC son capaces de detectar señales de radio frecuencia antes de enviar datos, por lo tanto si se llega a detectar una señal mayor que la de emisión, el envío de datos puede ser cancelado, previniendo este ataque.

Modificación de datos (*Data Modification*)

En este tipo de ataque el atacante trata de alterar los datos enviados, para ello, el atacante intercepta y manipula los datos mediante la modificación de los valores binarios de los datos, para luego enviarlos al receptor original.

La posibilidad de que este ataque ocurra depende en un gran porcentaje de la fuerza aplicada de la amplitud de modulación, ya que la decodificación de la señal es diferente para modulación 100% y 10%.

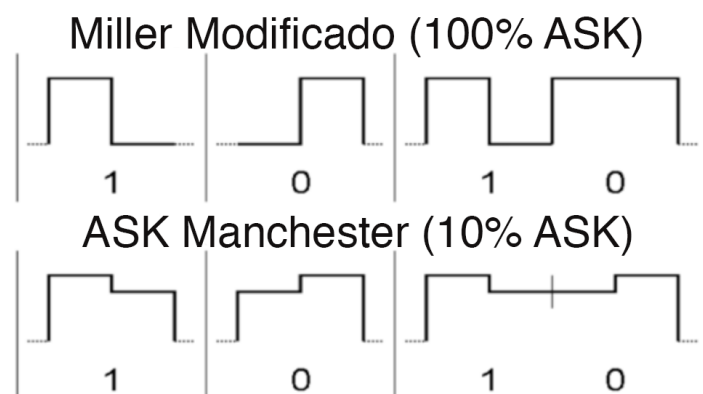


Ilustración 45. Esquemas de codificación

Fuente: (Haselsteiner y Breitfuß)

En modulación 100% el decodificador revisa los dos bits medios para la señal de radiofrecuencia encendida (no pausa) o señal de radiofrecuencia apagada (pausa). Para que el decodificador pueda entender un uno o cero, el atacante puede llevar a cabo dos cosas. (Haselsteiner y Breitfuß)

Inserción de datos (*Data Insertion*)

En este caso el atacante inserta mensajes en la comunicación de intercambio de datos entre dos dispositivos NFC habilitados, esto lo hace antes de que el receptor emita una respuesta hacia el emisor inicial. Esto solo puede suceder si el tiempo de

respuesta del receptor es elevado para permitir al atacante insertar los datos. Puede ocurrir que los datos insertados se superpongan a la respuesta oficial lo que generaría un caso de corrupción de datos.

Hombre en el medio (*Man in the Middle*)

El atacante actúa como un intermediario en la comunicación entre dos dispositivos NFC con el objetivo de interceptar los datos transmitidos para almacenarlos o manipularlos sin que los extremos NFC lleguen a tener conocimiento del ataque.



Ilustración 46. Esquema de ataque Hombre en medio

Fuente: (Haselsteiner y Breitfuß)

Para que un ataque de este tipo pueda ocurrir en NFC, un dispositivo debe actuar en modo activo y el otro en modo pasivo, un dispositivo genera un campo de radiofrecuencia y envía datos hacia el receptor. El atacante debe encontrarse lo suficientemente cerca para espiar los datos emitidos y ser capaz de distorsionar la transmisión para que el receptor no pueda recibir el mensaje. En el siguiente paso el atacante debe enviar datos hacia el receptor, y aquí es en donde se da el mayor problema ya que el atacante debería generar un segundo campo de radiofrecuencia activo y es prácticamente imposible alinear los dos campos de radiofrecuencia para armonizar la transferencia de datos.

Un segundo escenario sería que tanto el emisor como receptor actúen en modo activo, de la misma manera el atacante debe interceptar la comunicación y distorsionarla para que el receptor no la reciba, en este punto el atacante puede ser detectado por el emisor y cancelar la transferencia, sin embargo en caso de que no

sea detectado, debido a la conexión activo-activo el emisor debe apagar su campo de radiofrecuencia, por lo que el atacante puede enviar los datos hacia el receptor, pero el problema se da ya que tanto emisor como receptor están escuchando por una respuesta por lo que ambos recibirán el mensaje, detectando el problema y cancelando el protocolo de comunicación.

Por la corta distancia de proximidad necesaria para llevar a cabo una transmisión NFC y las capacidades de detección de la tecnología, se puede concluir que es prácticamente imposible que se lleve a cabo este tipo de ataque.

4.3 Mecanismos y Herramientas

Criptografía

La mayoría de los mecanismos para la implementación de seguridad, están basados en la criptografía, gracias a esta alternativa es posible implementar: canales seguros, almacenamiento de la información de contraseñas dentro de un disco duro, firmas digitales para operaciones financieras, etc. (Coskun, Ok y Ozdenizci)

El concepto de la criptografía es el de esconder la información, disfrazándola de tal forma que no sea comprensible a simple vista, para luego almacenarla en un disco duro o intercambiar dicha información con otro individuo de forma segura.

El proceso consiste en cifrar el mensaje o data original a través de una clave de encriptación, luego almacenar o transferir la data encriptada (denominada *Ciphertext*) al destino, entonces se desencripta utilizando la llave de desencriptación y se puede acceder a la data original (Coskun, Ok y Ozdenizci).

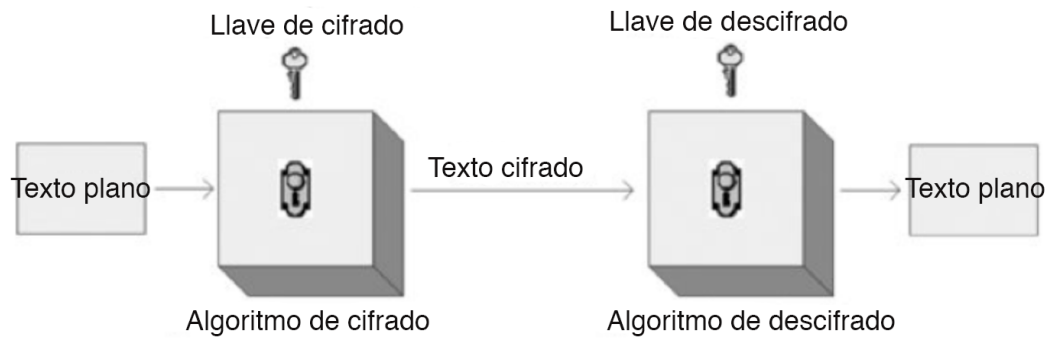


Ilustración 47. Proceso de Encriptación-Desencriptación

Fuente: (Coskun, Ok y Ozdenizci)

Inicialmente la criptografía fue desarrollada de manera simétrica, es decir que ambas partes (origen y destino) compartían una misma clave secreta. Pero en 1976 se introdujo el primer ejemplo de un algoritmo RSA, en el cual en origen y el destino poseían un par de claves diferentes. A continuación es preciso ampliar la diferencia entre criptografía Simétrica y Asimétrica (Coskun, Ok y Ozdenizci).

Criptografía Simétrica versus Criptografía Asimétrica

Al analizar cada una de estas formas de implementación de la criptografía no se puede concluir cual es mejor que la otra, lo que sí se puede citar son, las fortalezas y debilidades de cada una.

Criptografía Simétrica

También es conocida como criptografía de llave privada (*Private Key Cryptography*), esta forma de criptografía utiliza una sola llave, tanto para la encriptación de texto plano como para la desencriptación del texto cifrado. Por lo tanto la llave debe ser compartida entre el origen y el destino, este proceso se lo denomina intercambio de llave (*keyexchange*).

El uso de una sola llave se constituye en una de las principales debilidades de la criptografía simétrica, si la clave secreta está expuesta de esta manera, un atacante puede interceptar el mensaje, alterarlo, volver a encriptar y enviarlo al destino original reemplazando el mensaje original. De esta forma se puede

afirmar que la criptografía de una sola llave, provee únicamente confidencialidad más no asegura la integridad de la información. (Andress)

Ejemplos de algoritmos de clave simétrica son: DES, 3DES, y AES. El primer algoritmo DES se utilizó en 1976, está basado en un código de bloque (*block cipher*) que utiliza una clave de 56 bits. A pesar que fue un método muy seguro por un largo tiempo, en 1999 se un proyecto de computo distribuido fue lanzado para romper su seguridad intentando cada posible combinación de la clave secreta, y al término de 22 horas la llave fue encontrada. Posteriormente se utilizó el 3DES, el cual encripta cada boque tres veces, cada vez con una llave distinta. Por otro lado AES es una serie de códigos de bloque utilizado por el gobierno de los Estados Unidos, este algoritmo utiliza 3 llaves: una de 128 bits, una de 192 bits y otra de 256 bits, todas poseen una longitud de bloque de 128 bits. (Andress)

Criptografía Asimétrica

También conocida como criptografía de llave pública (*Public Key Cryptography*), esta forma utiliza 2 llaves: una llave pública y una llave privada. La llave pública es utilizada para cifrar la data original, se puede encontrar este tipo de llaves en: firmas de mensajes de correo electrónico, en servidores, en páginas web, etc. En tanto que la llave privada se utiliza para descifrar la data que llega al punto de destino, esta clave debe ser cuidadosamente custodiada por el destinatario. La llave pública es sometida a una serie de operaciones matemáticas complejas, garantizando de esta forma que no se pueda obtener la llave privada a partir de la llave pública. De esta forma la encriptación asimétrica elimina la necesidad de distribuir una llave como sí ocurre en la simétrica.

Ejemplo de algoritmos de asimétricos son: RSA y ECC. RSA es tal vez el algoritmo asimétrico más utilizado a nivel mundial, su nombre proviene de las siglas de sus creadores: Ron Rivest, Adi Shamir y Leonard Adleman, una implementación de este algoritmo puede ser observada en el protocolo de sockets seguro (*Secure Sockets Layer - SSL*). Este algoritmo fue creado en 1977. Por otra parte ECC (*Elliptic Curve Cryptography*), se llama de esta forma debido al problema matemático en el cual se basan sus funciones de encriptación. Este

algoritmo posee una mayor robustez, produce claves más pequeñas, es muy rápido y eficiente. Inclusive forma parte del algoritmo seguro de Hash, (SHA-2 *Secure Hash Algorithm 2*) y del algoritmo digital de firma de curva elíptica (*Elliptic Curve Digital Signature Algorithm – ECDSA*). (Andress)

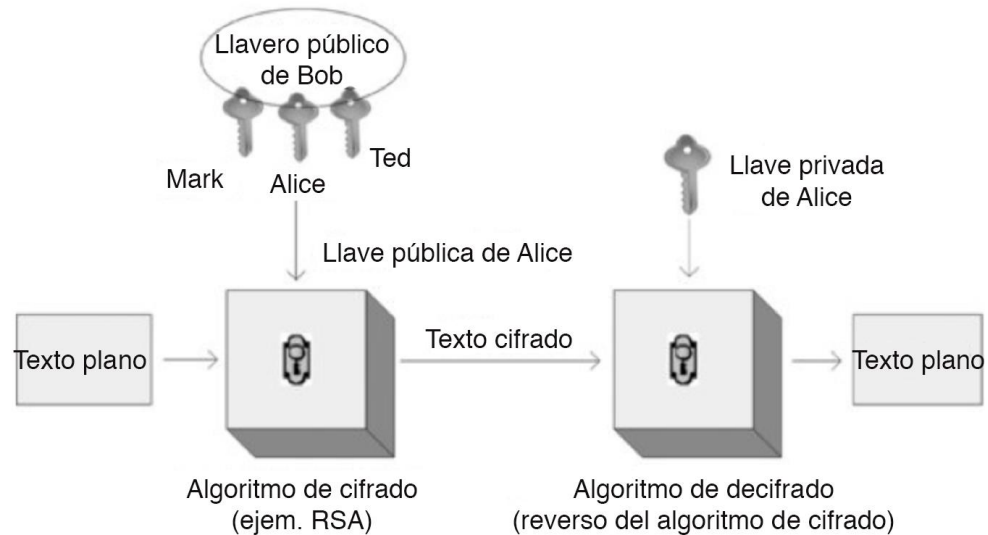


Ilustración 48. Esquema de algoritmo asimétrico de encriptación-RSA

Fuente: (Coskun, Ok y Ozdenizci)

Hashing

Es considerada como un tercer tipo de criptografía a parte de la simétrica y la asimétrica. También se denomina criptografía sin llave (*Keyless Cryptography*). Este método en vez de utilizar una llave, crea un valor largo de longitud fija denominado *Hash*, el cual está basado en el mensaje original. Este método no es utilizado para descubrir el contenido del mensaje original sino simplemente para determinar si el mensaje ha cambiado, de esta forma se puede precisar que el *Hashing*, ofrece confidencialidad pero no integridad de la información. Usualmente el valor *Hash* es enviado conjuntamente con el mensaje original para que el destinatario pueda confirmar su integridad. Este método es utilizado mucho en las comunicaciones o para archivos distribuidos. El destinatario aplica el mismo algoritmo que utilizó el origen, genera un valor y lo compara con el enviado, en caso de no coincidir, se sabe que el mensaje fue alterado. (Andress)

Ejemplos de algoritmo *Hash* son: MD2, MD4, MD5, RACE y SHA-2. Es preciso mencionar de igual forma que la seguridad de este método depende del tamaño el valor *Hash* generado, es decir: a medida que la longitud de dicho valor aumenta, más robusto y seguro se vuelve el sistema. (Andress)

MAC y HMAC

Con el propósito de comprobar la identidad del origen y el contenido de un mensaje, se puede optar por encriptar todos los parámetros del mensaje y luego enviarlo. El problema que se presenta es que dependiendo del algoritmo empleado (simétrico o asimétrico) su desencriptación tomará un tiempo considerable. Es entonces donde un código de autenticación de mensaje (*Message Authentication Code*-MAC) puede ser generado utilizando algún algoritmo de *Hashing*, que sería más rápido que encriptar el mensaje cuando el tiempo es el atenuante. El algoritmo MAC recibe como entrada una llave secreta y un mensaje, y genera un MAC como salida (Coskun, Ok y Ozdenizci).

HMAC es una mejora con respecto al algoritmo MAC original, el algoritmo tradicional no utiliza una llave mientras que HMAC utiliza una llave secreta compartida entre el origen y el destino. De esta forma el algoritmo MAC provee integridad de los datos en tanto que la llave secreta brinda autenticación al mismo tiempo. Pero cabe recalcar que él no repudio puede ser un problema en este caso. Ejemplos de algoritmos HMAC son: MD5, SHA-1 y SHA-2. La seguridad que brinda HMAC dependerá de: el algoritmo de encriptación utilizado, el tamaño del valor *Hash* de salida y el tamaño de la llave secreta (Coskun, Ok y Ozdenizci).

Firmas Digitales

Las firmas digitales son otra forma en la cual se pueden incluir algoritmos asimétricos y asociarlos con sus llaves públicas y privadas. Las firmas digitales permiten, como su nombre lo indica, firmar un mensaje con el propósito de establecer una seguridad, para detectar si hubo cambio en el contenido del mensaje original o no, de esta forma se asegura que dicho mensaje haya sido

enviado por parte de la persona esperada y se evita el no repudio por parte del origen, sobre el envío del mensaje. Para firmar un mensaje, el origen debe generar un valor *Hash* de mensaje, utilizar su llave privada para cifrar dicho valor *Hash*, generando de esta forma una firma digital. El remitente enviará el mensaje de forma conjunta con la firma digital. Una vez que el destinatario reciba el mensaje, utilizará su llave pública para descifrar la firma digital, obteniendo así el código *Hash* del mensaje, con lo cual puede verificar la integridad del mensaje, generando su propio código *Hash* del mensaje, y comparándolo con el descifrado. A pesar que todo este proceso puede sonar complicado y algo engorroso, usualmente dichas tareas son realizadas por un software de forma que sea invisible para el usuario. (Andress)

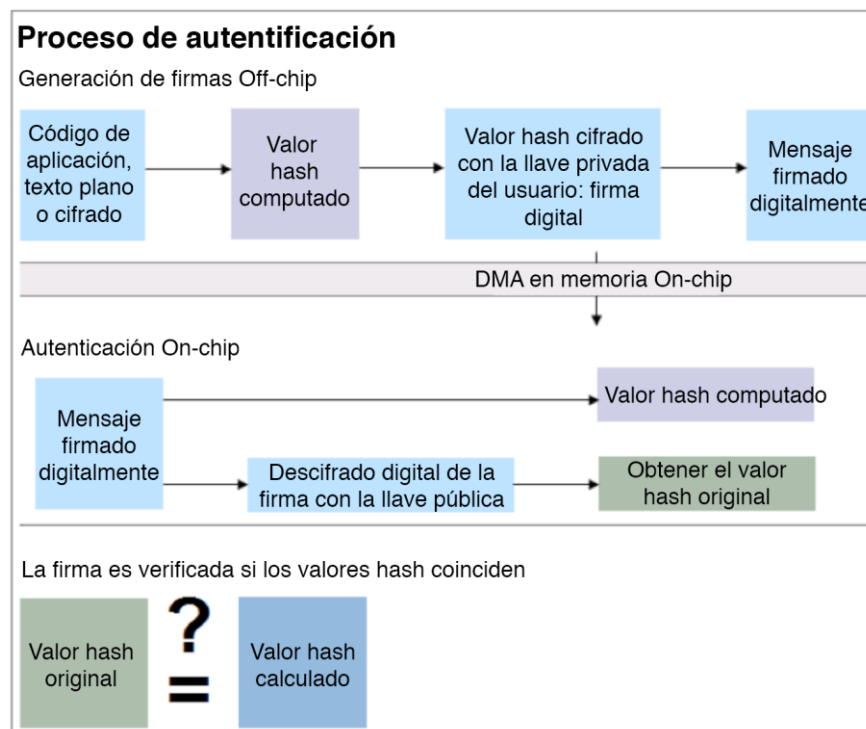


Ilustración 49. Proceso de Autenticación utilizando una firma digital

Fuente: (Andress)

Conclusión del Capítulo

NFC, por su estructura y sus características de funcionamiento, ayuda a que los problemas comunes de seguridad dentro de la comunicación o transferencia de datos puedan ser minimizados y de esta manera elevar la dificultad de los ataques. Para ello, la tecnología se apoya en varios mecanismos y herramientas como la criptografía, el *hashing* y las firmas digitales, para cumplir con los objetivos primarios de la seguridad de la información.

CAPÍTULO 5

PROTOTIPO DE UNA APLICACIÓN MÓVIL CON NFC

El campo de los teléfonos inteligentes ha sido uno de los sectores en lo que NFC está intentando ganar mercado gracias a la implementación del hardware en los dispositivos y a la amplia variedad de aplicaciones de valor agregado existentes. La empresa líder en la actualidad en el área de los teléfonos inteligentes es Google con su sistema operativo Android, es por ello que el siguiente capítulo se centra en el desarrollo de un prototipo de una aplicación móvil con NFC sobre el sistema operativo Android, para lo cual es necesario entender las características generales del sistema, las herramientas de desarrollo, los modos de programación NFC y las librerías existentes para hacer uso de esta tecnología.

El prototipo tiene como objetivo demostrar el uso de NFC y la comunicación entre etiquetas. Consiste en dos aplicaciones móviles y un sistema web de mantenimiento de datos, que permitirán a clientes y dueños de restaurantes de comida almacenar información de sus establecimientos dentro de las etiquetas NFC para que posteriormente un cliente pueda recuperar esta información y acceder de manera automática al menú del restaurante.

5.1 Pasos Iniciales

Antes de proceder a especificar el prototipo de una aplicación móvil en Android para una comunicación NFC, es preciso explicar los aspectos más importantes sobre el sistema operativo Android, al igual que de todas las herramientas empleadas para el desarrollo de una aplicación móvil y una aplicación administrativa Web.

Android

Este sistema operativo basado en Linux, fue originalmente creado por el licenciado en Ciencias de la Computación Andy Rubin, (El Economista.ES-Tecnología) en el año de 2003 a través de su empresa Android Inc. En 2005 la tecnológica Google, compra la compañía y nombró a Rubin como el director de las plataformas móviles de la empresa multinacional estadounidense (Jackson). A decir de muchas personas se piensa que esta decisión fue en gran parte motivada como respuesta al lanzamiento del *Iphone* de Apple, como también de sus competidores RIM *Blackberry*, Nokia *Symbian* y *Microsoft Windows Mobile*. De esta manera Google hizo esta adquisición con el propósito de incursionar también en el entonces nuevo mercado de los teléfonos móviles inteligentes. (Jackson)



Ilustración 50. Andy Rubin-Fundador de Android Inc.

Fuente: (Jackson)

Es entonces donde un nuevo concepto surgió, el denominado Internet 2.0 el cual permitía a los usuarios acceder a varias redes de datos a través de dispositivos electrónicos portables como teléfonos inteligentes, tabletas táctiles, lectores de libros electrónicos (*e-Book e-Readers*), etc. De esta manera se podía acceder a nuevos contenidos como: juegos, animaciones 3D, audio y video digital, imágenes en alta definición, etc. (Jackson)

La arquitectura de la pila del software de Android está dividida en 5 capas, siendo el *kernel* la capa más baja, continuando con las herramientas de bajo nivel, las librerías nativas, tiempo de ejecución, el *Framework* de aplicaciones y las aplicaciones se sitúan en la capa más alta. (Brahler)

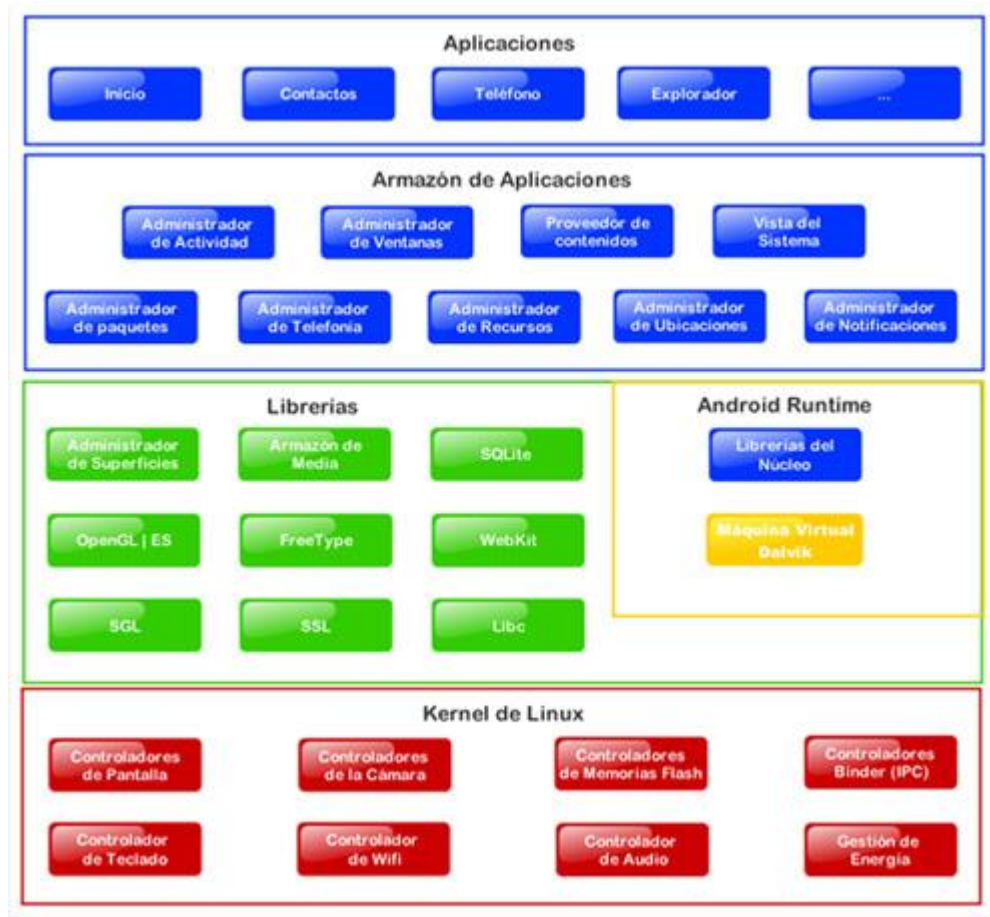


Ilustración 51. Arquitectura del Sistema Operativo Android

Fuente: (Brahler)

Las partes que se observan en la imagen corresponden a: verdes (están escritas en C/C++), azules (escritas en Java y corren en la máquina virtual *Dalvik*). El *kernel* utilizado es el de un Linux Serie 2.6 modificado para las necesidades especiales de manejo de energía, memoria y entorno de ejecución. Dado que Android está originalmente diseñado para ejecutarse en dispositivos con poca memoria y procesadores de bajo consumo, las librerías para la unidad de procesamiento y de control de gráficos son compiladas para optimizar el código nativo. (Brahler)

Durante la década pasada, Android ha evolucionado hasta convertirse en una plataforma extremadamente confiable, comenzando en la versión 1.0 hasta la 4.2 *JellyBean* actualmente. A continuación se encuentra la distribución de las versiones de Android en el mercado actual. (Android Inc)

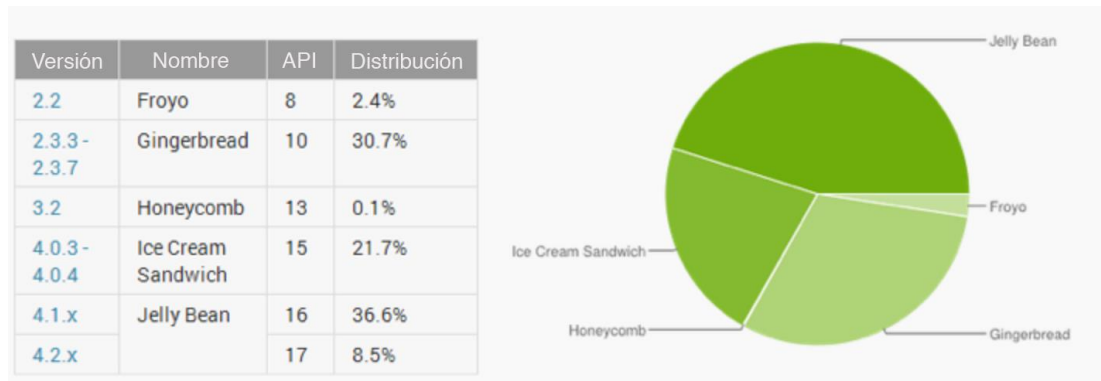


Ilustración 52. Distribución de Versiones de Android al 4 de Septiembre del 2013

Fuente: (Android Inc)

El tener un sistema operativo embebido en un pequeño chip, tan pequeño como para caber en un dispositivo electrónico de mano es como tener una computadora completa en nuestro bolsillo. Esto se alcanza debido a que algunos de estos teléfono inteligentes funcionan ya con doble o hasta cuádruple núcleo así como 2 GB de memoria RAM.

Una vez que Android comenzó a destacarse en el mundo de la telefonía móvil, las grandes empresas fabricantes de estos dispositivos no dudaron en incluirlo en sus productos y tabletas, entre las principales manufactureras se tiene: HTC, Samsung, LG Electrónica, Sony, Huawei, Motorola, Alcatel, etc.

Java

Es el lenguaje de programación base de las aplicaciones para Android, Java 6 *Standard Edition* contiene el núcleo del lenguaje de programación, hasta Android 4.1 todavía no se soporta Java versión 7. Para descargar este software es necesario acceder al sitio web de Oracle y entrar a la sección del directorio de Java. (Jackson)

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

Eclipse IDE

Es un entorno de desarrollo integrado (*Integrated Development Environment-IDE*), el cual es una pieza de software dedicado que permite la escritura de código de programación de una forma sencilla, ejecutarlo y testarlo en un solo entorno integrado. Actualmente Android requiere del IDE Eclipse y recomienda el uso de Eclipse Juno Version 4.2 para Java EE (Jackson). Se puede acceder a descargar este software ingresando a la dirección:

<http://www.eclipse.org/downloads/>

Android SDK

Denominado así por sus siglas en inglés (*Software Development Kit*), es una colección de archivos y utilidades que trabajan de la mano con Eclipse IDE para crear una herramienta especializada en desarrollo para Android. Las últimas versiones de este software pueden descargarse desde:

<http://developer.android.com/sdk/index.html>

Sistema de Ejecución de Etiquetas

La mayoría de etiquetas NFC son elementos pasivos, los cuales almacenan datos para ser leídos por teléfonos inteligentes con NFC en formato NDEF (*NFC Data Exchange Format*). Cuando se acerca un teléfono a cualquier etiqueta NFC habilitada, en realidad se procede a leer un mensaje NDEF por parte de una aplicación, luego pasa a un protocolo un manejador de pila de bajo nivel y finalmente la parte de radio frecuencia recupera los datos de la etiqueta. (Nokia)

El formato NDEF define un formato de encapsulación de mensaje para el intercambio de información. Es un formato liviano, de mensaje binario que puede utilizarse para encapsular una o más cargas de una aplicación definida o arbitraria y empaquetarlo todo en un solo mensaje (Nokia). Un mensaje NDEF está compuesto por uno o varios registros NDEF, en esencia se trata de un *array* de registros, el número máximo que se puede almacenar dependerá de la aplicación y del tipo de etiqueta empleadas. (Nokia)

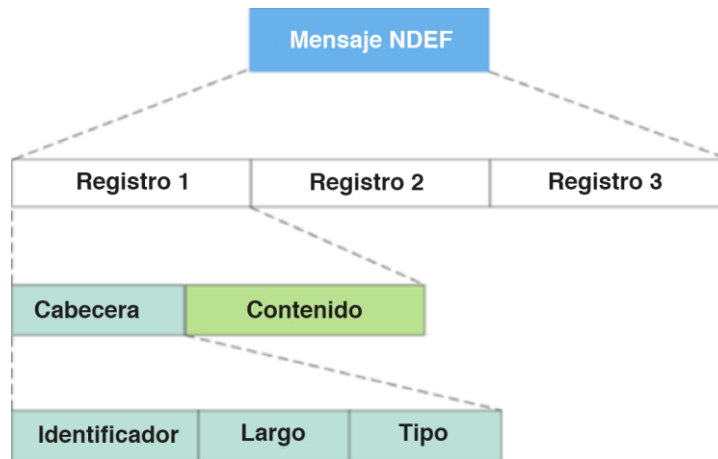


Ilustración 53. Composición General de un mensaje Tipo NDEF

Fuente: (Nokia)

Cuando un teléfono inteligente con NFC se comunica con otro dispositivo, lo que se lee será algo parecido a esto:

```
03 0e d1 01 0a 55 03 6e 6f 6b 69 61 2e 63 6f 6d fe
```

Ilustración 54. Código Hexadecimal de lectura de un mensaje NDEF

Fuente: (Nokia)

En donde:

03- Ese byte define qué tipo de registro es. Un registro NDEF será siempre representado por el byte hexadecimal 03.

0e-Este byte especifica al lector cuanto bytes existen en la carga

d1- es un código binario, en este caso corresponde a (11010001), cuyo formato es el siguiente:

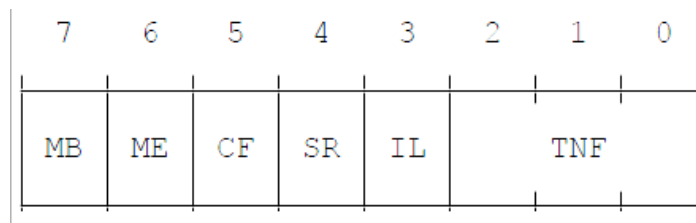


Ilustración 55. Formato del código binario contenido en un mensaje NDEF

Fuente: (Nokia)

En donde:

-MB=1 (si es verdadero significa que este es el primer registro del mensaje NDEF)

-ME=1 (si es 1 indica el final del mensaje, si es 0 le indica a la aplicación que aún hay más registros a continuación)

-CF=0 (significa que el mensaje no ha sido dividido, un mensaje NDEF puede contener cero o más cargas divididas. En caso que lo fuera, cada pedazo es codificado como un registro dividido inicial, seguido de cero o más registros intermedios y finalmente por un pedazo final.)

-SR=1 (*Short Record*, en caso de ser verdadero la longitud de la carga es de un octeto únicamente, este tipo de registros pequeños están diseñados para encapsular pequeñas cargas que oscilan entre 0 y 255 octetos.)

-IL=0 (*Identification Length*, si es verdadero indica que la longitud del campo de identificación está presente en la cabecera como un octeto único, en caso de ser cero, el tamaño del campo de identificación es omitido de la cabecera y del registro)

-TNF=001 (indica la estructura del valor del campo de tipo, e caso de contener 0x01 indica que el valor del campo de tipo sigue el formato de nombre definido por la especificación del *NFC Forum*).

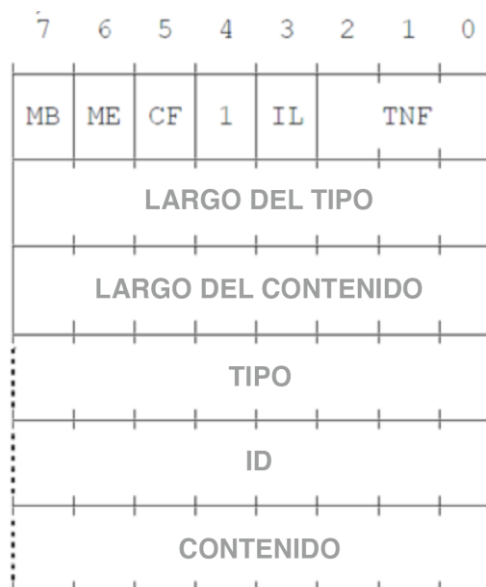


Ilustración 56. Estructura detallada del contenido de un mensaje en formato NDEF

Fuente: (Nokia)

Continuando con la definición del código hexadecimal original se tiene:

-01(*Type Length*, este campo contiene un número entero de 8 bits sin signo que especifica la longitud en octetos del campo de tipo)

-0A (*Pay load Length*, este campo contiene un número entero de 8 bits sin signo que especifica la longitud en octetos del campo de carga, el tamaño del campo de la longitud de la carga está definido por el valor de la bandera SR)

-55 (es el valor del campo de tipo, es un identificador que describe el tipo de la carga)

-03 (Es el identificador para “http://”)

-*Pay Load* (Es el resto del *string* en formato UTF-8)

-FE (Es el byte de terminación) (Nokia)

El *framework* de Android esencialmente brinda la capacidad de recibir y enviar datos por medio de NFC en forma de mensajes tipo NDEF (Android Inc.). El leer datos en el formato NDEF es manejado por el sistema de ejecución de etiquetas, el cual analiza las etiquetas descubiertas, categoriza apropiadamente los datos e inicia una aplicación especificada en dichos datos. La aplicación que desea manejar la etiqueta escaneada puede declarar un filtro de intención y solicitar manejar los datos. (Android Inc.)

La característica denominada Android *Beam* permite a un dispositivo transmitir un mensaje NDEF a otro dispositivo, tan solo acercando los dos dispositivos entre sí. Esta interacción brinda una forma más sencilla de enviar datos en comparación con otras tecnologías inalámbricas como Bluetooth, puesto que NFC no requiere de un emparejamiento manual de los dispositivos previamente, ya que la comunicación inicia automáticamente cuando ambos dispositivos se encuentran dentro del rango. Esta característica está disponible por medio de varias APIs de NFC de tal forma que cualquier aplicación la pueda utilizar para transmitir contactos, páginas web, videos, etc. (Android Inc.)

Los dispositivos Android usualmente buscan etiquetas NFC cuando su pantalla esta desbloqueada, al menos que la característica NFC este apagada desde las

configuraciones generales del dispositivo. Cuando el sistema descubre una etiqueta NFC dentro del rango, el comportamiento que se desea es, que la actividad apropiada maneje la interacción sin preguntar al usuario que aplicación debe usar. Puesto que las etiquetas NFC se escanean a un muy corto rango de distancia y si se pregunta algo al usuario, esto obligará a mover el dispositivo lejos de la etiqueta interrumpiendo la conexión. (Android Inc.)

Para alcanzar este objetivo, Android provee un sistema especial de ejecución de etiquetas el cual analiza las etiquetas escaneadas, las procesa y entonces trata de localizar las aplicaciones que están interesadas en manejar los datos escaneados. Esto lo consigue:

- a) Procesando la etiqueta NFC y averiguando el tipo de MIME o URI que identifica los datos cargados desde la etiqueta.
- b) Encapsula el tipo de MIME o URI y lo carga en un primer intento.
- c) Inicializa una actividad basado en el intento de carga (Android Inc.)

El sistema de ejecución de etiquetas define tres intentos, los cuales son atendidos desde la prioridad más alta a la menor.

- a) *ACTION_NDEF_DISCOVERED*: Este intento trata de iniciar una actividad cuando la etiqueta contiene una carga NDEF y al escanearla se reconoce el tipo.
- b) *ACTION_TECH_DISCOVERED*: Si ninguna actividad se registró para manejar el intento de *ACTION_NDEF_DISCOVERED* o no se reconoció el tipo MIME o URI contenido en el mensaje, el sistema trata de iniciar una aplicación con este intento.
- c) *ACTION_TAG_DISCOVERED*: se ejecuta este intento en caso de que ninguno de los anteriores haya conseguido ejecutar una actividad para manejar dichos datos. (Android Inc.)

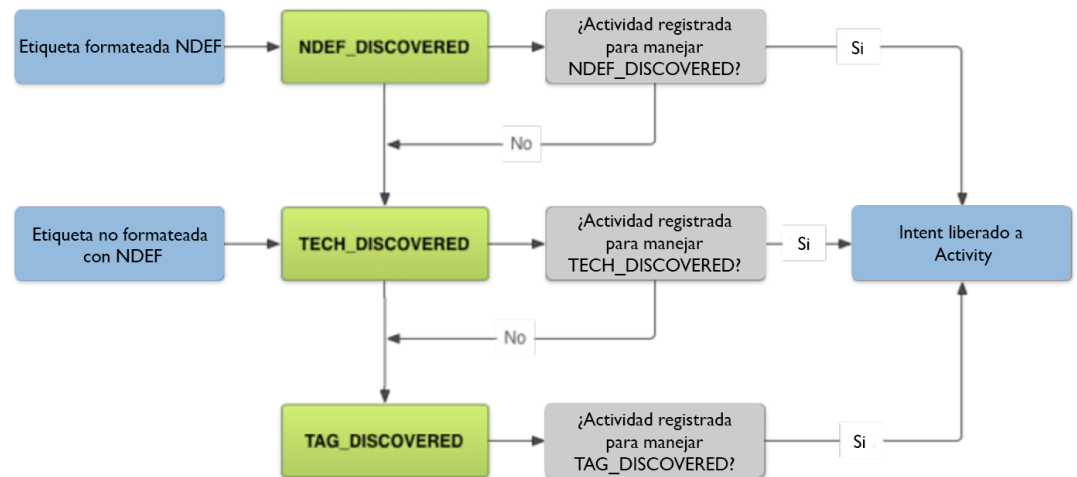


Ilustración 57. Flujo del sistema de ejecución de etiquetas

Fuente: (Android Inc.)

Wamp Server-Servidor Apache, PHP y BD MySQL

Es un ambiente de desarrollo diseñado para la plataforma Windows, el cual permite crear aplicaciones web y montarlas sobre un servidor Apache2, PHP e incluir una base de datos MySQL y manejarla de una forma sencilla a través de una interfaz PhpMyAdmin. De la misma forma este software nos permite dar acceso a cualquiera a visitar nuestro *localhost* (poner en línea el servidor), acceder a los *logs* del sistemas, manejar variedad de idiomas, etc (WampServer). Se puede obtener este paquete software en la siguiente dirección:

<http://www.wampserver.com/en/>

5.2 Preparación del entorno y herramientas

Android

Para iniciar con el desarrollo de aplicaciones Android, se debe instalar y adecuar una serie de herramientas que permitirán hacer uso del kit de desarrollo Android y explorar las diversas opciones que este presenta (librerías, *logs*, emuladores, servicios adicionales, etc.).

El primer paso consiste en obtener el Android SDK, que es el encargado de proporcionar las librerías y herramientas de desarrollo necesarias para construir, probar y depurar aplicaciones. Existen diversas maneras de adecuar nuestro entorno para desarrollar aplicaciones Android, sin embargo, la principal opción ofrecida por la documentación oficial consiste en descargar una herramienta unificada conocida como *ADT Bundle Developer (Android Tools)*, se lo puede descargar en el siguiente enlace <http://developer.android.com/sdk/index.html>, e incluye los siguientes componentes:

- Entorno de desarrollo Eclipse IDE for Java Developers. (Versión 3.6.2)
- *Plugin Android Developer Tools* (Versión 22.3.0 Octubre de 2013).
- SDK Android. (Versión r.22.6.2).
- *Android Platform-tools*. (Versión r.16.0.2).
- Imagen del sistema Android para el emulador. (Versión 4.2.2)

Se debe tener en cuenta algunos requerimientos del sistema necesarios para poder desarrollar aplicaciones Android:

- Sistema Operativo:
 - Windows XP (32-bit), Vista (32- or 64-bit), o Windows 7 (32- or 64-bit)
 - Mac OS X 10.5.8 o posterior (x86 solamente)
 - Linux (probado en Ubuntu Linux, Lucid Lynx)
 - GNU C Library (glibc) 2.7 o posterior.
 - En Ubuntu Linux, versión 8.04 o posterior.
 - Distribuciones de 64-bit deben ser capaces de correr aplicaciones de 32 bits.
- Eclipse IDE
 - Eclipse 3.6.2 (Helios) o posterior
 - Nota: Eclipse 3.5 (Galileo) no es soportado.
 - Plugin Eclipse JDT (incluido en la mayoría de paquetes Eclipse)
 - JDK 6
 - Plugin Android Development Tools (recomendado)
 - No es compatible con compilador GNU para Java (gcj)

Una vez descargado el ADT *Bundle*, se lo debe descomprimir en un directorio adecuado del computador, y abrir la siguiente ruta: `adt-bundle-<os_platform>/eclipse/` para ejecutar el IDE Eclipse, de esta manera se tendría el entorno listo y cargado con las herramientas de desarrollo Android para iniciar con el desarrollo de aplicaciones. (Android Inc.)

Wamp Server-Servidor Apache, PHP y BD MySQL

El prototipo va a implementar un sistema de administración que permitirá cargar información que podrá ser consumida desde la aplicación móvil, para ello es necesario instalar un entorno de desarrollo web con la finalidad de implementar el sistema back-end en el lenguaje de programación PHP.

Wampserver permite preparar un entorno Apache, PHP y MySQL en el sistema operativo Windows de una forma sencilla. Primero se debe descargar el instalador desde el siguiente enlace: <http://www.wampserver.com/en/>, se hace doble clic sobre el archivo descargado y se sigue las instrucciones ya que prácticamente todo es automático.

Para iniciar a usar este entorno de desarrollo web, se debe acceder al directorio que se creó automáticamente, por lo general, en la siguiente ruta `c:\wamp\www`, y colocar los archivos PHP en dicha ruta, de esta manera se puede acceder desde un navegador web y visualizar el sitio en la URL <http://localhost>. (WampServer)

5.3 Programación para el modo de operación lectura/escritura.

Modo de operación lectura/escritura: este modo permite al dispositivo NFC leer y/o escribir etiquetas o stickers NFC pasivos.

5.4 Programación para el modo de operación punto a punto.

Modo de operación punto a punto (modo P2P): permite a los dispositivos NFC intercambiar datos con otros dispositivos. Este modo de operación es usado por el sistema Android *Beam*, que es una característica introducida en la versión 4.0 de Android (*Ice Cream Sandwich*) para facilitar la transferencia de datos vía NFC, como por ejemplo, intercambio de marcadores web, información de contactos, direcciones, urls de videos, entre otra información.

5.5 Programación para el modo de operación emulación de tarjeta

Modo de operación emulación de tarjeta: permite al dispositivo NFC actuar como una tarjeta NFC. Luego la tarjeta emulada puede ser accedida por un lector NFC, como por ejemplo un terminal de un punto de venta. Actualmente, algunos dispositivos NFC ofrecen la funcionalidad de emulación de tarjeta, en la mayoría de casos, la emulación la realiza un chip adicional en el dispositivo, conocido como elemento seguro. Desde la versión Android 4.4, se implementó un método adicional de emulación de tarjeta que no involucra un elemento seguro, esto se lo conoce como emulación de tarjeta basada en el host.

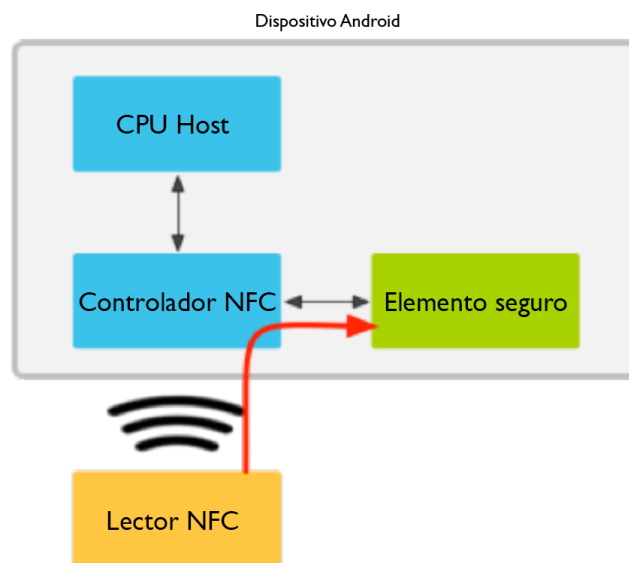


Ilustración 58. Emulación de tarjeta con un elemento seguro

Fuente: (Android Inc)

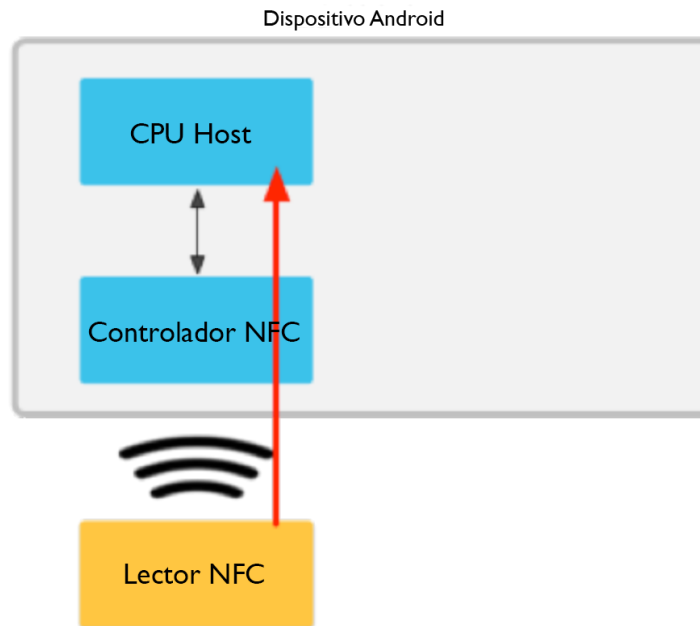


Ilustración 59. Emulación de tarjeta sin un elemento seguro.

Fuente: (Android Inc)

5.6 Análisis del prototipo

Especificación de Requisitos del Sistema

El paso inicial para el ciclo de vida del desarrollo de software, es la Especificación de Requisitos del Sistema (ERS). La elaboración de este documento tiene 2 objetivos principales: por un lado ayudar a los clientes a describir claramente lo que desean obtener de un determinado software, ya que el usuario tiene una visión mucho más detallada de los procesos que desea automatizar. Y por otro lado ayudar de igual manera a los desarrolladores a entender que desea el cliente, definiendo todos los requisitos necesarios del sistema. (Monferrer Agut)

Es muy importante citar que, de no realizarse una buena especificación de requisitos, los costes del desarrollo pueden incrementarse, de igual forma los plazos de tiempos estimados estarán sujetos a cambios constantes, esto tendrá una mala influencia para con el cliente, reduciendo nuestra credibilidad y ocasionando más de un conflicto. Inclusive es preciso citar que el documento de

especificación de requisitos puede ser utilizado como parte del fundamento legal al momento de realizar un contrato con el cliente, aquí se especificará claramente las funcionalidades y el alcance del producto, evitando cambios futuros que no fueron considerados inicialmente.

Es muy importante que durante la elaboración de este documento intervengan tanto analistas como los usuarios del sistema, el léxico empleado en el mismo deberá ser totalmente legible y evitando utilizar demasiadas palabras técnicas, de manera que cualquier persona pueda comprender el alcance del producto. (Monferrer Agut)

Para el desarrollo de la especificación de requisitos del sistema, se recomienda aplicar el estándar IEEE-830. En la sección de anexos, **6.1 Especificación de Requisitos del Sistema (ERS)**, se puede observar el documento de especificación de requisitos para *un menú virtual de patio de comidas*, que será el tema con el que se desarrollará a continuación un prototipo de una aplicación móvil que emplee la tecnología NFC.

Diagrama de Clases

Una vez que el alcance de la aplicación ha sido definido, el siguiente paso es realizar el diagrama de clases del sistema. El objetivo de este diagrama es mostrar la estructura estática del sistema que se está modelando, para el caso de una aplicación basada en orientación a objetos, las clases tienen atributos, operaciones y relaciones con otras clases. (Martin)

En este diagrama se podrá observar todas las entidades que formarán parte del sistema, así como sus atributos y operaciones. Para el caso del sistema de menú virtual de un patio de comidas, se ha considerado que las entidades necesarias son: Restaurantes, Categorías de Comida, Productos y Usuarios. A continuación se presenta las estructuras de estas entidades y como estas se relacionan entre sí.

restaurantes
-restaurantes_codigo -restaurantes_nombre -restaurantes_numeroLocal -restaurantes_telefono restaurantes_url_imagen
+obtenerCodigoRestaurante() +obtenerNombreRestaurante() +obtenerNumeroLocalRestaurante() +obtenerTelefonoRestaurante() +obtenerUrlImagenRestaurante() +insertarRestaurante(nombre,numeroLocal,telefono) +modificarRestaurante(codigo,nombre,numeroLocal,telefono) +consultarRestauranteXCodigo(codigo) +consultarRestauranteXNombre(nombre)

(Fuente: Autoría Propia)

categorias_comida
-categoriasComida_Codigo -categoriasComida_Descripcion
+obtenerCodigoCategoria() +obtenerNombreCategoria() +insertarCategoria(nombre) +modificarCategoria(codigo, nombre) +consultarCategoriaXCodigo(codigo) +consultarCategoriaxNombre(nombre)

(Fuente: Autoría Propia)

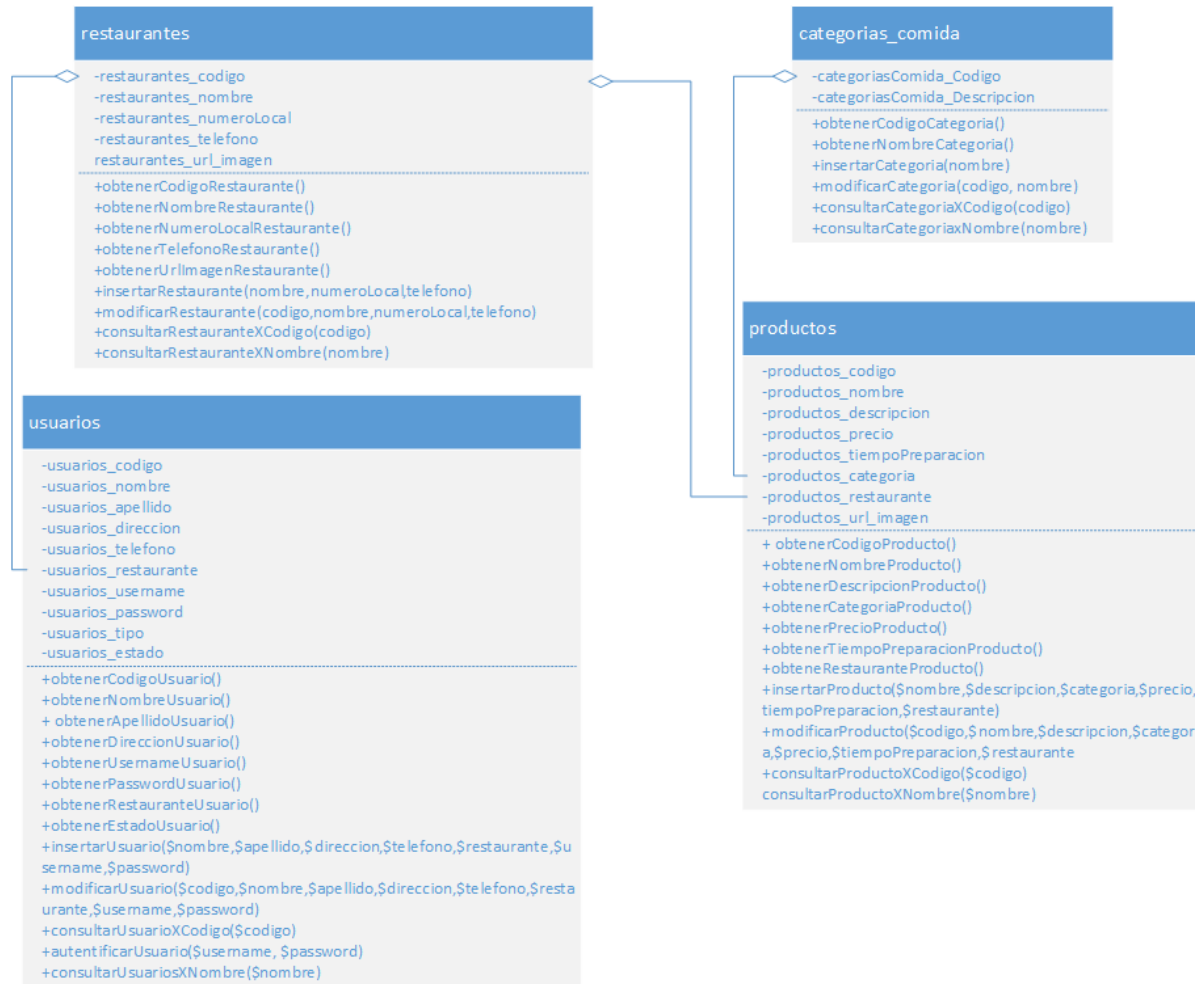
productos

```
-productos_codigo  
-productos_nombre  
-productos_descripcion  
-productos_precio  
-productos_tiempoPreparacion  
-productos_categoria  
-productos_restaurante  
-productos_url_imagen  
-----  
+ obtenerCodigoProducto()  
+ obtenerNombreProducto()  
+ obtenerDescripcionProducto()  
+ obtenerCategoriaProducto()  
+ obtenerPrecioProducto()  
+ obtenerTiempoPreparacionProducto()  
+ obteneRestauranteProducto()  
+ insertarProducto($nombre,$descripcion,$categoria,$precio,$  
tiempoPreparacion,$restaurante)  
+ modificarProducto($codigo,$nombre,$descripcion,$categori  
a,$precio,$tiempoPreparacion,$restaurante  
+ consultarProductoXCodigo($codigo)  
consultarProductoXNombre($nombre)
```

(Fuente: Autoría Propia)

usuarios
-usuarios_codigo
-usuarios_nombre
-usuarios_apellido
-usuarios_direccion
-usuarios_telefono
-usuarios_restaurante
-usuarios_username
-usuarios_password
-usuarios_tipo
-usuarios_estado
+obtenerCodigoUsuario()
+obtenerNombreUsuario()
+ obtenerApellidoUsuario()
+obtenerDireccionUsuario()
+obtenerUsernameUsuario()
+obtenerPasswordUsuario()
+obtenerRestauranteUsuario()
+obtenerEstadoUsuario()
+insertarUsuario(\$nombre,\$apellido,\$direccion,\$telefono,\$restaurante,\$username,\$password)
+modificarUsuario(\$codigo,\$nombre,\$apellido,\$direccion,\$telefono,\$restaurante,\$username,\$password)
+consultarUsuarioXCodigo(\$codigo)
+autenticarUsuario(\$username, \$password)
+consultarUsuariosXNombre(\$nombre)

(Fuente: Autoría Propia)



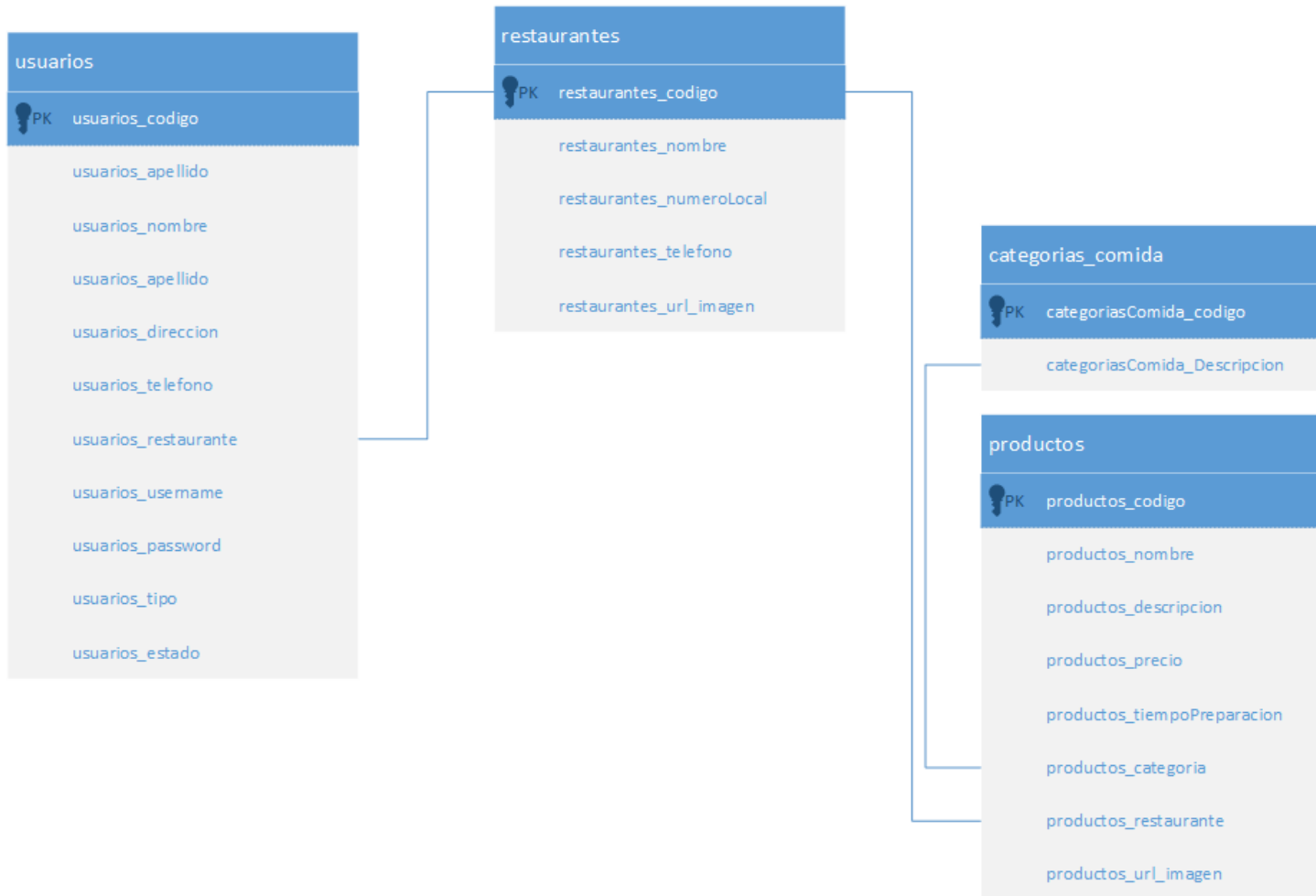
(Fuente: Autoría Propia)

Diagrama Entidad-Relación

Una vez terminado el diagrama de clases, es momento de pasar la información obtenida a un esquema, el cual permita crear un repositorio para almacenar información de las entidades en una base de datos. Para ello se recomienda diseñar un diagrama entidad – relación.

Este diagrama se basa en una percepción de un mundo real que consiste en un conjunto de objetos básicos llamados entidades y de relaciones entre estos objetos. Los objetos básicos en un modelo Entidad-Relación (ER) son: las entidades, relaciones y atributos. (Facultad de Ciencias Agrarias-Universidad Nacional del Litoral)

A continuación se presenta el diagrama entidad-relación para el sistema de menú virtual de un patio de comidas.



(Fuente: Autoría Propia)

Diccionario de Datos

Categorías_comida

Campo	Tipo	Nulo	Predeterminado	Comentarios
<u>categoriasComida_Codigo</u>	int(11)	No		Código identificador de la categoría de comida
categoriasComida_Descripcion	varchar(50)	No		Descripción de la categoría de comida

Productos

Campo	Tipo	Nulo	Predeterminado	Comentarios
<u>productos_codigo</u>	int(11)	No		Código identificador del producto
productos_nombre	varchar(50)	No		Nombre del Producto
productos_descripcion	tinytext	No		Pequeña descripción del producto

productos_precio	float	No		Precio del producto en USD
productos_tiempoPreparacion	int(11)	No		Tiempo aproximado de preparación del producto
productos_categoria	int(11)	No		Categoria de comida a la que pertenece
productos_restaurante	int(11)	No		Restaurante al que pertenece el producto
productos_url_imagen	varchar(100)	No		Nombre del archivo de imagen y extensión del producto

Restaurantes

Campo	Tipo	Nulo	Predeterminado	Comentarios
<u>restaurantes_codigo</u>	int(11)	No		Código identificador del restaurante
restaurantes_nombre	varchar(50)	No		Nombre del restaurante
restaurantes_numeroLocal	varchar(10)	No		Número del Local en el patio de comidas
restaurantes_telefono	varchar(10)	No		Teléfono del restaurante en la estructura (072856452)

restaurantes_url_imagen	varchar(100)	No		Nombre del archivo de imagen y extensión del restaurante
-------------------------	--------------	----	--	--

Usuarios

Campo	Tipo	Nulo	Predeterminado	Comentarios
<u>usuarios_codigo</u>	int(11)	No		Código identificador del usuario
usuarios_nombre	varchar(50)	No		Nombre del Usuario
usuarios_apellido	varchar(50)	No		Apellido del Usuario
usuarios_direccion	varchar(50)	No		Dirección del Usuario
usuarios_telefono	varchar(10)	No		Teléfono del usuario
usuarios_restaurante	int(11)	No		Restaurante al que pertenece
usuarios_username	varchar(20)	No		Alias del Usuario
usuarios_password	varchar(20)	No		Contraseña del Usaurio
usuarios_tipo	tinyint(4)	No	1	Tipo de Usuario (0=Super Administrador)(1=Administrador de Restaurante)
usuarios_estado	tinyint(4)	No	0	Estado del Usaurio, (1: Activo)(0:Inactivo)

5.7 Diseño del prototipo

Una vez completado el análisis del prototipo, es momento de proceder a realizar la estructuración tanto de las secciones que poseerá el aplicativo web, como el móvil.

El diseño del prototipo se especifica mediante un documento denominado “Manual de Estilos”.

Manual de Estilos

Es un documento en el cual se especifica tanto la estructura de los aplicativos como su diseño estético. Está compuesto por las siguientes secciones:

Wireframes

Es un conjunto de gráficos en los cuales se bosqueja la ubicación de los elementos de una interfaz. No se incluyen detalle gráficos puesto que el objetivo es especificar los detalles generales del sistema (esqueleto). Los wireframes constituyen una herramienta de comunicación muy poderosa, de la cual participan tanto arquitectos de la información, como analistas de sistemas, programadores, diseñadores y clientes. (Arquitectura de la Información-Chile). Dado que el diseño de un *wireframe* es bastante simple, es posible modificarlos con facilidad y analizar varias posibilidades, antes de aplicar el diseño definitivo. Generalmente está compuesto de bloques de texto, títulos, contenedores, cajas para elementos gráficos, etc. (Kyrnin)

Mockups

A diferencia de lo que se definió como *wireframe*, un *mockup* incluye el diseño estético de una interfaz, es decir: colores, imágenes, tipos de letra, tamaños, etc. De esta manera se puede brindar una sensación completa de lo que la aplicación llegará a ser. Con esta herramienta se puede concretar con el cliente el diseño final, incluso se puede conectar las interfaces por medio de enlaces, de modo que se pueda observar la navegabilidad del aplicativo. (Creately)

Color

Es preciso definir la paleta de colores que se utilizará en el diseño final del aplicativo. Usualmente se presenta un rectángulo con el color de muestra y su código hexadecimal. (Universidad de Málaga)

Imágenes e Íconos

Se puede incluir una lista de los distintos iconos que formarán parte del aplicativo, tamaños de imágenes y posiciones relativas o estáticas. (Universidad Politécnica de Valencia)

Títulos y Textos

Se definen los estilos de texto como: títulos, subtítulos, descripciones, etc. Para los cuales es necesario especificar: tamaño, fuente utilizada y colores.

Formularios

En esta sección se detallan las características gráficas de los distintos formularios y campos de entrada de datos que presentará el aplicativo. Especificando dimensiones, estructura, botones, fondos, encabezados y pies de página.

En la sección de anexos: **6.2 Manual de Estilos**, se presenta el documento con todos los conceptos descritos anteriormente y aplicados al prototipo de Menú Virtual de Patio de Comidas.

5.8 Desarrollo del prototipo**Aplicativo Web**

La aplicación web para el menú virtual de patio de comidas está desarrollada en el lenguaje de programación PHP, los datos están almacenados en una base de datos *MySql* y se ejecuta en un servidor web apache, simulado por medio del programa *WampServer*.

Este aplicativo tiene por objeto administrar los usuarios, categorías de comida, restaurantes y productos. En la misma existen dos perfiles de usuario, un super administrador, que es el encargado de gestionar: categorías de comida, restaurantes y

usuarios. Y por otro lado un administrador de restaurante, el cual administra los productos del restaurante al que pertenece.

Aplicativo Móvil

El sistema móvil está compuesto de dos aplicaciones que permitirán interactuar con la información gestionada desde el administrador web y con las etiquetas NFC. La primera aplicación está destinada a ser usada por un administrador y permitirá seleccionar un local y grabar la información necesaria en la etiqueta NFC, para que pueda ser procesada por la segunda aplicación cliente. El sistema Android se encargará de leer la etiqueta y ejecutar la aplicación cliente mostrando exclusivamente la información de interés al usuario.

En Android, la lectura de datos de una etiqueta NFC es manejado por el sistema de despacho de etiquetas, que se encarga de analizar la etiqueta, categorizar los datos y ejecutar la aplicación interesada en los datos categorizados, sin preguntar al usuario que aplicación usar. El sistema de despacho de etiquetas lleva a cabo las siguientes operaciones para procesar la lectura de etiquetas:

1. Analizar la etiqueta NFC y obtener el tipo MIME o la URI que identifica a los datos de la etiqueta.
2. Encapsular el tipo MIME o URI y los datos en un objeto *Intent*.
3. Iniciar la clase *Activity* basada en el *Intent*.

Para que una aplicación puede ser ejecutada luego de que el sistema de despacho de etiquetas ha encapsulado los datos, existen tres *Intents* que se pueden definir en el archivo *Manifest* de la aplicación para que esta sea capaz de manejar los datos de la etiqueta NFC:

ACTION_NDEF_DISCOVERED: este es el *Intent* con la mayor prioridad, y es usado para ejecutar un *Activity* cuando una etiqueta que contiene un mensaje NDEF es escaneada y es de un tipo reconocido.

ACTION_TECH_DISCOVERED: si no existe ningún *Activity* registrado para manejar el *Intent* ACTION_NDEF_DISCOVERED, el sistema de despacho de etiquetas trata de iniciar una aplicación que contenga este *Intent*.

ACTION_TAG_DISCOVERED: este *Intent* es iniciado si no existe ningún *Activity* que maneje los *Intents* ACTION_NDEF_DISCOVERED o ACTION_TECH_DISCOVERED.

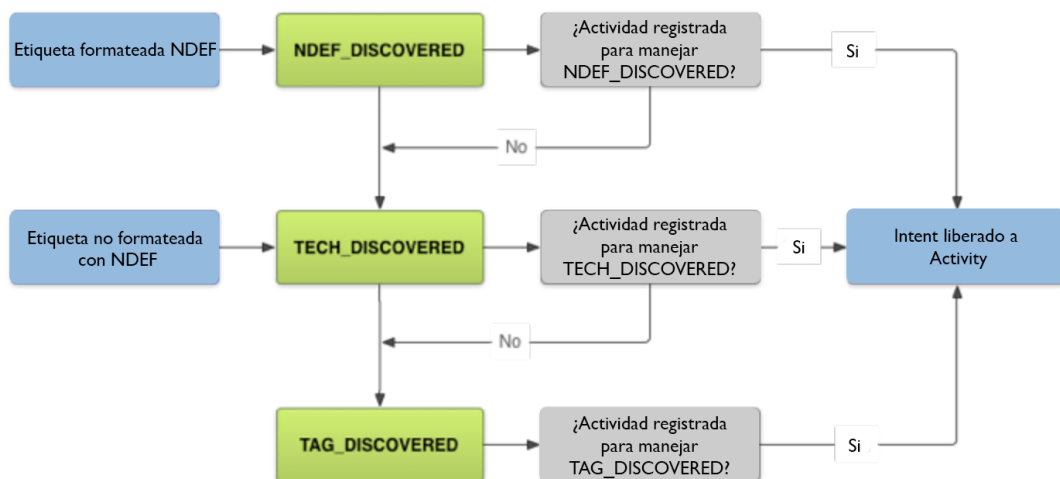


Ilustración 60. Sistema de despacho de etiquetas.

Fuente: (Android Inc.)

Solicitando permisos de acceso

El primer paso para que la aplicación sea capaz de manejar etiquetas NFC, consiste en solicitar ciertos permisos en el archivo Android *Manifest*:

- El permiso NFC `<uses-permission>` permite acceder al hardware NFC:
`<uses-permission android:name="android.permission.NFC" />`
- La mínima versión del SDK que la aplicación puede soportar es la API nivel 10, que incluye soporte de lectura/escritura:

```
<uses-sdkandroid:minSdkVersion="10"/>
```

- El elemento *uses-feature* permite que la aplicación sea visible solo para dispositivos que cuentan con el hardware NFC:

```
<uses-featureandroid:name="android.hardware.nfc"android:required="true" />
```

Filtrado de Intents NFC

Para iniciar la aplicación cuando una etiqueta NFC es escaneada, la aplicación debe filtrar mínimo uno de los tres tipos de *Intents* propuestos por el sistema de despacho de etiquetas (ACTION_NDEF_DISCOVERED, ACTION_TECH_DISCOVERED o ACTION_TAG_DISCOVERED).

En este caso se usará el *Intent* ACTION_NDEF_DISCOVERED que es el que posee la mayor prioridad para ejecutar una aplicación:

```
<intent-filter>
```

```
<action android:name="android.nfc.action.NDEF_DISCOVERED" />
```

```
<category android:name="android.intent.category.DEFAULT" />
```

```
<data android:mimeType="application/com.tesis.nfc" />
```

```
</intent-filter>
```

Recuperar la información de la etiqueta NFC desde un Intent

Si un Activity es iniciado a causa de un Intent NFC, se puede obtener la información de la etiqueta escaneada:

- EXTRA_TAG: consiste en un objeto *Tag* que representa la etiqueta escaneada.

- EXTRA_NDEF_MESSAGES: es un arreglo de mensajes NDEF obtenidos de la etiqueta.
- EXTRA_ID: el ID de la etiqueta.

Para obtener estos extras, se debe revisar si el *Activity* fue lanzado con uno de los *Intents* NFC para asegurar que la etiqueta fue escaneada, y luego proceder a recuperar la información.

```
NdefMessage[] msgs = null;

if (NfcAdapter.ACTION_NDEF_DISCOVERED.equals(intent.getAction())
    && intent.getType() != null
    &&
intent.getType().equals("application/com.tesis.nfc")){

    Parcelable[] rawMsgs = intent
        .getParcelableArrayExtra(NfcAdapter.EXTRA_NDEF_MESSAGES);

    if (rawMsgs != null) {

        msgs = new NdefMessage[rawMsgs.length];

        for (int i = 0; i < rawMsgs.length; i++) {

            msgs[i] = (NdefMessage) rawMsgs[i];

        }

    }

    if (msgs != null) {

        if (msgs.length > 0) {

            NdefRecord relayRecord = msgs[0].getRecords()[0];

            String nfcData = new String(relayRecord.getPayload());
```

```
arguments.putString("_nfc", nfcData);  
    }  
}  
} else {  
    LOGI(TAG, "Intent null or not com.tesis.nfc");  
}
```

A partir de este código se pueden obtener los datos almacenados en la etiqueta NFC y procesarlos en nuestra aplicación según su objetivo. En el caso del prototipo, se obtiene la información de los locales de comida para procesar y mostrar al usuario el catálogo de productos sin necesidad de que el usuario realice una búsqueda.

Escribir sobre una etiqueta NFC

El primer paso consiste en crear un registro NDEF mediante la función `createApplicationRecord()` y crear un nuevo objeto *NdefRecord*, este registro almacenará la información con el nombre del paquete de la aplicación para que esta pueda ser ejecutada cuando la etiqueta NFC es escaneada. Además se crea otro registro con los datos que se desean incluir para el propósito final de la aplicación, en este caso la información de los locales de comida, para ello se define al registro como tipo MIME de la forma `application/com.tesis.nfc` y se adicionan los datos mencionados.

Finalmente el dato que es grabado en la etiqueta NFC es un objeto *NdefMessage*, el cual es creado a partir de un arreglo de registros.

```
public static boolean writeTag(Context context, Tag tag, String data) {
```

```
NdefRecord appRecord = NdefRecord
.createApplicationRecord("com.tesis.nfc");

// Registro con los datos específicos

NdefRecord relayRecord = new
NdefRecord(NdefRecord.TNF_MIME_MEDIA,new
String("application/com.tesis.nfc").getBytes(Charset.forName("US-ASCII")),
null, data.getBytes());

// Mensaje NDEF con los registros

NdefMessage message = new NdefMessage(new NdefRecord[] {
relayRecord,appRecord });

try {

    // Si la etiqueta está formateada, solo se graban los datos

    Ndef ndef = Ndef.get(tag);

    if (ndef != null) {

        ndef.connect();

        // Asegurarse que la etiqueta sea grabable

        if (!ndef.isWritable()) {

            DialogUtils.displayErrorDialog(context,

                R.string.nfcReadOnlyErrorTitle,

                R.string.nfcReadOnlyError);

            return false;

        }

    }

}
```

```
// Verificar que existe suficiente espacio en la etiqueta
int size = message.toByteArray().length;
if (ndef.getMaxSize() < size) {
    DialogUtils.showErrorDialog(context,
                                R.string.nfcBadSpaceErrorTitle,
                                R.string.nfcBadSpaceError);
    return false;
}

try {
    // Grabar los datos en la etiqueta
    ndef.writeNdefMessage(message);

    DialogUtils.displayInfoDialog(context,
                                   R.string.nfcWrittenTitle,
                                   R.string.nfcWritten);
    return true;
} catch (TagLostException tle) {
    DialogUtils.showErrorDialog(context,
                                R.string.nfcTagLostErrorTitle,
                                R.string.nfcTagLostError);
    return false;
} catch (IOException ioe) {
    DialogUtils.showErrorDialog(context,
```



```
        R.string.nfcFormattingErrorTitle,
        R.string.nfcFormattingError);

    return false;
} catch (FormatException fe) {

    DialogUtils.showErrorDialog(context,

        R.string.nfcFormattingErrorTitle,
        R.string.nfcFormattingError);

    return false;
}

// Si la etiqueta no está formateada, formatear con el mensaje
} else {

    NdefFormatable format = NdefFormatable.get(tag);

    if (format != null) {

        try {

            format.connect();

            format.format(message);

            DialogUtils.displayInfoDialog(context,

                R.string.nfcWrittenTitle,
                R.string.nfcWritten);

            return true;

        } catch (TagLostException tle) {

            DialogUtils.showErrorDialog(context,

                R.string.nfcTagLostErrorTitle,
                R.string.nfcTagLostError);
```

```
        return false;
    } catch (IOException ioe) {
        DialogUtils.displayErrorDialog(context,
            R.string.nfcFormattingErrorTitle,
            R.string.nfcFormattingError);
        return false;
    } catch (FormatException fe) {
        DialogUtils.displayErrorDialog(context,
            R.string.nfcFormattingErrorTitle,
            R.string.nfcFormattingError);
        return false;
    }
} else {
    DialogUtils.displayErrorDialog(context,
        R.string.nfcNoNdefErrorTitle,
        R.string.nfcNoNdefError);
    return false;
}
}
} catch (Exception e) {
    DialogUtils.displayErrorDialog(context,
        R.string.nfcUnknownErrorTitle,
        R.string.nfcUnknownError);
}
return false;
}
```

Este código permite validar que la etiqueta se encuentre formateada, o la formatea en caso de ser necesario, además de verificar si es grabable ya que pueden existir etiquetas de solo lectura.

Conclusión del Capítulo

Conocer las herramientas actuales sobre las que se apoya NFC, permite que las opciones de uso y campos de aplicación de la tecnología se puedan identificar de mejor manera. Google con su sistema operativo Android, es una de las empresas que tienen planes reales de masificación del uso de NFC, es por esto que a pesar de que el porcentaje de utilización de la tecnología no es muy grande, las herramientas de desarrollo y librerías son bastante completas y permiten la interacción entre dispositivos y etiquetas NFC.

El prototipo ha permitido ejemplificar uno de los modos de comunicación de la tecnología NFC, y entender los fundamentos técnicos y modos de operación que hacen de NFC una mejor alternativa comparada con otras soluciones de comunicación inalámbrica.

CONCLUSIONES Y RECOMENDACIONES

En el presente trabajo se describió detalladamente los conceptos técnicos del funcionamiento de la tecnología NFC; desde su frecuencia de operación, modos de comunicación, modos de operación, componentes; pasando por los conceptos fundamentales de electromagnetismo para la comunicación inalámbrica, estructura de mensajes de comunicación; hasta la evolución de la tecnología partiendo del código de barras y llegando a RFID, tecnología que formó parte de la base del funcionamiento de NFC.

Se pudo constatar los beneficios que la tecnología representa en comparación a otras tecnologías inalámbricas de comunicación tales como: Bluetooth, RFID e Infrarrojo. Principalmente NFC se destaca por permitir una comunicación bidireccional entre dispositivos, un menor tiempo de configuración (0,1 segundos) y una velocidad de transferencia de 424Kbps, en tanto que las otras tecnologías permiten un alcance de 1 a 10 metros y en el caso de Bluetooth una mayor velocidad de transferencia (721Kbps). Es preciso citar que actualmente NFC está siendo utilizada como tecnología complementaria a otras como Wi-Fi y Bluetooth, y no como una competencia, ya que su inclusión en dispositivos como teléfonos móviles, cines en casa, sistemas de audio de hogar y otros dispositivos cotidianos, tiene como objetivo simplificar la configuración y la conexión con las tecnologías mencionadas anteriormente.

Como puntos débiles de la tecnología, se reitera su corto alcance (10 cm), y al ser una tecnología inalámbrica de comunicación, es susceptible a problemas de seguridad como *eavesdropping*, *data modification* o *man in the middle*. Por lo tanto los aplicativos que se desarrollen con NFC deben aplicar mecanismos de seguridad, como criptografía, *hashing* y firmas digitales, que disminuyan el riesgo de estas vulnerabilidades, especialmente cuando se trata de transacciones financieras, de modo que sea una tecnología segura y confiable para los usuarios, y que permita cumplir con los objetivos primarios de la seguridad de la información.

En la actualidad, gracias a la gran industria tecnológica dedicada al desarrollo, investigación y mejora de NFC, se ha logrado que surjan soluciones innovadoras que han captado un mercado de tamaño considerable. Uno de los puntos clave que han aportado al crecimiento de la tecnología ha sido la simplicidad en la integración con diferentes tecnologías ya existentes en el mercado, por lo que se vuelve una alternativa interesante al momento de buscar soluciones relacionadas a la comunicación inalámbrica.

El enfoque central de NFC consiste en crear una infraestructura robusta de pagos electrónicos, sin embargo, el objetivo no debe fijarse únicamente en soluciones de este tipo ya que por las características de la tecnología, se pueden explotar una gran variedad de campos con soluciones de control de acceso, automatización de tareas, seguimiento y control médico, en donde el criterio para el desarrollo de herramientas debe girar alrededor de mejorar la calidad de vida de las personas, aprovechando la confiabilidad, velocidad, seguridad, facilidad de uso, y sobre todo la posibilidad de crear aplicaciones de valor agregado.

Conocer las herramientas actuales sobre las que se apoya NFC, permitió que se desarrolle exitosamente una aplicación móvil para el sistema operativo Android, en la cual se ejemplificó la comunicación entre una etiqueta y un teléfono inteligente, mediante NFC. Este aplicativo tuvo como objetivo representar un menú virtual para un patio de comidas. Para el funcionamiento del aplicativo móvil, fue necesario el desarrollo de una aplicación web, en la cual se ingresa la información de: categorías de comida, restaurantes, usuarios y productos. Una vez ingresada dicha información a la base de datos; el aplicativo móvil accede a esta información por medio de un *web service*, el cual permite seleccionar el restaurante a grabar en una etiqueta NFC, para que finalmente el teléfono lee la etiqueta NFC previamente escrita y muestre los productos del restaurante seleccionado. El desarrollo del prototipo ha permitido ejemplificar uno de los modos de comunicación de la tecnología NFC, y entender los fundamentos técnicos que hacen de NFC una mejor alternativa comparada con otras soluciones de comunicación inalámbrica.

Finalmente, uno de los limitantes en la actualidad, es la masificación de dispositivos habilitados con NFC, haciendo que no existan ambientes de pruebas en nuestro medio, por lo que sería interesante llevar a cabo pruebas e implementaciones de mayor magnitud para validar el uso de la tecnología en ecosistemas de tamaño superior, que permitan obtener la retroalimentación necesaria para colaborar en la creación de soluciones y mejoras sobre NFC.

GLOSARIO

ECMA: es una asociación industrial fundada en 1961, que se dedica a la estandarización de las tecnologías de la Información y Comunicación (ICT) y de los consumibles electrónicos (CE). Entre sus objetivos se destacan: el desarrollo cooperativo con las organizaciones Europeas e Internacionales de estándares, dictar las pautas para un uso correcto de los estándares y publicar estos estándares y reportes técnicos brindando un acceso a los mismos sin ninguna restricción. (ECMA International)

Computación Ubicua: es un modelo de interacción en el que el procesamiento de información se integra fuertemente en las actividades y objetos cotidianos (Romero y Ceron). Este concepto fue introducido por Mark Weiser en 1988, la visión de este experto en ciencias de la computación era: que la tecnología es solo un medio para conseguir un fin, el usuario debería concretarse completamente en la tarea que desea realizar más no de la implementación tecnológica que esta actividad conlleva. (Bonalde)

EMV: *Europay MasterCard VISA*, es un estándar abierto para tarjetas inteligentes para sistemas de pago a nivel mundial, lo cual ha contribuido a la creación de estándares para pago mediante teléfonos móviles. El presente estándar define la interacción entre las tarjetas inteligentes y los dispositivos de procesamiento de tarjetas, a nivel físico, eléctrico, de datos y de aplicación, ciertas partes del estándar están basadas en la norma ISO 7816. (Coskun, Ok y Ozdenizci)

GlobalPlatform: es una asociación industrial sin fines de lucro la cual identifica, desarrolla y publica las especificaciones que faciliten el desarrollo seguro, la interoperabilidad y el mantenimiento de múltiples aplicaciones embebidas en las tarjetas de seguridad inteligente. Su objetivo es asegurar la interoperabilidad del manejo de contenidos de las tarjetas inteligentes, manejar dichas tarjetas sin dependencias de hardware, fabricantes o aplicaciones. (Coskun, Ok y Ozdenizci)

JavaCard OS: Es un sistema operativo que permite que las aplicaciones (o applets) escritos en el lenguaje JavaCard se ejecuten en las tarjetas inteligentes. Esta tecnología está estandarizada por Sun Microsystems y el JavaCardForum. Este SO provee seguridad, interoperabilidad, y multi-aplicaciones para las tarjetas inteligentes, utilizando las ventajas del lenguaje Java, programación orientada a objetos, reutilización, niveles de control de acceso, métodos y variables. Lo cual permite independencia a los desarrolladores sobre la arquitectura. (Coskun, Ok y Ozdenizci)

Phillips MIFARE System: es una tecnología de tarjetas inteligentes sin contacto basada en la norma ISO 14443 Tipo A que funcionan a una frecuencia de 13.56MHz, a una distancia de 10cm. Es de los sistemas más ampliamente instalados en el mundo con 250 millones de tarjetas y 1.5 millones de módulos lectores vendidos. Su capacidad de cómputo no permite realizar operaciones criptográficas o de autenticación de alto nivel, su utilización está enfocada a: monederos electrónicos simples, control de acceso y tarjetas de transporte urbano. (Phillips)

API: significa Interfaz para la Programación de Aplicaciones (*Application Programming Interface*), es una librería o grupo de rutinas provistas por un sistema operativo, aplicación o biblioteca, que implementa cierta funcionalidad mediante una interfaz con la cual el programador puede acceder a dicha funcionalidad. A menudo un API forma parte de un kit de desarrollo de software (*Software Development Kit-SDK*). (Reynoso)

Eclipse: es una comunidad compuesta por organizaciones y personas quienes colaboran en la comercialización de software de código abierto. Creada originalmente por IBM en Noviembre del 2011 y respaldada por un consorcio de vendedores de software, la fundación es creada en Enero del 2004 como una organización sin fines de lucro. Su objetivo es la construcción de una plataforma libre para el desarrollo de aplicaciones basada en herramientas que permitan depurar un software a lo largo de todo su ciclo de vida. (Eclipse Foundation)

IDE: Es un entorno integrado de desarrollo por sus siglas en inglés (*Integrated Development Environment*). Está compuesta generalmente por una interfaz gráfica (GUI, *Graphic User Interface*), la cual está diseñada para facilitar el desarrollo de aplicaciones *software* integrando las herramientas necesarias para su construcción y depuración. Este tipo de programas reduce considerablemente el tiempo de desarrollo, o de aprender un lenguaje de programación nuevo, puesto que incluyen ayudas, tutoriales, correctores de sintaxis y compiladores en su instalación. (Janssen)

Android (*Ice Cream Sandwich*): Es la versión número 4.0 del sistema operativo Android basado en Linux, creado por Google y fue presentada en Octubre del 2011. Algunas de sus mejoras en comparación a sus predecesores fueron: personalización de lanzadores de pantalla, capturas de pantalla integradas por medio del botón *home*, acceso a aplicaciones desde la pantalla bloqueada, software de reconocimiento de rostro, botón derecho para permitir la ejecución de varias aplicaciones, corrector de sintaxis de texto, etc. (Android Inc.)

Apache: es una fundación sin fines de lucro dedicada al desarrollo de *software*, la cual brinda ayuda organizacional, legal y financiera a un grupo de alrededor de 140 proyectos de software de código abierto. Uno de estos es el proyecto “Servidor Http”, el objetivo de este proyecto es proporcionar un servidor seguro, eficiente y extensible que permita alojar los estándares HTTP. Se ha convertido en el servidor de Internet más popular desde 1996, año en el que salió al mercado. (Apache Foundation)

PHP: Es un lenguaje de escritura de propósito general de lado del servidor, utilizado especialmente para el desarrollo web. Este lenguaje fue el primero que se pudo incorporar directamente en un documento HTML. Fue creado por Rasmus Lerdorf en el año de 1995. Su compatibilidad y facilidad de ejecución en muchos sistemas operativos sin ningún costo hizo que sea uno de los lenguajes más utilizados para el desarrollo de sitios web en la actualidad. (PHP Group)

MYSQL: Es hoy en día el software de base de datos de código abierto más popular del mundo, con una cifra de 100 millones de copias descargadas o distribuidas a lo largo de su historia. Entre las ventajas que ofrece están: alta velocidad, confiabilidad, facilidad de uso, mantenimiento y administración. Este software forma parte de

LAMP (Linux, Apache, MYSQL y PHP), una de las empresas de más alto crecimiento en el desarrollo de software de código abierto. (Oracle Corporation)

Wampserver: es una aplicación utilizada en el sistema operativo windows para facilitar el desarrollo de sitios web. Este aplicativo permite emular localmente un servidor web apache, ejecutar páginas desarrolladas en el lenguaje de programación PHP y enriquecerlas mediante la incorporación de bases de datos creadas en MySQL. (WampServer)

JDK: Es un software que brinda un conjunto de herramientas para el desarrollo, depuración y monitoreo de aplicaciones desarrolladas en el lenguaje de programación Java. Este paquete es gratuito e incluye: visor de applets, compilador, intérprete y generador de documentación de clases. (Oracle Corporation)

GNU: Es un sistema operativo que nació en 1983 de la mano de Richard Stallman, el cual tenía por objeto juntar a la gente para trabajar por la liberación de todos los usuarios de software, de modo que puedan controlar sus computadoras. Su éxito se basa en la colaboración de las personas al proyecto, ya sea de manera técnica o no. GNU ha sido impulsado principalmente por la fundación de software libre. Su misión textualmente dice “Preservar, proteger y promover el libre uso, estudio, copia, modificación y redistribución de software de computadora, defendiendo los derechos de los usuarios de software libre”. (Free Software Foundation, Inc)

BIBLIOGRAFÍA

- 123seminaronly. "Near Field Communication." (n.d.). 1 Julio 2013. <<http://123seminaronly.com/Seminar-Reports/023/52532252-NEAR-FIELD-COMMUNICATION.docx>>.
- Aguirre, Loui. *Tecnología 21-NFC vs. Bluetooth: ¿Cuál es mejor?* 15 Diciembre 2011. 1 Octubre 2013. <<http://tecnologia21.com/50804/nfc-vs-bluetooth>>.
- Álvarez Marañón, Gonzalo. *Servicios de Seguridad-Ministerio de Economía y Competitividad*. 2000. 2 Agosto 2013. <<http://www.iec.csic.es/cryptonomicon/seguridad/servicio.html>>.
- Amazon. "Toshiba Satellite U925T-S2120 12.5-Inch Touchscreen Ultrabook (Midnight Brown in Soft Touch Body)." 2013. 1 Agosto 2013. <http://www.amazon.com/Toshiba-Satellite-U925T-S2120-12-5-Inch-Touchscreen/dp/B00AY1FIGG/ref=sr_1_1?ie=UTF8&qid=1377536961&sr=8-1&keywords=Toshiba+Satellite+U925T>.
- Andress, Jason. *The Basics of Information Security*. Elsevier, 2011. 2 Agosto 2013.
- Android Inc. *Android Developers-Host-based Card Emulation*. 2013. 12 Octubre 2013. <<http://developer.android.com/guide/topics/connectivity/nfc/hce.html>>.
- . "Platform Versions-Android." 4 Septiembre 2013. 6 Septiembre 2013. <<http://developer.android.com/about/dashboards/index.html>>.
- Android Inc. "Get the Android SDK-Android Developers." 2013. *Android Developers*. 1 Octubre 2013. <<http://developer.android.com/sdk/index.html>>.
- . *Introducing Android 4.0-Android Inc.* 10 Octubre 2013. <<http://www.android.com/about/ice-cream-sandwich/>>.
- . "NFC Basics." 2013. 20 Agosto 2013. <<http://developer.android.com/guide/topics/connectivity/nfc/nfc.html>>.
- Apache Foundation. *HTTP Server Project-Apache Foundation*. 2013. 12 Octubre 2013. <<http://httpd.apache.org/>>.
-

- Apple Weblog. "NFC y el iPhone, la próxima revolución- Apple Weblog." 1 Agosto 2012. 1 Agosto 2013. <<http://appleweblog.com/2012/08/nfc-y-el-iphone-la-proxima-revolucion>>.
- Arquitectura de la Información-Chile. "Wireframe-Arquitectura de la Información." 2010. *Arquitectura de la Información-Chile*. 30 Octubre 2013. <<http://www.arquitecturadeinformacion.cl/como/wireframe.html>>.
- Bilginer, Bekir and Paul Ljunggren. "Near Field Communication." Febrero 2011. *Department of Measurement Technology and Industrial Electrical*. 20 Noviembre 2013. <http://cwi.unik.no/images/Master_thesis_lu_NFC.pdf>.
- Boden, Rian. "Harvard Medical School develops NFC medication tracking system- NFC World." 4 Abril 2013. 10 Agosto 2013. <<http://www.nfcworld.com/2013/04/04/323325/harvard-medical-school-develops-nfc-medication-tracking-system/>>.
- Bonalde, Gustavo. *Computación Ubicua*. n.d. 14 Julio 2013. <<http://www.slideshare.net/gbonalde/computacion-ubicua>>.
- Brahler, Stefan. "Analysis of the Android Architecture-Karlsruher Institut Technologie." 1 Junio 2010. 20 Agosto 2013. <http://os.ibds.kit.edu/downloads/sa_2010_braehler-stefan_android-architecture.pdf>.
- Bravo, José, Ramón Hervás and Gabriel Chavira. *From Implicit to Touching Interactions: RFID and NFC Approaches*. ICBM, 2008.
- Coskun, Vedat, Kerem Ok and Busra Ozdenizci. *Near Field Communication-From Theory to Practice*. Wiley, 2012. 10 Julio 2013.
- Creately. "Have you confused Wireframes with Mockups?-Creately." 2008. *Creately*. 31 Octubre 2013. <<http://creately.com/diagram-type/article/have-you-confused-wireframes-mockups>>.
- Eclipse Foundation. *About the Eclipse Foundation-Eclipse Foundation*. 2013. 2 Octubre 2013. <<https://www.eclipse.org/org/#about>>.
- ECMA International. *What is Ecma International-ECMA International*. n.d. 3 Julio 2013. <<http://www.ecma-international.org/memento/index.html>>.
-

El Economista.ES-Tecnología. *El responsable de Android, Andy Rubin, ha dejado el puesto.* 13 Marzo 2013. 20 Agosto 2013. <<http://www.economista.es/tecnologia/noticias/4671778/03/13/El-responsable-de-Android-Andy-Rubin-ha-dejado-el-puesto.html>>.

Facultad de Ciencias Agrarias-Universidad Nacional del Litoral. "Modelo Entidad-Relación: Universidad Nacional del Litoral-Argentina." n.d. *Universidad Nacional del Litoral-Argentina.* 21 Octubre 2013. <<http://www.fca.unl.edu.ar/agromatica/Docs/09-ModeloEntRel.PDF>>.

Falke, Oliver, Enrico Rukzio and Ulrich Dietz. "Mobile Services for Near Field Communication." Marzo 2007. 20 Julio 2013. <<http://www.mmi.ifi.lmu.de/pubdb/publications/pub/falke2007mobileServicesTR/falke2007mobileServicesTR.pdf>>.

Falke, Oliver, et al. "Mobile Services for Near Field Communication-Ludwig Maximilians University of Munich." Marzo 2007. *Ludwig Maximilians University of Munich.* <<http://www.mmi.ifi.lmu.de/pubdb/publications/pub/falke2007mobileServicesTR/falke2007mobileServicesTR.pdf>>.

Finkenzeller, Klaus. *RFID Handbook*. Wiley, n.d. 1 Agosto 2013.

Free Software Foundation, Inc. *About the GNU Operating System-Free Software Foundation, Inc.* 2013. 12 Agosto 2013. <<http://www.gnu.org/gnu/about-gnu.html>>.

Google Play. "Búsqueda Aplicaciones para NFC." 2013. 1 Agosto 2013. <<https://play.google.com/store/search?q=nfc&c=apps&hl=es>>.

Haselsteiner, Ernst and Klemens Breitfuß. "Security in Near Field Communication (NFC)." 2012. 25 Agosto 2013. <<http://events.iaik.tugraz.at/rfidsec06/program/papers/002%20-%20security%20in%20nfc.pdf>>.

Infocomm Development Authority of Singapore. "Near Field Communication (NFC) Payment and Mobile Services Initiative-Infocomm Development Authority of Singapore." 9 Julio 2013. 10 Agosto 2013.

<<http://www.ida.gov.sg/Collaboration-and-Initiatives/Initiatives/Store/Near-Field-Communication-NFC-Payment-and-Mobile-Services-Initiative>>.

International, Ecma. *Near Field Communication White Paper-Ecma International*. n.d. 2013 Junio 20. <<http://www.ecma-international.org/activities/Communications/tc32-tg19-2005-012.pdf>>.

ISO/IEC 18092 (ECMA-340). *Information technology - Telecommunications and information exchange between systems - NFC - Interface and Protocol (NFCIP-1)*. Vol. I. 2004.

Jackson, Wallace. *Android Apps for Absolute Beginners*. Apress, 2012. 22 Agosto 2013.

Janssen, Cory. *Integrated Development Environment-Technopedia*. 2013. 10 Octubre 2013. <<http://www.techopedia.com/definition/26860/integrated-development-environment-ide>>.

Kyrnin, Jennifer. "What is a Website Wireframe?" 2013. 31 Octubre 2013. <<http://webdesign.about.com/od/webdesign/qt/website-wireframes.htm>>.

Martin, Robert C. "UML Tutorial: Part 1 - Class Diagrams." 1997. *Object Mentor*. 20 Octubre 2013. <<http://www.objectmentor.com/resources/articles/umlClassDiagrams.pdf>>.

Monferrer Agut, Raúl. "Especificación de Requisitos Software según el estándar de IEEE 830." 2001. 1 Septiembre 2013. <<https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC0QFjAA&url=http%3A%2F%2Fsiml.googlecode.com%2Ffiles%2FFERS.pdf&ei=-IZJUvzBIMvh4AOq94CgBA&usg=AFQjCNFj2Xj8OMaKkue4Qcg5SHI5w4TYUg&bvm=bv.53217764,d.dmg&cad=rja>>.

Mundo NFC. *Diferencia entre NFC y RFID*. 8 Febrero 2012. 16 Julio 2013. <<http://mundonfc.wordpress.com/2012/02/08/diferencia-entre-nfc-y-rfid/>>.

NFC Organization. *Benefits of NFC for Business-NFC Organization*. n.d. 11 Julio 2013. <<http://www.nearfieldcommunication.org/business-benefits.html>>.

- . *Benefits of NFC for Individuals-NFC Organization*. n.d. 10 Julio 2013. <<http://www.nearfieldcommunication.org/benefits.html>>.
- NFC Task Launcher. "NFC Task Launcher." 2013. 1 Agosto 2013. <<http://launcher.tagstand.com/>>.
- Nokia. "Understanding NFC Data Exchange Format (NDEF) messages-Nokia Developer." 2013. 20 Agosto 2013. <[http://developer.nokia.com/Community/Wiki/Understanding_NFC_Data_Exchange_Format_\(NDEF\)_messages](http://developer.nokia.com/Community/Wiki/Understanding_NFC_Data_Exchange_Format_(NDEF)_messages)>.
- Oracle Corporation. *About-MySQL*. 2013. 13 Octubre 2013. <<http://www.mysql.com/about/>>.
- . *Java Downloads-Oracle Corporation*. 2012. 10 Agosto 2013. <<http://www.oracle.com/technetwork/es/java/javase/downloads/index.html>>.
- Oxford, Tasmin . "NFC The Magic Touch." 2012. 1 Agosto 2013. <http://www.gemalto.com/techno/inspired/magic_touch/>.
- Pankaj , Agrawal and Sharad Bhuraria. "Near Field Communication." *SETLabs Briefings* 10.1 (2012): 67-74. 2013 Junio 18. <<http://www.infosys.com/infosys-labs/publications/Documents/winning-it.pdf>>.
- Parrish, Kevin. "Toshiba Satellite U925T is First NFC-Enabled Ultrabook- Tom's Hardware." 14 Septiembre 2012. 1 Agosto 2013. <<http://www.tomshardware.com/news/PayPass-NFC-Satellite-U925T-MasterCard-Ultrabook,17567.html>>.
- Paus, Annika. *Near Field Communication in Cell Phones*. 24 Julio 2007. 15 Octubre 2013. <http://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/near_field_communication_in_cell_phones.pdf>.
- Phillips. "Mifare-Data Sheet." Noviembre 1999. 1 Agosto 2013. <<http://www.itworksolutions.com/brochure/catalogue/RFID/Mifare%20S50.pdf>>.
- PHP Group. *Download-PHP*. 2013. 12 Octubre 2013. <<http://www.php.net/>>.
-

Pintado, Pablo. *Negocios Electrónicos*. Cuenca, 2013.

Point About. "NFC: Near Field Communication. A look into the Future of NFC." 23 Febrero 2011. 25 Julio 2013. <http://www.slideshare.net/pointabout/nfc-near-field-communication-a-look-into-the-near-future-of-nfc?from_search=4>.

Prakash Sharma, Ram. *Near Field Communication NFC is set of Techison*. 14 Enero 2012. 2 Julio 2013. <<http://hellorps.blogspot.com/2012/01/near-field-communication-nfc-is-set-of.html>>.

Rapid NFC. *The Difference Between NFC and RFID - Explained*. 2013 Abril 2013. 15 Julio 2013. <http://rapidnfc.com/blog/72/the_difference_between_nfc_and_rfid_explained>.

RapidNFC. *NFC Enabled Phones And Tablets-RapidNFC*. n.d. 3 Julio 2013. <http://rapidnfc.com/nfc_enabled_phones>.

—. *NFC Tag Antennas-RapidNFC*. n.d. 1 Julio 2013. <http://rapidnfc.com/nfc_tag_antennas>.

Rebello, Jagdish. *Cell Phone Mobile Payment Market Set for Take Off*. n.d. 3 Julio 2013. <<http://www.isuppli.com/mobile-and-wireless-communications/news/pages/cell-phone-mobile-payment-market-set-for-take-off.aspx>>.

Reynoso, Gonzalo Javier. "Qué es y para qué sirve una API?" 12 Octubre 2010. 20 Agosto 2013. <Gonzalo Javier Reynoso>.

RFID Point. "Futuro de NFC va más allá de los pagos - RFID Point." 5 Junio 2013. 1 Agosto 2013. <<http://www.rfidpoint.com/noticias/futuro-de-nfc-va-mas-alla-de-los-pagos/>>.

Rolf, Erik and Viktor Nilsson. "Near Field Communication(NFC) for Mobile Phones: Lund University." Agosto 2006. 1 Agosto 2013. <<http://web.uettaxila.edu.pk/CMS/SP2013/teMCTTms/notes/5%20-%20TEAT-5082.pdf>>.

Romero, Cristian and Stephany Ceron. *Computación Ubicua*. n.d. 10 Julio 2013. <<http://es.scribd.com/doc/56437752/COMPUTACION-UBICUA>>.

- Shalaby, David . "Why the Future of NFC Is In The Enterprise-TapTrack." 10 Julio 2013. *TapTrack*. 20 Julio 2013. <<http://taptrack.com/2013/07/10/blog/>>.
- Smart Card Alliance. "The Mobile Payments and NFC Landscape: A U.S. Persepctive." Septiembre 2011. 1 Agosto 2013. <http://www.smartcardalliance.org/resources/pdf/Mobile_Payments_White_Paper_091611.pdf>.
- Universidad de Málaga. "Manual de Estilo web 2.0." 2013. 31 Octubre 2013. <http://www.uma.es/media/files/GUIA_WEB.pdf>.
- Universidad Politécnica de Valencia. "Manual de Estilos- Centros / Servicios." n.d. <http://www.upv.es/entidades/ASIC/manuales/guia_estilos_upv.pdf>.
- WampServer. "A Windows Developente Environment -WampServer." 2013. 20 Agosto 2013. <<http://www.wampserver.com/en/>>.
- . "WampServer." 2013. *WampServer*. 1 Octubre 2013. <<http://www.wampserver.com/en/>>.
- Wikipedia. "Código de Barras." (n.d.). 22 Julio 2013. <http://es.wikipedia.org/wiki/C%C3%B3digo_de_barras>.
- Wozniaki, Tanya. *Near Field Communication NFC-NFC versus Bluetooth*. 2013. 3 Octubre 2013. <<http://www.nearfieldcommunicationnfc.net/nfc-vs-bluetooth.html>>.

ANEXOS

ANEXO 1



Especificación de Requisitos de Sistema

))NFC))

ERS-MENU VIRTUAL DE UN PATIO DE COMIDAS
JORGE PADILLA-WILBER IÑIGUEZ

Contenido

1. Introducción.....	2
1.1 Propósito.....	2
1.2 Ámbito del Sistema.....	2
1.3 Definiciones, Acrónimos y Abreviaturas.....	3
1.4 Referencias.....	3
2. Descripción General.....	4
2.1 Perspectiva del Producto.....	4
2.2 Funciones del Producto.....	4
2.3 Características de los usuarios.....	4
2.4 Restricciones.....	5
2.5 Suposiciones y Dependencias.....	5
2.6 Requisitos Futuros.....	6
3. Requisitos Específicos.....	6
3.1 Requisitos Funcionales.....	6
3.2 Funciones.....	7
3.3 Requisitos de Rendimiento.....	8
3.4 Restricciones de Diseño.....	8
4 Apéndices.....	8
4.1 Descripción de Casos de Uso.....	8

1. Introducción

El presente documento recopila los requisitos necesarios para el desarrollo de un menú virtual de un patio de comidas.

Esta especificación se ha realizado en concordancia al estándar *IEEE-Recommended Practice for Software Requirements Specification* IEEE Std 830-1998.

1.1 Propósito

Este sistema tiene por objetivo poner a disposición de los clientes de un centro comercial, los diferentes productos que ofrecen los locales presentes en el patio de comidas del mismo. Dichos productos podrán ser vistos desde una aplicación móvil disponible para el Sistema Operativo Android y requerirán el uso del chip NFC de un dispositivo móvil.

1.2 Ámbito del Sistema

El producto llamado food menu debe ser capaz de:

El sistema de super administrador Web contempla lo siguiente:

- Gestión de Restaurantes
- Gestión de Categoría de Comidas

El sistema de super administrador Móvil contempla:

- Grabado de etiquetas NFC para cada restaurante

El sistema de administrador de restaurante incluye:

- Gestión de productos (platos de comida y otros productos alimenticios)

El sistema cliente en el dispositivo móvil contempla:

- Selección de Restaurantes
- Consulta de Menús de Comida

1.3 Definiciones, Acrónimos y Abreviaturas

NFC: Near Field Communication, tecnología inalámbrica de comunicación de corto alcance, que permite el intercambio de datos entre dispositivos.

Android: es un sistema operativo móvil basado en Linux desarrollado por Google.

S.O: acrónimo de Sistema Operativo

B.D: acrónimo de Base de Datos

1.4 Referencias

Especificación de Requisitos según el estándar de IEEE 830-IEEE-22 Octubre de 2008

<http://www.fdi.ucm.es/profesor/gmendez/docs/is0809/ieee830.pdf>

Near Field Communication

<http://www.nearfieldcommunication.org/>

Android

<http://www.android.com/>

2. Descripción General

2.1 Perspectiva del Producto

El presente sistema está pensado y respaldado por un grupo de restaurantes cuyo objetivo común es brindar una forma fácil y cómoda para el usuario al momento de seleccionar su comida. El sistema centraliza todos los productos de los restaurantes y los presenta al cliente, quien a través de la lectura de una etiqueta NFC, podrá observar el menú del restaurante de su preferencia en la pantalla de su teléfono inteligente Android.

2.2 Funciones del Producto

El sistema contempla lo siguiente:

- Gestión de Restaurantes y grabado de sus respectivas etiquetas NFC
- Gestión de Categoría de Comidas
- Gestión de menús (platos de comida y productos alimenticios)
- Selección de Restaurantes
- Consulta de Menús de Comida

2.3 Características de los usuarios

El sistema involucra 3 tipos de usuarios:

Super Usuario: persona encargada de gestionar los restaurantes asociados, proporcionar al administrador de cada local sus datos de identificación y acceso al sistema. Al mismo tiempo será quien provea al administrador del local su etiqueta NFC, para ser ubicada en el lugar de su preferencia. Finalmente es la persona que gestionará las categorías de comidas a usarse en todos los restaurantes.

Administrador de Restaurante: persona con conocimiento total sobre los diferentes productos que su restaurante ofrece, ya que será el encargado de gestionar dichos productos, su información y actualización.

Cliente: persona que desea observar el menú de comida disponible en cualquier local de comida presente en el centro comercial. Dicha persona deberá contar con un teléfono inteligente Android con chip NFC.

2.4 Restricciones

El sistema móvil, tanto el super administrador como el público, serán desarrollados para dispositivos móviles que cuenten con un S.O Android con soporte para NFC, estos dispositivos deberán contar con una conexión a Internet para uso de la aplicación respectiva.

Para el caso del super usuario y administradores de restaurantes su aplicación web estará desarrollada en el lenguaje de programación PHP y con un motor de base de datos Mysql. Lo que incluye que ambos administradores deben contar con acceso a Internet para poder acceder al sistema.

Cada restaurante deberá poseer el número de etiquetas NFC que desee, y posterior a su grabado colocarlas en un lugar accesible para el cliente

2.5 Suposiciones y Dependencias

El sistema está pensado para un grupo de restaurantes afiliados, más no como un producto único para cada restaurante.

El aplicativo Web tendrá las seguridades correspondientes de tal forma que, solo las personas autorizadas puedan ingresar al sistema.

La aplicación móvil pública estará disponible para el acceso al público en general, sin ningún tipo de exclusión. En tanto que la parte móvil privada estará solamente disponible para el super administrador del sistema.

Esta versión de la aplicación en primera instancia no permite realizar pedidos, ni el cobro al cliente, solamente muestra los productos ofrecidos por los locales de comida.

2.6 Requisitos Futuros

- Registro de clientes previo al uso de la aplicación móvil
- Generación de pedidos desde la aplicación móvil
- Cobro de la orden mediante la vinculación de tarjetas de crédito con la aplicación móvil.

3. Requisitos Específicos

3.1 Requisitos Funcionales

El proceso inicia con el registro del restaurante por parte del super administrador, recepción de las categorías de alimentos a vender en el local, continuando con la entrega de los datos de identificación del administrador del restaurante. Entonces se procede a la escritura de la primera etiqueta NFC del local registrado. En caso de requerir más tarjetas NFC, el administrador del restaurante deberá solicitar al super administrador el grabado de las mismas.

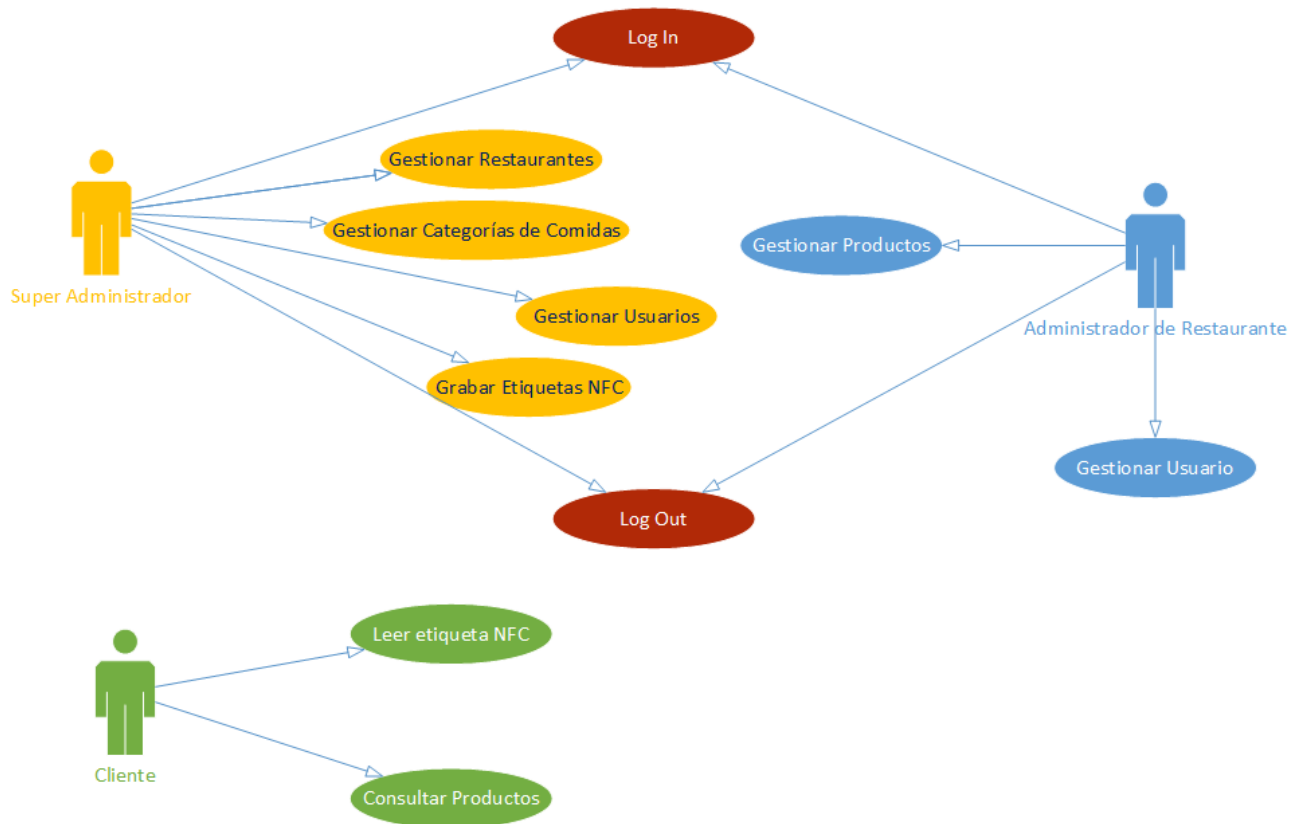
El administrador del restaurante ingresará al sistema y registrara todas las comidas y productos que ofertan.

Las etiquetas NFC son dispositivos de lectura/escritura que cuenta con una pequeña memoria de 1 KB de tipo EEPROM, de los cuales 716 bytes son utilizables, en estas etiquetas se almacenará el

código identificador del restaurante, el mismo que será leído por el teléfono al momento de acercarlo a la etiqueta, entonces se abrirá la aplicación con la información del restaurante seleccionado.

El cliente será capaz de navegar por el menú de comidas y productos de restaurante, pudiendo en cualquier momento leer otra etiqueta, en cuyo caso se abrirá la aplicación con la información del otro restaurante leído.

3.2 Funciones



(Fuente: Autoría Propia)

Casos de Uso del Sistema Menú Virtual de un Patio de Comidas

3.3 Requisitos de Rendimiento

La aplicación móvil pública debe asegurar que la navegación en el menú de comidas sea intuitiva y con rapidez.

El super administrador debe constatar y asegurarse de que el contenido grabado de la etiqueta NFC sea el correcto.

El sistema debe permitir que los cambios realizados por parte de los administradores de los restaurantes, se reflejen inmediatamente en la aplicación móvil pública.

3.4 Restricciones de Diseño

La aplicación destinada al cliente debe poseer una interfaz muy amigable con el usuario, ser muy intuitiva y atractiva, que motive al cliente a adquirir el producto.

El aplicativo web para los administradores de comida debe contemplar la prevención y control de errores al momento de gestionar la información de los productos, para evitar que información incorrecta se presente al cliente en la aplicación móvil pública.

4 Apéndices

4.1 Descripción de Casos de Uso

Caso de uso 1	Login
<i>Actor:</i>	Super administrador, Administrador de Restaurante
<i>Descripción:</i>	Se realiza la verificación de credenciales para acceder al sistema y se inicia una sesión
<i>Prioridad:</i>	Obligatorio
REQUISITOS ASOCIADOS	
R.1.1 El sistema permitirá ingresar los datos del usuario tanto nombre de usuario como contraseña	
R.1.2 El sistema validará los datos ingresados por el usuario contra las tablas almacenadas en la Base de Datos	
R.1.3 El sistema dará ingreso al usuario si el registro fue exitoso, caso contrario mostrara un mensaje de error	

Caso de uso 2	Gestionar Restaurantes
<i>Actor:</i>	Super administrador
<i>Descripción:</i>	Se realiza el ingreso, modificación y consulta de los restaurantes
<i>Prioridad:</i>	Obligatorio
REQUISITOS ASOCIADOS	
R.2.1 El sistema registrarlos datos tanto del local de comida como de las categorías de comida que desean utilizar, en caso de no existir alguna categoría a través del caso de uso respectivo se gestionarán el ingreso de nuevas categorías necesarias.	

Caso de uso 3	Gestionar Categorías de Comidas
<i>Actor:</i>	Super administrador
<i>Descripción:</i>	Se realiza el ingreso, modificación y consulta de las categorías de comida
<i>Prioridad:</i>	Obligatorio
REQUISITOS ASOCIADOS	
R.3.1 Cada administrador de restaurante en caso de considerarlo necesario, puede solicitar al super administrador un ingreso o modificación de un categoría que desee utilizar su restaurante.	
R.3.2 Los cambios realizados en las categorías tendrán influencia en todos los productos registrados en dicha categoría.	

Caso de uso 4	Gestionar Usuarios Administradores de Restaurantes
<i>Actor:</i>	Super administrador
<i>Descripción:</i>	Ingreso y Consulta de Usuarios Administradores de Restaurantes
<i>Prioridad:</i>	Obligatorio
REQUISITOS ASOCIADOS	
R.4.1 Cada restaurante poseerá un administrador el cual será registrado como usuario	
R.4.2 Una vez creado el usuario, el super administrador solo podrá consultar sus datos, a partir de ese momento la gestión de sus campos queda a responsabilidad de cada usuario	

Caso de uso 5	Grabar Etiquetas NFC
<i>Actor:</i>	Super administrador
<i>Descripción:</i>	Escritura de las etiquetas con el código identificador de cada restaurante
<i>Prioridad:</i>	Obligatorio
REQUISITOS ASOCIADOS	
R.5.1 La escritura se realizará por medio de un dispositivo móvil	
R.5.2 Cada restaurante puede grabar el número de etiquetas NFC que considere	

Caso de uso 6	Log Out
<i>Actor:</i>	Super Administrador, Administrador de Restaurante
<i>Descripción:</i>	Cierre de sesión del usuario actual
<i>Prioridad:</i>	Obligatorio
REQUISITOS ASOCIADOS	
R.6.1 El vínculo hacia la opción de Log Out deberá estar presente en todas las páginas del sistema	
R.6.2 Se destruye la sesión en el servidor	

Caso de uso 7	Gestionar Productos
<i>Actor:</i>	Administrador de Restaurante
<i>Descripción:</i>	Se realiza el ingreso, modificación y consulta de los productos
<i>Prioridad:</i>	Obligatorio
REQUISITOS ASOCIADOS	
R.7.1 Los atributos serán validados antes de su ingreso o modificación	
R.7.2 La imagen del producto se copiará de forma física al servidor y en la BD existirá una referencia a su ubicación	

Caso de uso 8	Gestionar Usuario
<i>Actor:</i>	Administrador de Restaurante
<i>Descripción:</i>	Se realiza la consulta y modificación del usuario
<i>Prioridad:</i>	Obligatorio
REQUISITOS ASOCIADOS	
R.8.1 El administrador del restaurante puede consultar su información y modificarla	
R.8.2 El usuario no puede consultar la lista de usuarios del sistema	

Caso de uso 9	Leer etiqueta NFC
<i>Actor:</i>	Cliente
<i>Descripción:</i>	Se acerca el dispositivo móvil con NFC hacia una etiqueta escogida, el dispositivo procede a la lectura correspondiente.
<i>Prioridad:</i>	Obligatorio
REQUISITOS ASOCIADOS	
R.9.1 Es necesario contar con un dispositivo móvil con S.O Android y chip NFC incluido.	
R.9.2 La distancia entre el dispositivo y la etiqueta debe ser de aproximadamente 1 cm.	

Caso de uso 10	Consultar Productos
<i>Actor:</i>	Cliente
<i>Descripción:</i>	Se visualiza el menú del restaurante seleccionado en el dispositivo móvil
<i>Prioridad:</i>	Obligatorio
REQUISITOS ASOCIADOS	
R.10.1 Cliente puede escoger otra etiqueta en cualquier momento para leerla	
R.10.2 La función NFC del dispositivo debe estar encendida	
R 10.3 El dispositivo debe estar conectado a Internet a fin de observar los productos en la aplicación	

ANEXO 2

2014



Manual de Usuario

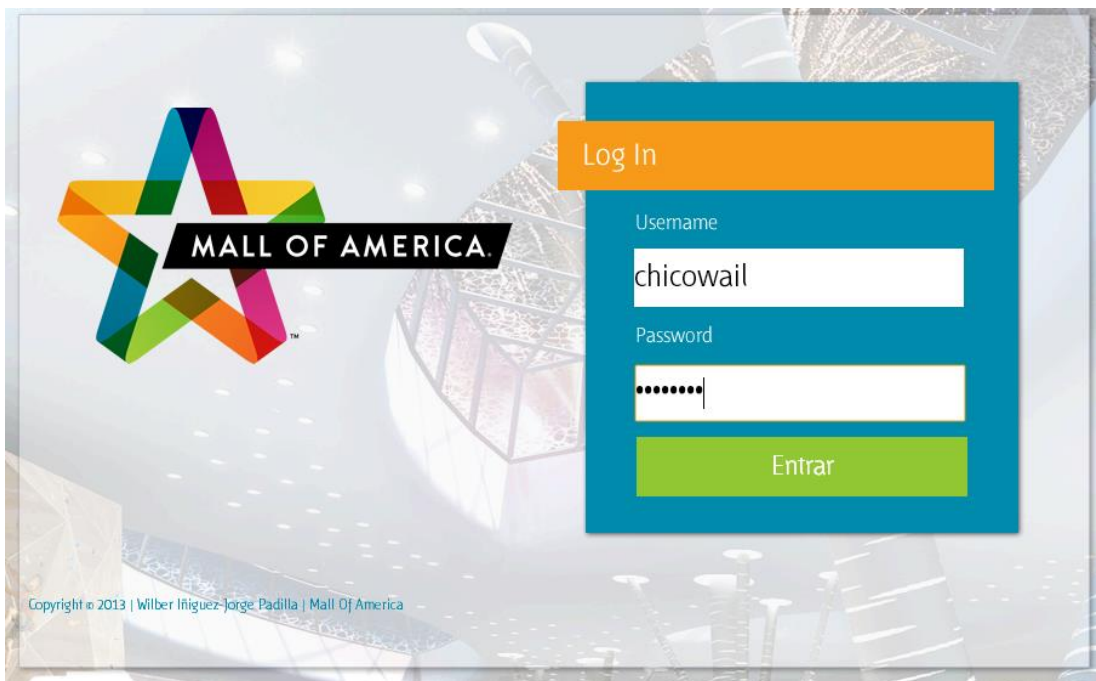
FOOD MENU

JORGE PADILLA-WILBER IÑIGUEZ

Aplicativo Web

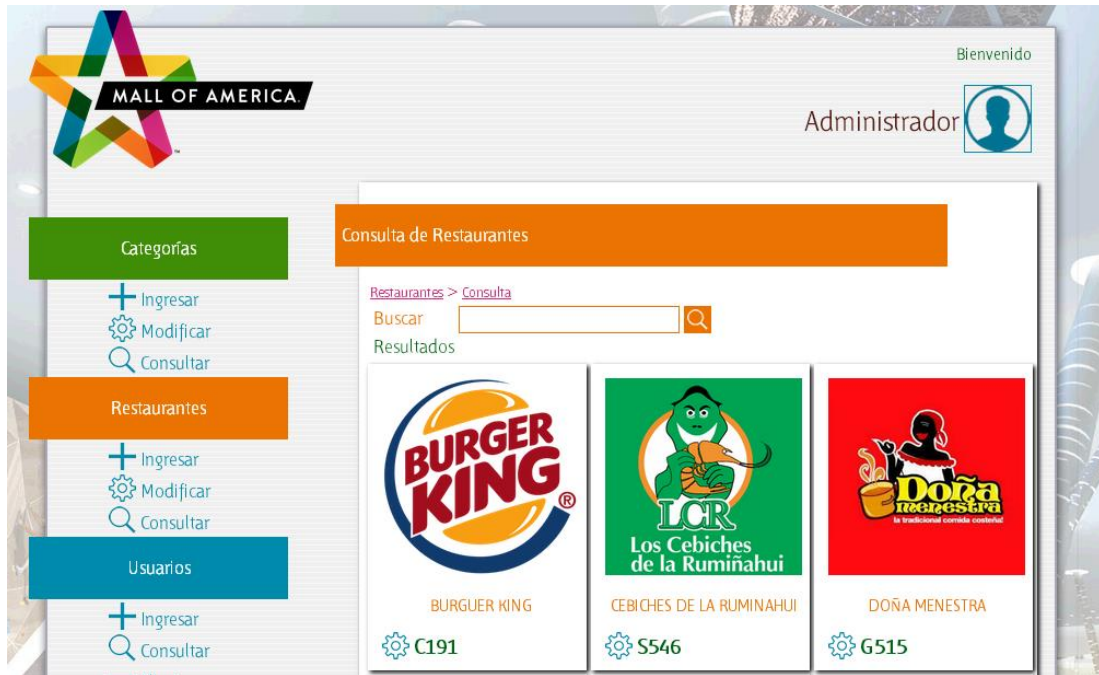
Con el objetivo de probar toda la secuencia de funcionamiento del prototipo, se realizará paso a paso la creación de categorías, restaurantes, usuarios y productos.

El primer paso es identificarse como super administrador en el sistema, puesto que solo los usuarios con dicho privilegio es capaz de gestionar las categorías de comida, restaurantes y usuarios.



(Fuente: Autoría Propia)

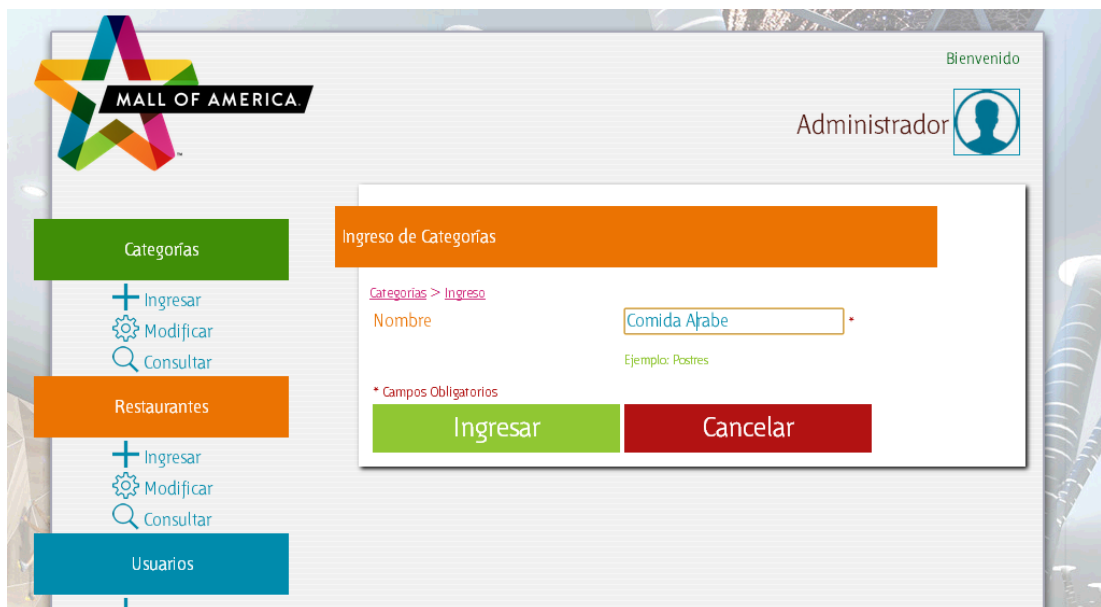
Se presenta la pantalla principal del sistema super administrador



(Fuente: Autoría Propia)

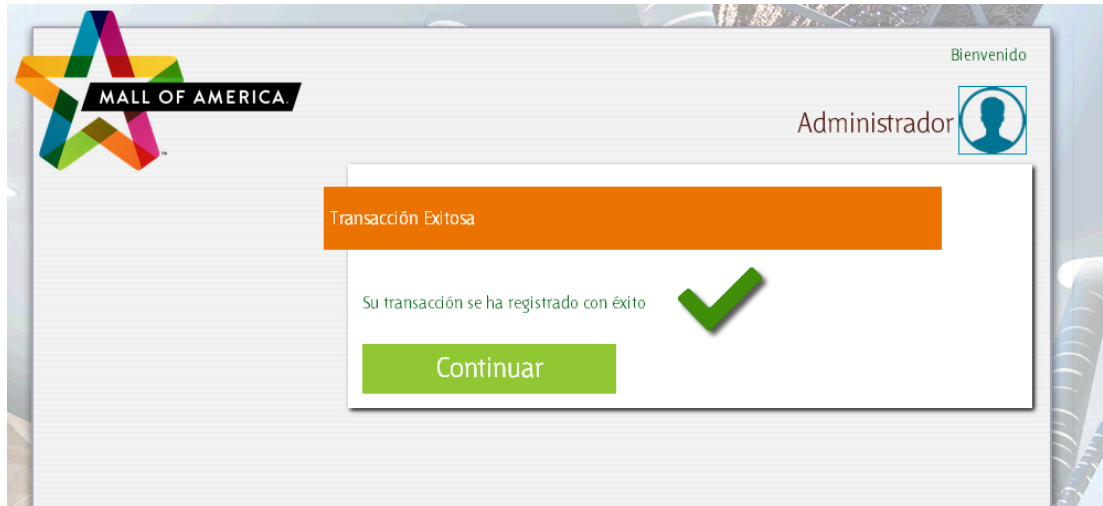
Categorías de Comida

a) Ingreso de Datos de Categoría: Nombre



(Fuente: Autoría Propia)

b) Mensaje de confirmación de ingreso exitoso



(Fuente: Autoría Propia)

c) Verificación en listado de categorías ingresadas



(Fuente: Autoría Propia)

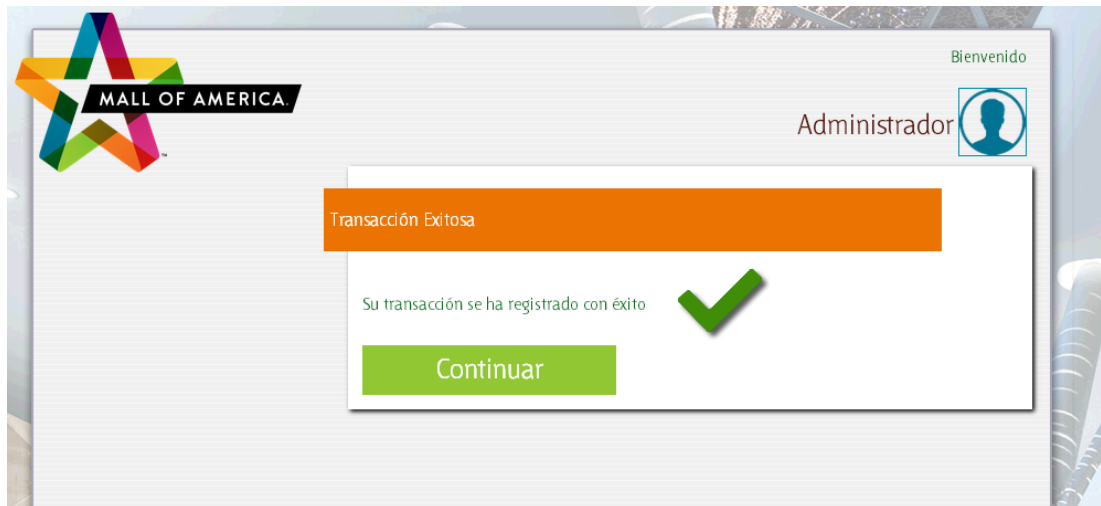
Restaurante

- a) Ingreso de datos del restaurante: nombre, número de local, número de teléfono y el logo del local.

The screenshot shows a web application interface for adding a restaurant. The main content area is titled 'Ingreso de Restaurantes'. It contains several input fields: 'Nombre' (Name) with the value 'Taj Mahal', 'Número de Local' (Local Number) with 'E123', and 'Teléfono' (Phone) with '2854623'. There is also an 'Imagen' (Image) field showing a preview of the 'Taj Mahal Restaurant' logo. A sidebar on the left provides navigation for 'Categorías', 'Restaurantes', and 'Usuarios'. At the bottom, there are 'Ingresar' and 'Cancelar' buttons. A copyright notice for Wilber Iñiguez-Jorge Padilla is visible in the bottom left corner.

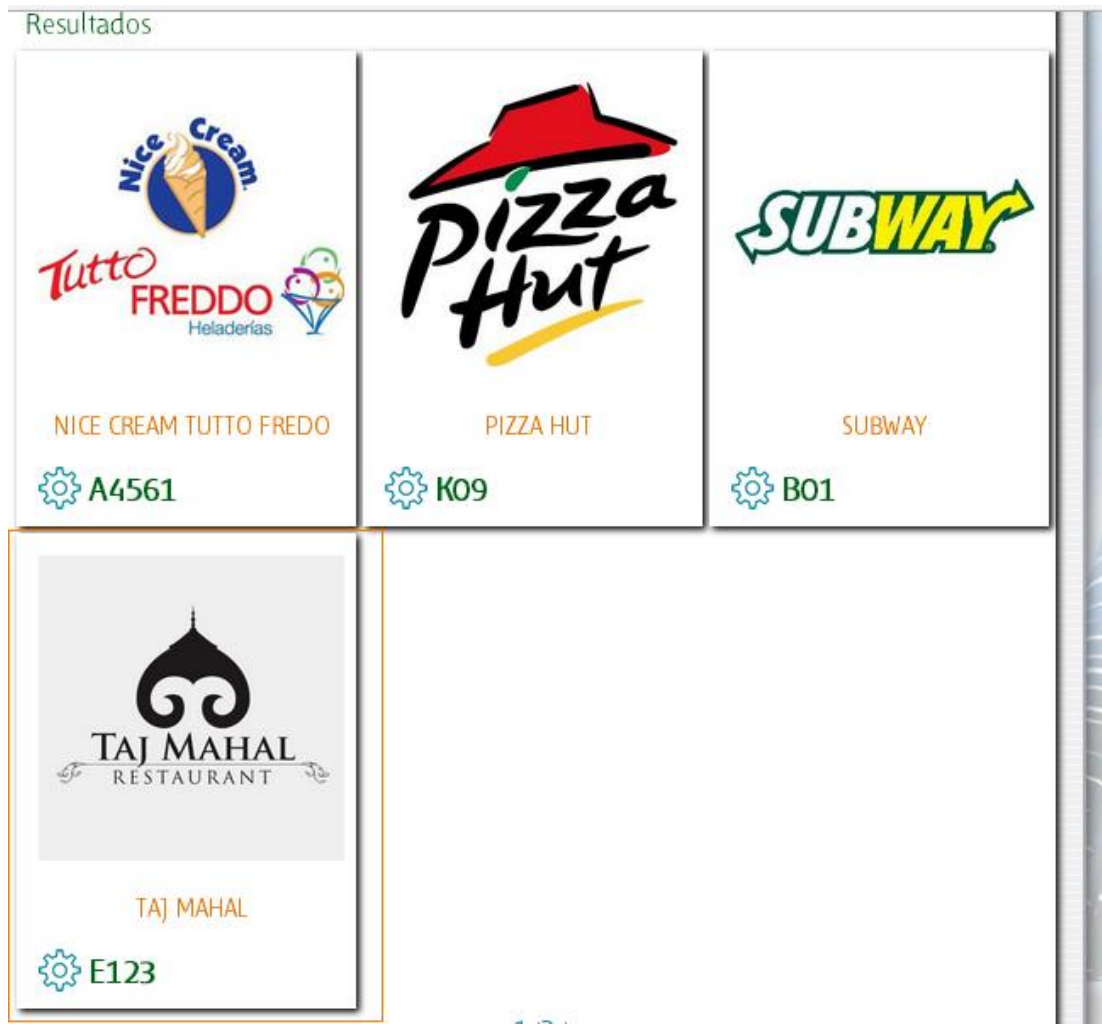
(Fuente: Autoría Propia)

- b) Mensaje de confirmación de ingreso exitoso.



(Fuente: Autoría Propia)

- c) Verificación en listado de restaurantes ingresados.



(Fuente: Autoría Propia)

Usuarios

- a) Ingreso de datos del usuario: restaurante al que pertenece, nombre, apellido, dirección, teléfono, *username*, *password*, y el tipo de usuario (Administrador de Restaurante o Super Administrador).

Ingreso de Usuarios

[Usuarios > Ingreso](#)

Restaurante: TAJ MAHAL

Nombre: Carlos Luis *

Apellido: Ponce *

Dirección: Av. de las Américas 1-123

Teléfono: 0994584523
Ex: 0992747162

Username: tajmahal *
✓ El nombre de usuario ingresado si está disponible

Password: *

Repetir Password: *

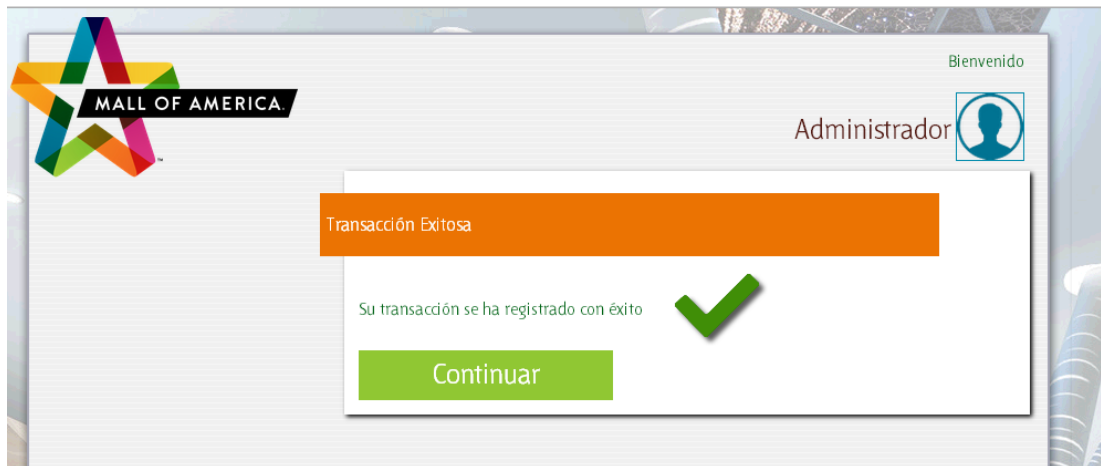
Tipo de Usuario: Administrador de Restaurante

* Campos Obligatorios

Ingresar **Cancelar**

(Fuente: Autoría Propia)

b) Mensaje de confirmación de ingreso exitoso.



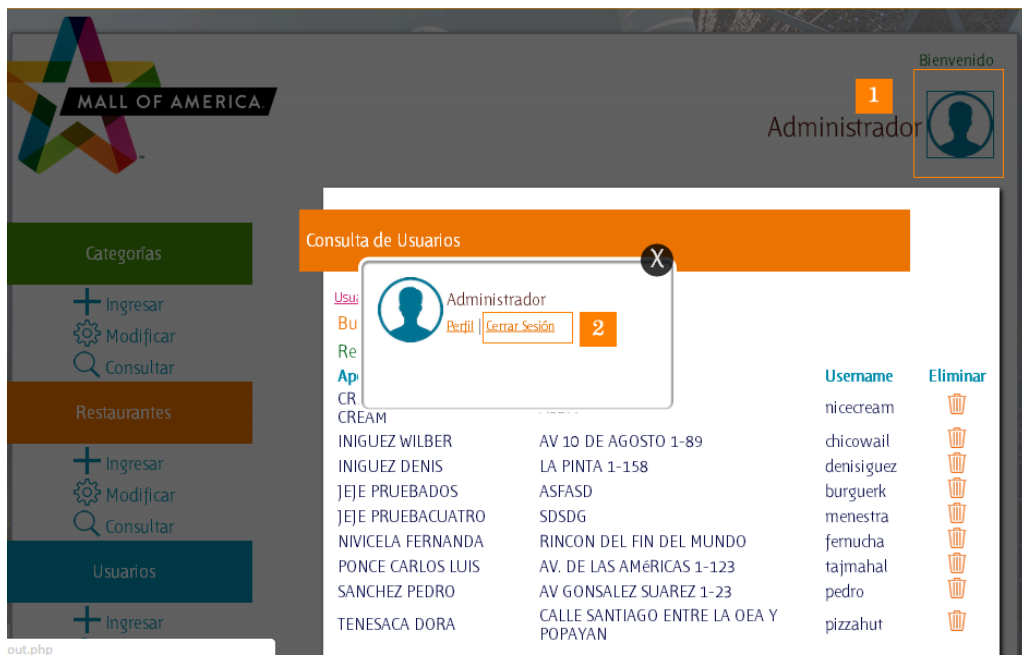
(Fuente: Autoría Propia)

c) Verificación en listado de usuarios ingresados.



(Fuente: Autoría Propia)

d) Cierre de sesión

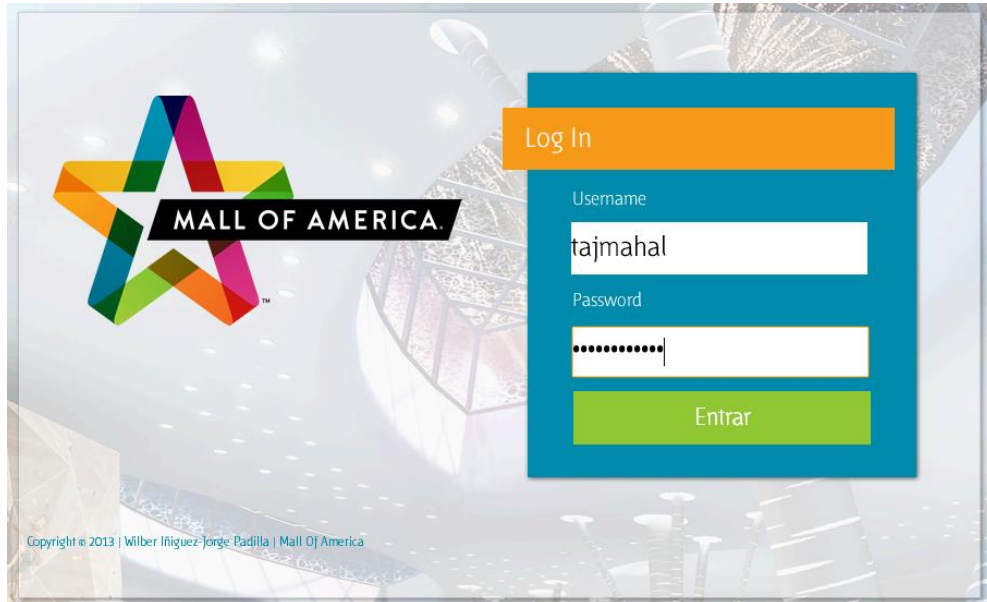


(Fuente: Autoría Propia)

Para poder gestionar los productos, es necesario que un usuario administrador de restaurante inicie sesión.

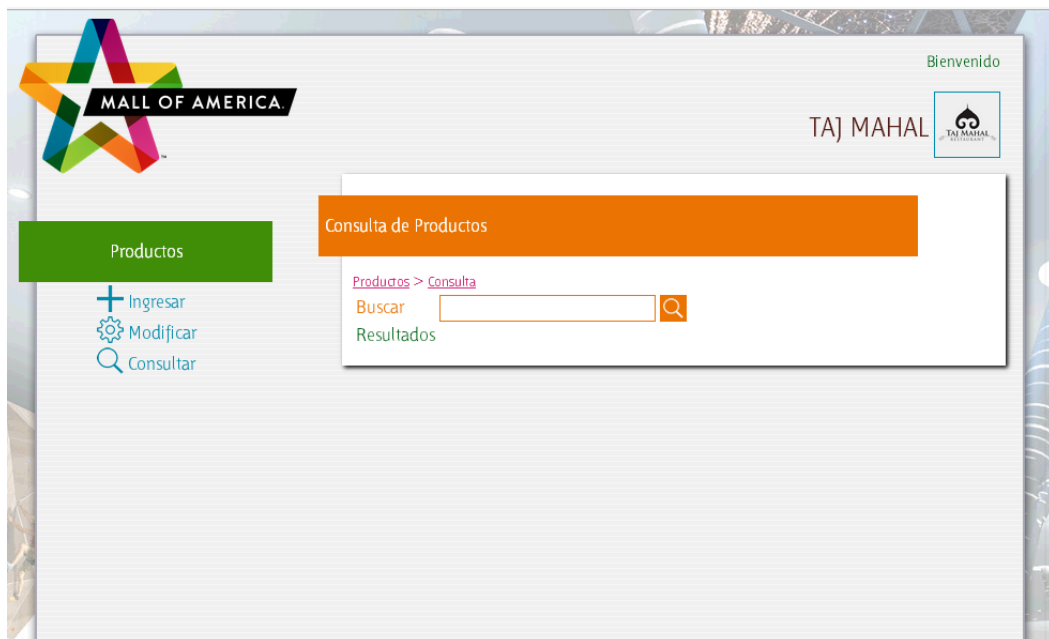
Productos

- a) Inicio de sesión por parte del usuario administrador del restaurante.



(Fuente: Autoría Propia)

- b) Listado de productos ingresados.



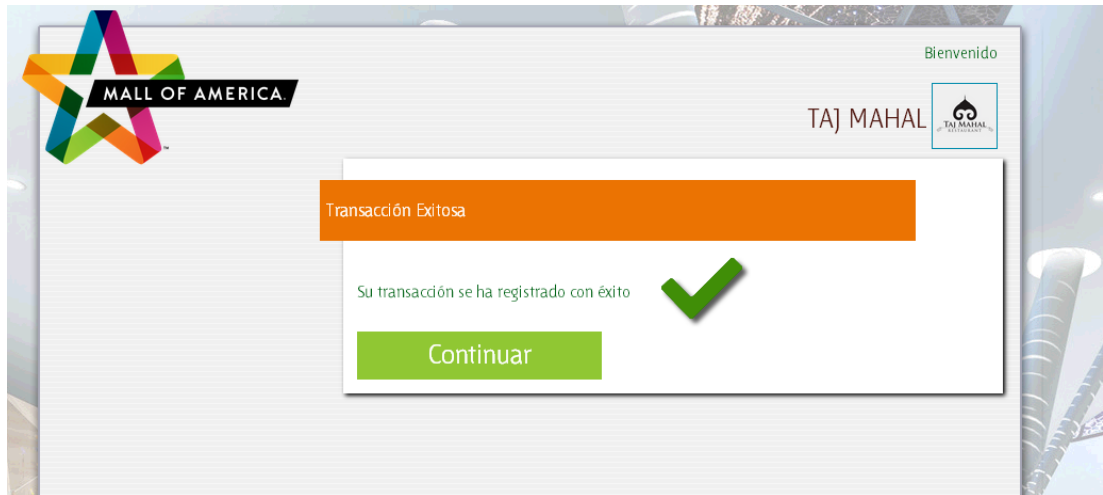
(Fuente: Autoría Propia)

- c) Ingreso de datos del producto: nombre, descripción, imagen, precio y tiempo de preparación.

The screenshot shows a web interface for adding a product. At the top right, the logo for 'TAJ MAHAL' is visible. Below it, a blue header bar contains the text 'Ingreso de Productos'. The main form area has a left sidebar with labels: 'Productos > Ingreso', 'Categoría', 'Nombre', 'Descripción', 'Imagen', 'Precio', and 'Tiempo de Preparación'. The 'Categoría' dropdown is set to 'COMIDA ARABE'. The 'Nombre' field contains 'Shawarma'. The 'Descripción' field contains 'Carne de cordero en finas láminas asadas, lechuga y tomate, envueltos en una tortilla de maíz. Acompañado de salsa de ajo'. The 'Imagen' field shows a file selection button and the filename 'beef-shawarma-sandwich-1.jpg', with a corresponding image of a shawarma sandwich. The 'Precio' field is 'USD \$ 2.35' and the 'Tiempo de Preparación' field is '(min) 8'. At the bottom, there are two buttons: a green 'Ingresar' button and a red 'Cancelar' button. A small note at the bottom left of the form says 'Campos Obligatorios'.

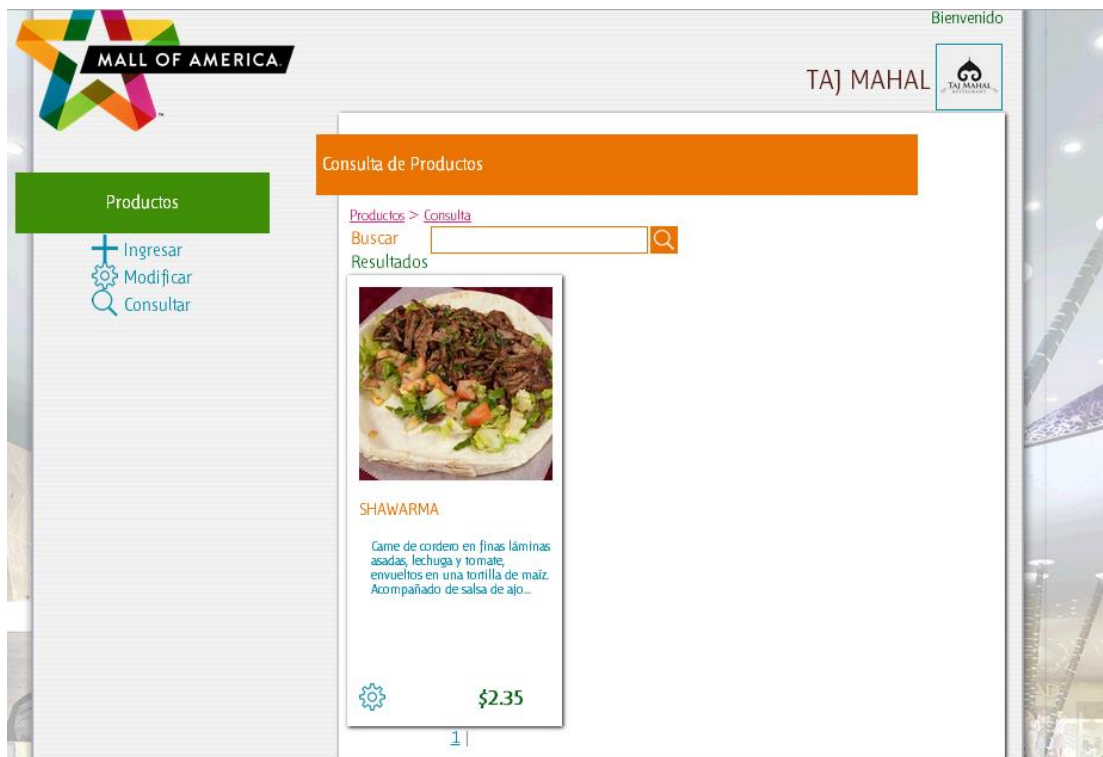
(Fuente: Autoría Propia)

d) Mensaje de confirmación de ingreso exitoso.



(Fuente: Autoría Propia)

e) Verificación en el listado de productos ingresados.



(Fuente: Autoría Propia)

Estas son las acciones que se puede realizar desde el aplicativo web, a continuación se detalla la interacción con la aplicación móvil.

Aplicativo Móvil

Con el objetivo de validar el correcto funcionamiento de las aplicaciones móviles desarrolladas sobre la plataforma Android, se realizará paso a paso la escritura y lectura de etiquetas NFC.

Para iniciar, se debe ejecutar la aplicación llamada NFC Escritura, como ya se indicó anteriormente, esta aplicación es la encargada de consumir dinámicamente la información de locales de comida almacenados en un servidor de base de datos, presentarlos al usuario y grabar la información necesaria en la etiqueta NFC, para que posteriormente pueda ser procesada por la segunda aplicación cliente.



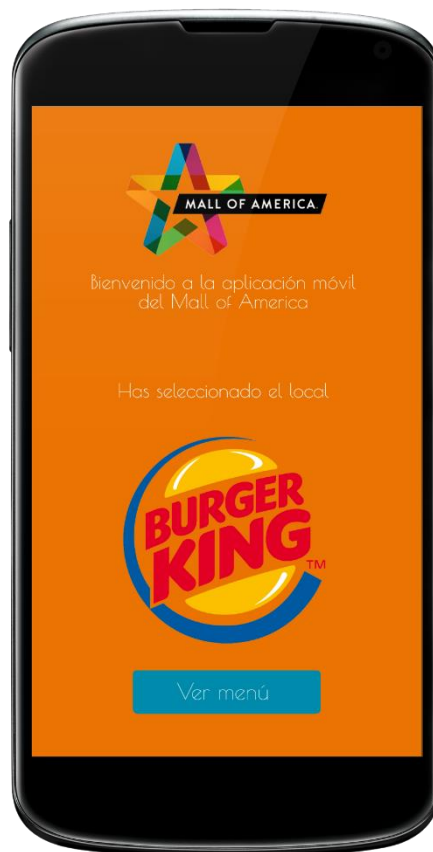
(Fuente: Autoría Propia)

Manual de Usuario-Food Menu

El usuario administrador debe seleccionar un local de comida y presionar el botón de grabar. Aparecerá un mensaje de confirmación en la pantalla y después de aceptarlo, el usuario deberá acercar el dispositivo móvil a una etiqueta NFC válida para finalizar el proceso de escritura.

Como segundo paso, un usuario cliente deberá instalar en su dispositivo habilitado con NFC la aplicación llamada NFC Lectura, que se encargará de leer la etiqueta NFC, recuperar los datos almacenados en la misma y procesarlos de acuerdo a los intereses del prototipo, que en este caso son desplegar automáticamente el menú de comida de cada uno de los locales almacenados en las etiquetas.

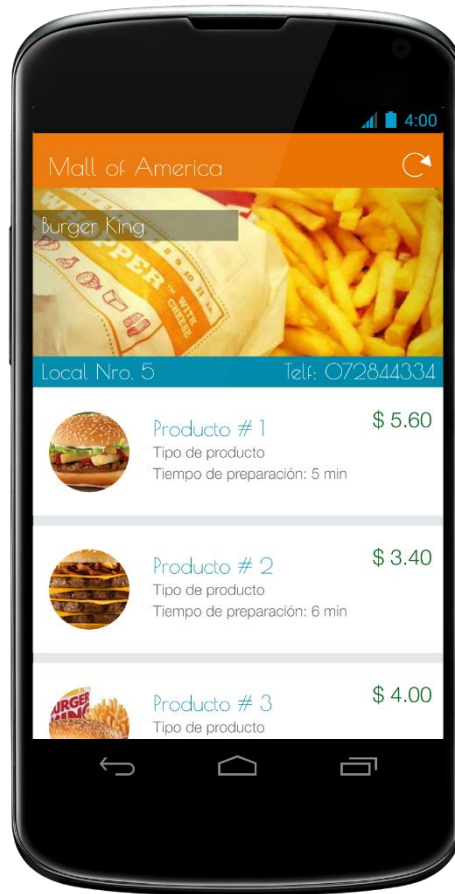
Una vez escaneada la etiqueta NFC, el usuario observará una pantalla de bienvenida con la imagen e información del local almacenado en la etiqueta.



(Fuente: Autoría Propia)

Manual de Usuario-Food Menu

Deberá presionar el botón Ver menú, para acceder directamente al menú de comida de dicho local.



(Fuente: Autoría Propia)

Manual de Usuario-Food Menu

Se visualizará el menú de comida completo, y permitirá al usuario acceder al detalle de cada uno de los ítems.



(Fuente: Autoría Propia)

ANEXO 3



Manual de Estilos

Guía de uso para aplicación Web y Móvil de Patio de Comidas



Contenido

- Introducción 4
- Wireframes..... 4
 - Aplicativo Web..... 4
 - Categorías 4
 - Restaurantes..... 6
 - Productos 8
 - Usuarios 10
 - Aplicación Móvil 12
 - Apartado Público 12
 - Apartado Privado..... 15
- Mockups..... 15
 - Aplicativo Web..... 16
 - Categorías 16
 - Restaurantes..... 18
 - Productos 20
 - Usuarios 22
 - Aplicación Móvil 24
 - Apartado Público 24
 - Apartado Privado..... 27
- Color 28
- Cabecera 29
 - Uso de cabeceras 29
 - Uso de pie de páginas..... 30
- Fotos y Logos 30
- Íconos..... 30
- Títulos y Textos 31
 - Títulos de Página 31



Títulos de Sección de página31

Títulos de Sección lateral.....31

Texto de enlaces de sección lateral32

Texto de ubicación actual.....33

Formularios33

 Etiquetas de Formularios.....33

 Campos de Textos33

 Textos de Ayuda.....34

 Listas Desplegables.....34

 Botones de Ingreso y Cancelar35

Listados.....36

 Búsqueda de Restaurantes36

 Búsquedas de Productos37

 Búsquedas de Categorías y Usuarios38

Pantalla de Inicio de Sesión39

Introducción

El presente documento está diseñado para brindar todos los parámetros de desarrollo, diseño y presentación para la aplicación FoodMenu. Aquí se detalla a profundidad los colores, tipografía y tamaño de los distintos elementos de las páginas del sitio web y la aplicación móvil, además muestra de manera gráfica ejemplos de las distintas secciones del aplicativo para mejorar la comprensión.

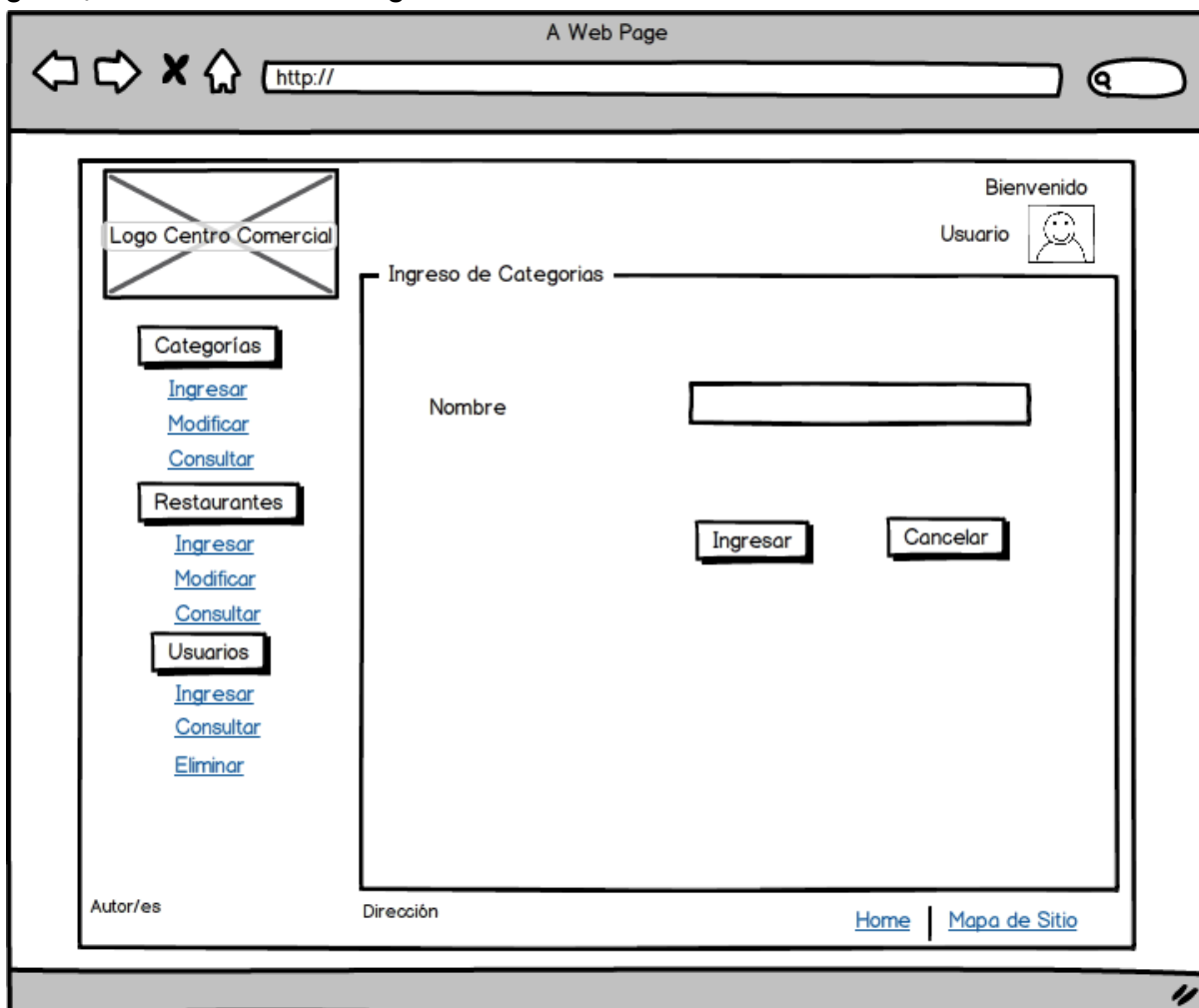
Wireframes

Esta sección está destinada a mostrar la estructura tanto de las páginas web como de las pantallas del aplicativo móvil. En este apartado solo se especifica la composición, omitiendo por el momento el diseño estético.

Aplicativo Web

Categorías

Ingreso / Modificación de Categorías



A Web Page

http://

Logo Centro Comercial

Bienvenido Usuario

Ingreso de Categorías

Nombre

Ingresar Cancelar

Categorías

[Ingresar](#)

[Modificar](#)

[Consultar](#)

Restaurantes

[Ingresar](#)

[Modificar](#)

[Consultar](#)

Usuarios

[Ingresar](#)

[Consultar](#)

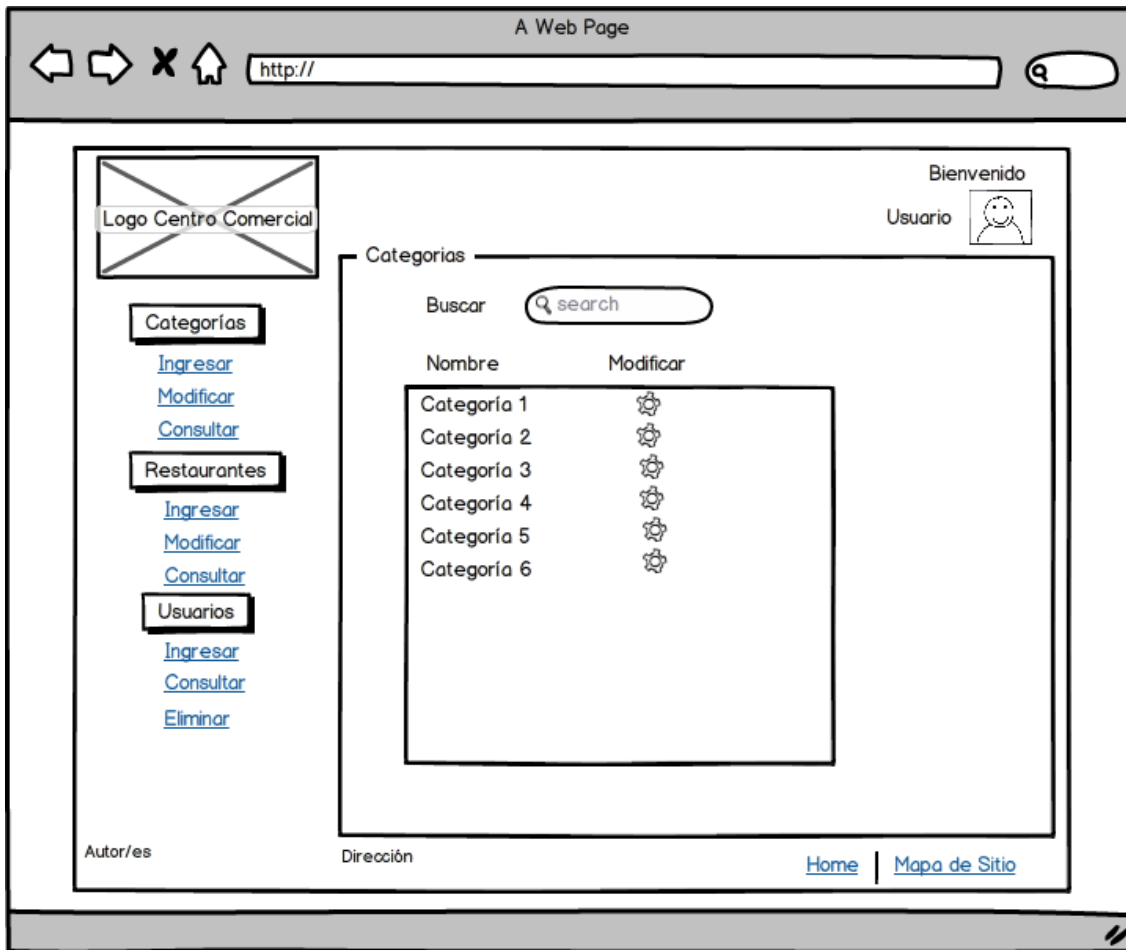
[Eliminar](#)

Autor/es Dirección

[Home](#) | [Mapa de Sitio](#)

(Fuente: Autoría Propia)

Consulta de Categorías



(Fuente: Autoría Propia)

Restaurantes

Ingreso / Modificación de Restaurantes

A Web Page

http://

Logo Centro Comercial

Bienvenido
Usuario

Ingreso de Restaurantes

Nombre

Número de Local

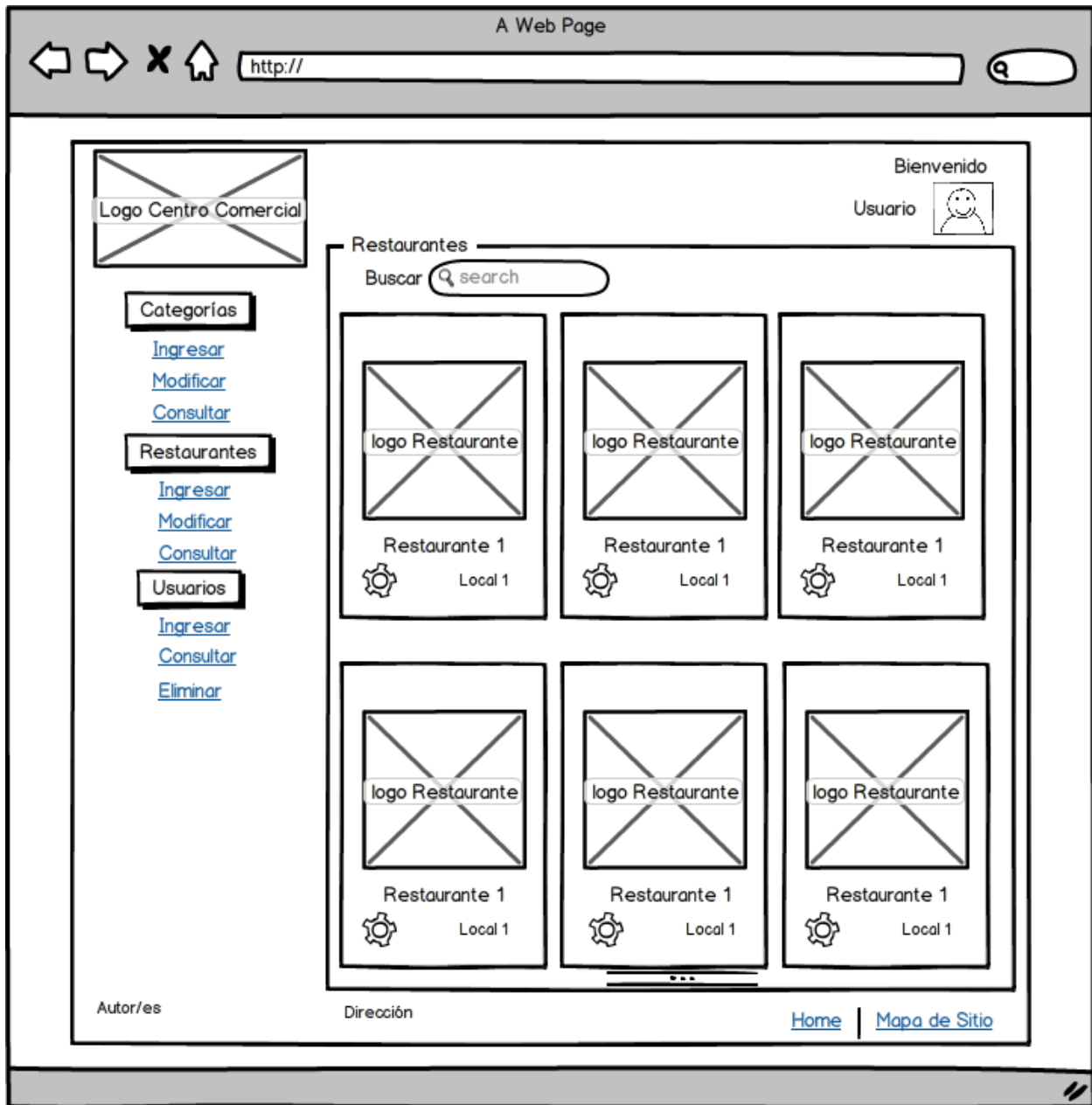
Teléfono

Logo de Restaurante

Autor/es Dirección [Home](#) | [Mapa de Sitio](#)

(Fuente: Autoría Propia)

Consulta de Restaurantes



(Fuente: Autoría Propia)

Productos

Ingreso / Modificación de Productos

A Web Page

http://

Logo Centro Comercial

Bienvenido Usuario

Categorías
[Ingresar](#)
[Modificar](#)
[Consultar](#)

Restaurantes
[Ingresar](#)
[Modificar](#)
[Consultar](#)

Usuarios
[Ingresar](#)
[Consultar](#)
[Eliminar](#)

Ingreso de Productos

Categoría

Nombre

Descripción

Imagen

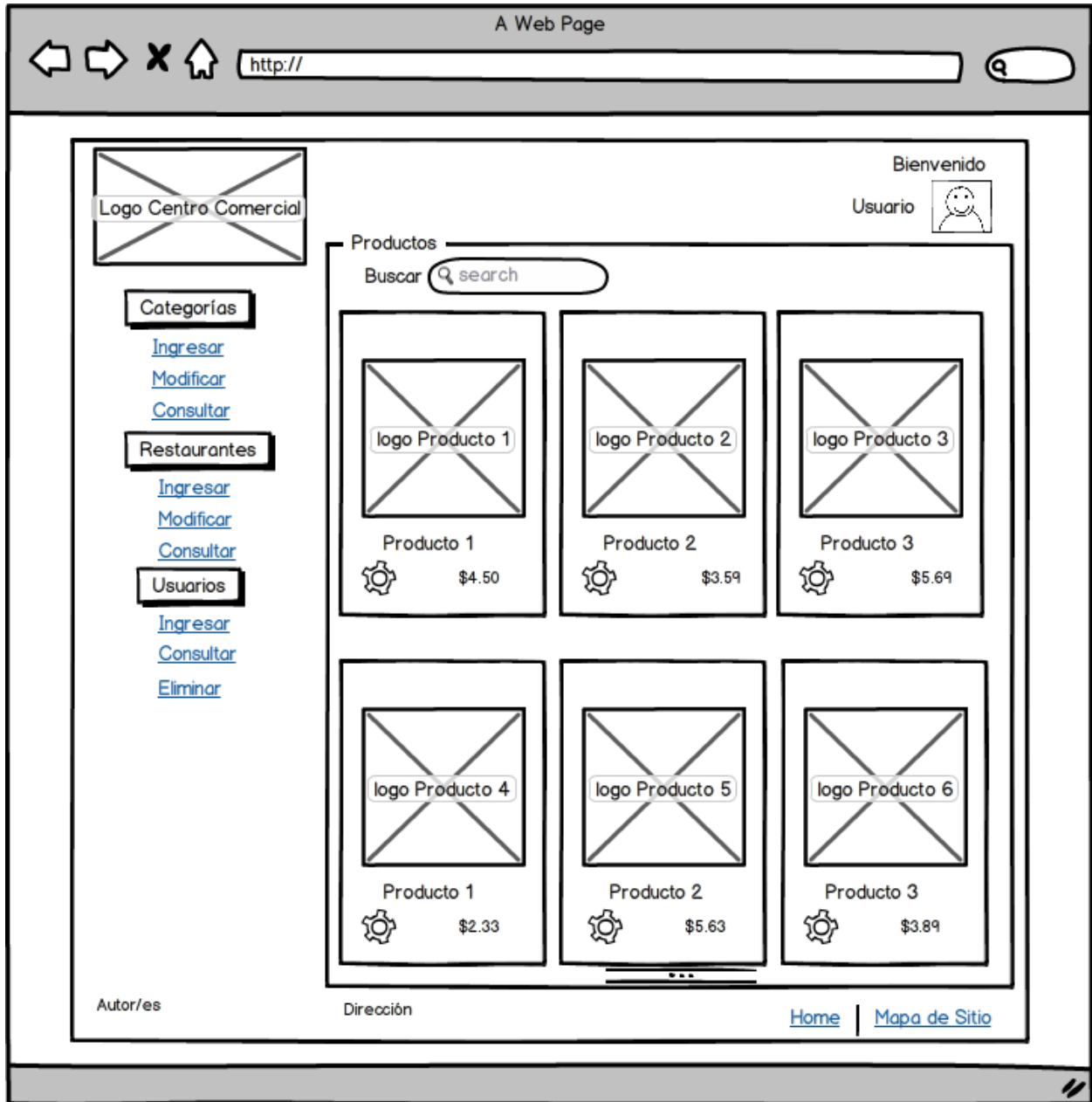
Precio

Tiempo Preparacion

Autor/es Dirección [Home](#) | [Mapa de Sitio](#)

(Fuente: Autoría Propia)

Consulta de Productos



(Fuente: Autoría Propia)

Usuarios

Ingreso / Modificación de Usuarios

A Web Page

http://

Logo Centro Comercial

Bienvenido Usuario

Ingreso de Usuarios

Restaurante

Nombre

Apellido

Dirección

Teléfono

Username

Password

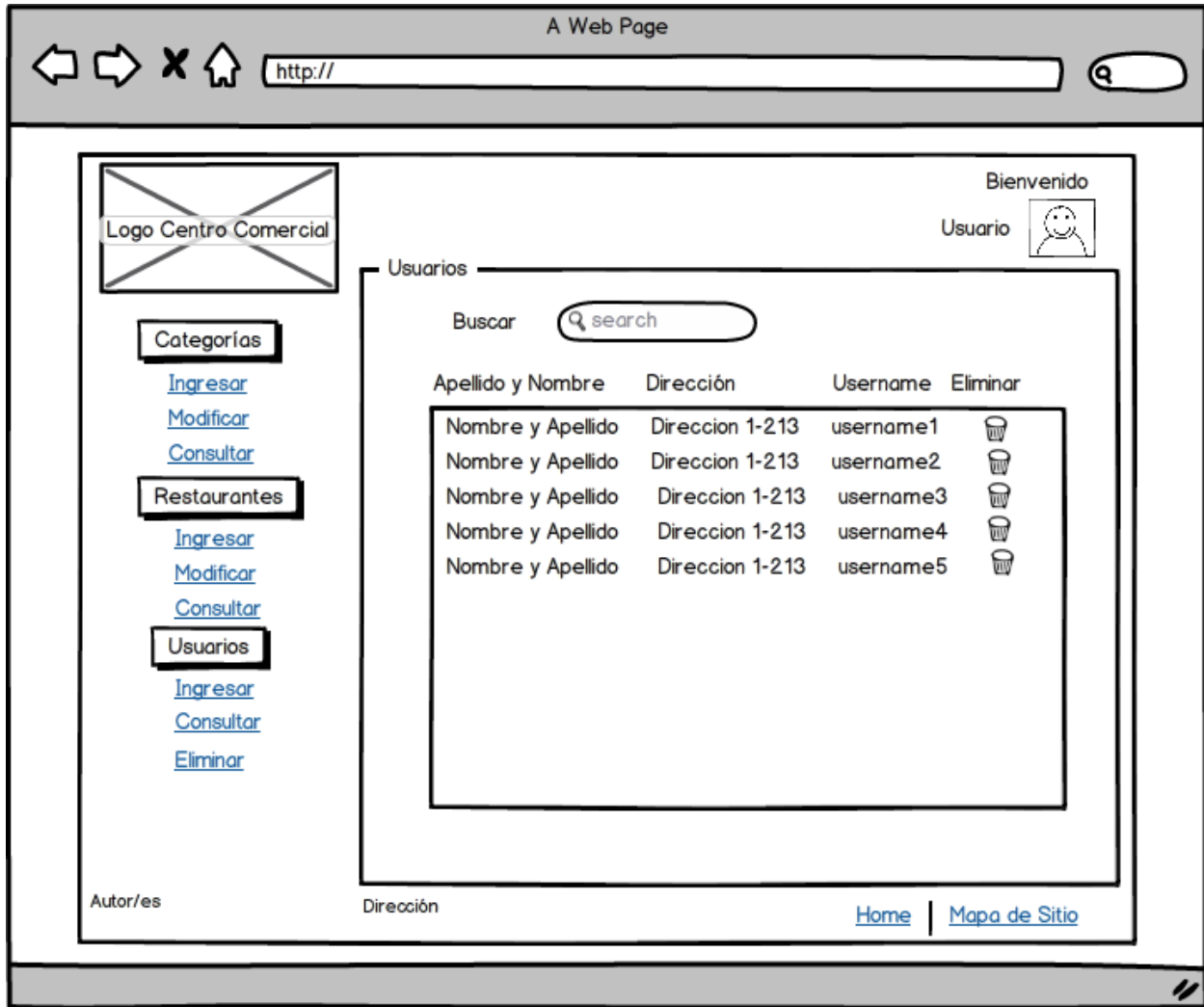
Repetir Password

Tipo de Usuario

Autor/es Dirección [Home](#) | [Mapa de Sitio](#)

(Fuente: Autoría Propia)

Consulta de Productos



(Fuente: Autoría Propia)

Aplicación Móvil
Apartado Público

Selección de Restaurante



(Fuente: Autoría Propia)

Consulta de Productos



(Fuente: Autoría Propia)

Detalle de Producto



(Fuente: Autoría Propia)

Apartado Privado

Grabación de Etiqueta



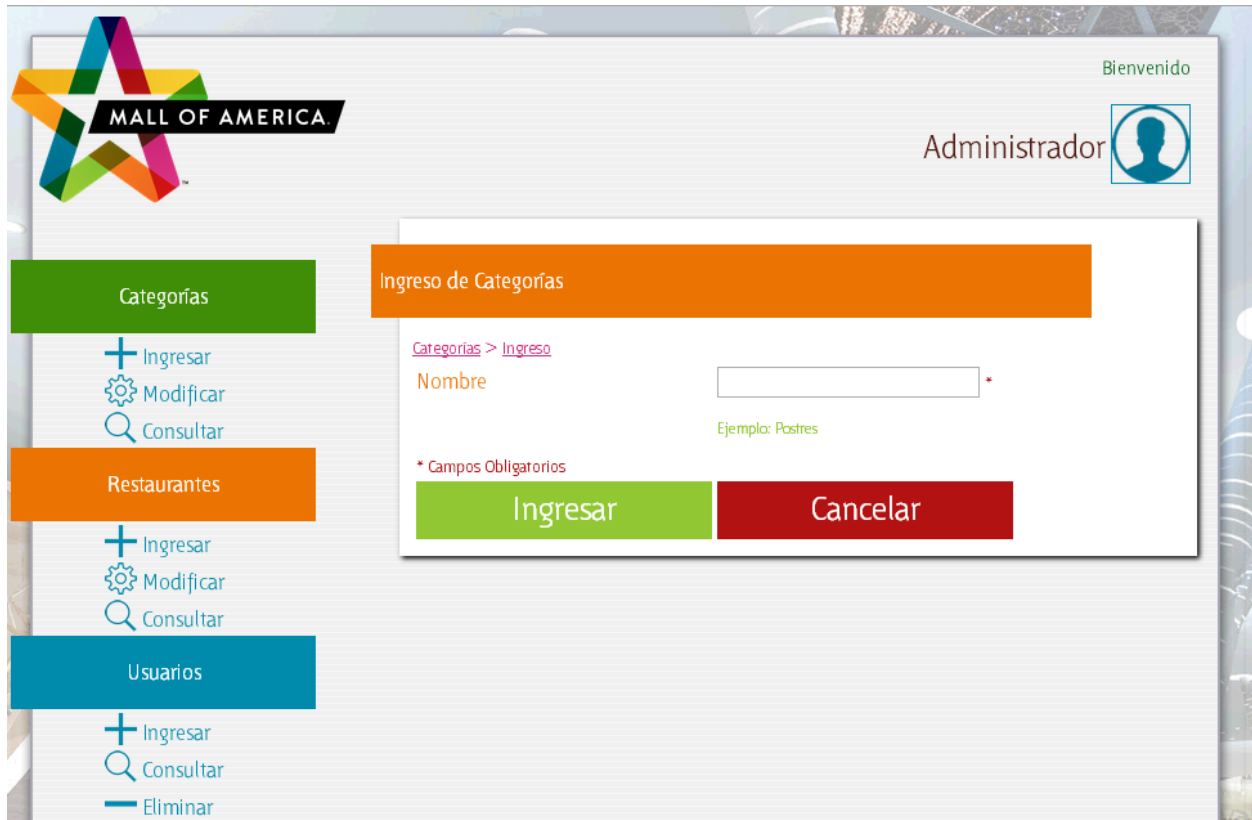
(Fuente: Autoría Propia)

Mockups

Luego de haber especificado la estructura, es momento de agregar y definir el diseño para cada parte tanto del aplicativo web como del móvil.

Aplicativo Web
Categorías

Ingreso/Modificación de Categorías



(Fuente: Autoría Propia)

Consulta de Categorías

BIENVENIDO

MALL OF AMERICA

Administrador

Categorías

- + Ingresar
- ⚙ Modificar
- 🔍 Consultar

Restaurantes

- + Ingresar
- ⚙ Modificar
- 🔍 Consultar

Usuarios

- + Ingresar
- 🔍 Consultar
- Eliminar

Consulta de Categorías

[Categorías](#) > [Consulta](#)

Buscar 🔍

Resultados

Categoría	Modificar
ALITAS Y COSTILLAS BBQ	⚙
BEBIDAS	⚙
COMIDA CHINA	⚙
ENSALADAS	⚙
HAMBURGUESAS	⚙
HELADOS	⚙
MARISCOS	⚙
MENESTRAS	⚙
PAPAS	⚙
PARRILLADAS	⚙

(Fuente: Autoría Propia)

Restaurantes

Ingreso / Modificación de Restaurantes

Bienvenido

Administrador

Ingreso de Restaurantes

[Restaurantes](#) > [Ingreso](#)

Nombre *

Ejemplo: Postres

Número de Local *

Ejemplo: A539

Teléfono

Ejemplo: 072803543

Imagen No se ha seleccionado ningún archivo

* Campos Obligatorios

Categorías

- + Ingresar
- ⚙ Modificar
- 🔍 Consultar

Restaurantes

- + Ingresar
- ⚙ Modificar
- 🔍 Consultar

Usuarios

- + Ingresar
- 🔍 Consultar
- Eliminar

(Fuente: Autoría Propia)

Consulta de Restaurantes

MALL OF AMERICA

Bienvenido

Administrador

Consulta de Restaurantes

Restaurantes > Consulta

Buscar

Resultados

 BURGUER KING C191	 CEBICHES DE LA RUMINAHUI S546	 DOÑA MENESTRA G515
 KENTUCKY FRIED CHICKEN A11	 MC DONALD'S C19	 MENESTRAS DEL NEGRO K215

1 | 2 |

Copyright © 2013
Wilber Iñiguez-Jorge Padilla
Mall of America

Dirección: 13416 Washington 527 Mill Creek, WA 98012, USA | Teléfono: 877-247-5223

[Home](#) | [Mapa del Sitio](#)

(Fuente: Autoría Propia)

Productos

Ingreso / Modificación de Productos

Bienvenido

MALL OF AMERICA

PIZZA HUT

Productos

- + Ingresar
- ⚙ Modificar
- 🔍 Consultar

Ingreso de Productos

Productos > Ingreso

Categoría: ALITAS Y COSTILLAS BBQ

Nombre:

Descripción:

Imagen: No se ha seleccionado ningún archivo



Precio: USD \$

Tiempo de Preparación: (min)

* Campos Obligatorios

(Fuente: Autoría Propia)

Consulta de Productos


Bienvenido


Consulta de Productos







Productos

- Ingresar
- Modificar
- Consultar

Productos > Consulta

Buscar

Resultados

 <p style="font-weight: bold; color: #990000;">CINNAMON STICKS</p> <p style="font-size: x-small;">Diez irresistibles panecitos de canela homeados, bañados en suaves capas de icing ...</p> <div style="display: flex; justify-content: space-between; align-items: center;"> \$4.55 </div>	 <p style="font-weight: bold; color: #990000;">HAWAYAN LOVER'S</p> <p style="font-size: x-small;">Queso mozzarella, doble jamón y doble piña ...</p> <div style="display: flex; justify-content: space-between; align-items: center;"> \$10.5 </div>	 <p style="font-weight: bold; color: #990000;">MEAT LOVER'S</p> <p style="font-size: x-small;">¡Para los amantes de la carne! Queso mozzarella, pepperoni americano, jamón, tocino, topping pork, y salchicha italiana...</p> <div style="display: flex; justify-content: space-between; align-items: center;"> \$12.33 </div>
 <p style="font-weight: bold; color: #990000;">PEPPERONI LOVER'S</p> <p style="font-size: x-small;">Extra queso mozzarella y doble pepperoni americano...</p> <div style="display: flex; justify-content: space-between; align-items: center;"> \$18.99 </div>	 <p style="font-weight: bold; color: #990000;">PRUEBA</p> <p style="font-size: x-small;">Q MAS LOCO...</p> <div style="display: flex; justify-content: space-between; align-items: center;"> \$5.89 </div>	 <p style="font-weight: bold; color: #990000;">SUPER SUPREME PIZZA</p> <p style="font-size: x-small;">Super Supreme Pizza is prepared with a blend of pepperoni, smoked chicken, cabanossi, beef, minced onions, green peppers, olives and mushrooms with a ...</p> <div style="display: flex; justify-content: space-between; align-items: center;"> \$18.96 </div>

1 |

Copyright © 2013
Wilber Iñiguez-Jorge Padilla
Mall of America

Dirección: 13416 Washington 527 Mill Creek, WA 98012, USA | Teléfono: 877-247-5223

[Home](#) | [Mapa del Sitio](#)

(Fuente: Autoría Propia)

Usuarios

Ingreso / Modificación de Usuarios

The screenshot shows a web application interface for user management. On the left is a sidebar with navigation menus for 'Categorías', 'Restaurantes', and 'Usuarios'. The main content area is titled 'Ingreso de Usuarios' and contains a form with the following fields:

- Restaurante:** A dropdown menu with 'BURGUER KING' selected.
- Nombre:** A text input field with a red asterisk indicating it is required.
- Apellido:** A text input field with a red asterisk indicating it is required.
- Dirección:** A large text area for address input.
- Teléfono:** A text input field with an example 'Ex: 0992747162' below it.
- Username:** A text input field with a red asterisk indicating it is required.
- Password:** A text input field with a red asterisk indicating it is required.
- Repetir Password:** A text input field with a red asterisk indicating it is required.
- Tipo de Usuario:** A dropdown menu with 'Administrador de Restaurante' selected.

At the bottom of the form are two buttons: 'Ingresar' (green) and 'Cancelar' (red). A note at the bottom left of the form states '* Campos Obligatorios'. The footer of the page includes copyright information for 2013, contact details for Wilber Iñiguez-Jorge Padilla, and links for 'Home' and 'Mapa del Sitio'.

(Fuente: Autoría Propia)

Consulta de Usuarios

Bienvenido

Administrador

Categorías

- Ingresar
- Modificar
- Consultar

Restaurantes

- Ingresar
- Modificar
- Consultar

Usuarios

- Ingresar
- Consultar
- Eliminar

Consulta de Usuarios

Usuarios > Consulta

Buscar

Resultados

Apellido y Nombre	Dirección	Username	Eliminar
CREAM PRUEBA NICE CREAM	ASDA	nicecream	
INIGUEZ WILBER	AV 10 DE AGOSTO 1-89	chicowail	
INIGUEZ DENIS	LA PINTA 1-158	denisiguez	
JEJE PRUEBADOS	ASFASD	burguerk	
JEJE PRUEBACUATRO	SDSDG	menestra	
NIVICELA FERNANDA	RINCON DEL FIN DEL MUNDO	fernucha	
SANCHEZ PEDRO	AV GONSALEZ SUAREZ 1-23	pedro	
TENESACA DORA	CALLE SANTIAGO ENTRE LA OEA Y POPAYAN	doritamemos	

(Fuente: Autoría Propia)

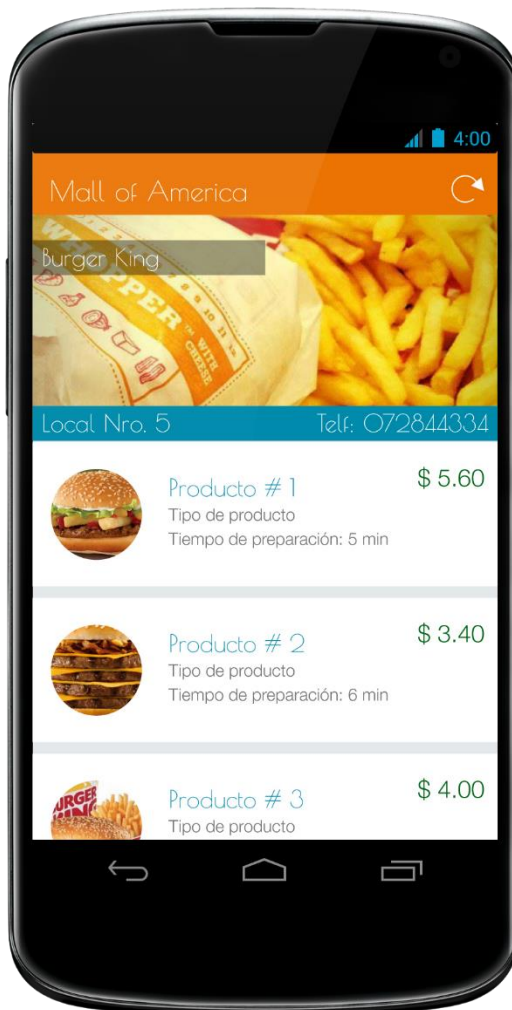
Aplicación Móvil
Apartado Público

Selección de Restaurante



(Fuente: Autoría Propia)

Consulta de Productos



(Fuente: Autoría Propia)

Detalle de Producto



(Fuente: Autoría Propia)

Apartado Privado

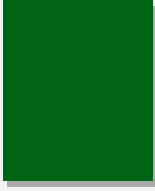
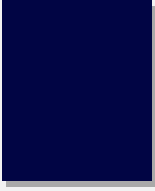

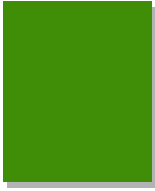
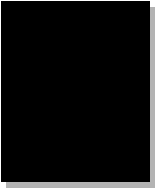



Grabación de Etiqueta



(Fuente: Autoría Propia)

Color

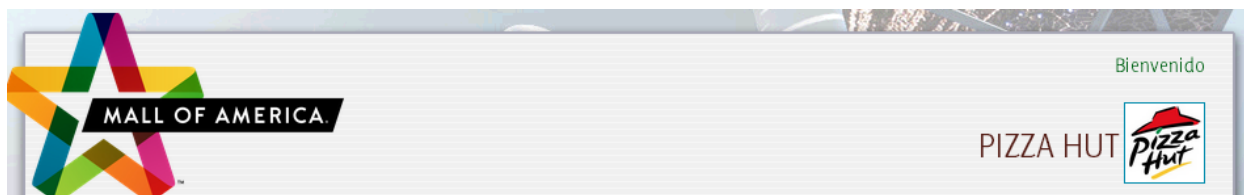
Los colores utilizados en las aplicaciones son

	Azul #008BAC R: 0 G: 139 B: 172		Naranja #EB7302 R: 235 G: 115 B: 2		Amarillo #F0B118 R: 240 G: 117 B: 24
	Verde #016316 R: 1 G: 99 B: 22		Azul Marino #010544 R: 1 G: 5 B: 68		Púrpura #D12B7C R: 171 G: 13 B: 100
	Rojo #B21212 R: 178 G: 18 B: 18		Verde Claro #408E07 R: 64 G: 142 B: 7		Negro #000000 R: 0 G: 0 B: 0
	Café #531c15 R: 81 G: 28 B: 21		Blanco #FFFFFF R: 81 G: 28 B: 21		Verde Pastel #90C733 R: 144 G: 199 B: 51

Cabecera

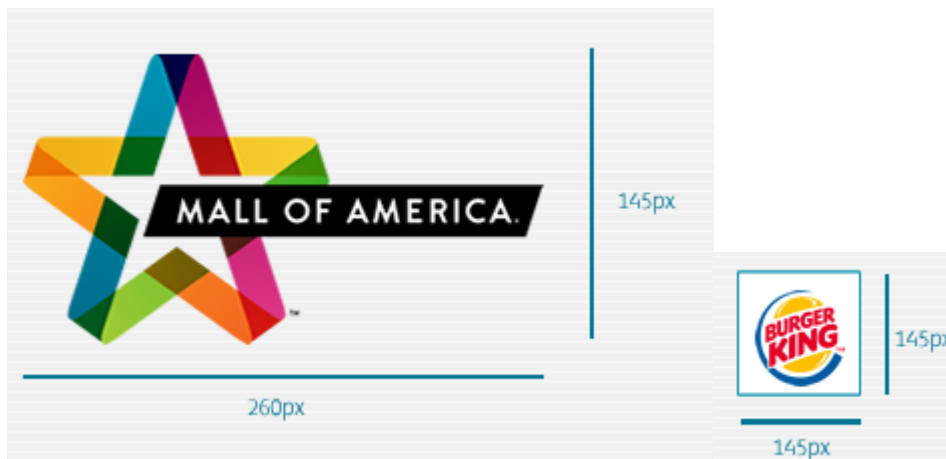
Uso de cabeceras

El encabezado superior de la web se compone de dos elementos: logo del centro comercial (izquierda) y descripción del local que ha iniciado sesión (derecha). Exceptuando la página de inicio de sesión, la misma que se detallará posteriormente.



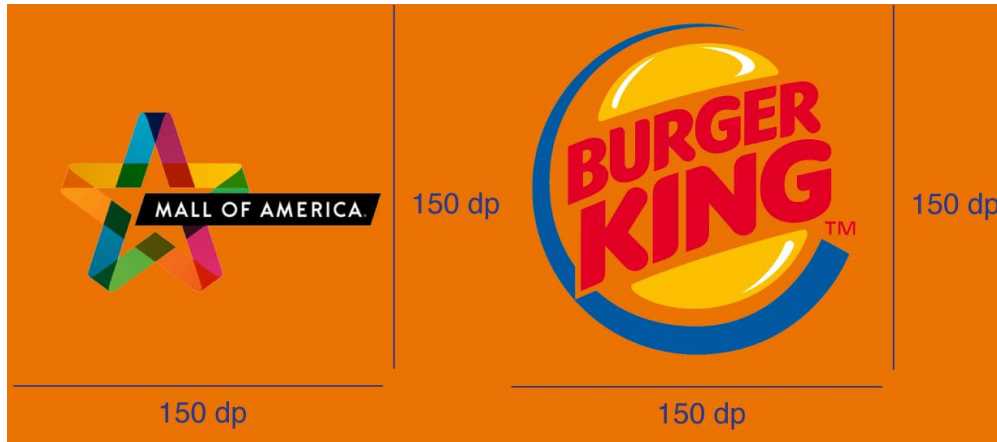
(Fuente: Autoría Propia)

El logo del centro comercial tendrá un tamaño fijo en todas las páginas (260px x 145px), de la misma forma el logo del local comercial será de (60px x 60 px), cabe recalcar que dicho logo posee un borde de 1px de ancho de color azul. El tamaño de la fuente de la palabra "Bienvenido" será de 15px de color verde, en tanto que el nombre del local poseerá un tamaño de fuente de 25px de color café, en ambos casos el tipo de fuente será "Fontana ND Aa".



(Fuente: Autoría Propia)

En el aplicativo móvil el logo del centro comercial tendrá un tamaño de 150 dp x 150 dp, que corresponde a una medida relativa a la densidad de la pantalla del dispositivo móvil usado. De igual manera el logo del local comercial será de 150 dp x 150 dp.



(Fuente: Autoría Propia)

Uso de pie de páginas

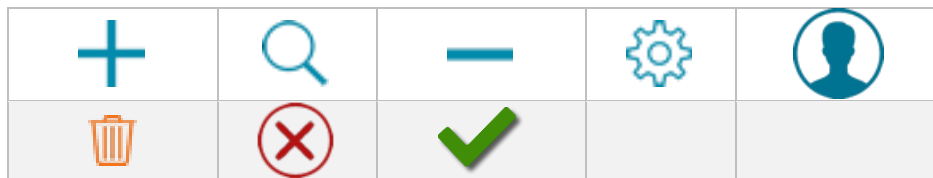
Los pies de página de las diferentes secciones de la aplicación están compuestos de 3 textos principales. Con alineación izquierda el año en el que fue desarrollado el aplicativo, su autor/es y el centro comercial para el que de implemento dicho sistema, lo cual poseerá un color azul. Seguido de un texto con alineación central con la dirección, teléfono, ciudad y país del domicilio del centro comercial, de color verde. Finalmente con una alineación derecha se incluirá un texto con dos enlaces: hacia la página inicial o "Home" de la aplicación y hacia el mapa del sitio, de color naranja. En los tres casos el tamaño de la fuente "Fontana ND Aa" será de 12px.



Fotos y Logos

Íconos

Los iconos utilizados en las distintas partes del aplicativo se listan a continuación



Títulos y Textos

Títulos de Página

Esta sección poseerá un recuadro color naranja de 560px x46px, un tamaño de fuente de 18px; el texto un ancho de tipo negrita, de la misma forma utilizará una fuente Fontana ND Aa de color blanco.



(Fuente: Autoría Propia)

Títulos de Sección de página

Esta sección de las páginas de la aplicación servirá para nombrar párrafos o subsecciones dentro del sitio, poseen un tamaño de letra de 17px, de color verde y una fuente Fontana ND Aa



(Fuente: Autoría Propia)

Títulos de Sección lateral

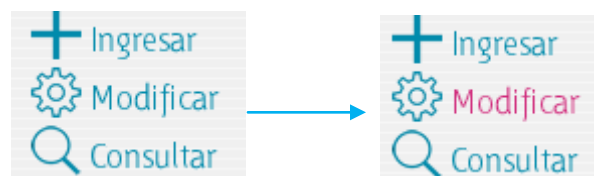
Estos subtítulos servirán para categorizar los principales enlaces de navegación en el sitio web, poseen un ancho fijo de 237px y un alto de 57px, sus colores de fondo pueden variar entre verde claro, naranja y azul. Su tipografía posee una fuente Fontana ND Aa de tamaño 17px siempre de color blanco.



(Fuente: Autoría Propia)

Texto de enlaces de sección lateral

Estos enlaces están pendiente siempre a lo largo de las diversas secciones del aplicativo, y poseen 2 elementos: un ícono descriptivo de tamaño (25px x 25px) y su texto correspondiente de 17px de tamaño, color azul, cuando el puntero se posesione sobre dichos enlaces su color de texto cambiará a púrpura.



(Fuente: Autoría Propia)

Texto de ubicación actual

Esta parte de la aplicación poseerá un tamaño de fuente de 13px, será de color púrpura y su tipo de letra será Fontana ND Aa. Su función es la de informar al usuario en todo momento la posición actual dentro del aplicativo.



Productos > Ingreso

(Fuente: Autoría Propia)

Formularios

Etiquetas de Formularios

Para el uso de formularios, las etiquetas serán de color naranja, con una fuente Fontana ND Aa de 17px

Categoría

Bebidas ▼

Nombre

Té Helado

(Fuente: Autoría Propia)

Campos de Textos

Dentro de los formularios los campos de texto poseerán un color de letra azul, un tamaño de 17px y tipografía Fontana ND Aa.

BURGUER KING *

Ejemplo: Postres

C191 *

Ejemplo: A539

0999451265

Ejemplo: 072803543

(Fuente: Autoría Propia)

Textos de Ayuda

Con el fin de ayudar a un ingreso correcto de los datos en los diferentes formularios, en ciertas ocasiones se proporciona un ejemplo de texto en un campo. Este texto será de color verde claro, tipografía Fontana ND Aa de tamaño 12px.

Ejemplo: Postres

Ejemplo: Postres

(Fuente: Autoría Propia)

Listas Desplegables

Estos elementos poseerán un color de letra azul, un tamaño de 17px y tipografía Fontana ND Aa.

BURGUER KING
BURGUER KING
CEBICHES DE LA RUMINAHUI]E]E]E
DOÑA MENESTRA
KENTUCKY FRIED CHICKEN
MC DONALD'S
PIZZA HUT
SUBWAY

(Fuente: Autoría Propia)

En el aplicativo móvil serán con fondo transparente y color de letra blanco y tipografía Roboto.

A rectangular button with an orange background and rounded corners. The text "Burger King" is centered in white, sans-serif font. A thin white horizontal line is positioned below the text, ending in a small triangle on the right side.

Burger King

(Fuente: Autoría Propia)

Botones de Ingreso y Cancelar

Estos elementos poseen un ancho fijo de 230px y un alto de 45px. Su color de fondo varía entre el verde claro (Ingresar/Modificar) y el rojo (Cancelar). Una letra de tamaño 25px, de color blanco y tipografía Fontana ND Aa.

A rectangular button with a light green background and rounded corners. The text "Ingresar" is centered in white, sans-serif font.

Ingresar

A rectangular button with a dark red background and rounded corners. The text "Cancelar" is centered in white, sans-serif font.

Cancelar

(Fuente: Autoría Propia)

En el aplicativo móvil tendrán un tamaño relativo al contenido y a la densidad de pantalla. El fondo será de color azul. Una letra de tamaño de 20dp de color blanco y tipografía Roboto.

A rectangular button with a blue background and rounded corners. The text "Ver menú" is centered in white, sans-serif font. The button is surrounded by a thick orange border.

Ver menú

(Fuente: Autoría Propia)

Listados

En esta sección se visualizan los distintos tipos de listados que ofrecen especialmente en las consultas a lo largo del aplicativo.

Búsqueda de Restaurantes










(Fuente: Autoría Propia)

En esta sección se visualizarán los distintos restaurantes ingresados en la aplicación. Los mismos se presentarán en páginas de 6 elementos cada una. Cada restaurante se mostrará en un <div> de 180px de ancho por 260px de alto. El logo del restaurante poseerá 180px de alto por 180px de ancho, el texto de su nombre será de color naranja, de tamaño 15px de y en la parte inferior se colocará con alineación a la izquierda un ícono de 25px x 25px para modificar los datos del restaurante y su número de local de color verde, tamaño 20px. Todos estos textos tienen una tipografía Fontana ND Aa.



(Fuente: Autoría Propia)

Búsquedas de Productos

 <p>B.L.T.</p> <p>The sub that proves great things come in threes. In this case, these three things happen to be crisp bacon, lettuce and juicy tomato. While there's...</p> <p> \$7.89</p>	 <p>BLACK FOREST HAM</p> <p>Black Forest Ham. The Black Forest Ham has never been better. Load it up with all the crunchy veggies you like on your choice of freshly baked bread...</p> <p> \$5.89</p>	 <p>BUFFALO CHICKEN</p> <p>You might wonder how something could taste this incredible. But when you bite into a sandwich this tender, juicy and irresistibly bold, the only thing...</p> <p> \$8.56</p>
 <p>CHICKEN & BACON RANCH MELT</p> <p>Saddle up & try the fresh toasted SUBWAY® Chicken & Bacon Ranch sandwich. Stuffed with melted Monterey cheddar cheese, tender all-white meat chicken...</p> <p> \$4.59</p>	 <p>CHICKEN CORDON BLEU MELT</p> <p>This mouthwatering melt doesn't hold back. The Chicken Cordon Bleu Melt is piled high with juicy chicken, Black Forest Ham, melty cheese and all you...</p> <p> \$8.96</p>	 <p>COLD CUT COMBO</p> <p>Can't decide what kind of meat you want? Get them all. The Cold Cut Combo is stacked with turkey-based meats - ham, salami and bologna. It's topped w/...</p> <p> \$5.78</p>

(Fuente: Autoría Propia)







De manera similar a lo presentado en la sección de restaurantes, los productos se visualizarán en páginas con 6 elementos cada una. Pero con la diferencia que cada <div> poseerá una dimensión de 400px de alto x 180px de ancho. La imagen del producto será de tamaño 180px x 180px. Su nombre será de color naranja, de tamaño 15px de y en la parte inferior se colocará con alineación a la izquierda un ícono de 25px x 25px para modificar los datos del restaurante y su número de local de color verde, tamaño 20px. El texto de la descripción del producto poseerá un tamaño de 15px de color azul. Todos estos textos tienen una tipografía Fontana ND Aa.








(Fuente: Autoría Propia)

Búsquedas de Categorías y Usuarios

Estas secciones se presentarán a manera de tabla y sin paginación. Los títulos de cada columna serán de color azul y ancho negrita, de tamaño 16px. El texto del nombre de la categoría poseerá un color negro de 16px. Y el enlace para su modificación / eliminación será de tamaño 25px x 25px. Todos los textos tienen una tipografía Fontana ND Aa.

Categoría	Modificar
ALITAS Y COSTILLAS BBQ	
COMIDA CHINA	
HAMBURGUESAS	
HELADOS	
MARISCOS	
PARRILLADAS	

(Fuente: Autoría Propia)

Apellido y Nombre	Dirección	Username	Eliminar
INIGUEZ WILBER	AV 10 DE AGOSTO 1-89	chicowail	
INIGUEZ DENIS	LA PINTA 1-158	denisiguez	
NIVICELA FERNANDA	RINCON DEL FIN DEL MUNDO	fernucha	
SANCHEZ PEDRO	AV GONSALEZ SUAREZ 1-23	pedro	
TENESACA DORA	CALLE SANTIAGO ENTRE LA OEA Y POPAYAN	doritamemos	

(Fuente: Autoría Propia)

Listado de productos en aplicativo móvil

Esta sección se presentará a manera de lista y sin paginación. Los títulos de cada fila serán de color azul y ancho negrita, de tamaño 18sp. El texto del nombre de la categoría y tiempo de preparación poseerá un color negro de 16sp. El texto de precio será de color verde de tamaño 18sp. Todos los textos tienen una tipografía Roboto.



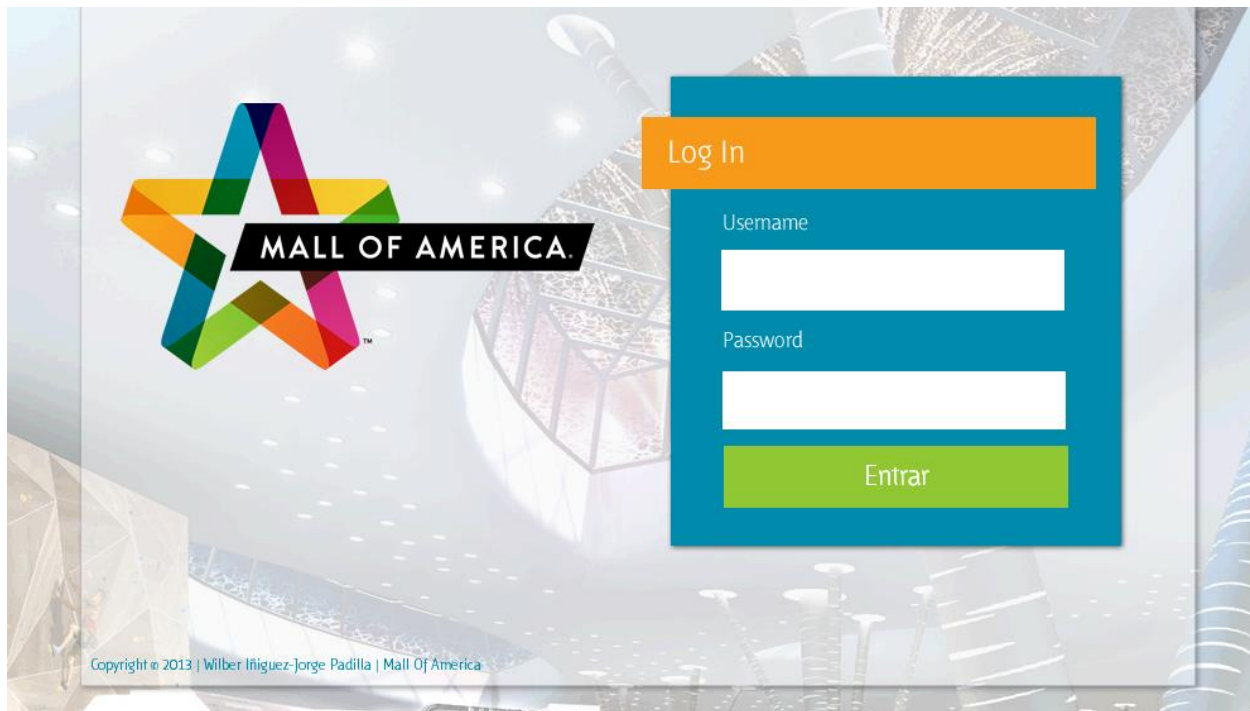
Producto # 1 \$ 5.60

Tipo de producto

Tiempo de preparación: 5 min

(Fuente: Autoría Propia)

Pantalla de Inicio de Sesión



(Fuente: Autoría Propia)

Esta sección posee una distribución única, compuesta por: un rectángulo de fondo de tamaño 882px de ancho x 536px de alto, posee un color de fondo blanco con 50% de transparencia. En la parte izquierda el logo del centro comercial de tamaño 376px x 211px. En la parte derecha un recuadro de 357px x 371px de color azul, sobre el cual se ubica un rectángulo de color naranja de tamaño 360px x 57px, con la palabra "Log In", de tamaño 25px y color blanco. Los textos de "Username/Password" poseen un tamaño de 17px de color blanco, los campos de texto y el botón de ingresar poseen un tamaño de 272px x 46px, los campos de color de fondo blanco y el botón de "Entrar" verde claro. El texto en ambos casos es de tamaño 25 px. Toda la tipografía de la pantalla es de tipo Fontana ND Aa.