UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE CIENCIAS PURAS Y NATURALES

CARRERA DE INFORMÁTICA

TESIS DE GRADO

SISTEMA DE SEGURIDAD MULTINIVEL DE ACCESO Y ALERTAS UTILIZANDO LA TECNOLOGIA NFC

Tesis de Grado para obtener el Título de Licenciatura en Informática

Mención Ingeniería de Sistemas Informáticos

POR: MADELEM NAYRA MAMANI NINA

TUTOR METODOLÓGICO: M.SC. ROSA FLORES MORALES

ASESOR: LIC. MARCELO GERMAN ARUQUIPA CHAMBI

LA PAZ – BOLIVIA

Diciembre, 2021

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

LA CARRERA DE INFORMÁTICA DE LA FACULTAD DE CIENCIAS PURAS Y NATURALES PERTENECIENTE A LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la referencia correspondiente respetando normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

TODOS LOS DERECHOS RESERVADOS. EL USO NO AUTORIZADO DE LOS CONTENIDOS PUBLICADOS EN ESTE SITIO DERIVARA EN EL INICIO DE ACCIONES LEGALES CONTEMPLADOS EN LA LEY DE DERECHOS DE AUTOR.

DEDICATORIA

A mi mamita Julieta Nina Gutiérrez por el apoyo incondicional que me brindo para seguir adelante y no dejarme caer, a nunca rendirme y seguir con mis sueños, enseñarme a ser una mujer trabajadora y luchadora, motivándome siempre para alcanzar mis anhelos y metas.

A mis tíos y primos que siempre confiaron en mi en todo momento, por los consejos y apoyo que siempre me brindan.

A Franco Martínez quien siempre estuvo conmigo en todo momento alentándome para lograr mis metas, pese a las muchas dificultades que hemos pasado juntos, nunca dejo de confiar en mí.

mmadelemnayra@gmail.com

AGRADECIMIENTOS

Gracias a Dios por acompañarme, guiarme y darme la capacidad para poder finalizar este proyecto en mi vida, por darme la dicha de compartir este logro con mi familia, bendecir mi hogar y estar presente todos los días de mi vida.

A mi familia y especialmente a mi madre quien siempre lucho por mí, por ser el cimiento principal en mi vida, comprensión y valores que necesitaba en cada etapa de mi vida, que sin ella este logro no habría sido posible, por ser un ejemplo a seguir, ¡por formarme con muchos valores y principios forjando la persona que soy ahora, Gracias!

A mi tutora metodológica M. Sc. Rosa Flores Morales por la paciencia que tuvo conmigo, por el conocimiento que me brindo, el tiempo y su colaboración, indispensables en la elaboración de este proyecto.

Al Lic. Marcelo German Aruquipa Chambi. Docente Revisor, por brindarme su apoyo, consejos y sugerencias en el desarrollo de este trabajo.

A mis amigos de la universidad por el compañerismo, en especial a Antonio, por el apoyo, guía y colaboración, sobre todo por la confianza y el cariño depositado en mí, a Karen que siempre estuvo junto apoyándonos mutuamente para poder concluir juntos esta etapa de nuestras vidas, por la amistad y alegrías.

Finalmente agradecer a la Universidad Mayor de San Andrés por su recibimiento durante el transcurso de estos años y la estimada Carrera de Informática.

GRACIAS.

RESUMEN

En el presente trabajo se hizo uso de la tecnología NFC (comunicación de campo cercano) debido a las ventajas y el nivel de seguridad que ofrece frente a otras tecnologías, el control de acceso en diferentes entornos, el problema de seguridad en el control de acceso debido al grupo masivo que existe en muchos eventos.

El sistema de control de acceso se realizó empezando con el análisis de conceptos importantes de la tecnología NFC, se escogió las herramientas útiles para el desarrollo de la aplicación, posteriormente se creó un diseño para la red de comunicación en el control de acceso e intercambio de datos, para la seguridad del sistema se implementó el cifrado de la información cuando se hace peticiones a la base de datos, se procesó la información requerida por los receptores NFC para determinar los permisos de acceso a los usuarios.

En la aplicación se ha logrado comprobar que para el 98% de los casos es factible identificar los usuarios que han ingresado a un evento, también se realizó encuestas a los usuarios para verificar la usabilidad, respecto a la funcionalidad se aplicó la eficiencia en la eliminación de defectos para la calidad y control de la aplicación, en las pruebas de compatibilidad más del 50% cuenta con tecnología NFC.

Palabras clave: Comunicación de campo cercano, Control de acceso, Seguridad, Tarjetas inteligentes, Mobile D.

ABSTRACT

In the present work, NFC technology (Near Field Communication) was used because of the advantages and the level of security it offers compared to other technologies. So that is applied to access control in different environments, and thus be able to solve the problem of security in access control due to the massive group that exists in many events.

The access control system was made starting with the analysis of important concepts of NFC technology, the useful tools were chosen for the development of the application, then a design was created for the communication network in access control and data exchange, for the security of the system was implemented the encryption of information when making requests to the database, processed the information required by the NFC receivers to determine the access permissions to users.

In the application it has been possible to verify that for 98% of the cases it is feasible to identify the users who have entered an event. Also, user surveys were conducted to verify the usability, with respect to the functionality, efficiency was applied in eliminating defects for the quality and control of the application, in the compatibility tests more than 50% have NFC technology.

Keywords: Near Field Communication, Access Control, Security, SmartTag, Mobile D.

ÍNDICE DE CONTENIDOS

CAPÍTULO I. vii
1.1 INTRODUCCIÓN 1
1.2 ANTECEDENTES 2
1.3 DESCRIPCION DEL PROBLEMA 4
1.4 OBJETIVOS 5
1.4.1 OBJETIVO GENERAL 5
1.4.2 OBJETIVOS ESPECÍFICOS 5
1.5 JUSTIFICACIÓN 5
1.5.1 JUSTIFICACIÓN ECONOMICA 5
1.5.2 JUSTIFICACIÓN SOCIAL 5
1.5.3 JUSTIFICACIÓN TECNOLÓGICA 6
1.6 ALCANCES Y LÍMITES 6
1.6.1 ALCANCES 6
1.6.2 LÍMITES 7
1.7 METODOLOGÍA 7
1.7.1 METODOLOGÍA DE INVESTIGACIÓN 7
1.7.2 METODOLOGÍA DE DESARROLLO 7
2 CAPÍTULO II. 9
2.1 TELEFONOS INTELIGENTES (sMARTPHONE) 10
2.2 DESCRIPCIÓN DE LA TECNOLOGÍA NFC 10
2.2.1 Origen y desarrollo del NFC 11
2.2.2 Compatibilidad RFID con NFC 12
2.2.3 NFC Fórum 13
2.2.4 Aplicación de la tecnología NFC 14
2.2.5 Tarjetas sin contacto 15
2.2.6 NFC Y OTROS PROTOCOLOS SIN CONTACTO 16
2.2.7 ESPECIFICACIONES TÉCNICAS DE NFC 17
2.2.8 Fases de la comunicación en NFC 23
2.3 SEGURIDAD EN NFC 24
2.3.1 Principales riesgos y amenazas de seguridad 24
2.3.2 Escuchas no autorizadas 24
2.3.3 Corrupción de datos 25

2.3.4 Inserción de datos 25
2.3.5 Clonación 26
2.3.6 Componentes de seguridad 26
2.3.7 ISO/IEC 27001 26
2.4 ANDROID 28
2.4.1 Aplicaciones Android 28
2.4.2 Características de Android 29
2.4.3 Arquitectura de Android 30
2.4.4 ANDROID NFC 33
2.5 METODOLOGÍAS DE DESARROLLO 35
2.6 Metodologías agiles para el desarrollo de software móvil 36
2.6.1 Desarrollo ágil: programación extrema (XP). 37
2.6.2 Desarrollo ágil: Scrum. 39
2.6.3 Mobile-d 40
2.6.4 Fase de exploración 41
2.6.5 Fase de inicialización 42
2.6.6 Fase de producción 43
2.6.7 Fase de estabilización 44
2.6.8 Prueba y corrección del sistema 45
3 CAPÍTULO III. 46
3.1 introducción 47
3.2 desarrollo DE la metodología mobile-d 47
3.3 FASE DE EXPLORACIÓN 48
3.3.1 Propuesta del producto e historias de usuario 48
3.3.2 Historias de usuario 48
3.3.3 Requerimientos funcionales y no funcionales 51
3.4 FASE DE INICIALIAZCIÓN 51
3.4.1 Establecimiento de recursos físicos y técnicos 52
3.4.2 Modelo entidad – relación 53
3.4.3 Diagrama de clases 54
3.5 fase de producción 55
3.5.1 Producto 55
3.6 fase de Estabilización 57

3.7 fase de prueba 59
3.7.1 Identificación del tag NFC 59
3.7.2 Conexión a la base de datos 59
3.7.3 Spring Boot Security 60
4 CAPÍTULO IV. 62
4.1 MÉTRICAS DE CALIDAD DEL PROYECTO 63
4.1.1 PRUEBA DE USABILIDAD 63
4.1.2 FUNCIONALIDAD 64
4.1.3 PRUEBA DE COMPATIBILIDAD 65
4.2 SEGURIDAD 68
4.2.1 A NIVEL DE APLICACIÓN 68
4.2.2 AUTENTIFICACIÓN Y AUTORIZACIÓN 69
4.2.3 SEGURIDAD EN LA BASE DE DATOS 70
5 CAPÍTULO V. 71
5.1 CONCLUSIONES 72
5.2 RECOMENDACIONES 73
6 74
7 Bibliografía 74

ÍNDICE DE FIGURAS

Figura 2.1: Transferencia de energía. Por NFC Fórum 14
Figura 2.2: Aplicaciones NFC. 15
Fuente: Ceballos, 2013. 15
Figura 2.3: tarjetas inteligentes con NFC. 16
Fuente: (Cacahuango D, Zapata E, 2015) 16
Figura 2.4: Registro NDEF. Por NFC Forum 19
Figura 2.5: estructura de un mensaje NDEF. Por NFC Forum. 20
Figura 2.6: Estructura de un Campo URI (0x55) y una URL como registro URI. NFC. 22
Figura 2.7: Arquitectura Android. 31
Fuente: Android developers,2020. 31
Figura 2.8. Ciclo de desarrollo Mobile – D adaptado de Amaya (2013), Metodologías ágiles en el desarrollo de aplicaciones para dispositivos móviles. 41
Figura 2.9: ciclo de inicialización Mobile-D 43
Fuente: Koskela, 2004. 43
Figura 2.10: ciclo de producción Mobile – D 44
Fuente: Koskela,2004. 44
Figura 2.11: ciclo de producción Mobile – D 45
Fuente: Koskela,2004. 45
Figura 2.12: Ciclo fase prueba y corrección del sistema Mobile-D 45
Fuente: Koskela, 2004 45
Figura 3.1: cuota de mercado de los sistemas operativos para teléfonos móviles 2010 a 2018 52
Fuente: Statista, 2021 52
Figura 3.2: Modelo vista controlador 53
Fuente: Pkmuaz, 2016 53
Figura 3.1: diagrama entidad relación 54
Figura 3.2: diagrama de clases 54
Figura 3.4. Pantalla principal 55
Figura 3.5. Pantalla de registro 56
Figura 3.6. Pantalla principal 2 57
Figuran 3.7. Pantalla de control del sistema 57
Figura 3.8: registro del formulario 58
Figura 3.9 desarrollo de la interfaz de usuario con sus respectivos módulos 58

Figura 3.10. Identificación del tag NFC. 59
Figura 3.11: Implementación de los servicios. 60
Figura 3.12: implementación de la seguridad para el usuario 60
Figura3.13: prototipo final de la aplicación 61

ÍNDICE DE TABLAS

Tabla 2.1: Metodologías agiles para el desarrollo móvil – análisis comparativo 36
Tabla 3.1: Historia de usuario 1 49
Tabla 3.2: Historia de usuario 2 49
Tabla 3.3: Historia de usuario 3 49
Tabla 3.4: Historia de usuario 4 50
Tabla 3.5: Historia de usuario 5 50
Tabla 3.6: Historia de usuario 6 50
Tabla 4.1. Escala de valores para la usabilidad 63
Tabla 4.2. Usabilidad de la aplicación 64
Tabla 4.3. Tabla de resultados -1 66
Tabla 4.4: Tabla de resultados -2 66
Tabla 4.5. Tabla de resultados -3 67
Tabla 4.6. Tabla de resultados – 4 67
Tabla 4.7. Tabla de resultados – 5 68

CAPÍTULO I.

MARCO INTRODUCTORIO

1.1 INTRODUCCIÓN

La comunicación de campo cercano es una tecnología que permite que dos dispositivos se comuniquen de forma inalámbrica a corta distancia compartiendo datos con una velocidad de 424 kbit/s.

En este proyecto se ha creado un servicio que permite el control de acceso de los usuarios a las diferentes estancias de un evento de forma segura.

Para identificar a los usuarios se usan tarjetas identificativas NFC (comunicación de campo cercano) pasivas, que será leídas por un dispositivo móvil compatible con esta tecnología. Se ha desarrollado una aplicación móvil que permite la administración y el diseño de las políticas de control de acceso.

Los smartphones o teléfonos inteligentes ofrecen una multitud de aplicaciones con gran cantidad de funcionalidades, siendo así como una pequeña computadora dentro de un celular, por tal motivo se ha decidido implementar una aplicación móvil para dispositivos con sistema operativo Android que funcione a modo de cerradura para el acceso a cada una de las estancias de un evento.

Para la comunicación de la aplicación Android con la base de datos se hizo uso del framework Spring Boot, para el consumo de las Apis, la administración de salas, permisos, registros de cada estancia del usuario.

El control de acceso se realiza con el uso de distintas tecnologías:

- Android es el sistema en el que se ha programado la aplicación.
- Etiquetas NFC almacenan datos del usuario que quiere acceder a una sala.
- Java es el lenguaje en el que se ha programado las Apis.
- Spring Security es un marco que se centra en proporcionar autenticación y autorización a las aplicaciones Java.
- Postgres es el gestor de la base de datos.

Por medidas de seguridad, es necesario llevar un control de las personas que entran o salen de cualquier estancia. Siendo necesario un sistema que permita identificar, controlar la cantidad y dar accesos a cada persona que permanecen en diferentes áreas.

Este trabajo fue organizado en cinco capítulos; en el capítulo uno se describe la introducción del trabajo de investigación, investigaciones o proyectos similares, el planteamiento del problema que servirá para la justificación del de la tesis, el objetivo general y objetivos específicos. En el capítulo dos se realizó la descripción de las herramientas y metodología a utilizar para el desarrollo del sistema, la descripción del a tecnología NFC y su funcionamiento, el uso del sistema operativo Android. En el capítulo tres se aplicó la metodología para la implementación y desarrollo del sistema, el prototipo y las pruebas de funcionamiento. En el capítulo cuatro se realizó un análisis de los resultados. En el capítulo cinco se realizó las conclusiones y recomendaciones obtenidas en el desarrollo del proyecto.

1.2 ANTECEDENTES

Desde hace muchos años la tecnología ha buscado facilitar el día a día del hombre, dando paso a un sin fin de nuevas tecnologías, entre ellas una de las más recientes y con un alto crecimiento en el mercado de los teléfonos móviles es el NFC (*Near Field Communication* – Comunicación de campo cercano).

En el 2004 NFC Forum fue fundada por PHILIPS, NOKIA, SONY entre otras, que se encargan de regular y determinar los estándares NFC, que opera en una banda de 13,56 MHz. A la que no aplica ninguna restricción y no requiere de licencia alguna para su funcionamiento. El usuario puede tener contacto con una etiqueta o compartir información con un objeto acercando los dos dispositivos que incorporan esta tecnología a menos de 20 cm.

La tecnología NFC también es compatible con la infraestructura de RFID (identificación por radiofrecuencia). “Es una tecnología de intercambio, almacenamiento y recuperación de datos remotos que utilizan dispositivos

denominados etiquetas, el propósito de esta tecnología es transmitir la identidad de un objeto por medio de ondas de radio". (Chavarría Chavarría Daniel, 2011)

El uso del NFC está transformando la forma de relacionarnos con el entorno, ya que el teléfono móvil se ha convertido en la tarjeta de crédito, en llavero o en mando a distancia entre otros muchísimos usos. El uso de la tecnología comienza a ser adoptada por empresas y ciudades como Japón, España, EEUU e Inglaterra.

Es una tecnología segura, ya que para activar cualquier servicio o intercambiar información el usuario tendrá que hacerlo manualmente, o bien juntar dos dispositivos móviles, confirmando nuevamente el usuario cada acción. Además, como está integrada en un dispositivo móvil podemos incluir varios niveles de seguridad.

Frente al tema de investigación Vicente (2011) Con este proyecto nos permite acercamos a la tecnología NFC (Near Field Communication) integrada en los dispositivos móviles, aprovechando las posibilidades que nos ofrece. Para el desarrollo de una aplicación que permite implementar sistemas de identificación y control de acceso.

Según Arroyo (2014) en su trabajo de investigación, expone las bases teóricas, necesarias para el desarrollo del sistema de identificación y control de acceso a espacios controlados mediante teléfonos inteligentes y tecnología NFC. Entre las bases que se presentaran en el desarrollo del trabajo de investigación están los diferentes tipos de metodologías para el desarrollo de sistemas y también está la metodología Mobile D la cual se usa para el desarrollo en teléfonos inteligentes.

EL trabajo de investigación según Ortega (2018) está basada en tres principios autenticación, autorización y trazabilidad usando medidas biométricas para la autenticación de personas con el uso de smartphones con tecnología NFC y con un microcontrolador que gobierne el elemento que controla el acceso. Realizando un estudio de la tecnología NFC, el uso que tiene para transmitir

información entre teléfonos inteligentes y el hardware basado en microcontroladores.

1.3 DESCRIPCION DEL PROBLEMA

Últimamente se han notado grandes avances en los sistemas para el control de acceso, los cuales se han ido implementando casi en cada lugar que cuente con visitas masivas. Gracias a la gran demanda que existe se han incorporado tecnologías mejoradas de comunicación e identificación de datos con diferentes niveles de seguridad.

La seguridad en controles de acceso es un tema de gran importancia en todo tipo de infraestructura especialmente en las que tienen información o material de gran valor.

Para la seguridad de la información se debe tener en cuenta los principios fundamentales que son la confidencialidad, integridad y accesibilidad. En la actualidad diferentes alternativas permiten brindar seguridad de manera inteligente, pero a un gran costo y con muchas limitaciones, encontrando inconvenientes a la hora de la administración y control del personal a distintas áreas.

Es por tal motivo que surge la necesidad del uso de la tecnología NFC en aplicaciones móviles siendo ideal para el control de acceso a eventos que se realicen al aire libre, recintos donde no haya una infraestructura previa o incluso en eventos deportivos, congresos talleres o charlas, donde el control a los diferentes eventos se realiza de manera manual mediante la validación del carnet o recibo, lo que implica una demora en el acceso, provocando largas filas, muchas veces no se cuenta con un registro de los eventos asistidos por el participante.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Desarrollar un sistema de seguridad multinivel de acceso y alertas a las diferentes dependencias de un evento a través de la tecnología inalámbrica NFC.

1.4.2 OBJETIVOS ESPECÍFICOS

- Describir los principios y herramientas bajo los cuales se empleará la tecnología NFC.
- Realizar un control de acceso a través de la tecnología NFC.
- Implementar un prototipo para el desarrollo del sistema.

1.5 JUSTIFICACIÓN

1.5.1 JUSTIFICACIÓN ECONOMICA

El hardware necesario para implementar un sistema mediante teléfonos inteligentes y tecnología NFC es bastante accesible, actualmente la mayoría de las empresas móviles están incorporando NFC en sus dispositivos debido a la gran variedad de usos que se le puede dar, además de estos el costo de implementación es bajo en comparación a otras tecnologías, ya que las tarjetas o tags oscilan en un costo menor a 10 Bs, lo cual beneficia a una empresa o institución para el desarrollo de este sistema.

1.5.2 JUSTIFICACIÓN SOCIAL

Una vez finalizado el desarrollo del sistema será una herramienta útil para los usuarios puesto que el NFC está siendo utilizado bastante en diferentes países para transacciones monetarias, control y verificación de identificación. Además,

que en la actualidad el número de personas que tienen acceso a un smartphone es bastante significativo.

El prototipo del sistema va permitir adquirir y manejar información en tiempo real para poder tener un mejor control de acceso de los usuarios, además que la aplicación a desarrollar será fácil y segura de manejar.

1.5.3 JUSTIFICACIÓN TECNOLÓGICA

Esta aplicación contribuirá para un mejor control de acceso de manera segura y eficiente gracias al avance de las tecnologías inalámbricas, el uso de smartphones con tecnología NFC está revolucionando ya que estos dos van de la mano debido a la variedad de aplicaciones que se puede realizar y la forma en que se pueden activar con tan solo acercar el smartphone a un Smart tags o un dispositivo que use este.

1.6 ALCANCES Y LÍMITES

1.6.1 ALCANCES

- El trabajo realizado permitirá obtener información del móvil, tag o tarjeta con tecnología NFC de manera inalámbrica en tiempo real con solo pasar por la terminal correspondiente.
- La aplicación móvil reconoce los permisos de acceso del usuario.
- En la aplicación móvil se muestra la fecha y hora en la que el usuario ingreso o salió de un evento.
- La comunicación entre la aplicación móvil y los servicios debe estar cifrada para una mayor seguridad.

1.6.2 LÍMITES

- La aplicación está diseñada para dispositivos móviles con sistema operativo Android que cuenten con tecnología NFC.
- El personal no tendrá acceso al sistema de forma que pueda manipular la información, alterar o cambiar datos.
- El usuario necesita un smartphone, tag o tarjeta inteligente que cuente con la tecnología NFC para el reconocimiento y control de acceso.

1.7 METODOLOGÍA

1.7.1 METODOLOGÍA DE INVESTIGACIÓN

En el presente proyecto se hace uso del método heurístico, "Según Pólya (1965), la heurística moderna trata de comprender los métodos que conducen a la solución de problemas, en particular las operaciones mentales típicamente útiles en este proceso."

Los procedimientos heurísticos se dividen en principios reglas y estrategias, buscando la manera de reducir los problemas grandes a más pequeños.

Otra metodología usada también es el método sistémico, porque habla de la teoría general de sistemas. Este método es muy general y puede ser aplicado a diferentes procesos para hallar la solución desde la perspectiva de un sistema, ya que todo es parte de un sistema.

1.7.2 METODOLOGÍA DE DESARROLLO

El objetivo es conseguir ciclos de desarrollos muy rápidos en equipos muy pequeños. Según este método, trabajando de esa manera se deben conseguir productos funcionales en menos de diez semanas (Vique, 2011).

Mobile-D es una metodología ágil de desarrollo que se compone de distintas fases: exploración, inicialización, fase de producto, fase de estabilización y la fase de pruebas donde cada etapa posee un día de planeamiento y un día de entregas de las tareas asignadas. Una vez acabada todas las fases se debería tener una aplicación publicable y entregable al cliente.

CAPÍTULO II.

MARCO TEÓRICO

En este capítulo se hará referencia a la tecnología inalámbrica NFC, la cual se aplicó en el desarrollo del presente proyecto, detallando su definición, características, modo de comunicación, estándares de comunicación para el correcto intercambio de datos entre dispositivos NFC. Por otro lado, el modo de funcionamiento del sistema operativo Android con NFC, su funcionamiento, arquitectura y seguridad. Además de hablar de la metodología de desarrollo de software móvil.

2.1 TELEFONOS INTELIGENTES (SMARTPHONE)

En algunos teléfonos móviles se pueden hacer las mismas funciones de un computador. En ellos, puedes editar documentos, navegar por internet, compartir con tus amigos en Facebook y jugar videojuegos.

Son más conocidos como teléfonos inteligentes o smartphones y su teclado está integrado en la pantalla, solo aparece cuando le estás indicando al tu teléfono que necesitas escribir algo.

La mayor ventaja de estos teléfonos inteligentes y tabletas es que puedes acceder a la red en cualquier instante. Además, de la gran variedad de equipos que encuentras en el mercado.

Estos teléfonos están diseñados para ejecutar una variedad de aplicaciones. Además de brindar un servicio telefónico, son básicamente pequeñas tabletas que se pueden utilizar para navegar en internet, ver vídeos, leer libros electrónicos, jugar y hacer muchas cosas más, funciones adicionales a las de un teléfono tradicional.

2.2 DESCRIPCIÓN DE LA TECNOLOGÍA NFC

La comunicación de corto alcance (comúnmente conocida como NFC por sus siglas en inglés – *Near Field Communication*) hace referencia a una tecnología inalámbrica que provee una comunicación intuitiva, segura y simple entre dispositivos electrónicos como el teléfono móvil. La tecnología NFC ha alcanzado

un punto donde no solo es factible y técnicamente posible el desarrollo de cientos de aplicaciones con uso reales, sino que son viables comercialmente. [López, 2012]

NFC es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio bidireccional de datos entre dispositivos a una distancia corta menor a 10 cm.

NFC forum (2012) define la tecnología NFC como una simple extensión del estándar ISO 14443 (RFID). La integración de la telefonía móvil con la Identificación por radiofrecuencia ha proporcionado una comunicación intuitiva, simple y segura entre dispositivos electrónicos. Trabaja a una distancia entre 5–10 cm., a 13.56 MHz y transfiere datos hasta 424 Kbits/seg.

En comparación con otras tecnologías inalámbricas de corto alcance NFC es de un alcance extremadamente pequeño. Prácticamente es necesario que se toquen el emisor y el receptor para su funcionamiento. Esta funcionalidad lo convierte en un sistema ideal de identificación o pagos electrónicos, ya que para el usuario supone comunicación muy sencilla, transacción rápida y un simple intercambio de datos. [López, 2012]

2.2.1 Origen y desarrollo del NFC

Para poder describir la tecnología NFC, es importante señalar primero que se trata de una técnica basada en RFID. Una tecnología de comunicación inalámbrica que permite un uso mucho más avanzado que otros sistemas como los códigos de barras o incluso los códigos de respuesta rápida QR. Por su parte “Near Field Communications”, conocido también como NFC, es sólo un tipo de RFID que limita el rango de alcance en 10cm. [López, 2012]

Un dispositivo NFC puede comunicarse con cualquier tarjeta inteligente y lector, existentes dentro del estándar ISO/IEC 1444324, tan bien como con otros dispositivos NFC, y es por lo tanto compatible con la infraestructura sin contacto ya en uso para la transportación pública y de pago, NFC está destinado

principalmente para el uso en teléfonos celulares ya que no está orientada para la transmisión masiva de datos como Wi-FI.

2.2.2 Compatibilidad RFID con NFC

Tag o Chip NFC/RFID utilizados en la tecnología NFC tienen un número de identificación único (con un tamaño de 4 a 10 bytes), que se da por la combinación entre código de empresa fabricante y tipo de tecnología del tag (MIFARE, FeliCa, etc.), nos define que existen cuatro tipos de tags que se pueden manejar con los dispositivos. [Campa, 2011]

Las especificaciones operativas para el funcionamiento de los diferentes tipos de tag descritos por el NFC Fórum, proporcionan la información técnica necesaria para aplicar la lectura/escritura y las funciones de control del dispositivo NFC para interactuar con los tags, nos define los siguientes tipos de tags:

- Tag Tipo 1: Se basa en la norma ISO14443A. Los tags permiten ser de lectura y reescritura, aunque los usuarios pueden configurar el tag sólo para lectura. La memoria disponible es de 96 Bytes y expandible a 2 Kb; la velocidad de comunicación es de 106 Kbps.
- Tag Tipo 2: Se basa en la norma ISO14443A. Los tags permiten ser de lectura y reescritura, aunque los usuarios pueden configurar el tag sólo para lectura. La memoria disponible es de 48 Bytes y expandible a 2 Kb; la velocidad de comunicación es de 106 Kbps.
- Etiqueta Tipo 3: Se basa en la *Japanese Industrial Standard (JIS)* X 6319-4, también conocido como FeliCa. Se encuentran ya configuradas desde la fabricación, ya sea para escritura, o sólo para lectura. La memoria disponible es variable, pero teóricamente el límite de memoria es 1 MB por servicio; la velocidad de comunicación es de 212 Kbps o 424 Kbps.
- Etiqueta Tipo 4: Es completamente compatible con ISO14443A y los estándares B. Este tipo de etiqueta vienen ya configuradas desde la fabricación, ya sea para lectura y escritura, o de sólo lectura. La memoria

disponible es variable, de hasta 32 KB por servicio; la velocidad de comunicación es de hasta 424 Kbps.

Las bandas de frecuencia en las cuales trabaja dependen del tipo de aplicación y en la región en donde se encuentre, agrupando en cuatro rangos de frecuencia:

Banda de Alta Frecuencia HF (13,56 MHz): Esta frecuencia le permite tener compatibilidad con otras tecnologías como el caso de NFC y trabaja sin restricción en todo el mundo, ISO 14443 es el estándar para tarjetas *smartcard* sin contacto.

2.2.3 NFC Fórum

El *Near Field Communication* (NFC) Fórum es una asociación industrial sin ánimo de lucro fundada por NXP *Semiconductors*, *Sony Corporation* y Nokia para regular el uso de la interacción inalámbrica de corto alcance en la electrónica de consumo, dispositivos móviles y los PC. [Sánchez, 2011]

El NFC Fórum promueve la implantación y la estandarización de la Tecnología NFC como mecanismo para la interoperabilidad entre dispositivos y servicios. Para conseguir esto, se encarga de:

- Desarrollar especificaciones basadas en estándares.
- Asegurarse del uso de las especificaciones del NFC Fórum.
- Trabajar para que los productos con tecnología NFC cumplan con las especificaciones del NFC Fórum.
- Educar a los consumidores y las empresas respecto de la tecnología NFC.

Near Field Communication (NFC) es una tecnología de comunicación sin contacto basada en un campo de radiofrecuencia (RF) que utiliza una frecuencia base de 13,56 MHz. Las etiquetas NFC Fórum no necesitan baterías ni otras fuentes de alimentación para funcionar, ya que el campo de RF proporciona la energía necesaria para la comunicación. figura 2.1. Cuando el modo de carga

inalámbrica está activo, la intensidad del campo de RF se puede aumentar, lo que permite una transferencia de energía de hasta 1 W. (NFC Forum, 2020)

El dispositivo NFC envía información a una etiqueta de foro NFC modulando la señal de campo de RF (modulación de señal).

El dispositivo NFC recibe información de una etiqueta NFC Fórum al detectar la modulación de la carga generada por la etiqueta NFC Fórum (modulación de carga).

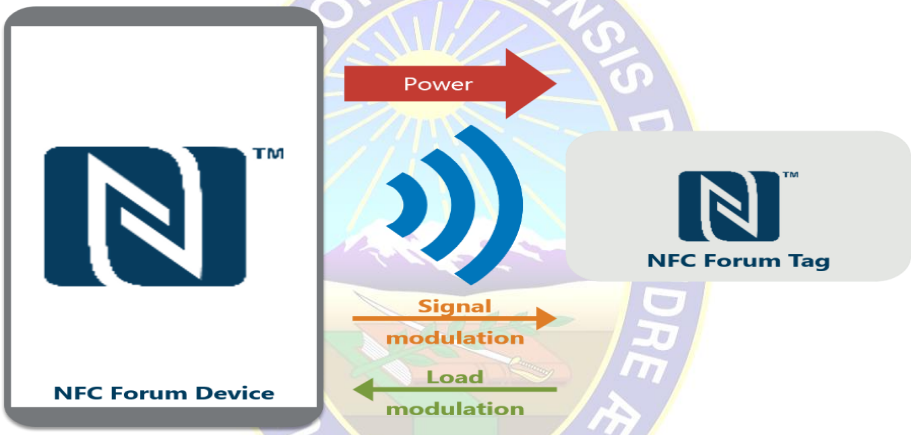


Figura 2.1: Transferencia de energía. Por NFC Fórum

Los usuarios de dispositivos de foro NFC utilizan gestos táctiles para determinar qué entidad debe realizar la comunicación NFC, lo que dificulta la conexión de los atacantes. Como resultado, en comparación con otros protocolos de comunicación inalámbrica, el nivel de seguridad de la comunicación NFC es más alto de forma predeterminada. Además, el NFC Fórum ha agregado "Comunicación entre pares" un mecanismo que encripta todos los datos intercambiados para evitar que los espías interpreten la comunicación grabada. (NFC Forum, 2020).

2.2.4 Aplicación de la tecnología NFC

Existe diferentes aplicaciones de la tecnología NFC, siendo la principal el pago móvil, tickets electrónicos, identificaciones, monedas electrónicas, basada en estándares ISO/IEC 14443. [López, 2012] figura 2.2

Figura 2.2: Aplicaciones NFC.
Fuente: Ceballos, 2013.

Las ventajas que ofrece la tecnología NFC son:

- **Velocidad:** al interactuar los dispositivos NFC entre si en el rango determinado, su respuesta es instantánea reduciendo los tiempos de comunicación.
- **Versatilidad:** los dispositivos NFC pueden comunicarse con otras tecnologías lo cual permite ampliar sus aplicaciones creando una gran opción en el mercado.
- **Comunicación**: la comunicación inalámbrica NFC resulta más rápida y sencilla que otras tecnologías como wifi o bluetooth que requieren de un proceso de emparejamiento previo al inicio de la comunicación.
- **Seguridad:** se considera como seguro debido al rango de alcance determinado para el intercambio de datos entre dispositivos es pequeño.
- **Estandarizado**: al encontrarse dentro de las normas ISO/IEC puede trabajar con diversas tecnologías a nivel mundial y trabajar en una frecuencia que no tiene ninguna restricción (Fórum, 2004)

2.2.5 Tarjetas sin contacto

Las tarjetas sin contacto son el avance tecnológico de las tarjetas inteligentes estas fueron inventadas y patentadas en los setenta. Existe una gran

controversia acerca del inventor original entre los supuestos están, Juergen Dethloff de Alemania, Arimura de Japón y Roland Moreno de Francia, a este ultimo se le adjudica este gran descubrimiento que dio lugar a las tarjetas de crédito y ha evolucionado hasta las tarjetas SIM utilizadas en teléfonos móviles.

Las tarjetas sin contacto tienen mayor costo en comparación alas tarjetas de contacto, pero tienen una vida útil mas extensa y mayor confiabilidad, como las Smart Cards o tarjetas inteligentes entre las que a nivel mundial destacan las tarjetas MIFARE Y FELICA de donde deriva la tecnología NFC figura 2.3

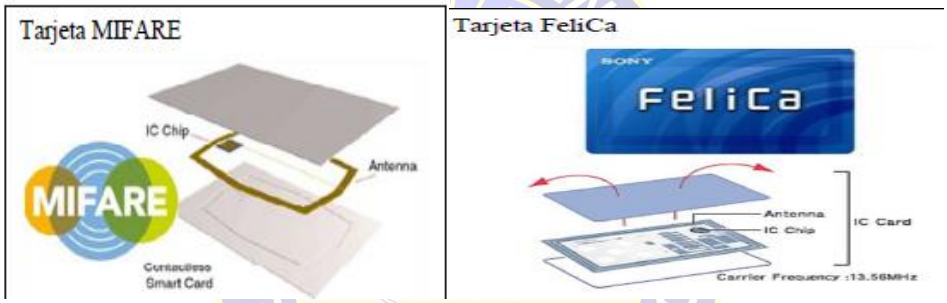


Figura 2.3: tarjetas inteligentes con NFC.
Fuente: (Cacahuango D, Zapata E, 2015)

2.2.6 NFC Y OTROS PROTOCOLOS SIN CONTACTO

La tecnología de comunicación NFC es utilizada por varios protocolos de comunicación sin contacto existentes en el mercado que utilizan diferentes codificaciones para la modulación de señal y carga. Los dispositivos NFC Fórum pueden comunicarse con:

- Lectores y tarjetas que cumplen con el estándar ISO / IEC 14443 Tipo A
- Lectores y tarjetas que cumplen con el estándar ISO / IEC 14443 Tipo B
- Tarjetas que cumplen con el estándar ISO / IEC 15693
- Dispositivos que cumplen con el estándar ISO / IEC 18092
- Lectores y tarjetas compatibles con el estándar JIS-X 6319-4

- Etiquetas del foro NFC
- Otros dispositivos NFC Fórum

Dependiendo del protocolo de comunicación utilizado y la capacidad del dispositivo remoto, NFC *Fórum Devices* admite una velocidad de comunicación de hasta 424 Kbit / s. (NFC Fórum, 2020).

2.2.7 ESPECIFICACIONES TÉCNICAS DE NFC

Esta tecnología usa circuitos inductivos emparejados que pueden intercambiar un flujo de datos cuando están próximos entre sí. El uso de este tipo de acoplamiento es la principal diferencia entre NFC y otras tecnologías inalámbricas como Bluetooth y Wifi, que trabajan a una distancia máxima 10 y 100 metros respectivamente.

La comunicación es *half-duplex* (ambos sentidos, pero no simultáneamente), ya que se emplea una única portadora. Además, los dispositivos NFC pueden verificar el campo de Radio Frecuencia y detectar una colisión si la señal recibida no coincide con la señal transmitida. (NFC Fórum, 2020).

NFC no es una tecnología pensada para la transmisión masiva de datos, porque la tasa de transferencia de datos máxima aproximada es de 424 Kbps. En comparación con otras tecnologías como Bluetooth con una tasa de transferencia de 3 Mbps, o Wifi con 54 Mbps.

Las tarjetas (Tags) pueden insertarse en dispositivos como teléfonos móviles, PDAs tarjetas de pago o tickets. Existen cuatro configuraciones diferentes para utilizar NFC lo que hace que sea más adaptable y eficiente que otras tecnologías: (NFC Fórum, 2020).

- **Modo lector / escritor:** El dispositivo NFC Fórum funciona como un dispositivo lector sin contacto que puede comunicarse con etiquetas o

tarjetas sin contacto. Un caso de uso típico es leer carteles inteligentes, por ejemplo, abrir un sitio web de Internet específico.

- **Emulación de tarjetas:** El dispositivo NFC se comporta como una *contactless card*. Se puede utilizar las características de seguridad avanzadas del elemento seguro, siendo útil para el manejo de sistemas de pagos basados en diferentes métodos o controles de acceso.

- **Emulación de tarjeta de host:** Con esta implementación, una aplicación HCE ubicada en *Device Host* se está encargando de emular la tarjeta sin contacto. En esta configuración, el controlador NFC reenvía todos los comandos sin contacto recibidos al host del dispositivo. La aplicación HCE puede comunicarse con el dispositivo lector sin contacto mediante la API de NFC.

- **Modalidad P2P:** Dos dispositivos NFC se comunican entre sí para el intercambio de información. La comunicación NFC se podría utilizar para establecer parámetros de una comunicación inalámbrica como Bluetooth o Wifi.

- **Emulación de tarjeta basada en elementos seguros:** Con este modo, la emulación de la tarjeta sin contacto se gestiona mediante un elemento seguro dentro del dispositivo NFC Fórum. Este elemento seguro puede ser un chip de seguridad integrado en el dispositivo NFC Fórum o una tarjeta SIM habilitada para NFC insertada en el dispositivo NFC Fórum. Para ambas soluciones, los comandos recibidos del lector sin contacto se enviarán al elemento seguro para su procesamiento. Esta implementación permite el mismo nivel de alta seguridad para las transacciones que las que brindan las soluciones de tarjetas inteligentes sin contacto.

Estos modos de funcionamiento están disponibles al mismo tiempo que el dispositivo NFC Fórum genera periódicamente durante un período breve un campo de RF para detectar un dispositivo remoto. El dispositivo NFC Fórum iniciará un modo de operación Lector / Escritor, *Peer-to-Peer* o Carga inalámbrica en caso de que se detecte un dispositivo remoto. El resto del tiempo, el dispositivo NFC Fórum escucha las solicitudes de comunicación de los dispositivos lectores remotos sin contacto o los dispositivos NFC Fórum y responde a sus solicitudes de comunicación. (NFC Fórum, 2020).

Según Albiñana, Cardona, Ferrer (2012) afirman que en el 2006 “NFC Forum” anuncio las primeras cinco especificaciones para NFC son:

- *NFC Data Exchange Format (NDEF)*
- *NFC Record Type Definition*
- *NFC Uniform Resource Identifier Service Record Type Definition*
- *NFC Text Record Type Definition*
- *NFC Smart Poster Record Type Specification.*

2.2.7.1 NDEF (NFC Data Exchange Format)

Define el formato de intercambio de información pudiendo estar compuesto por uno más registros, como se muestra en la figura 2.4 formando de esta manera un mensaje NDEF.

	NDEF message				
R_1 MB=1	...	...	...	...	R_n ME=1

Figura 2.4: Registro NDEF. Por NFC Forum

El primer registro en el mensaje NDEF contiene el mensaje de Begin (flag MB =1bit) y el último registro contiene el mensaje END (ME = 1bit). En la figura 2.5 se puede observar que el primer registro (índice de 1) tiene el flag MB, mientras que el último registro del mensaje (índice n) ha establecido el flag ME que También señala que el mensaje es la que tiene el principio hacia la izquierda y el fin hacia la derecha. Si el mensaje contiene un registro sólo entonces MB y ME se establecen al inicio y al final del mismo registro. (NFC Forum,2020)

El formato NDEF o *NFC Data Exchange Format* es un formato común registrado por el NFC Forum para poder compartir datos entre los dispositivos NFC y las etiquetas. Por lo tanto, las etiquetas que son leídas o escritas utilizando este formato, se les conoce como etiquetas NDEF o etiquetas NFC.

NDEF propone una forma de organizar el contenido almacenado en bytes en la etiqueta que viaja de un dispositivo a otro. Se caracteriza por poseer una cabecera de datos, denominada cabecera NDEF a partir de la cual se encuentran los bloques de información. Cada bloque de información se agrupa en registros que contienen a su vez los datos agrupados en mensajes NDEF y caracterizados por un tipo MIME definido. (NFC Forum, 2020)

Una de las desventajas del formato NDEF es que la totalidad de los bloques de información son accesibles por todos los dispositivos NFC ya que la clave empleada para acceder a estos datos es la clave por defecto (en hexadecimal: FF FF FF FF FF FF). Por tal razón datos escritos previamente en una etiqueta RFID por un dispositivo NFC puedan ser borrados o sobrescritos con otra información en cualquier momento y por cualquier dispositivo. Si esto supusiera un inconveniente, podría ser solventado combinando las ventajas de los formatos NDEF y MIFARE en el que se pone de manifiesto la existencia de claves de acceso. (Chavarría, 2011)

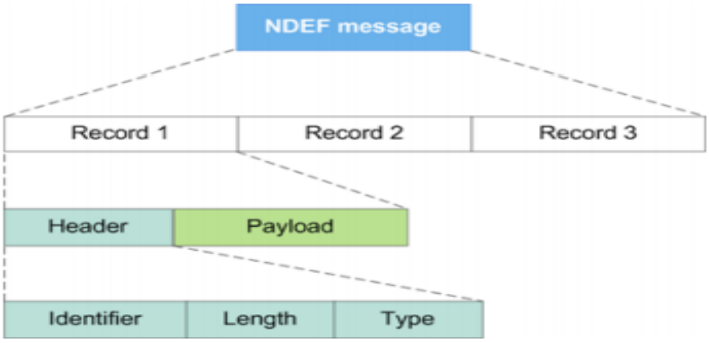


Figura 2.5: estructura de un mensaje NDEF. Por NFC Forum.

Este formato es soportado por la totalidad de dispositivos NFC y constituye un estándar para el intercambio y almacenamiento de información. Por ejemplo,

para el desarrollo de aplicaciones NFC en dispositivos móviles NFC usando el estándar NDEF existen un gran número de APIs o librerías que proporcionan los medios necesarios para su desarrollo.

2.2.7.2 NFC Record Type Definition (registry NDEF)

La especificación NDEF define el formato común de la información, pero no especifica ninguno en detalle. Esta especificación esta por separado.

Cada NDEF contiene una cadena con el nombre del tipo registro, cada RTN (*Records Type Name*) se puede especificar en diferentes formatos como puede ser *MIME Types*, *URIs* o tipos NFC conocidos.

Los tipos conocidos por NFC Forum contienen un identificador (NID) “nfc.” Nadie puede utilizar este identificador para especificar otro espacio de este tipo. Existen de dos tipos, locales y globales.

Los tipos externos son usados por organizaciones que deseen asignar un espacio de nombres que utilizaran para sus propios fines. El tipo externo es similar al conocido, pero tiene otro identificador (por ejemplo 'ext.') y se usa para determinar su espacio de trabajo. (NFC Forum, 2020).

2.2.7.3 NFC Forum URI Record Type (RTD)

NFC URI es el tipo de registro que es usado por NDEF para recibir la URI de la (figura 2.6) almacenada en una etiqueta de un elemento como pudiera ser un póster inteligente. RTD puede ser considerado como una extensión de un tipo reconocido por NFC y por ejemplo el código es (0x03) y el campo URI contiene “www.unaweb.com” el dispositivo recibirá “https://www.unaweb.com” mientras que si fuera (0x04) será “http://www.unaweb.com”.(NFC Forum)

Name	Offset	Size	Value	Description
ID Code	0	1 Byte	URI ID Code	ID code of URI
URI	1	N	UTF-8 String	URI

Offset	Content	Description
0	0 × D1	SR = 1, TNF = 0 × 01, MB = 1, ME = 1
1	0 × 01	Length of record type
2	0 × 13	Size of payload
3	0 × 55	NFC well-known record type URI (U)
4	0 × 01	URI Identifier (http://www.)
5	0 × 6D 0 × 6f 0 × 62 0 × 69 0 × 6C 0 × 65 0 × 72 0 × 61 0 × 64 0 × 69 0 × 63 0 × 61 0 × 6C 0 × 73 0 × 2E 0 × 63 0 × 6f 0 × 6D	String "mobileradicals.com" in UTF 8

Figura 2.6: Estructura de un Campo URI (0x55) y una URL como registro URI. NFC.

2.2.7.4 Text Record

Es de texto plano o simple sin ningún formato y puede ser utilizado en combinación con otros campos para proporcionar una información extra de contenido de la etiqueta.

Como el texto de esta etiqueta puede ser sobrescrito por agentes externos la especiación recomienda usarlo solo para propósitos informativos, es decir no vincularlos a ninguna otra acción. (NFC Forum, 2020)

2.2.7.5 Smart Poster

El tipo Smart Poster define la capacidad de añadir metadatos a la URI (cosa que RTD no podía hacer). Una etiqueta Smart poster al acercar el teléfono (o PDA / Tablet) sobre ella puede proporcionar acciones a realizar embebidas como parte del registro, que desencadenen acciones a realizar por parte del dispositivo como iniciar el navegador en una determina URL, etc.

Los datos enviados a través de NDEF del Smart Poster es un conjunto de múltiples mensajes de registros NDEF. Una etiqueta de Smart Poster puede llevar una o más de los siguientes componentes: (NFC Forum, 2020)

- Campo *Title*: Opcional y puede ser usado más de una vez. Este registro es una instancia de Text_RTD.

- Campo URI: Es una extensión del campo URI añadiendo metadatos a la URI, forma parte del núcleo del registro de la etiqueta y no puede ser repetido (una sola URI por campo de smart Poster).
- Campo *Action*: Es opcional y se usa para desencadenar acciones como lanzar el navegador, etc.
- Campo *Icon*: Es opcional y se puede usar para incluir una o más imágenes tipo MIME para que el dispositivo las guarde, por ejemplo, para visualizar una imagen en la URI del navegador.
- Campo *Size*: Opcional e indica el tamaño del contenido. Útil usado con una combinación del tipo para que el dispositivo determine si puede o no referenciado.
- Campo *Type*: Opcional y se usa para determinar si el dispositivo este capacitado (en combinación con el campo size) para acceder al objeto externo o no.

2.2.8 Fases de la comunicación en NFC

La comunicación NFC consta de cinco fases las cuales describe Chavarría, (2011) y son importantes para la comunicación entre dispositivos ya que tienen una función específica y siempre están presentes en el establecimiento de esta. Estas etapas son: [Broseta, 2012]

a) **Descubrimiento:** En esta fase los dispositivos inician la etapa de rastrearse el uno al otro y posteriormente su reconocimiento.
b) **Autenticación**: En esta parte los dispositivos verifican si el otro dispositivo está autorizado o si deben establecer algún tipo de cifrado para la comunicación.
c) **Negociación:** En esta parte del establecimiento, los dispositivos definen parámetros como la velocidad de transmisión, la identificación del dispositivo, el tipo de aplicación, su tamaño, y si es el caso también definen la acción a ser solicitada.
d) **Transferencia:** Una vez negociados los parámetros para la comunicación, se puede decir que ya está realizada exitosamente la comunicación y ya se puede realizar el intercambio de datos.

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

2.3 SEGURIDAD EN NFC

La tecnología NFC es relativamente segura por la característica de su rango de alcance que es limitado a unos pocos centímetros.

Un dispositivo pasivo, que no genera su propio campo de radio frecuencia, es mucho más difícil intervenir que un dispositivo activo. Las principales amenazas son esquemas de fraude teóricos aplicables a cualquier tecnología inalámbrica que incluyen determinadas particularidades. (Ceballos, 2013)

2.3.1 Principales riesgos y amenazas de seguridad

NFC por sí sola no asegura comunicaciones seguras, no ofrece protección contra los que se dedican a escuchar comunicaciones y es también vulnerable a modificación de datos. Las aplicaciones deben usar protocolos criptográficos para establecer un canal seguro. Sin embargo, esto se contrarresta con la distancia de operación necesaria de NFC, ya que las transacciones sólo se pueden activar en un rango de acción muy limitado lo que limita seriamente el uso de la tecnología sin conocimiento del usuario.

La sencillez y simplicidad, por tanto, de la interacción “aproximación del dispositivo” lleva inherentemente las características de confianza y seguridad. Además, al ser de corto alcance, evita los errores de comunicación, asegura una mayor eficacia en la transmisión de datos y hace que el posible deba estar dentro de ese corto rango, en el que el usuario podría darse cuenta fácilmente. (Campa, 2011)

2.3.2 Escuchas no autorizadas

Al ser una comunicación radio en un entorno compartido, y si dichas comunicaciones no van cifradas a nivel de enlace, un atacante podría ser capaz de escuchar u observar el contenido de la comunicación NFC.

Una ventaja a favor de NFC sería la corta distancia de alcance (del orden de 10 cm o menor). Dependiendo de una serie de factores (geometría de la antena, calidad del receptor, calidad de decodificador de la señal, la configuración del escenario, etc.) se determina que, si el dispositivo que envía los datos está en modo activo, se escuchara la comunicación desde una distancia aproximada menor a 10 cm., por el contrario, si el dispositivo que envía los datos está en modo pasivo, la distancia se reduce sustancialmente hasta aproximadamente 1 cm.

2.3.3 Corrupción de datos

Consiste en un ataque de denegación de servicio (DoS) en el que se modificarían los datos con intención de impedir la comunicación entre dispositivos.

Los dispositivos NFC contrarrestan estos ataques, ya que comprueban el campo de radiofrecuencia mientras están transmitiendo datos. Si un dispositivo NFC hace esto, será capaz de detectar el ataque. La potencia que se necesita para alterar los datos es significativamente más grande que la potencia que se detectada por el dispositivo NFC. Por lo tanto, el ataque puede ser detectable. (Ceballos, 2013)

2.3.4 Inserción de datos

Esto significa que el atacante es capaz de insertar mensajes dentro de los datos intercambiados por dos dispositivos. Pero esto solo es posible si el dispositivo que responde necesita mucho tiempo para responder. El atacante podría enviar sus datos antes que el dispositivo correcto. La inserción solo se efectuará si los datos a insertar son transmitidos antes que el dispositivo correcto empiece con la respuesta. Si ambos datos se solapan, los datos se corromperán.

Existes tres posibles contramedidas. La primera es que el dispositivo que responde lo haga sin retraso. En este caso, el atacante no puede ser más rápido que el dispositivo correcto, pero si los dos dispositivos responden al mismo tiempo se recibirán datos no correctos. La segunda sería escuchar al dispositivo que responde por un canal concreto. (Ceballos, 2013)

2.3.5 Clonación

Una nueva tarjeta se crea con el mismo contenido que la original; no obstante, las etiquetas o tarjetas más caras disponen de mecanismos adicionales de prevención de lectura de los contenidos, y por tanto serán más difíciles de leer y por tanto de realizar una clonación exacta. Para aquellas etiquetas o tarjetas que no ofrezcan estos mecanismos, o se conozca algún ataque que las vulnere se puede aplicar en un servidor un listado de tarjetas negras o clonadas que deberían ser verificadas.

Las etiquetas se utilizan para identificar a las máquinas expendedoras y permite que los clientes paguen utilizando el teléfono móvil. Un ejemplo de clonación es que el atacante clone la etiqueta de una máquina y ponga en otra. Después volver a la primera máquina y esperar a que alguien utilice la etiqueta clonada para luego pagar, de esta manera, el pago iría a la primera máquina y el atacante obtendrá el producto pagado por otro. (Ceballos, 2013)

2.3.6 Componentes de seguridad

Los principales componentes de un dispositivo móvil NFC son una antena incorporada en el interior del teléfono, el chip NFC y el denominado elemento seguro que es un chip con características de seguridad similares a las encontradas en las tarjetas inteligentes y que se encarga de procesar de forma segura las transacciones sin que otro dispositivo interfiera, además por la distancia mínima de contacto la hace más segura y confiable. (Ceballos, 2013)

2.3.7 ISO/IEC 27001

La norma ISO 27001, creada por la *International Organization for Standardization* (ISO), tiene por objeto proporcionar una metodología universal para la implementación, administración y mantenimiento de la seguridad de la información dentro de una organización.(Siles,2009)

- Una auditoría ISO 27001 demuestra la conformidad de su Sistema de Gestión de la Seguridad de la Información (SGSI) con los estándares documentados.

- Por lo general es utilizada por organizaciones que quieren demostrar la madurez de su seguridad de la información.
- Satisface las obligaciones contractuales y puede ayudar a obtener una exclusividad competitiva frente a su competencia.

La norma ISO 27001 es un instrumento base para la gestión de la seguridad de la información, estructurándose en un conjunto de controles y de recomendaciones dirigido a los responsables de promover, implantar y mantener la seguridad en las entidades. Mediante ella las empresas pueden certificar sus Sistemas de gestión de Seguridad de la Información (SGSI). Un SGSI es un sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información en función de los requisitos técnicos, legales y organizativos identificados en la organización.(Siles, 2009)

Toda norma que regule la materia de seguridad de la información, tiene como finalidad asegurar los tres requisitos básicos:

- **Confidencialidad**. Exclusivamente las personas autorizadas a disponer de la información pueden acceder a ella.
- **Integridad**. La información ha de encontrarse operativa tal y como se encuentra en los sistemas de información. No ha de ser manipulada ni en su origen, ni en su destino, salvo por aquellas personas autorizadas.
- **Disponibilidad**. El acceso continúo a la información, en cualquier momento, por aquellas personas autorizadas a tratar y disponer de aquella.

Los tres requisitos precedentes son los pilares para asegurar la información y cualquier proceso que haga uso de esta como por ejemplo, la normativa de firma electrónica, el funcionamiento del D.N.I. electrónico, las medidas de seguridad en materia de protección de datos de carácter personal, etc. (Laura ,2017)

Pasos para un control de acceso

- Identificación se refiere a las cosas como nombres de usuario y tarjetas de identificación, siendo el medio por el cual un usuario del sistema identifica quienes son, realizado generalmente al iniciar sesión.
- Autenticación es el uso de las contraseñas, reconocimiento de voz, y escáneres biométricos son métodos comunes de autenticación. Verificando la identidad de usuario.

- Autorización verifica los permisos del usuario para saber si está autorizado a utilizar el sistema.

2.4 ANDROID

Android es un sistema operativo pensado para teléfonos móviles inteligentes que está basado en kernel Linux, un sistema operativo libre y multiplataforma. Siendo este el principal responsable de la enorme demanda de equipos inteligentes ya que su mercado se ha expandido no solo para teléfonos sino también para televisores Smart, relojes y algunos modelos de coches.

Este sistema operativo es de código libre, y para su desarrollo se utiliza el lenguaje de programación que tiene el mismo nombre. Este lenguaje está basado en el lenguaje de programación de java y tiene una serie de herramientas de desarrollo llamadas, kit de desarrollo de software, más conocida por sus siglas SDK (Software Development Kit).

2.4.1 Aplicaciones Android

La mayoría de las aplicaciones Android se encuentran disponibles en Google Play, aunque también existen desarrolladores que crean aplicaciones que se pueden encontrar en sitios web independientes. En este último caso, es recomendable estar seguro de que el sitio web en cuestión es confiable para evitar la instalación de virus o malware en general en los dispositivos Android.

En la actualidad existe un gran número de desarrolladores que escriben aplicaciones específicas para la plataforma Android hasta el punto de que el número de aplicaciones que puedes encontrar actualmente supera las 400.000.

2.4.2 Características de Android

Android es una plataforma neutral en cuanto al desarrollo de aplicaciones, es decir, el programador tiene las mismas posibilidades para crear una aplicación que Google o que cualquier empresa. La siguiente lista destaca las características funcionales más importantes de Android:

- Amplia variedad de diseños (VGA, librerías de gráficos 2D y 3D, etc.)
- Almacenamiento de datos en BBDD SQLite.
- Mensajería (SMS y MMS).
- Navegador Web.
- Máquina virtual de Java.
- Soporte de formatos (MPEG-4, H.264, MP3, AMR, JPEG, PNG, GIF).
- Soporte para hardware adicional (cámaras de vídeo, pantallas táctiles, GPS, acelerómetros, etc.).

Entorno de desarrollo (emulador, herramientas de depuración, perfiles de memoria y funcionamiento, plugin para Eclipse IDE).

Además de las características más funcionales, existen otro tipo de características que es necesario nombrar y hacen de Android un sistema operativo especial. (Broseta, 2012)

Plataforma realmente abierta: es una plataforma de desarrollo libre basada en Linux y de código libre. Se puede usar el sistema sin pagar regalías.

- Portabilidad asegurada: al desarrollar las aplicaciones en Java, y gracias al concepto de máquina virtual, las aplicaciones podrán ser ejecutadas en gran variedad de dispositivos tanto presentes como futuros.
- Arquitectura basada en componentes inspirados en internet: por ejemplo, las interfaces se hacen en XML, lo que permite el uso de una misma interfaz en dispositivos de pantallas dispares.
- Filosofía de dispositivo siempre conectado a internet.

- Gran cantidad de servicios incorporados: Reconocimiento y síntesis de voz, localización basada en GPS y torres de comunicación, potentes bases de datos, NFC, etc.
- Alto nivel de seguridad: los programas se encuentran aislados unos de otros. Cada aplicación dispone de una serie de permisos que limitan su rango de actuación.
- Alta calidad de gráficos y sonido: gran variedad de formatos soportados.

2.4.3 Arquitectura de Android

En las siguientes líneas se dará una visión global por capas de cuál es la arquitectura empleada en Android. Figura 2.7. Cada una de estas capas utiliza servicios ofrecidos por las anteriores, y ofrece a su vez los suyos propios a las capas de niveles superiores.

Android utiliza el núcleo de Linux 2.6 como una capa de abstracción para el hardware disponible en los dispositivos móviles. Esta capa contiene los drivers necesarios para que cualquier componente hardware pueda ser utilizado mediante las llamadas correspondientes.

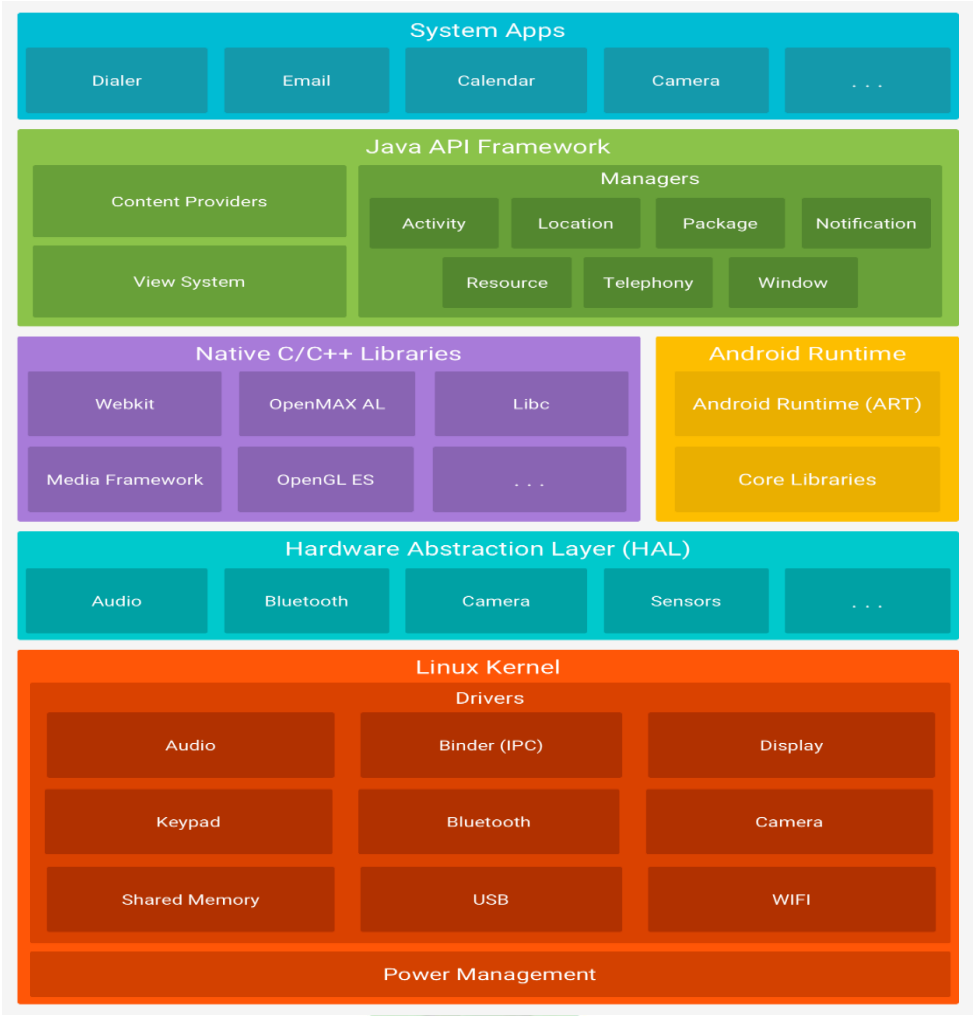


Figura 2.7: Arquitectura Android.
Fuente: Android developers,2020.

Siempre que un fabricante incluya un nuevo elemento de hardware, lo primero que se debe realizar para que pueda ser utilizado desde Android es crear las librerías de control o drivers necesarios dentro de este kernel de Linux embebido en el propio Android. (Android developers,2020).

2.4.3.1 *Kernel* de Linux

La base de la plataforma Android es el *kernel* de Linux, para la generación de subprocesos y la administración de memoria de bajo nivel, permitiendo que Android aproveche funciones de seguridad claves. (Android developers,2020)

2.4.3.2 Capa de abstracción de hardware (HAL)

Son estándares que exponen las capacidades de hardware del dispositivo al marco de trabajo de la API de Java de nivel más alto. La HAL consiste en varios módulos de biblioteca y cada uno de estos implementa una interfaz para un tipo específico de componente de hardware, como el módulo de la cámara o de Bluetooth. (Android developers,2020)

2.4.3.3 Tiempo de ejecución de Android

Para los dispositivos con Android 5.0 (nivel de API 21) o versiones posteriores, cada app ejecuta sus propios procesos con sus propias instancias del tiempo de ejecución de Android (ART – *Android RunTime*). Para ejecutar varias máquinas virtuales en dispositivos de memoria baja ejecutando archivos DEX, un formato de código de bytes diseñado especialmente para Android y optimizado para ocupar un espacio de memoria mínimo. (Android developers,2020)

2.4.3.4 Bibliotecas C/C++ nativas

La plataforma Android proporciona API del marco de trabajo de Java para exponer la funcionalidad de algunas de estas bibliotecas nativas a las apps. Por ejemplo, puedes acceder a OpenGL ES a través de la API de OpenGL de Java del marco de trabajo de Android para agregar a tu app compatibilidad con los dibujos y la manipulación de gráficos 2D y 3D.

Si desarrollas una app que requiere C o C++, puedes usar el NDK de Android para acceder a algunas de estas bibliotecas de plataformas nativas directamente desde tu código nativo. (Android developers,2020)

2.4.3.5 Marco de trabajo de la Api de java

Todo el conjunto de funciones del SO Android está disponible mediante API escritas en el lenguaje Java. Son cimientos que se necesita para crear apps de

Android simplificando la reutilización de componentes del sistema y servicios centrales y modulares, como los siguientes (Android developers,2020):

- Un sistema de vista enriquecido y extensible para compilar la IU de una app; se incluyen listas, cuadrículas, cuadros de texto, botones e incluso un navegador web integrable.
- Un administrador de recursos que te brinda acceso a recursos sin código, como strings localizadas, gráficos y archivos de diseño.
- Un administrador de notificaciones que muestra alertas personalizadas en la barra de estado.
- Un administrador de actividad que administra el ciclo de vida de las apps y proporciona una pila de retroceso de navegación común.
- Proveedores de contenido que permiten que las apps accedan a datos desde otras apps, como la app de Contactos, o compartan sus propios datos.

2.4.3.6 Apps del sistema Android

En Android se incluye un conjunto de apps centrales para correo electrónico, mensajería SMS, calendarios, navegación en Internet y contactos, entre otros elementos. Las apps incluidas en la plataforma no tienen un estado especial entre las apps que el usuario elije instalar; por ello, una app externa se puede convertir en el navegador web, el sistema de mensajería SMS o, incluso, el teclado predeterminado del usuario. (Android developers,2020)

2.4.4 ANDROID NFC

Es una forma de enviar y recibir datos NFC en forma de mensajes NDEF y describe las API de marco de trabajo de Android. Existe dos casos prácticos importantes para tener en cuenta al trabajar con datos NDEF y Android:

- Lectura de datos NDEF de una etiqueta NFC

- Transmisión de mensajes NDEF de un dispositivo a otro con Android Beam

La lectura de los datos NDEF de una etiqueta NFC se realiza con el sistema de envío de etiquetas, que analiza las etiquetas NFC detectadas, categoriza los datos de forma apropiada y, luego, inicia una aplicación que está interesada en los datos categorizados. Una aplicación que desea controlar la etiqueta NFC escaneada puede declarar un filtro de intento y solicitar el manejo de los datos.

La función Android Beam permite que un dispositivo envíe un mensaje NDEF a otro cuando los dispositivos están físicamente en contacto. Esta interacción proporciona una forma más sencilla de enviar datos que otras tecnologías inalámbricas, como Bluetooth, ya que con NFC no se requiere la sincronización ni la detección manual de dispositivos. (Android developers,2020)

2.4.4.1 Sistema de envío de etiquetas NFC

Por lo general, los dispositivos con tecnología Android buscan etiquetas NFC cuando la pantalla está desbloqueada, cuando un dispositivo con Android descubre una etiqueta NFC, el comportamiento deseado es hacer que la actividad más adecuada maneje el *intent* sin preguntarle al usuario qué aplicación usar.

Android proporciona un sistema especial de envío de etiquetas que analiza las etiquetas NFC escaneadas y trata de ubicar las aplicaciones que están interesadas en los datos escaneados haciendo lo siguiente: (Android developers,2020)

- Analizando la etiqueta NFC y averiguando el tipo MIME o un URI que identifica la carga útil de datos en la etiqueta
- Encapsulando el tipo MIME o URI y la carga útil en un *intent.* Estos dos primeros pasos se describen en Cómo se asignan las etiquetas NFC a los tipos MIME y los URI.

- Iniciando una actividad basada en el *intent*. Esto se describe en cómo se distribuyen las etiquetas NFC a las aplicaciones.

2.5 METODOLOGÍAS DE DESARROLLO

Tras una reunión llevada a cabo en febrero del 2001, nace el concepto de metodologías de desarrollo ágil aplicado al desarrollo software. La principal meta era conseguir que los proyectos de software no se dilaten y exista una gestión de cambios de tal manera que sean accesibles a cambios durante el desarrollo. Esto en respuesta a las metodologías de desarrollo de aplicaciones tradicionales, definidos por su carácter rígido e intolerantes en el sentido de la documentación. (Ramos, 2014)

La aparición de estas metodologías "ágiles" aparentemente fue un reflejo del alto número de proyectos que terminan en el fracaso o se toman más tiempo del estimado y la calidad no mejorada ni explotada por parte de proyectos de desarrollo de software. Una vez asentados estos conceptos se establece *The Agile Alliance14*, propuesta a extender la nueva noción de Desarrollo de software "Ágil" destacando la creación de conceptos contenidos en el Manifiesto Ágil, conceptos y valores primordiales como: (Ramos, 2014)

- "El individuo y las interacciones del equipo de desarrollo están por encima del proceso y las herramientas. Construir un buen equipo y que éste configure su propio entorno de desarrollo en base a sus necesidades".
- "Desarrollar software que funciona más que conseguir buena documentación. No producir documentos a menos que sean necesarios de una forma inmediata. Si el software no funciona, los documentos no valen de nada".
- "La colaboración con el cliente es más importante que la negociación de contratos. Tiene que haber una interacción constante entre el cliente y el equipo de desarrollo".
- "La respuesta ante el cambio es más importante que el seguimiento de un plan. La planificación no debe ser estricta sino flexible y abierta, la

habilidad de responder a los cambios que surjan determina el éxito o fracaso del proyecto".

2.6 METODOLOGÍAS AGILES PARA EL DESARROLLO DE SOFTWARE MÓVIL

Aunque existen un amplio número de metodologías de desarrollo de software ágiles, ninguna se ha centrado en el entorno y en la caracterización que el desarrollo de software para móviles necesita. Pero lo que sí se puede apreciar es que dichas metodologías coincidan con ciertos valores o criterios apreciables al desarrollo dirigido para plataformas móviles. (Ramos, 2014)

En forma de un análisis comparativo, se presenta la igualdad de criterios de los métodos ágiles sobre el desarrollo de software para móviles partiendo de una motivación lógica, que se muestra en la Tabla 2.1.

Características ágiles	Motivación lógica	En el caso del desarrollo para plataformas móviles
Alta volatilidad del entorno	Debido a la alta frecuencia en el cambio que sufren los requerimientos, tendremos menos necesidad de diseño y planificación inicial y mayor necesidad de desarrollos incrementales e iterativos.	Alta incertidumbre, entornos dinámicos, cientos de nuevos terminales cada año

Tabla 2.1: Metodologías agiles para el desarrollo móvil – análisis comparativo

Aunque la forma de desarrollar aplicaciones para un entorno o plataformas móviles no está exenta de los problemas presentados con el desarrollo de aplicaciones convencionales, se ha estimado que la corta duración del desarrollo que las plataformas móviles exigen es relativamente corta. Esto interviene a la hora de optar por una metodología específica de desarrollo. (Ramos, 2014)

El mayor beneficio de una metodología específica para el desarrollo es sin duda la organización de tareas, sistematización del procedimiento y sobre todo un

modelo estático y predictivo que nos informe intuitivamente la situación del proyecto en cualquier período de tiempo en que nos lo preguntemos. A continuación, vamos a analizar una serie de metodologías aplicables, bajo los criterios antes mencionados, para el desarrollo de aplicaciones móviles:

2.6.1 Desarrollo ágil: programación extrema (XP).

Formulado y creado inicialmente por Kent Beck es el más destacado de los procedimientos ágiles de desarrollo de software. La programación extrema se diferencia de metodologías tradicionales en que se encarga de la adaptabilidad y la previsión a la gestión de cambios y temas relacionados a la metodología.

Adeptos a esta metodología aseguran que los cambios de requerimientos no es algo fuera de lo común, es más, siempre han sido considerados y algunas veces hasta deseados a diferencia de otras prácticas. Se pretende que una gestión de cambios activa en cualquier punto del proyecto representa y simboliza una aproximación más realista que definir todos los requerimientos al comienzo y sobre invertir energías en tratar de controlar la gestión de cambios en dichos requerimientos. (Ramos, 2014)

Esta metodología tiene cinco valores mencionados a continuación:

a) Simplicidad.

   En este valor se basa toda la programación extrema, se agiliza el desarrollo y se facilita el mantenimiento al tratarse de una implementación sencilla. Aunque se trata en esta metodología de cuidar la simplicidad, las sucesivas modificaciones del código y de su diseño hacen que aumente la complejidad.

   Refactorizando el código, se mantiene este principio mientras el código crece con las múltiples modificaciones. Asimismo, la simplicidad se mantiene en la documentación, juntamente con el desarrollo del código se comenta en justa medida y sin sobre

esforzarse, manejando estándares de tal manera que se cuide la auto documentación de dicho código.

b) Comunicación.

La comunicación es primordial y mejor mostrada cuando el código es simple. Si el código es complejo, debe esforzarse y tratar a toda costa de hacerlo inteligible.

Las pruebas unitarias de una u otra forma transmiten información acerca del diseño de sus clases y de ciertos métodos al mostrar formaciones concretas de cómo utilizar la funcionalidad. Gracias a la programación en parejas, la comunicación se muestra constantemente entre desarrolladores.

c) Retroalimentación (*feedback*).

Mientras el cliente, según la filosofía de la metodología, esté al tanto del desarrollo dentro del proyecto, su opinión y su perspectiva del mismo es considerado en tiempo real. Las iteraciones cortas hacen que se muestren tanto los resultados y su proyección en el proyecto en el instante que está ocurriendo. El desarrollo y planificación de pruebas tienen embebido este valor a través de su especificación, por ejemplo, las pruebas y análisis de resultados muestran la calidad y sobreestima del código dentro de la solución.

d) Coraje o valentía.

Este valor es fundamental para reconstruir código cuando sea necesario o cuando el requerimiento esbozado por el usuario amerite su replanteamiento. Con esto, se evita empantanarse en el diseño y a su vez estimar demasiado tiempo en su dedicación para la implementación. En el diseño también es fundamental a la hora de planificarlo para satisfacer las necesidades a corto plazo para estimar el tiempo y no centrarse en el trabajo a futuro.

La valentía también está asociada en la moral del desarrollador para desechar el código que no sirve o a su vez, ha perdido a través del tiempo su funcionalidad. Este valor se relaciona a pesar de cuanto esfuerzo, tiempo y recursos se hayan requerido para su implementación.

e) Respeto.

Valor fundamental y de carácter moral. Gracias a este existe un ambiente de respeto y armonía entre desarrolladores, como la implementación es colaborada se respeta el esfuerzo y los recursos usados por un desarrollador en un momento específico. Además, no se pueden hacer cambios, adiciones, modificaciones ni eliminación de código que implique que las pruebas fallen o que demore más trabajo en su construcción.

2.6.2 Desarrollo ágil: Scrum.

Más que una metodología, es un marco de trabajo para el desarrollo de software, bajo un proceso iterativo e incremental usado para ambientes de desarrollo basado en desarrollo ágil de software. Orientado inicialmente en gestión de procesos de desarrollo de software, puede ser usado en equipos de mantenimiento de software. (Ramos, 2014)

Scrum define un conjunto de roles y prácticas y se toma como un punto de partida para definir procesos de desarrollo, en los cuales, la estima de los recursos humanos es primordial. Scrum maneja varios roles dentro de la metodología como el *Scrum Master*, el *Product Owner* y en general, se hace referencia al equipo. (Ramos, 2014)

El *Scrum Master* es el encargado de la dirección del proyecto; mientras que el *Product Owner* se encarga de la gestión de los *stakeholders* o interesados del proyecto, tanto internos como externos, y el equipo de desarrollo encargado de

la implementación. Sus períodos iterativos denominados *sprint* comprenden un período entre una y cuatro semanas. Están conformados y designados por el equipo de desarrollo, este equipo definirá un entregable que será un incremento de software potencialmente utilizable. (Ramos, 2014)

El *Product Backlog* es un conjunto de requerimientos de alto nivel que poseen una prioridad definida y establecen los parámetros fijos y precisos enfocándose en el esfuerzo que se realizará. Este *Product Backlog* definirá las características de cada sprint y su realización. (Ramos, 2014)

El procedimiento se realiza desde el punto de vista del *Product Owner* que identifica los elementos que contendrá el *Product Backlog* y se los define en la reunión de *Sprint Planning*. El equipo analiza la cantidad de esfuerzo y se plantea si se puede o no realizar dicho trabajo en el siguiente *sprint*. Durante el desarrollo de *sprint* en ejecución, no se aceptan cambios dentro del tiempo que este durará, dando así la certeza de que la gestión de cambios se encuentra congelada durante el período de tiempo determinado que durará el *sprin*t.

Se permiten los equipos auto organizados dentro del desarrollo, considerando la comunicación verbal de los miembros y demás disciplinas dentro del proyecto. Una ventaja por sobre otras metodologías y procesos de desarrollo de software es que *Scrum* es muy fácil de aprender y requiere poco esfuerzo tanto de interesados en el proyecto como desarrolladores para utilizar inicialmente. La desventaja mayor indicada es que, aunque su gestión de cambios sea actualizada en gran medida y propuesta directamente por el cliente, no es tan flexible como otras metodologías ágiles de desarrollo de software. (Ramos, 2014)

2.6.3 Mobile-d

La metodología *Mobile – D* para el desarrollo de aplicaciones móviles tienen como objetivo conseguir ciclos de desarrollo muy rápidos en equipos muy pequeños para desarrollar software que funcione satisfaciendo una serie de requisitos para obtener productos de calidad. En la mayoría los sistemas operativos móviles van cambiando rápidamente debido a la competencia del

mercado, lo que demanda realizar aplicaciones en corto tiempo, razón por la cual se utilizará el presente método para el proyecto de investigación.

Amaya (2013) afirma que la metodología *Mobile-D* está basada en prácticas agiles como *Extreme Programming (XP), Cristal Methodologies y Rational Unified Process (RUP).* Este método tiene un ciclo de vida que se divide en cinco fases: exploración, inicialización, producción, estabilización y prueba del sistema (figura 2.8).

Figura 2.8. Ciclo de desarrollo Mobile – D adaptado de Amaya (2013), Metodologías ágiles en el desarrollo de aplicaciones para dispositivos móviles.

2.6.4 Fase de exploración

Siendo ligeramente diferente del resto del proceso de producción, se dedica al establecimiento de un plan de proyecto y los conceptos básicos. Por lo tanto, se puede separar del ciclo principal de desarrollo (aunque no debería obviarse). Los autores de la metodología ponen además especial atención a la participación de los clientes en esta fase. [Koskela, 2004].

Los objetivos del establecimiento del cliente son:

- Identificar al cliente participativo para el producto.

- Lograr el compromiso de los clientes identificados para la participación del proyecto.
- Definir el modo, tareas, funciones y responsabilidades del grupo de cliente.

2.6.5 Fase de inicialización

Los desarrolladores preparan e identifican todos los recursos necesarios. Se preparan los planes para las siguientes fases y se establece el entorno técnico (incluyendo el entrenamiento del equipo de desarrollo). Los autores de Mobile-D afirman que su contribución al desarrollo ágil se centra fundamentalmente en esta fase, en la investigación de la línea arquitectónica. Esta acción se lleva a cabo durante el día de planificación. Se agregan las observaciones, se identifican similitudes y se extraen soluciones viables para su aplicación en el proyecto. Finalmente, la metodología también contempla algunas funcionalidades nucleares que se desarrollan en esta fase, durante el día de trabajo.

Los objetivos de la fase de inicialización son los siguientes: [Koskela, 2004]

- Adquirir un buen conocimiento general del producto para el equipo del proyecto de los requisitos iniciales y descripciones de línea de arquitectura.
- Preparar los recursos físicos, técnicos y humanos, así como de los clientes comunicación, los planes del proyecto y todas las cuestiones fundamentales de desarrollo para que todos ellos están en plena preparación para la implementación de los requisitos seleccionados por el cliente durante las próximas fases del proyecto.

El patrón de fase de inicialización puede llevarse a cabo a través de las siguientes etapas en la figura 2.9:

Figura 2.9: ciclo de inicialización Mobile-D
Fuente: Koskela, 2004.

2.6.6 Fase de producción

Se repite la programación de tres días (planificación trabajo-liberación) se repite iterativamente hasta implementar todas las funcionalidades. Primero se planifica la iteración de trabajo en términos de requisitos y tareas a realizar. Se preparan las pruebas de la iteración de antemano (de ahí el nombre de esta técnica de *Test-Driven Development,* TDD). Las tareas se llevarán a cabo durante el día de trabajo, desarrollando e integrando el código con los repositorios existentes. Durante el último día se lleva a cabo la integración del sistema (en caso de que estuvieran trabajando varios equipos de forma independiente) seguida de las pruebas de aceptación. [Koskela, 2004]

Los objetivos son:

- Implementar la funcionalidad priorizada cliente para el producto.
- Se centran en la funcionalidad del núcleo fundamental de su ejecución a principios del incrementar para permitir múltiples ciclos de mejora.

Después de iteración 0, los criterios de ingreso son:

- La fase de iteración precedente ha sido completada.
- Se han identificado los requisitos funcionales más importantes.
- El equipo se ha reunido y ha sido entrenado para el método de desarrollo.
- El entorno de desarrollo ha sido establecido.

Después de iteraciones posteriores, los criterios de ingreso son:

- Precediendo la producción de iteración se completa.

Las etapas de la fase producción se presentan en la siguiente figura 2.10:

Figura 2.10: ciclo de producción Mobile – D
Fuente: Koskela,2004.

2.6.7 Fase de estabilización

Se llevan a cabo las últimas acciones de integración para asegurar que el sistema completo funciona correctamente. Esta será la fase más importante en los proyectos multiequipo con diferentes subsistemas desarrollados por equipos distintos. En esta fase, los desarrolladores realizarán tareas similares a las que debían desarrollar en la fase de "producción", aunque en este caso todo el esfuerzo se dirige a la integración del sistema. Adicionalmente se puede considerar en esta fase la producción de documentación. [Koskela, 2004]

Los objetivos del modelo fase estabilización son:

- Finalizar la aplicación del producto.
- Mejorar y garantizar la calidad del producto.
- Finalizar la documentación del producto.

Los criterios de ingreso:

- La fase precedente se ha completado. Esto significa que la funcionalidad esencial y valor de negocio del proyecto ha sido implementado y se muestra al cliente.

El modelo de la fase estabilización puede llevarse a cabo a través de las siguientes etapas. Figurar 2.11:

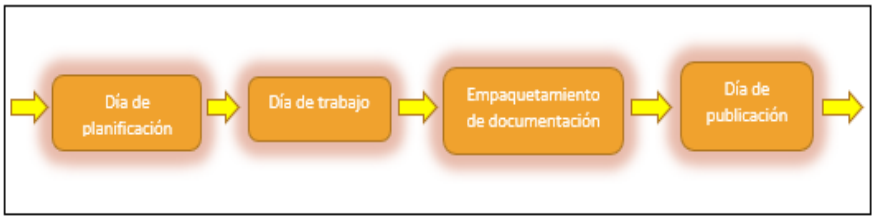


Figura 2.11: ciclo de producción Mobile – D
Fuente: Koskela,2004.

2.6.8 Prueba y corrección del sistema

Tiene como meta la disponibilidad de una versión estable y plenamente funcional del sistema. El producto terminado e integrado se prueba con los requisitos de cliente y se eliminan todos los defectos encontrados. [Koskela, 2004]

Los objetivos del sistema de prueba y corrección son:

- Pruebe el sistema en base a la documentación presentada en el proyecto
- Proporcionar información de los defectos encontrados
- Deje que el equipo de proyecto para planificar solución para los defectos encontrados
- Corregir los defectos
- Producir como error de sistema libre como sea posible

Los criterios de ingreso:

- Las fases anteriores necesitan ser terminado, por lo que la prueba puede llevarse a cabo con un sistema en funcionamiento.
- Roles definidos por el equipo de pruebas.

La siguiente figura 2.12 ilustra las etapas de las cuales el sistema de prueba y fase de corrección está compuesto:

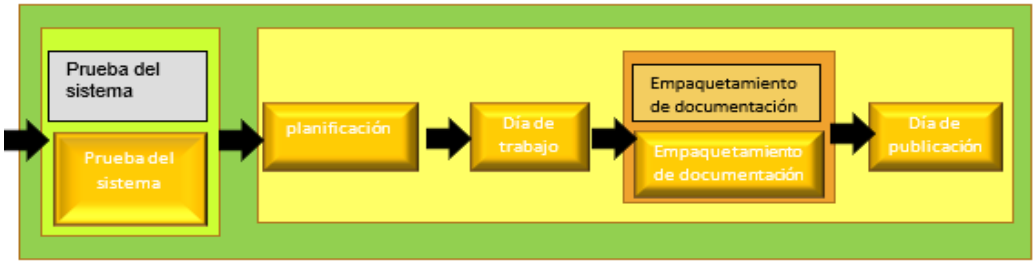


Figura 2.12: Ciclo fase prueba y corrección del sistema Mobile-D
Fuente: Koskela, 2004

CAPÍTULO III.

MARCO APLICATIVO

3.1 INTRODUCCIÓN

En el capítulo anterior se mencionó la metodología a desarrollar Mobile-d, la cual será de mucha utilidad para la construcción de este capítulo y así poder cumplir con los objetivos del proyecto.

En este capítulo se detalla los elementos de la aplicación móvil definiendo los aspectos esenciales del modelo de forma teórica. La aplicación móvil con tecnología NFC comunicación de corto alcance para la identificación de información del usuario a través de un código que genera este TAG-NFC (chip) el cual la aplicación detectara.

La administración del proyecto es importante, de tal manera que la programación extrema intenta definir rápidamente un plan global del sistema, desarrollar y liberar rápidamente el software y posteriormente revisarlo continuamente para incorporarles características adicionales que propone metodología Mobile-D.

3.2 DESARROLLO DE LA METODOLOGÍA MOBILE-D

- En la fase de inicialización se hace una documentación inicial en la cual se estudia los procedimientos a seguir desde el punto de vista del usuario definiendo los requerimientos que permite describir las funcionalidades de módulos de control y registró de información del usuario.
- En la fase de producción se repetirá iterativamente hasta implementar todas las funcionalidades del sistema. Las tareas se llevarán a cabo durante el día de trabajo, desarrollando e integrando los códigos.
- En la fase de estabilización se comprueba que los documentos de arquitectura, diseño y la interfaz de usuario incluyen los arreglos como parte de algunos modelos de documentos de software, aunque muchos simplemente serán descartados una vez que han cumplido su propósito para la aplicación móvil.
- Todas las historias, las tareas y los documentos tienen que hacerse por lo que la prueba puede ser ya realizada. El sistema desarrollado debe estar preparado para las pruebas junto a las descripciones de interfaz de usuario completando así las pruebas. Los defectos encontrados deben dar

prioridad a fin de que los defectos más graves se arreglen lo más antes posible.

- La última fase de prueba y reparación del sistema tiene como meta la disponibilidad de una versión estable y plenamente funcional del sistema tras las iteraciones ya echas. El producto terminado e integrado se prueba con los requisitos de cliente y se eliminan todos los defectos encontrados.

3.3 FASE DE EXPLORACIÓN

Esta fase se encarga de la planificación y el establecimiento del presente proyecto de desarrollo. Esta fase es de suma importancia para establecer las bases, la arquitectura, como también el entorno donde opera el sistema. Así mismo es necesario conocer y especificar las distintas partes o grupos necesarios para la continuidad del proyecto.

3.3.1 Propuesta del producto e historias de usuario

Se propone una aplicación móvil desarrollada con la metodología Mobile-D junto con la tecnología de comunicación de corto alcance NFC, la cual esta aplicación hará posible el control y registro de los participantes que asisten a un evento los cuales deben contar con tags o dispositivos con tecnología NFC.

El usuario de la aplicación móvil será el personal administrativo que este a cargo de un evento el cual debe tener acceso a un dispositivo móvil y tener instalada la aplicación.

3.3.2 Historias de usuario

La descripción del usuario será útil para el desarrollo de la aplicación móvil para el control de acceso a los diferentes eventos, en las tablas encuentra detallada las descripciones necesarias.

Tabla 3.1: Historia de usuario 1

HISTORIAS DE USUARIO	
Numero:1	Nombre historia: Registro del formulario
Usuario: Usuario móvil	Iteración asignada:1
Prioridad de negocio: media	Riesgo en desarrollo: media
DESCRIPCIÒN	
Almacenar la información y generar un código único para el control de acceso	

Tabla 3.2: Historia de usuario 2

HISTORIAS DE USUARIO	
Numero:2	Nombre historia: Ingreso de usuario
Usuario: Usuario móvil	Iteración asignada:2
Prioridad de negocio: media	Riesgo en desarrollo: alta
DESCRIPCIÒN	
El inicio de sesión en el dispositivo móvil debe tener un usuario y contraseña para poder ingresar a la aplicación.	

Tabla 3.3: Historia de usuario 3

HISTORIAS DE USUARIO	
Numero:3	Nombre historia: Validar
Usuario: Usuario móvil	Iteración asignada:3
Prioridad de negocio: alta	Riesgo en desarrollo: alta
DESCRIPCIÒN	
La aplicación realiza el reconocimiento del tag	

Tabla 3.4: Historia de usuario 4

HISTORIAS DE USUARIO	
Numero:4	Nombre historia: modificar
Usuario: Usuario móvil	Iteración asignada:4
Prioridad de negocio: alta	Riesgo en desarrollo: alta
DESCRIPCIÒN	
El administrador puede modificar los datos necesarios y los almacena en la aplicación.	

Tabla 3.5: Historia de usuario 5

HISTORIAS DE USUARIO	
Numero:5	Nombre historia: Buscar
Usuario: Usuario móvil	Iteración asignada:5
Prioridad de negocio: media	Riesgo en desarrollo: media
DESCRIPCIÒN	
Realiza una búsqueda por id de participante en la base de datos y muestra los resultados en pantalla	

Tabla 3.6: Historia de usuario 6

HISTORIAS DE USUARIO	
Numero:6	Nombre historia: Eliminar
Usuario: Usuario móvil	Iteración asignada:4
Prioridad de negocio: media	Riesgo en desarrollo: media
DESCRIPCIÒN	
Se realiza una búsqueda para ver si el participante está en la base de datos y eliminarlo.	

3.3.3 Requerimientos funcionales y no funcionales

Requerimientos funcionales

Los requerimientos funcionales sirven para poder definir el comportamiento interno del sistema y las funciones que podrá realizar. También sirve para describir los resultados producidos de acuerdo a las entradas. En este caso la lista a continuación muestra los requerimientos observados para la aplicación:

- La aplicación debe realizar un formulario de registro del participante
- La aplicación debe iniciar sesión con un usuario y contraseña
- La aplicación debe ser capaz de establecer conexión con otro dispositivo con tecnología nfc.
- La aplicación debe poder registrar los tags nfc.
- La aplicación debe eliminar o modificar datos de un participante.
- La aplicación debe permitir o denegar el acceso a un evento.
- El usuario debe restringir el ingreso dependiendo del paquete adquirido.

Requerimientos no funcionales

Los requerimientos no funcionales ayudaran a ver los aspectos del sistema visible para el usuario. Son criterios que juzgan el desempeño del sistema. Entre los requerimientos no funcionales se tiene los siguientes:

- La aplicación debe ser fácil de usar
- Las interfaces de la aplicación deben ser amigables e intuitivas
- La aplicación debe ser eficiente y eficaz
- La aplicación requiere que el dispositivo móvil cuente con nfc.

3.4 FASE DE INICIALIAZCIÓN

Para el desarrollo del sistema seguimos con la fase de iniciación, configurando y preparando los recursos necesarios, en esta fase se analizará todos los módulos que el sistema tendrá para su funcionamiento.

3.4.1 Establecimiento de recursos físicos y técnicos

En este punto se describirán las herramientas utilizadas para la implementación de la aplicación.

- **Plataforma Android**: La elección de esta plataforma se debe al gran porcentaje de mercado que utiliza un dispositivo móvil con el sistema operativo Android a nivel global ver figura 11.

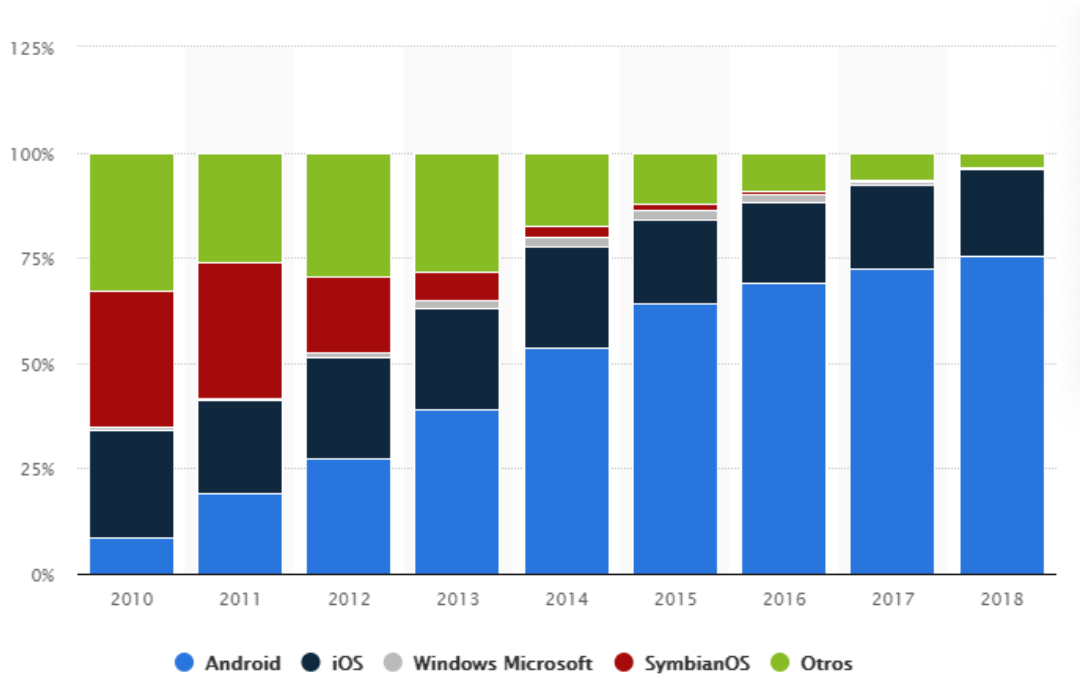


Figura 3.1: cuota de mercado de los sistemas operativos para teléfonos móviles 2010 a 2018
Fuente: Statista, 2021

Según las estadísticas para el año 2018 el sistema operativo más utilizado es Android con un porcentaje del 75,45% es por tal razón que se ha tomado en cuenta para el presente proyecto.

Para desarrollar la aplicación en el sistema operativo Android se hará uso de las siguientes herramientas:

- Android Studio 4.1
- Android SDK Tools versión 30.0.2
- Android SDK Platform Tools versión 30

- **Spring Boot:** es un recurso importante que facilita la creación de aplicaciones independientes para el desarrollo de las API REST servicios de backend y aplicaciones de Android.

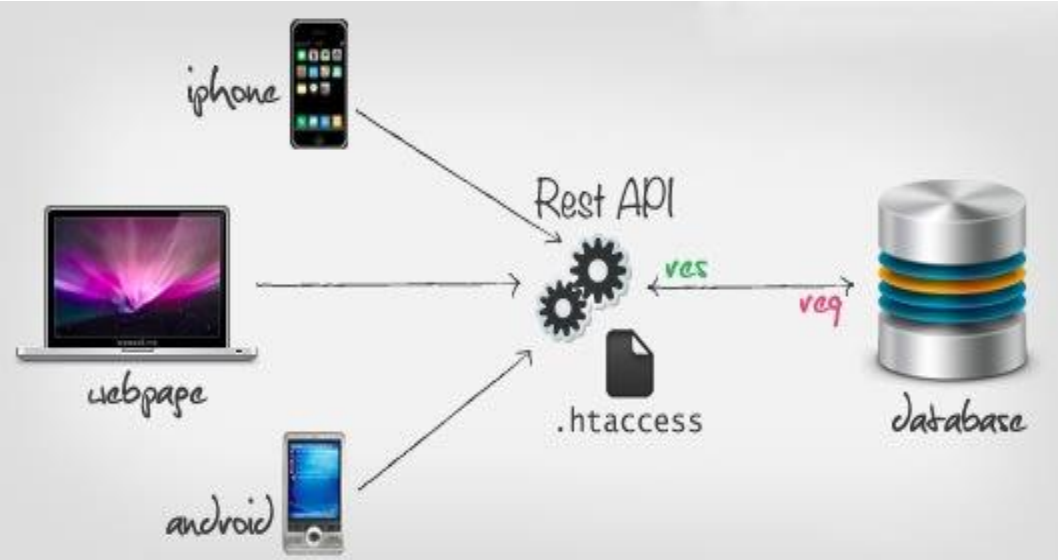


Figura 3.2: Modelo vista controlador
Fuente: Pkmuaz, 2016

  - Java versión 11
  - Spring Boot versión 2.4.3
  - Spring Boot Security
  - Maven 4.0

- **PostgreSQL**: recurso utilizado para la creación de la base de datos donde se almacena la información del usuario.

3.4.2 Modelo entidad – relación

Según los requerimientos ya expuestos en la fase uno se pudo elaborar el siguiente modelo entidad – relación en la figura 3.1

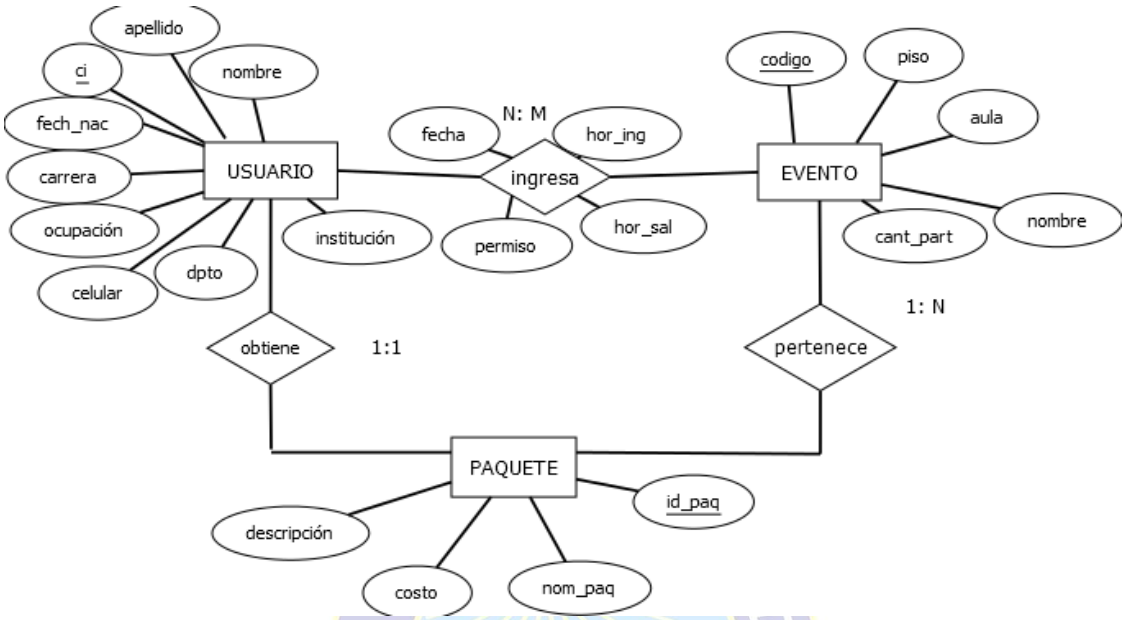


Figura 3.1: diagrama entidad relación

3.4.3 Diagrama de clases

Después de haber analizado y posteriormente elaborado la base de datos en Postgres, se pasa a la Elaboración de un diagrama de relación en DBeaver. Figura 3.2

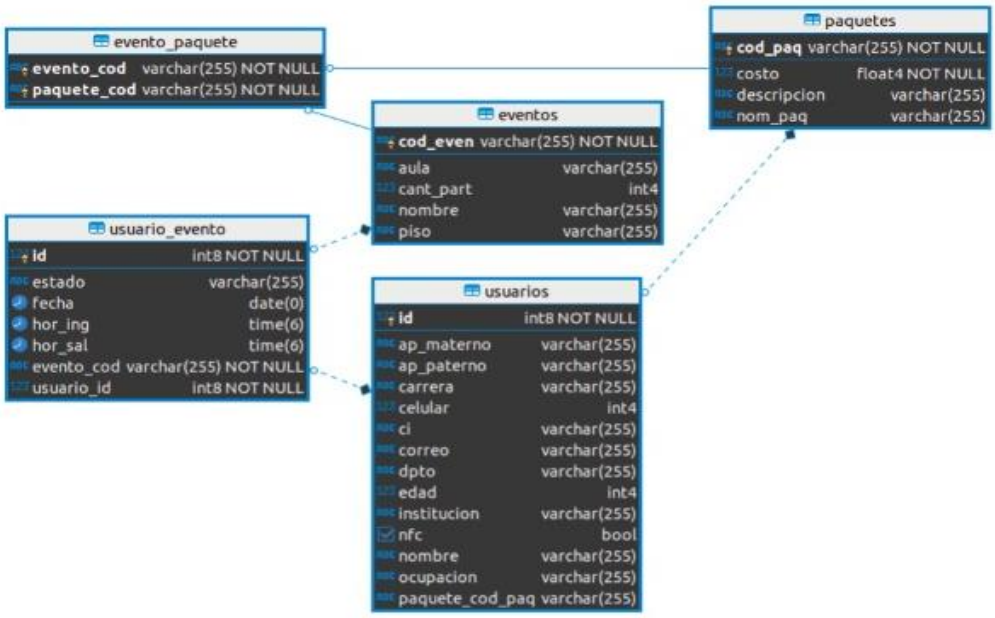


Figura 3.2: diagrama de clases

3.5 FASE DE PRODUCCIÓN

En esta fase se desarrolla el código para creación de la base de datos, el prototipo del sistema y las funcionalidades de la aplicación móvil.

3.5.1 Producto

Se puede observar en la figura 3.4 el prototipo del sistema mostrando la pantalla principal del usuario el cual solo podrá registrarse para acceder a los diferentes eventos dependiendo del paquete adquirido.

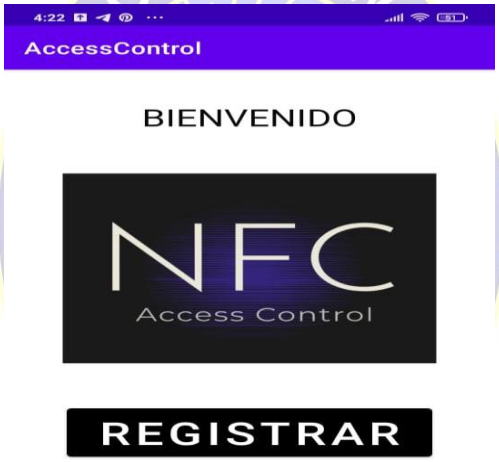


Figura 3.4. Pantalla principal

Para la figura 3.5 se muestra el formulario de registro del usuario, los datos almacenados en el formulario por cuestión de seguridad serán cifrados a la hora realizar el envió a la base de datos para evitar robo de información.

Figura 3.5. Pantalla de registro

También se realizó una segunda aplicación para la administración general del sistema, en la figura 3.6 la pantalla principal nos muestra un acceso diferente del sistema a diferencia de la primera aplicación es esta pantalla el administrador debe tener una usuario y contraseña únicos para poder acceder a la aplicación.

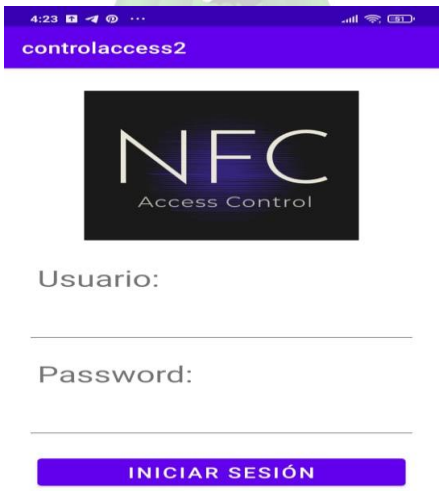


Figura 3.6. Pantalla principal 2

Esta segunda aplicación (figura 3.7) podrá eliminar a un usuario, modificar los datos del usuario en caso de algún error, añadir un nuevo usuario si es que tuvo algún problema a la hora de registrarse o mostrar los datos de todos los usuarios inscritos en el sistema, también podrá realizar el control de acceso a los diferentes eventos y tener un registro de la hora y fecha de cada usuario.

Figuran 3.7. Pantalla de control del sistema

3.6 FASE DE ESTABILIZACIÓN

En esta fase del proyecto como nos indica la metodología Mobile D llegamos a ensamblar todos los módulos del sistema en uno solo para su funcionalidad. Para a continuación llevar a cabo las diferentes pruebas al sistema de identificación y control.

En la figura 3.8 se puede observar el código para la creación de la interfaz móvil en la cual solo se realiza el registro del formulario.

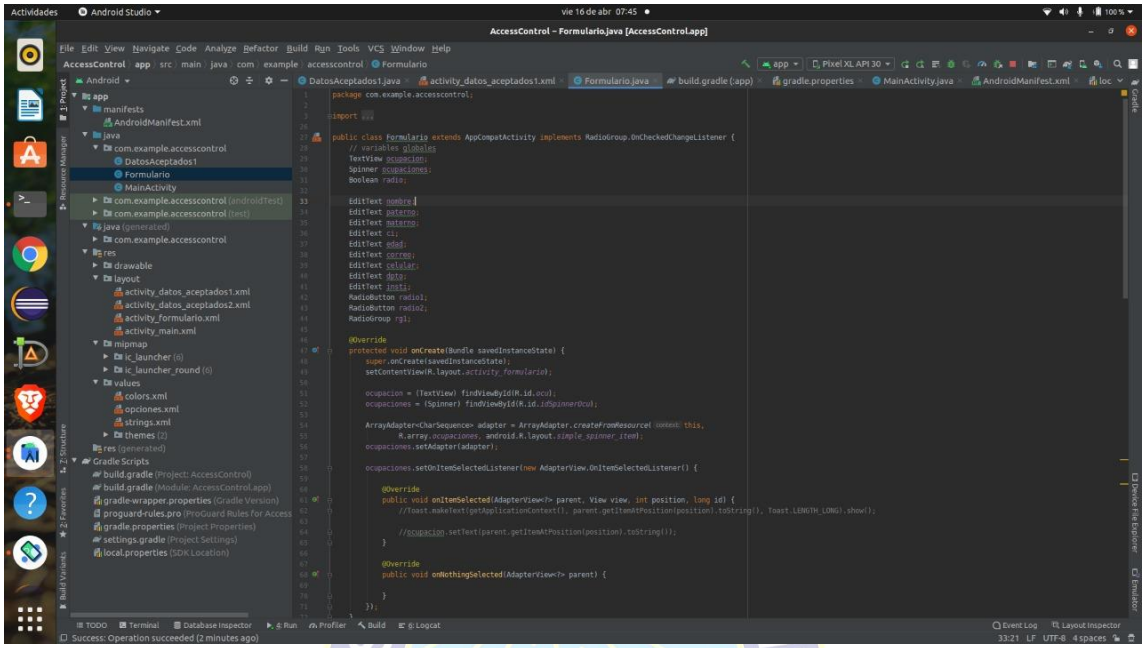


Figura 3.8: registro del formulario

En la figura 3.9 se observa el código de la interfaz del usuario para el control de acceso y además de los diferentes módulos implementados.

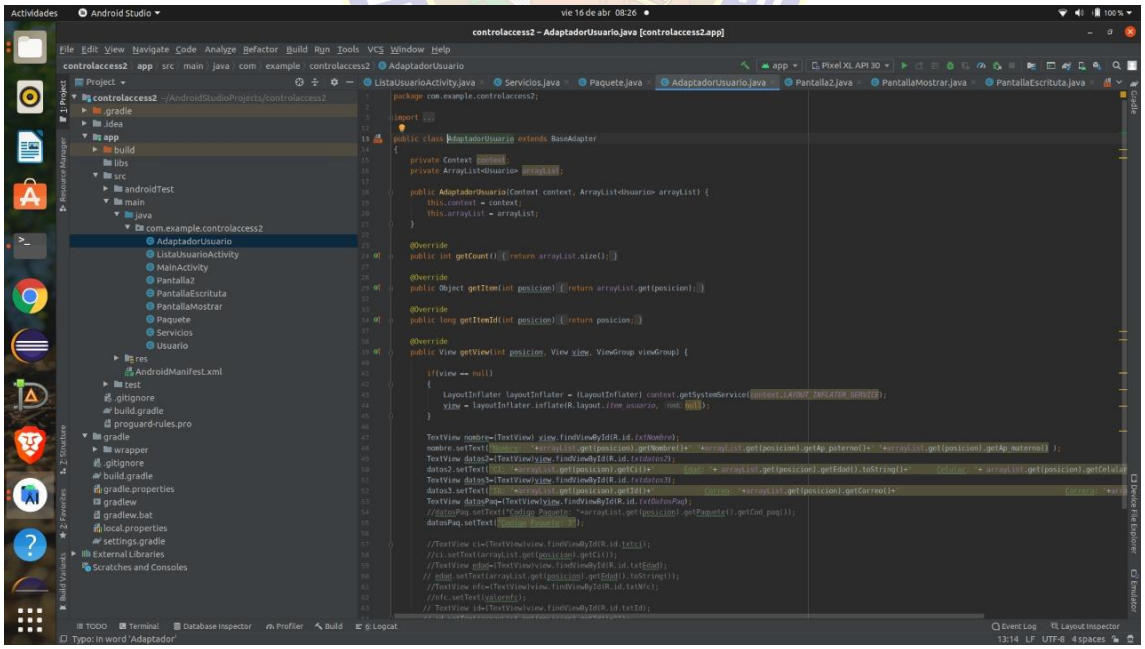


Figura 3.9 desarrollo de la interfaz de usuario con sus respectivos módulos

3.7 FASE DE PRUEBA

En esta fase del proyecto el sistema debe estar terminado ya con una estabilidad suficiente y requerida además de todos las APIS en Spring Boot para poder consumir los servicios desde Android, también se podrá observar la aplicación de Spring Security OAuth para la correcta identificación del usuario.

3.7.1 Identificación del tag NFC

Se puede observar en la figura 3.10 los datos recogidos en el momento de la aproximación de la tarjeta.

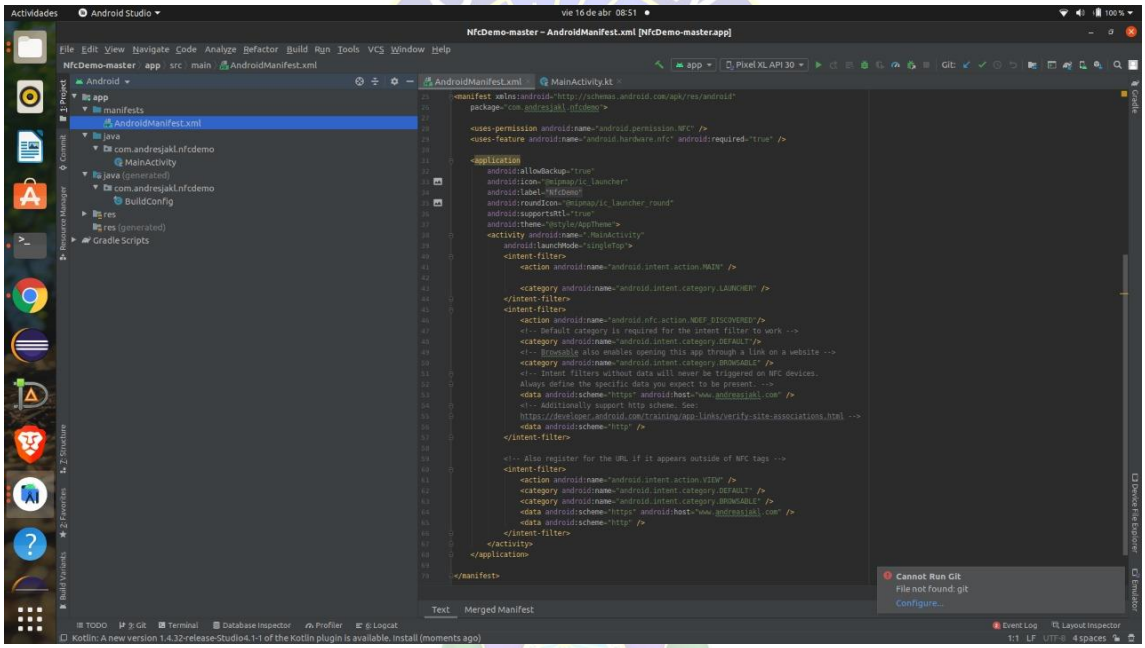


Figura 3.10. Identificación del tag NFC.

3.7.2 Conexión a la base de datos

En la figura 3.11 se puede observar la construcción del backend, la implementación de todos los servicios.

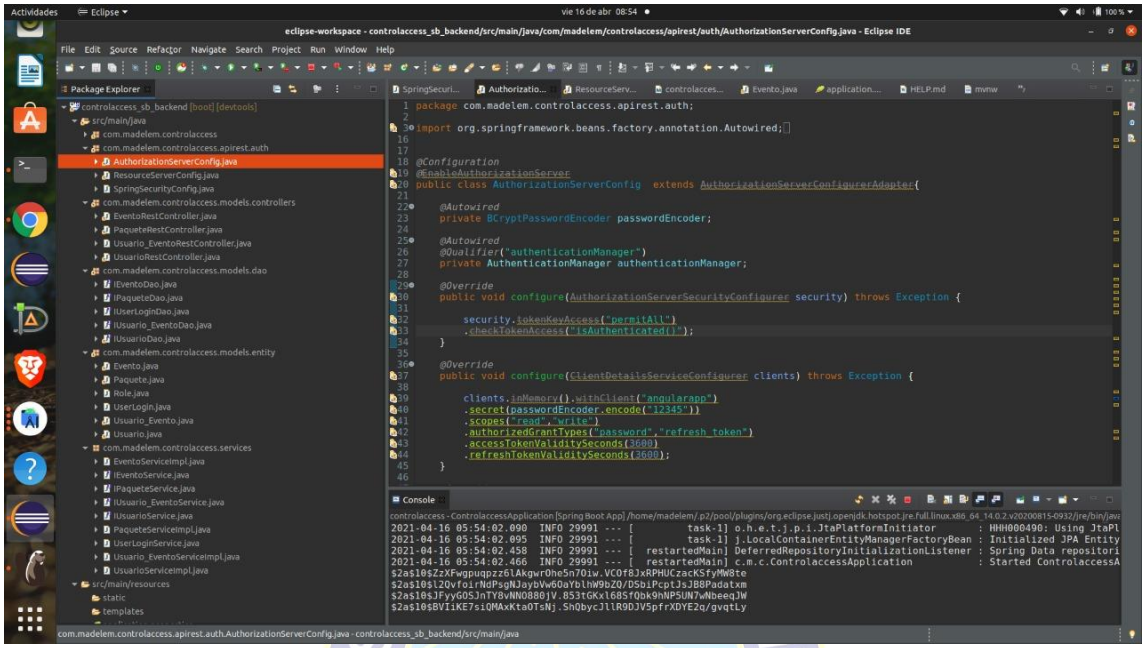


Figura 3.11: Implementación de los servicios.

3.7.3 Spring Boot Security

En la figura 3.12 se puede observar la implementación de la seguridad del usuario al ingresar a la base de datos.

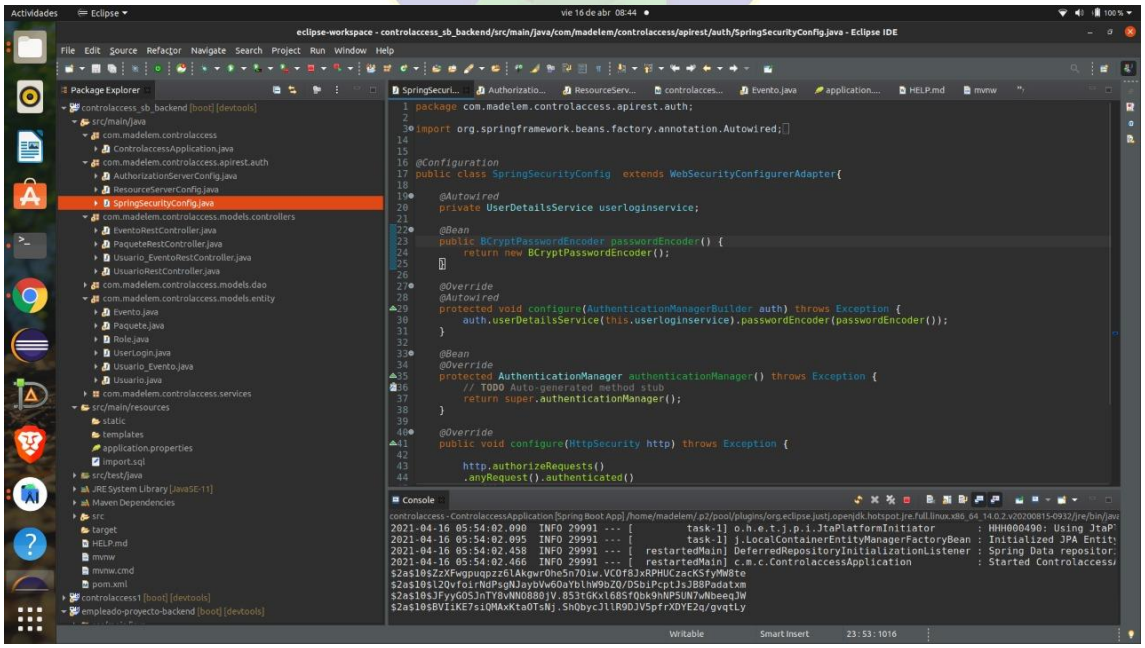


Figura 3.12: implementación de la seguridad para el usuario

Hasta este punto la aplicación debe estar desarrollada en su totalidad con sus respectivos módulos funcionando de manera eficiente como se muestra en la figura 3.13.

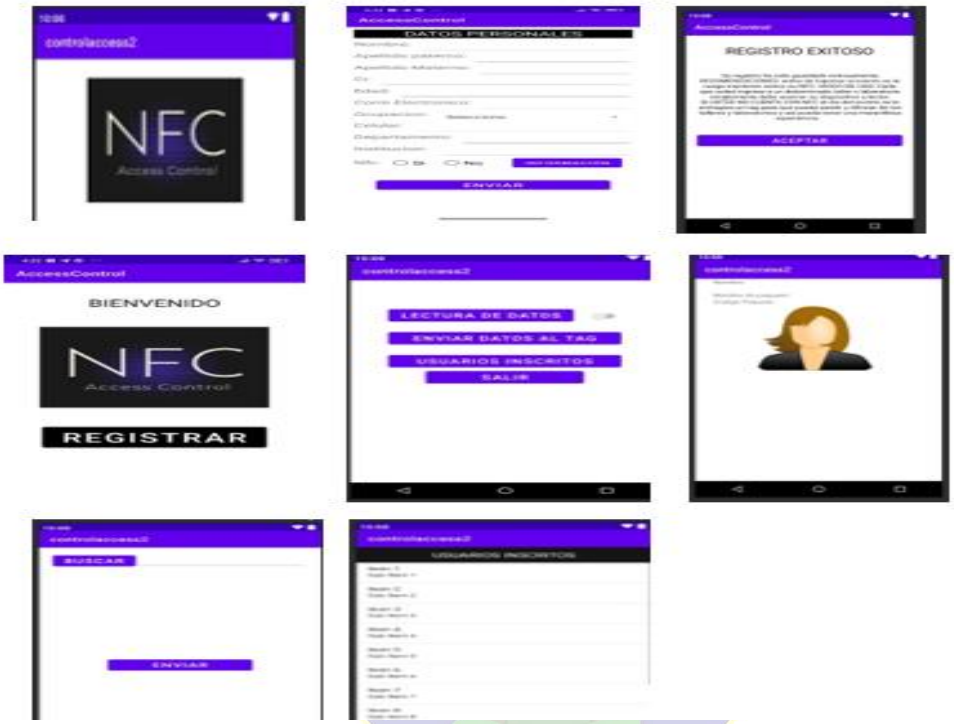


Figura3.13: prototipo final de la aplicación

CAPÍTULO IV.

PRUEBAS Y RESULTADOS

En esta etapa del proyecto para la comprobación del correcto funcionamiento y verificación de calidad de la misma se realizaron las pruebas respectivas para asegurar que la aplicación móvil funciona correctamente, Para esto se hicieron encuestas a los usuarios.

4.1 MÉTRICAS DE CALIDAD DEL PROYECTO

Son todas las pruebas que definen de una u otra forma la calidad del software, siendo los puntos críticos en el diseño, codificación, pruebas y mantenimiento, basada en las normas ISO 9126 que esta medida de acuerdo a su usabilidad, funcionalidad, confiabilidad, mantenibilidad y compatibilidad.

4.1.1 PRUEBA DE USABILIDAD

Permite evaluar el esfuerzo que debe tener el usuario para el manejo del sistema, el grado en el que el software es fácil de usar. En la tabla 4.1 se pude observar algunas preguntas respecto a la usabilidad del sistema. Para tal efecto se realizó las pruebas en 40 personas.

Tabla 4.1. Escala de valores para la usabilidad

ESCALA	VALOR
Extremadamente satisfecho	5
Muy satisfecho	4
Moderadamente satisfecho	3
Poco satisfecho	2
No satisfecho	1

Tabla 4.2. Usabilidad de la aplicación

Nro.	Características	Resultado
1	La aplicación es fácil de usar	5
2	Se puede realizar tareas de manera eficiente	5
3	Es atractivo a la vista	3
4	Los registros son eficientes y seguros	4
5	El tiempo de registro es eficiente	4
6	Considera que la aplicación es útil	5
	Total	4.33

Por tanto, la usabilidad de la aplicación está determinada por el promedio de las características anteriores en la tabla 4.2.

$$Usabilidad = \frac{5+5+3+4+4+5}{6} = 4.33 * \frac{100}{5} = 86.66\%$$

4.1.2 FUNCIONALIDAD

Es el grado en que el sistema satisface las necesidades indicadas. La eficiencia en la eliminación de defectos (EED) es una métrica que permite medir la habilidad de filtrar las actividades de la garantía de calidad y control. Esta se define de la siguiente manera:

$$EED = E/(E + D)$$

Donde:

E = Número de errores antes de la entrega del software.

D = Número errores después de la entrega.

El valor ideal de EED es 1, esto quiere decir que no se encontraron errores o defectos en el sistema.

En las pruebas antes de la entrega del Sistema se encontraron los siguientes errores.

1. El registro de un usuario es muy lento.
2. Muestra de manera infinita a un usuario.

3. No se cuenta con un nivel de seguridad en el registro de usuario y contraseña.
4. No se cuenta con un listado de eventos.
5. No se cuenta con registro de quien hizo la modificación de a un usuario.
6. Existe una demora al hacer la lectura del tag.
7. No reconoce el smartphone como tag solo le permite función de lectura.

Por tanto:

$$E = 8$$

Se encontraron con algunos defectos en los requerimientos después de la entrega de la entrega al cliente.

Se fueron desarrollando la solución de cada defecto, excepto la numero siete de los anteriores ya mencionados, por lo tanto, D=1, y reemplazando en la ecuación tenemos:

$$EED = 7/(7+1) = 0{,}875$$

Por lo que se pudo obtener un 87,5% de funcionalidad.

4.1.3 PRUEBA DE COMPATIBILIDAD

Para las pruebas de compatibilidad con NFC se aplicaron en dispositivos reales ya que el emulador de Android no incluye hardware virtual para NFC el cual nos permite poder realizar el control de acceso de manera eficiente, la aplicación para el registro a los diferentes eventos se realiza de manera eficiente en diferentes dispositivos móviles o Tablet que cuenten con Android superior o igual a 4.1.

4.1.3.1 ENCUESTA A USUARIOS

La presente encuesta se realizó con el fin de saber si los usuarios cuentan con la tecnología NFC en sus smartphones, esto es de gran importancia para tomar la decisión de optar por tags o tarjetas NFC que contaran con la misma funcionalidad.

Tabla 4.3. Tabla de resultados -1

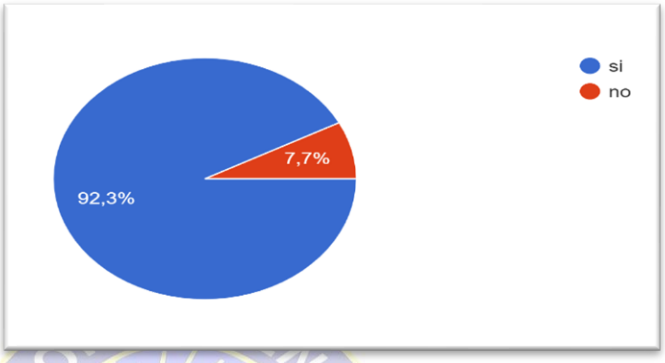
Pregunta	¿Usted cuenta con un smartphone?
Gráfico	
Objetivo	Determina la cantidad de usuarios que cuenta con teléfonos inteligentes lo que nos permite evaluar si la aplicación estará al alcance de la mayoría de los usuarios.

Tabla 4.4: Tabla de resultados -2

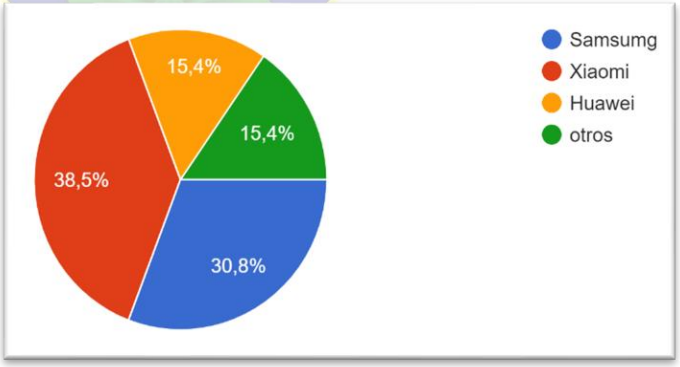
Pregunta	2. ¿Cuál es la marca de su smartphone?
Gráfico	
Objetivo	Se determinó que Xiaomi es la marca mas usada por los usuarios lo cual es beneficioso para la presente investigación ya que esta marca salió hace poco al mercado queriendo competir con marcas conocidas como Samsung e implantó NFC a su smartphone a precios económicos, lo que nos indica que NFC podría estar al alcance de todos los usuarios en poco tiempo.

Tabla 4.5. Tabla de resultados -3

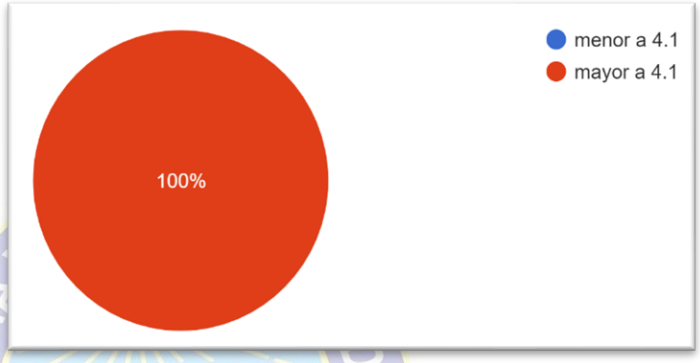
Pregunta	3. ¿Con qué versión de Android cuenta su smartphone?
Gráfico	
Objetivo	La pregunta se hizo con fin de saber si la aplicación estará al alcance de todos los usuarios, ya que como requisito para la aplicación es necesario contar con un Android superior a 4.1.

Tabla 4.6. Tabla de resultados – 4

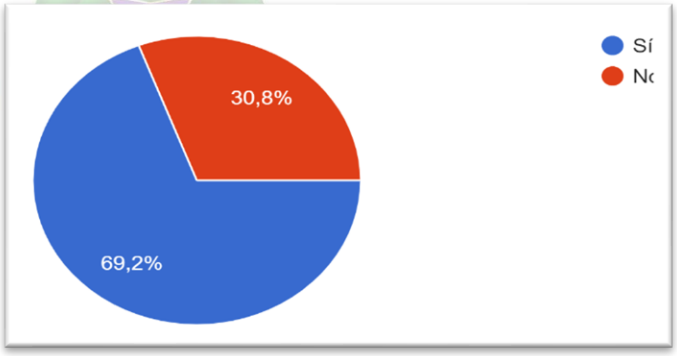
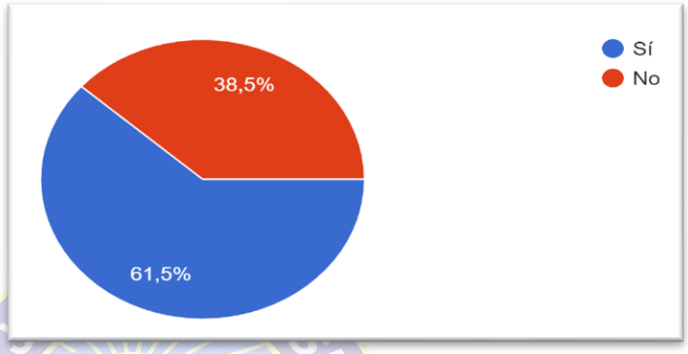
Pregunta	4. ¿Usted conoce acerca de la tecnología NFC?
Gráfico	
Objetivo	Determinar si el usuario se familiariza con la tecnología NFC para en un futuro se realizan diferentes investigaciones al respecto y así se pueda aprovechar los diferentes usos que se le pueda dar.

Tabla 4.7. Tabla de resultados – 5

Pregunta	5. ¿Usted cuenta con tecnología NFC en su dispositivo?
Gráfico	
Objetivo	Determina que existe una cantidad mínima que a pesar de tener un smartphone no cuentan con tecnología NFC.

4.2 SEGURIDAD

La seguridad una parte importante durante el desarrollo de la aplicación, la autentificación de usuarios y la encriptación de las contraseñas, la validación para los datos de entrada que tiene el sistema y finalmente la seguridad en la base de datos.

4.2.1 A NIVEL DE APLICACIÓN

En este proyecto se hizo la utilización del framework JSON que tiene las siguientes características en cuanto a seguridad.

Una de las principales preocupaciones de las codificaciones JSON es evitar la ejecución arbitraria de código remoto Javascript en el navegador o en el servidor.

Para evitarlo resulta vital usar un serializador JSON para codificar correctamente los datos enviados por el cliente y evitar la ejecución de código incluido dentro de la información introducida por el cliente.

La información que va en la url es susceptible de ser almacenada y hay que evitar como sea incorporar información sensible en la misma: como números de cuenta,

datos de la tarjeta, teléfono, email o incluso datos de salud personal así como datos asociados a la autenticación y autorización DOM tokens o password. (ciberseguridad ,2020)

4.2.2 AUTENTIFICACIÓN Y AUTORIZACIÓN

No todos los métodos HTTP realizan la misma funcionalidad ni todos los clientes de la API deben tener permiso y acceso a dichos métodos.

Es habitual que sobre un mismo recurso se exponen métodos de consulta como el GET y métodos con un rol operativo como POST, PUT, y DELETE siendo estas susceptibles de un control de acceso más estricto, ya que solo personas con permisos especiales como un gestor o los propios dueños de los datos las puedan realizar. (ciberseguridad ,2020)

Tipos de tokens y casos de uso

- Data token: En su forma serializada un JWT es muy compacto y fácil de transmitir en peticiones HTTP y se usa para el intercambio de datos.
- ID token: Emitido por un gestor de identidades, a petición de una aplicación cliente, tras haber autenticado a un usuario. Permite a la aplicación cliente obtener datos del usuario de manera confiable sin tener que gestionar sus credenciales.
- Access token: Emitido por un servidor de autorización, a petición de una aplicación cliente, y permite a esta el acceso a un recurso protegido en nombre de un usuario. Este token se usa como método de autenticación y autorización por parte de la aplicación cliente frente al servidor que aloja el recurso.

JWT permite el intercambio de datos de manera segura entre partes de manera más eficiente que otros estándares (SAML) debido a su menor tamaño, lo que lo hace ideal para los siguientes casos de uso:

- Intercambio de datos de sesión entre cliente y servidor: Debido a su mecanismo de serialización a veces son usados para transmitir información de sesión y estado entre el servidor y sus clientes. Se suelen usar » tokens inseguros» (sin firma).

- Autenticación federada: Elimina la necesidad de que las aplicaciones gestionen las credenciales de sus usuarios, delegando en un gestor de identidad de confianza el proceso de autenticación de los mismos. El gestor genera un token verificable por la aplicación que contiene los datos necesarios del usuario.
- Autorización de acceso: El token contiene la información necesaria para que un servicio de APIs pueda evaluar si la operación solicitada por el tenedor del token se puede permitir.

Cada caso de uso tiene distinto destinatario (aplicación cliente y servicio de API), pero en el caso de que se ejerza control simultáneo sobre las dos, un único token puede ser usado para ambos casos (ciberseguridad ,2020).

4.2.3 SEGURIDAD EN LA BASE DE DATOS

Todos los ficheros almacenados en la base de datos están protegidos contra escritura por cualquier cuenta que no sea la del súper usuario de Postgres. Y este es el único que pueda: Leer, escribir y ejecutar sin restricción.

El “Postmaster” que es el responsable de aceptar las comunicaciones con el cliente, autentificar y dar acceso. El “Postmaster” se encarga de la administración de los querys y comandos enviados por el cliente. Las conexiones de los clientes se pueden restringir por dirección IP y/o por nombre de usuario.

CAPÍTULO V.

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Hoy en día se puede encontrar una variedad de aplicaciones para el control de acceso en la Play Store, pero son pocas las que ofrecen movilidad y flexibilidad, la mayoría de proyectos o aplicaciones requieren de Arduino lo que implementa en gastos para el desarrollo del sistema. La aplicación desarrollada para la tesis no necesita contar con una infraestructura, únicamente requiere de un dispositivo con sistema operativo Android que tenga incorporado NFC.

La aplicación necesita que el dispositivo disponga de una conexión a internet para su uso, ya que la comunicación de la aplicación con la base de datos para el consumo de servicios será a través de Spring Boot.

Después del desarrollo de aplicación se puede evidenciar que se ha cumplido con cada uno de los objetivos planteados en la tesis.

- En el marco teórico se logró realizar la descripción de los principios básicos del uso y funcionamiento de la tecnología NFC y las herramientas útiles para el desarrollo del sistema.
- Con el uso de la tecnología NFC, se logró realizar un control de acceso a diferentes áreas con tan solo obtener el tag o el móvil con NFC y pasarlo por el lector para el despliegue la información del usuario y hacer las comprobaciones necesarias para permitir el acceso.
- Mediante la metodología de desarrollo Mobile-D se logró implementar un prototipo para el desarrollo del sistema y de esta manera cumplir con los requerimientos de inicio.
- Se logro centralizar toda la información en una base de datos de la aplicación móvil principal.

- La aplicación móvil desarrollada está preparada para adaptarse a diferentes tipos de terminales móviles que existen actualmente en el mercado. además, está preparada para ser utilizada desde una versión de Android 4.1 (Ice CreamSandwich), ya que la API mínima en la que se ha

creado el proyecto es la API 15, hasta la versión Android 7.1 (Nougat), el proyecto se ejecuta por defecto en una API 25.

5.2 RECOMENDACIONES

Se recomienda el desarrollo de un sistema web como complemento a la investigación realizada.

Para futuros proyectos de investigación se aconseja aprovechar al máximo las utilidades de la tecnología NFC, viendo la gran variedad de usos que se le puede dar como son los pagos sin contacto, control de acceso, cerraduras o la combinación del NFC con otras tecnologías como bluetooth, código QR o Arduino.

En vista de que la tecnología NFC tiene un bajo costo y un gran potencial se recomienda sea desarrollado para el área de salud en el control de sus pacientes, historias clínicas, y otros. Los cuáles serán de gran ayuda para la sociedad.

BIBLIOGRAFÍA

- Terra, “¿Qué es NFC?” ,2008. http://www.terra.es/personal/ccossio/tecnologiaNFC_2.htm [Última vista, octubre 2010]

- Chavarría Chavarría Daniel, A. (13 de 12 de 2011). http://eie.ucr.ac.cr. Recuperado el 2 de 9 de 2013, de http://eie.ucr.ac.cr: http://eie.ucr.ac.cr/uploads/file/proybach/pb2011/pb2011_012.pdf

- Vicente G. E. (2011) Desarrollo de una Aplicación de Control de Acceso y Sistemas de Identificación mediante la Tecnología NFC. [Proyecto de tesis. Ingeniería de Telemática]. Universidad Carlos III. Escuela Politécnica Superior.

- Arroyo G. I. (2014) Identificación y Control a Espacios controlados mediante teléfonos inteligentes y tecnología NFC [Tesis de grado. Mención Ingeniería de Sistemas]. Universidad Mayor de San Andrés.

- Ortega P. A (2018) Control de acceso NFC mediante autorización biométrica con smartphone. [Trabajo final. Master Universitario de Ingeniería de Telecomunicaciones]. Universitat Oberta de Catalunya.

- Vique, R. R. (2011). Métodos para el desarrollo de aplicaciones móviles. España: Universidad Oberta de Catalunya.

- Ramos R. J. (2014). “Tecnología de comunicación de corto alcance NFC bajo plataforma móvil para el control vehicular” [tesis de grado]. Universidad Mayor de San Andrés.

- Bauer, Friedrich L. (1972). "Ingeniería de software". Procesamiento de información. Págs. 71.

- M. V. Zelkovitz, A. C. Shaw y J. D. Gannon, Principles of Software Engineering and Design. Englewoods Clif, NJ, USA: Prentice-Hall, 1979.

- Amaya Y (2013) Metodologías ágiles en el desarrollo de aplicaciones para dispositivos móviles. Estado actual. Revista de Tecnología Journal Technology. Volumen 12. Págs. 111-124. https://www.academia.edu/9603029/Metodolog%C3%ADas_%C3%A1giles_en_el_desarrollo_de_aplicaciones_para_dispositivos_m%C3%B3viles_Estado_actual_Agile_methodologies_in_the_development_of_applications_for_mobile_devices_present_state

- arquitectura de la plataforma android (s.f.) Android. Android Development https://developer.android.com/guide/platform?hl=es-419

- Android – Historia de la Informática https://histinf.blogs.upv.es/2012/12/14/android/

- Acerca de la tecnología - Foro NFC (2020). NFC Forum. https://nfc-forum.org/what-is-nfc/about-the-technology/

- Albiñana, A. Cardona, E. Ferrer D (2012) https://histinf.blogs.upv.es/files/2012/11/HDI-Trabajo_NFC.pdf

- [Koskela, 2004] Koskela, Juha (2004). Release Project Process .Mobile-D [version 3.0]. 20050316

- [Broseta, 2012] Broseta Gutiérrez, Raúl (2012, septiembre). Dispositivos Móviles y NFC aplicados al cajero de tickets: BEEPVIP. Tesis de Master,Universidad Politécnica Valencia, valencia. Disponible en: http://riunet.upv.es/bitstream/handle/10251/18021/Raul_Broseta_TFM.pdf

ANEXOS

DOCUMENTACIÓN