



**FACULTAD DE CIENCIAS E INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA
DE SISTEMAS E INFORMÁTICA**

TESIS

**DISEÑO E IMPLEMENTACIÓN DE APLICACIÓN MULTIPLATAFORMA MÓVIL
CON FUNCIONES DE ENCRIPCIÓN Y PRIVACIDAD DE DATOS
ORIENTADA A LA SEGURIDAD ESTUDIANTIL DE LA UNIVERSIDAD
DE CIENCIAS Y HUMANIDADES, DISTRITO - LOS OLIVOS 2014**

**PRESENTADO POR
ALCÁNTARA CASTRO, JOSÉ LUIS**

**ASESOR
LAPA ASTO, ULISES SEMILIS**

Los Olivos, 2017



FACULTAD DE CIENCIAS E INGENIERÍA

**ESCUELA PROFESIONAL DE INGENIERÍA
DE SISTEMAS E INFORMÁTICA**

**DISEÑO E IMPLEMENTACIÓN DE APLICACIÓN
MULTIPLATAFORMA MÓVIL CON FUNCIONES DE
ENCRIPCIÓN Y PRIVACIDAD DE DATOS
ORIENTADA A LA SEGURIDAD ESTUDIANTIL DE LA
UNIVERSIDAD DE CIENCIAS Y HUMANIDADES,
DISTRITO – LOS OLIVOS 2014**

**TESIS
PARA OPTAR EL TÍTULO PROFESIONAL
DE INGENIERO DE SISTEMAS E INFORMÁTICA**

PRESENTADO POR:

ALCÁNTARA CASTRO, JOSÉ LUIS

ASESOR:

LAPA ASTO, ULISES SEMILIS

LIMA – PERÚ

2017

SUSTENTADO Y APROBADO POR LOS SIGUIENTES JURADOS:

JURADO 1
ANDRADE ARENAS,
LABERIANO MATÍAS
PRESIDENTE

JURADO 2
MELGAREJO SOLÍS,
RONALD ALFONSO
SECRETARIO

JURADO 3
GUEVARA JIMÉNEZ,
JORGE ALFREDO
VOCAL

ASESOR
LAPA ASTO,
ULISES SEMILIS

Dedicatoria

Por supuesto este trabajo está dedicado para mi madre María silvestre Cano de Alcántara que nos bendices desde los cielos.

Alcántara Castro, José Luis

Resumen

La solución propuesta en el presente trabajo, se muestra en el desarrollo de Yappo!, una aplicación de mensajería instantánea con encriptamiento de datos para Android, bajo entorno colaborativo, seguro y privado. Este proyecto surge como respuesta a la necesidad de los alumnos de emplear estos nuevos recursos tecnológicos con la finalidad de que tengan la posibilidad de interactuar, sugerir contenidos, resolver dudas, proponer debates en cualquier momento, bajo un canal seguro y sin comprometer la privacidad de los datos del usuario. Esta aplicación ha sido resultado de las necesidades propiamente experimentadas durante la carrera universitaria, sumado a un estudio realizado a los estudiantes que arrojó como resultado la necesidad de comunicarse con sus compañeros y docentes fuera de los horarios académicos; así como la importancia de que tengan un canal seguro donde puedan transferir y garantizar la privacidad de sus datos. El objetivo principal de este proyecto consiste en proveer una herramienta a los alumnos y docentes que les permita comunicarse con ciertas matrices de privacidad y seguridad, las cuales las diferenciaría del resto de aplicaciones que son duramente criticadas por falta de seguridad e intrusión a la intimidad de datos del usuario.

Palabras claves: Seguridad de datos, cifrado, *smartphone*, *android*, sistema operativo, servicio web, aplicación móvil, implementación, servicio web

Abstract

The solution proposed in this paper, the development of Yappo! an instant messaging application with data encryption for Android under collaborative environment, secure and private is shown. This project is a response to the need for teachers and students to use these new technological resources for the ability to interact, suggesting content, resolving doubts, proposing discussions anytime, under a secure channel without compromising privacy user data. This application was the result of actual needs experienced during college career, coupled with a study of students that resulted in the need to communicate with teachers outside the academic schedules the importance of a secure channel which can transfer and ensure data privacy. The main objective of this project is to provide a tool for teachers and students to enable them to communicate with certain matrices of privacy and security that differ from other applications that are widely criticized for lack of security and intrusion into the privacy of user data.

Key Words: data security, encryption, Smartphone, android, operating system, web service, Mobile Application, Implementation

Contenido

Resumen.....	iv
Abstract.....	v
Contenido.....	vi
Lista de tablas.....	x
Lista de figuras	xiii
INTRODUCCIÓN	1
CAPÍTULO I: ASPECTOS GENERALES.....	3
1.1. DIAGNÓSTICO DE LA ORGANIZACIÓN	4
1.1.1 Datos de la organización.....	4
1.1.2 Localización de la empresa	4
1.1.3 Diagnóstico estratégico	5
1.1.4 Cadena de valor	11
2.1 DEFINICIÓN DEL PROBLEMA DE INVESTIGACIÓN.....	13
2.1.1 Planeamiento y descripción del problema.....	13
2.1.2 Formulación del problema.....	14
2.1.3 Problema específico	14
2.2 DEFINICIÓN DE LOS OBJETIVOS DE LA INVESTIGACIÓN	14
2.2.1 Objetivo general.....	14
2.2.2 Objetivos específicos	15
2.3 JUSTIFICACIÓN DE LA INVESTIGACIÓN.....	15
2.3.1 Justificación tecnológica.....	15
2.4 ALCANCES Y LIMITACIONES	16
2.4.1 Alcances	16

2.4.2	Limitaciones	17
3.1	ANTECEDENTES	19
3.1.1	Antecedentes internacionales	19
3.2	MARCO TEÓRICO.....	24
3.2.1	Introducción a la seguridad informática	24
3.2.2	Conceptos básicos de la seguridad informática	24
3.2.3	Servidor <i>Web</i> /HTTP	39
3.2.4	Tecnología móvil	42
3.2.5	¿Qué es mi metodología?.....	55
3.3	Marco metodológico.....	69
3.4	Marco legal.....	70
3.5	ARQUITECTURA DEL SISTEMA O METODOLOGÍA.....	72
4.1	LEVANTAMIENTO DE INFORMACIÓN.....	76
4.1.1	Planificación del proyecto	76
4.1.2	Recopilación de información.....	84
4.2	MODELAMIENTO	96
4.2.1	Modelo de casos de uso de negocio.....	96
4.2.2	Planificación del sistema de la aplicación	104
4.3	HISTORIAS DE USUARIO	104
4.3.1	<i>Product backlog</i>	106
4.3.2	Especificación de requisitos	111
4.3.3	Catálogo de requisitos.....	112
4.3.4	Trazabilidad de requisitos – historias de usuario	121
4.3.5	Especificación de casos de uso.....	122
4.4	DESARROLLO	133

4.4.1	Diseño de la BD.....	133
4.4.2	Diseño de la Interfaz del sistema.....	141
4.5	APLICACIÓN	154
4.6	IMPLEMENTACIÓN.....	160
4.6.1	Instalación y configuración de YAPPO!	160
4.6.2	Manual de la aplicación	172
4.6.3	Capacitación a los usuarios	185
4.7	MONITOREO	190
4.7.1	Desarrollo de pruebas en producción	190
4.7.2	Lista y control de cambios	193
4.7.3	Reajustes y aprobación del usuario final.....	195
5.1	ANÁLISIS DE COSTOS	197
5.1.1	Costos de implementación.....	197
5.1.2	Costos de mantenimiento	199
5.1.3	Otros gastos.....	199
5.2	Análisis de Beneficios.....	199
5.2.1	Beneficios cuantitativo	199
5.2.2	Beneficios cualitativos	200
5.3	Análisis de sensibilidad	201
5.3.1	Desarrollo de flujo de caja.....	201
5.4	Análisis de VAN	203
5.4.1	Análisis del TIR.....	203
5.4.2	Análisis del ROI	204
	CONCLUSIONES	205
	RECOMENDACIONES	207

REFERENCIAS.....	208
GLOSARIO.....	215
ANEXOS.....	218

Lista de tablas

Tabla 1: FODA.....	8
Tabla 2: Diferencias Metodologías.....	83
Tabla3: ResolMin_ Información.....	73
Tabla 4: Metodología MMCPM.....	75
Tabla5: MCUN_Registro_Academico.....	99
Tabla 6: MCUN_Encar.Regis.Aca.....	100
Tabla 7: MCUN_Dep.Academico.....	100
Tabla 8: MCUN_Dep_Produccion.....	101
Tabla 9: MCUN_Direc_Academica.....	102
Tabla 10: MCUN_Dep.Sistemas.....	103
Tabla 11: Backlog historias de usuario	107
Tabla 12: Backlog_historias_usuario.....	108
Tabla 13: Plantilladerequisitos.....	113
Tabla 14: RF-001-Agregar contactos.....	114
Tabla 15: RF-002-Identificacion con FB.....	115
Tabla 16: RF-003-Responder mensajes.....	115
Tabla 17: RF-004-Listar mensajes.....	116
Tabla 18: RF-005-iniciar nueva sesión.....	116
Tabla 19: RF-006 Crear tarea nueva.....	117
Tabla 20: RF-007-Modificar tarea.....	117

Tabla 21: RF-008-Borrar tarea/nota.....	118
Tabla 22: RF-009-Crear grupo.....	118
Tabla 23: RF-010-Envio de ficheros.....	119
Tabla 24: RF-0011-Cerrar sesiones.....	119
Tabla 25: RF-0012-Recibir mensajes.....	120
Tabla 26: RNF-001-Dispositivos soportados.....	121
Tabla 27: RNF-002-Version-minima-de-la-plataforma.....	121
Tabla 28: Requisito RNF-003-Interfaz adaptativa.....	122
Tabla 29: TR_HU.....	123
Tabla 30: Descrip_Inic.....	126
Tabla 31: Descrip_ validación.....	128
Tabla 32: Descrip_ EnvioMensaje.....	129
Tabla 33: Descrip_ LecturaMensaje.....	130
Tabla 34: Descrip_ CreacionTarea.....	132
Tabla 35: DescriLectura_Tareas.....	133
Tabla 36: TR_RQ_CU.....	134
Tabla 37: Diseño_Tablas_Yappo.....	135
Tabla 38: capacitación de usuario.....	188
Tabla 39: Formato de asistencias.....	190
Tabla 41: Formato de usuario.....	191
Tabla 42: Casos de Prueba.....	193

Tabla 43: Control de cambios.....	196
Tabla 44: Reajuste de usuario final.....	197
Tabla 45: Usuario aprobar.....	197
Tabla 46: RRHH.....	199
Tabla 47: RRHH Hardware.....	199
Tabla 48: RR Software.....	200
Tabla 49: Costos de implementación.....	200
Tabla 50: Costos de variables.....	201
Tabla 51: Costos de otros gastos.....	201
Tabla 52: BE Cuantitativos.....	201
Tabla 53: BE Cualitativos.....	202
Tabla 54: Beneficios tangibles e intangibles.....	202
Tabla 55: Desarrollo de flujo de caja.....	203
Tabla 56: Análisis van.....	205
Tabla 57: Análisis TIR.....	205
Tabla 58: Análisis TOR.....	206

Lista de figuras

Figura 1: Localización de la Universidad	25
Figura 2: Análisis FODA	27
Figura 3: Organigrama Nominal	30
Figura 4: Organigrama Funcional	31
Figura 5: Cadena de valor	32
Figura 6: esquema de envío de información criptográfica	47
Figura 7: esquema de envío de información simétrica	48
Figura 8: esquema de envío de información asimétrica	49
Figura 9: esquema de envío de información híbrido	51
Figura 10: Esquema de funciones Hash	52
Figura 11: Esquema de algoritmo hash	54
Figura 12: Esquema de envío de información digital	55
Figura 13: Esquema de creación de firma	56
Figura 14: Esquema de verificación de firma digital	57
Figura 15: Certificado de seguridad	59
Figura 16: Detached Signature	59
Figura 17: Enveloping Signature	60
Figura 18: EnvelopedSignature	61
Figura 19 Criptografía esquema clave pública	62

Figura 20: Proceso de servidor web	67
Figura 21: Seguridad de plataformas Móviles	72
Figura 22: Seguridad de plataforma Android	76
Figura 23: Tipos de aplicaciones	76
Figura 24: aplicación web	77
Figura 25: Aplicación Nativa	78
Figura 26: Aplicación Híbrida	79
Figura 27: Sprint Scrum	85
Figura 28: HU Kanban	87
Figura 29: Tablero Kanban	88
Figura 30: SCRUMBAN	90
Figura 31: Arquitectura Yappo!	98
Figura 32: Metodología MMCPM	105
Figura 33: Plataformas más utilizadas	108
Figura 34: SO Mobile más vendidos	109
Figura 35: Actividades más realizadas en internet móvil	111
Figura 36: Grafico estadístico de formula población infinita	117
Figura 38: Grafico estadístico de la pregunta 1 a estudiantes	118
Figura 39: Grafico estadístico de la pregunta 2 a estudiantes	119
Figura 40: Grafico estadístico de la pregunta 3 a estudiantes	120
Figura 41: Grafico estadístico de la pregunta 4 a estudiantes	121

Figura 42: Grafico estadístico de la pregunta 5 a estudiantes	122
Figura 43: Grafico estadístico de la pregunta 6 a estudiantes	123
Figura 44: Grafico estadístico de la pregunta 7 a estudiantes	124
Figura 45: Grafico estadístico de la pregunta 8 a estudiantes	125
Figura 46: Grafico estadístico de la pregunta 9 a estudiantes	126
Figura 47: Grafico estadístico de la pregunta 10 a estudiantes	127
Figura 48: MCUN_Registro_Academico	128
Figura 49: MCUN_Encar.Regis.Aca	129
Figura 50: MCUN_Dep.Academico	130
Figura 51: MCUN_Dep_Produccion	131
Figura 52: MCUN_Direc_Academica	131
Figura 53: MCUN_Dep.Sistemas	132
Figura 54: MCUN_General	133
Figura 55: MCUN_GeneralCUS	134
Figura 56: Tablero Kanban	138
Figura 57: Tablero Kanban-Testeo-Finalizado	139
Figura 58: Tablero Kanban-Cola-de-espera	140
Figura 59: Tablero Kanban-Diseño-Desarrollo	142
Figura 60: DiagramaCUS	155
Figura 61: Pr_Inicio_sesion CUS	156
Figura 62: Pr_validacion	157

Figura 63: Pr_EnvioMensaje	159
Figura 64: Pr_LecturaMensaje	160
Figura 65: Pr_CreacionTarea	162
Figura 66: Pr_Lectura_Tareas	163
Figura 67: Diagrama_RE_BD	168
Figura 68: Prototype_Menu	175
Figura 69: Prototype_Anastasia	176
Figura 70: Prototype_Proyectos	177
Figura 71: Prototype_search	178
Figura 72: Prototype_DondeEstoy	179
Figura 73: Prototype_Inicio	180
Figura 74: Prototype_Lista_Contactos	181
Figura 75: Prototype_Lista_solicitudes	182
Figura 76: Prototype_Lista_MensajesNoleidos	183
Figura 77: Prototype_Interfaz_Chat	184
Figura 78: Prototype_Interfaz_Chat	185
Figura 79: Prototype_Agregar_Amistad	186
Figura 80: Prototype_Agregar_Amistad	187
Figura 81: Prototype_Grupos	188
Figura 82: Launch_Dispatch	189
Figura 83: Dispatch_Ignition	189

Figura 84: RunAs_Yappo	190
Figura 85: Splash_Yappo	190
Figura 86: Login_Yappo	191
Figura 87: Interf_Yappo	191
Figura 88: Interf_Chats	192
Figura 89: Interf_Conver	192
Figura 90: Interf_Notes	193
Figura 91: Interf_Projects	193
Figura 92: About_Yappo	194
Figura 93: Cerrar_Yappo	194
Figura 94: Anb_Sdk_Manager	195
Figura 95: Package_Install	195
Figura 96: Jdk_Jvers	196
Figura 97: Installer_IIS	197
Figura 98: Localhost_IIS	197
Figura 99: Inges_IIS_Manager	198
Figura 100: Adm_IIS	198
Figura 101: Ingres_IIS_Ma_Yappo	199
Figura 102: Test_IIS_Mang_YAPPO	199
Figura 103: Local_Host_Yappo	200
Figura 104: Serv_Yappo	200

Figura 105: Enviar_Mensaje	201
Figura 106: Res_Mensaje	201
Figura 107: Leer_Mensaj	202
Figura 108: XML_Leer_Mens	202
Figura 109: Valid_User	203
Figura 110: XML_User	203
Figura 111: Direc_IP	204
Figura 112: Port_Forwar	204
Figura 113: Login_NOIP	205
Figura 114: DUC_NOIP	205
Figura 115: EDIT_HOSTS_NOIP	206
Figura 116: EDIT_HOSTS_NOIP	207
Figura 118: Res_Yappo	208
Figura 119: Alm_Usb	210
Figura 120: Apk_Yappo	210
Figura 121: Orig_Desc	211
Figura 122: Login_Yappo	212
Figura 123: Yappo!_Ingreso	213
Figura 124: Yappo!_BE_chat	214
Figura 125: Yappo!_contac	215
Figura 126: Yappo!_Chat1	215

Figura 127: Yappo!_Chatt2	216
Figura 128: Yappo!_Chat_3	216
Figura 129: Yappo!_Note	217
Figura 130: Yappo!_Project	218
Figura 131: Yappo!_AboutYappo	219
Figura 132: Yappo!_CerrarYappo	220

Introducción

La presente tesis desarrolló una aplicación cliente-servidor de mensajería instantánea bajo un estándar seguro de cifrado y encriptado para dispositivos móviles, basado en el sistema operativo “*Android*” para la comunidad universitaria de la Universidad Ciencias y Humanidades

En los últimos años, las aplicaciones móviles han evolucionado llegando a significar un factor innovador e importante para la comodidad y adaptabilidad dentro del desarrollo de las comunicaciones integrales de cualquier institución, empresa o entidad corporativa con ello se puede tomar decisiones acertadas y rápidas, esto solo lo hace posible la tecnología móvil, implementando una aplicación móvil de comunicación segura, bajo un entorno colaborativo que se adapte a las necesidades específicas que existen dentro de la actual comunidad universitaria. Dando como resultado un crecimiento vertiginoso dentro de las tecnologías de la información y la comunicación TICS; tanto en la demanda y la rentabilidad de estos servicios los cuales otorgan flexibilidad al usuario, además recrean una inmediata necesidad de aplicaciones orientadas a la seguridad de estos dispositivos móviles adaptadas a las actuales y nuevas plataformas.

Además, tenemos que reflexionar que en la actualidad existen soluciones móviles corporativas que realizan todo tipo de operaciones desde cualquier lugar y con diversas funcionalidades. Sin embargo no existe la debida importancia de aplicaciones orientadas a la seguridad en la comunicación de datos, pero si existe una gran demanda por parte de la comunidad universitaria que exigen una mejor solución a sus problemas de comunicación y transferencia de información.

El objetivo del trabajo será diseñar e implementar una aplicación con funciones de cifrado, encriptado de datos y privacidad de comunicación, a base de una comunicación colaborativa, flexible y rápida que garantice la seguridad de este tipo de comunicación de forma no intrusiva en la confidencialidad del estudiante.

El presente trabajo se dividió en dos partes: por un lado el desarrollo y configuración del servidor web que permitió gestionar las presentes comunicaciones y por el otro lado el cliente que se instalará en los diferentes terminales móviles “*Android*”. La aplicación es desarrollada en Eclipse, BD SQL Server 2012 y *Visual Studio* 2012 las cuales son requeridas para dicha tecnología de información y mejoras para los distintos servicios web desarrollados y levantados para una correcta comunicación (TIC)

En el primer capítulo se recopiló la información que sirvió para el diagnóstico de la situación actual de la institución, además de la misión y visión, así como la de sus procesos principales de negocio orientados a su rubro general.

En el segundo capítulo se describió los problemas generales y específicos. Se detalló la situación actual del sector que abarcamos las motivaciones para desarrollar este proyecto y sus objetivos

En el tercer capítulo se explicó el marco teórico de la investigación, y los antecedentes, las tecnologías utilizadas para el desarrollo del proyecto, y las razones de su elección.

En el cuarto capítulo se planificó el cronograma de actividades, historias de usuarios, planteamientos de desarrollo, como se ha llevado a cabo la solución del proyecto, se detallan aspectos de la implementación bajo un nuevo estándar metodológico

Finalmente, en el quinto capítulo se detalló los costos y presupuestos, los recursos humanos, los recursos de hardware, recursos de software y distintos gastos para la implementación del proyecto. También se redactó los beneficios tangibles como intangibles, se determinó la rentabilidad de la inversión como indicadores de rentabilidad del proyecto anual. Para finalmente presentar las conclusiones y recomendaciones del uso de la solución.

CAPÍTULO I: ASPECTOS GENERALES

1.1.3 Diagnóstico estratégico

La UCH surge para forjar una formación integral que abarque no solo el ámbito académico, sino también el cultivo de las artes y cultura, el conocimiento de nuestra realidad social y el compromiso con la comunidad.

A. Misión

Formar profesionales capaces de contribuir al mejoramiento de la comprensión del mundo contemporáneo y de la calidad de vida de todos los pueblos; que demuestren ser personas creativas y capaces de desarrollar nuevas ideas y proyectos, de identificar y resolver problemas de su medio, es decir profesionales comprometidos con el destino común de sus semejantes, para que en conjunto puedan construir, compartir, producir, complementar y enriquecer su experiencia formativa y calificación profesional, con talento y entusiasmo.

B. Visión

La formación y posicionamiento de la institución como una entidad de educación superior innovadora de alto nivel académico. Forjada a partir de principios, que educa, investiga y promueve la cultura y el desarrollo, en aquellas áreas de conocimiento que requieren mayor énfasis de proyección y arraigo en la comunidad educativa existente en el país.

C. Análisis FODA

El análisis FODA es un acrónimo que permite el análisis de fortalezas y debilidades internas de una empresa, las oportunidades y amenazas ambientales que pueden existir o ocurrir dentro de la organización. El análisis se basa en la suposición estratégica eficaz que se deriva a los recursos internos (fortalezas y debilidades), su situación externa (oportunidades y amenazas)

En nuestro caso la Universidad de Ciencias y Humanidades (UCH) se determinaron sus principales fortalezas.



Figura 2: Analisis foda

En la figura se muestra las fortalezas de la Universidad de Ciencias y Humanidades.

- **Innovación**

La universidad de Ciencias y humanidades está en continuo crecimiento tecnológico, integrando consigo una gran gama de nuevas oportunidades asociándolas a su currículo educacional.

- **Formación Integral**

Es definitivamente e irrefutable el gran proceso continuo, permanente y participativo que busca en desarrollar la universidad, en cada una de sus dimensiones, a fin de otorgar una formación de primer nivel a sus estudiantes.

- **Programas**

Las coordinaciones de la universidad de ciencias y humanidades con el departamento de investigación científico, fomenta el desarrollo de áreas de investigación multidisciplinarias y la formación de recursos humanos, a fin de resolver los grandes complejos problemas que acude a nuestro país.

- **Capacidad**

La categoría se consigue mediante esfuerzo y gran calidad de una industria determinada, si bien es cierto, la universidad no se hace ajena a dicha descripción, la capacidad de su plantel educativo demuestran el fortalecimiento requerido para que sea reconocida más adelante como una de las universidad que representen al país.

D. Calidad

Los límites y deficiencias se encuentran en cualquier tipo de operación, las observaciones de varios puntos débiles, demuestran cual es el desempeño mediocre que dentro del contexto de innovación aumentaría sus resultados esperados, la calidad es el subvenir de dichos demostración, la calidad se consigue en un determinado estudio en donde los competidores amenazantes se encuentran.

Tabla 1: FODA



Como se muestra en la tabla de oportunidades y fortalezas (FO), sus fortalezas de una intensiva búsqueda de programas académicos y de formación integral

E. Organigrama nominal

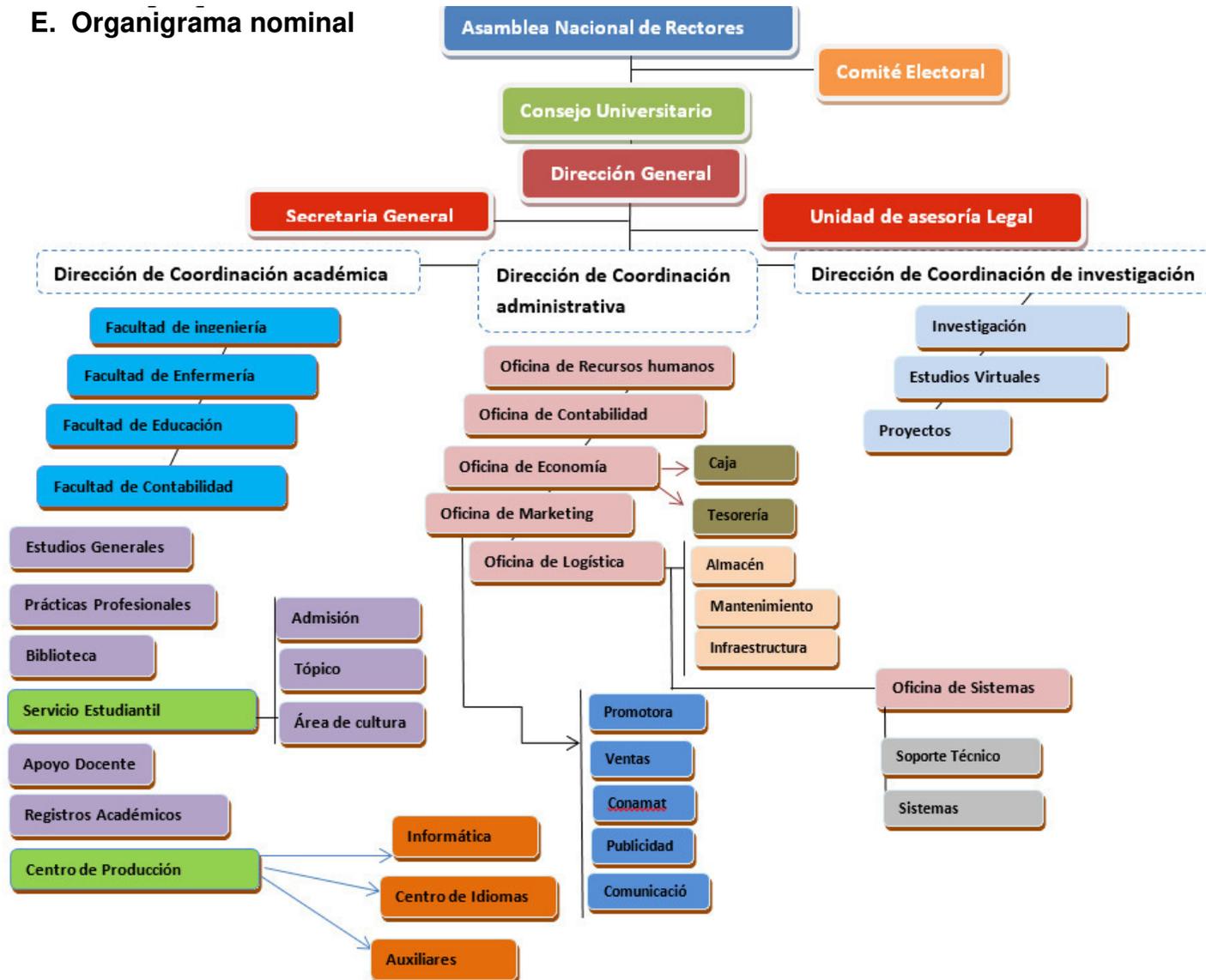


Figura 3: Organigrama nominal

F. Organigrama funcional

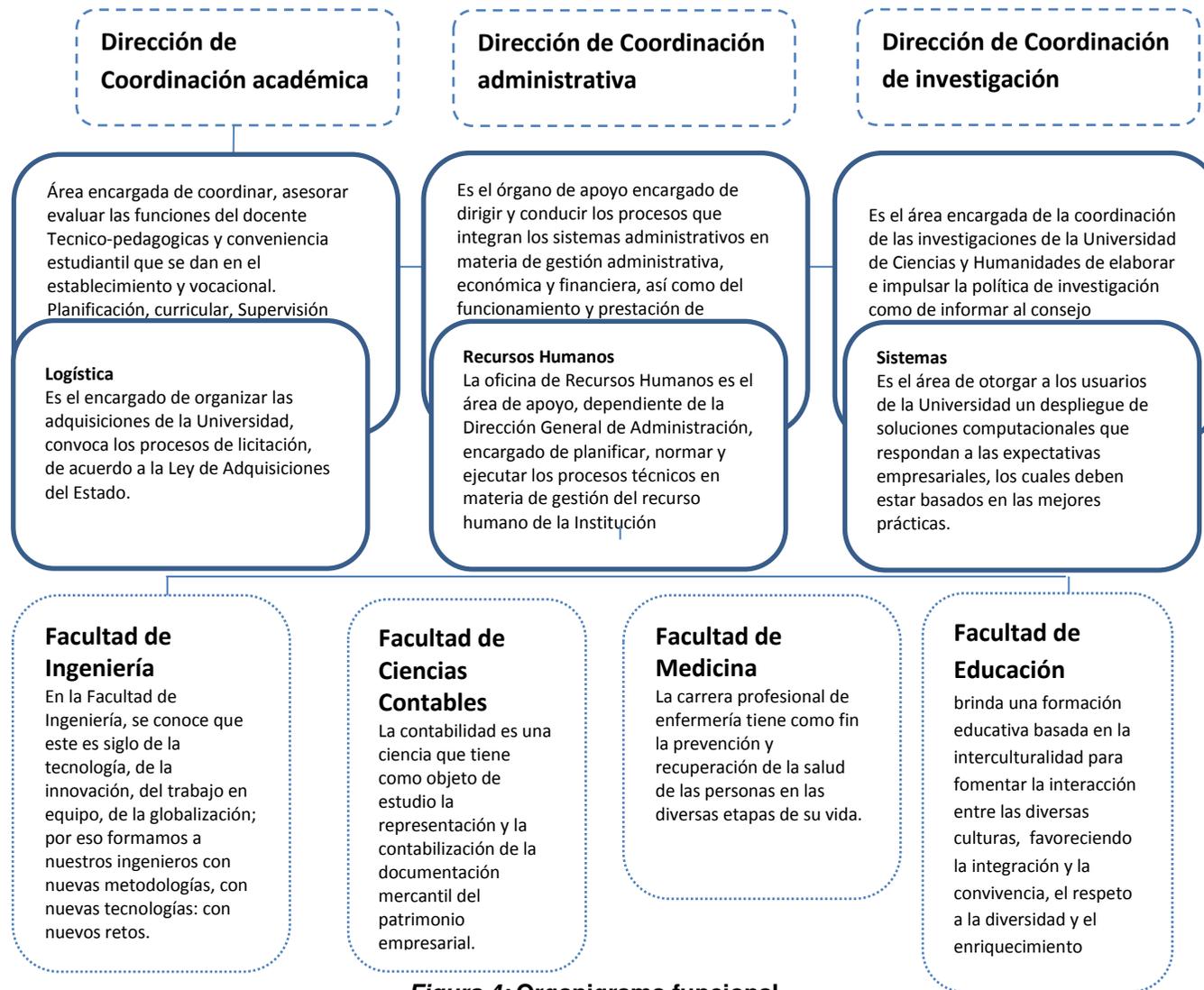


Figura 4: Organigrama funcional

Con los organigramas se visualiza el orden y jerarquía de todas las área involucradas en la casa de estudios

1.1.4 Cadena de valor

CONTABILIDAD					
• ELABORACION DE ASIENTOS CONTABLES		ELABORACION DE BALANCE GENERAL		ANALISIS ECONOMICO Y FINANCIERO	
• GESTIONA LOS INGRESOS Y EGRESOS		GESTIONA LOS REGISTROS CONTABLES			
ECONOMÍA					
• ELABORACION DE ESTADOS FINANCIEROS		ENDEUDAMIENTO CON ENTIDADES FINANCIERAS			
• ELABORACION DE ESTADOS PROFORMA		EMISION DE ACCIONES			
ADMINISTRACION DE RECURSOS HUMANOS					
• CONTRATACION DE PERSONAL		PROMOCION DE PERSONAL			
• CAPACITACION DE PERSONAL		REMUNERACION DE PERSONAL		DESPIDO DE PERSONAL	
SISTEMA DE INFORMACION – TECNOLOGIAS DE INFORMACION Y COMUNICACIONES					
• CENTRO DE INFORMÁTICA		SOPORTE TECNICO			
• SISTEMA DE INFORMACIÓN (CONTROL DE ASISTENCIA, BIBLIOTECA, CURSOS, MATRÍCULA, NOTAS).					
• SISTEMAS MANUALES (FALTA DE AUTOMATIZACION DE UN SISTEMA QUE PUEDA INTEGRAR SU INFORMACION)					
• SISTEMAS MANUALES (FALTA DE UN SIISTEMA QUE PUEDA INTEGRAR LA INFORMACION DEL RENDIMIENTO ACADEMICO DEL ALUMNO)					
MARKETING					
• GESTIONA LA PUBLICIDAD DE LA UNIVERSIDAD		GESTIONA BECAS / CONVENIOS			
LOGISTICA					
• EVALUA PEDIDOS		REALIZA ORDENES DE COMPRA		REALIZA CONSOLIDADOS	
• DIRECCION ACADEMICA		DIRECCION DE REGISTROS ACADEMICOS		CENTROS DE PRODUCCION	
COORDINADOR DE FAC ULTAD		REGISTROS ACADEMICOS		AUXILIARES	
COORDINADOR DE CARRERA PROFESIONAL		APOYO DOCENTE - TUTORIA		CENTRO DE IDIOMAS	
DEPARTAMENTO ACADEMICOS		ADMISION Y BIBLIOTECA			
ABASTECIMIENTO	LOGISTICA DE ENTRADA	OPERACIONES	LOGISTICA DE SALIDA	MARKETING Y VENTAS	SERVICIOS
• EVALUACION DE REQUERIMIENTOS	• RECEPCION DE EQUIPOS.	• MANTENIMIENTO DE EQUIPOS	• ALMACENAMIENTO DE MATERIAL	• CONVENIOS CON LOS BANCOS Y OTRAS	• RECEPCION Y ATENCION DE TRÁMITES, QUEJAS Y SUGERENCIAS.
• ELABORACION DE ORDENES DE COMPRA.	• VERIFICACION DE EQUIPOS.	• SEGURIDAD	• BIBLIOGRÁFICO, CONTROL DE EQUIPOS	• INSTITUCIONES, PUBLICIDAD CON AFICHES, BECAS, TALLERES	• ELABORACIÓN DE ENCUESTAS
	• DEVOLUCION DE EQUIPOS.	• PLAN DE ESTUDIO		• VIVENCIALES	• MATRICULA ALUMNO
	• ALMACENAMIENTO DE EQUIPOS.	• ELABORACIÓN DE SYLLABUS			• NOTA DE ALUMNOS
	• TO DE EQUIPOS.	• ELABORACIÓN DE MATERIAL DE ESTUDIO			• SERVICIO BIBLIOTECA
		• REVISIÓN DE LA INFORMACIÓN.			

Figura 5: Cadena de valor
Es el identificador responsable de todos los procesos de negocio

CAPITULO II

**PLANTEAMIENTO Y FORMULACIÓN DEL
PROBLEMA**

2.1 DEFINICIÓN DEL PROBLEMA DE INVESTIGACIÓN

2.1.1 Planeamiento y descripción del problema

La Universidad de Ciencias y Humanidades cuenta, actualmente, con un sistema de seguridad en la red principal del campus universitario, el cual es altamente refinado por sus ingenieros y técnicos profesionales de tal manera el ingreso a esta red es con un usuario y contraseña solo para los estudiantes de la Universidad.

Sin embargo, los estudiantes enfrentan serios problemas; ya que, esto no es del todo seguro pues dichos canales de comunicación e interfaces no son seguras con sus aplicativos móviles. Desencadenando altos índices de inseguridad, disminuyendo así el entusiasmo de distribución y compartimiento de información dentro del centro universitario.

Para identificar la demanda y la situación problemática de la comunidad universitaria, basta echar un vistazo al creciente uso de dispositivos móviles en los últimos años. Es así que, no existen estrategias adecuadas para disminuir el riesgo de pérdida de información comunicativa y colaborativa entre los docentes y alumnos.

Cabe destacar que los actuales sistemas de mensajería móvil instantánea, a pesar de estar muy extendidos entre los estudiantes, no destacan en cuanto a la preservación de la seguridad de datos. El actual proyecto intenta cubrir estas lagunas que otros sistemas no han tenido en cuenta para abrir paso a estos nuevos servicios que permitan la movilidad y disponibilidad de la transferencia segura de información y crear nuevas alternativas que permitan al estudiante compartir y distribuir información dentro de un canal seguro, adaptable y flexible para todo tipo de demandas. Se propondrá utilizar tecnologías de

cifrado y encriptado bajo el estándar y requerimientos de la plataforma con mayor influencia y favorita por la comunidad universitaria, *Android*.

2.1.2 Formulación del problema

¿Cómo se podrá garantizar la correcta seguridad de transferencia de información para plataformas móviles, con funciones de cifrado, encriptado de datos y privacidad de comunicación?

2.1.3 Problema específico

P.E.1: ¿Cómo se podrá mejorar el rendimiento en la transferencia o transacciones de envío de datos?

P.E.2: ¿De qué manera la aplicación permitirá que la comunicación sea de tipo no intrusiva en la confidencialidad del estudiante?

P.E.3: ¿Cuál es el nivel de disposición hacia la aplicación móvil de comunicación, por parte de los estudiantes de la universidad ciencias y humanidades?

2.2 DEFINICIÓN DE LOS OBJETIVOS DE LA INVESTIGACIÓN

2.2.1 Objetivo general

Implementar una aplicación para dispositivos móviles en Android que apoyen el resguardo de transferencia de información, con funciones de cifrado, encriptación de datos y privacidad de comunicación para la optimización de seguridad de la información hacia los estudiantes de la Universidad de Ciencias y Humanidades.

2.2.2 Objetivos específicos

O.E.1: Incrementar el rendimiento de seguridad en el envío y transferencia de datos para mejorar los procesos de comunicaciones móviles a estudiantes de la UCH.

O.E.2: Enviar mensajes a otros usuarios de la aplicación sin dejar marcas de conexión, sin exponer información intrusiva al emisor, como la recepción del mensaje, o su estado en línea.

O.E.3: Reconocer el nivel de disposición al uso de la aplicación móvil de comunicación, por parte de estudiantes de la Universidad de Ciencias y Humanidades

2.3 JUSTIFICACIÓN DE LA INVESTIGACIÓN

El presente proyecto está dirigido a fomentar y proveer servicios que permitan una comunicación integra, disponible y privada hacia el alumnado estudiantil de la Universidad de Ciencias y Humanidades. A partir de la evaluación de seguridad de la presente aplicación, ya sea manualmente o mediante una herramienta, se proseguirá con los resultados obtenidos como indicadores para el posterior diseño del estado de arte en cuanto a las plataformas de desarrollo móvil y el uso de tecnologías de seguridad basadas en la criptografía y encriptación; así como, protocolos de seguridad y privacidad de data que resulten aptos para los servicios móviles.

2.3.1 Justificación tecnológica

Para el desarrollo de esta aplicación, los requisitos mínimos que debe tener el móvil es un sistema operativo Android versión 2.3 y como características de Hw: memoria de 250 MB, un Mph de 1.0 GHz. Con tecnología 3G y 4G.

Hoy en día casi todos los estudiantes tienen y manejan un dispositivo con dichas características; por lo tanto es factible dicha aplicación. El proyecto está enfocado específicamente en el diseño y desarrollo de una herramienta de optimización móvil de seguridad en la comunicación, acceso y cobertura de almacenamiento en la nube y conexión con la base de datos del servidor. Utilizando herramientas que han tomado gran relevancia en los últimos años dentro del desarrollo de las aplicaciones modernas.

2.4 ALCANCES Y LIMITACIONES

2.4.1 Alcances

La presente investigación demostrará los límites existentes en la transferencia y envío de datos, así como las transacciones privadas dentro de los dispositivos móviles. En referencia a las funciones de seguridad que abarca la tecnología actual paramétrica mediante el filtrado de información o la desfragmentación y piratería cibernética. Por ende, la solución ante esta problemática será dirigida no solo para los presentes estudiantes, sino también como un aporte para la comunidad de usuarios móviles.

Por consiguiente, Yappo! será una aplicación con una arquitectura cliente- servidor de mensajería instantánea segura, que sea capaz de comunicar a los estudiantes que tengan instalada la aplicación.

Los estudiantes a través de la aplicación serán capaces de comunicarse mediante mensajes de texto, además de enviarse distintos links, paginas, blogs, etc. Desde cualquier parte del planeta con internet, a través de su smartphone o tablet.

También podrán crear grupos de conversación en cual los interlocutores se comunican con más de un receptor a la vez, además de tener implementado su propia agenda de tareas todo bajo un entorno seguro, flexible y colaborativo.

2.4.2 Limitaciones

- Yappo! estará dirigida solamente a la facultad de sistemas
- La función principal de Yappo! será la entrega de mensajes instantáneos
- No será una solución directa en la mejora de la seguridad informática estudiantil, sino que disminuirá el nivel de riesgo e inseguridad en la transferencia comunicativa de información.
- La falta de experiencia y fondo, dificulta que la solución sea para todas las plataformas disponibles, que se utilizan actualmente.

CAPÍTULO III:
FUNDAMENTO TEÓRICO

3.1 ANTECEDENTES

3.1.1 Antecedentes internacionales

- A. Esta investigación ayuda entender el comportamiento y la dinámica de la transferencia de mensajes encriptados, así como el tiempo de respuesta, ejemplos de algoritmos y recomendaciones bajo las buenas prácticas de la seguridad informática

En su estudio, Cujano (2010) se extrae que “El diseño e implementación de un sistema de control electrónico por un automóvil por medio de mensajes encriptados puede bloquear su vehículo en el mismo instante que realice el mensaje de texto desde su dispositivo móvil”. (pág.121)

- B. El extracto que se tomó como referencia en el artículo se utilizó como parte del aprendizaje del desarrollo y proceso de la firma digital, de los sistemas de cifrado y demás algoritmos

De la revista científica Vínculos podemos resumir lo siguiente: “Dentro de las funciones que exige la seguridad de la Información, donde hace parte la criptografía (Arte de ocultar la información), se encuentran la firma digital, el intercambio de claves de forma segura y el cifrado y descifrado de la información” (Gerardo,2011, pág. 131)

- C. Los modelos de seguridad que se presentaron dieron facilidades en la implementación de las metodologías y parámetros de seguridad para la aplicación, es adecuado medir el nivel de control de riesgos para evitar y disminuir las fallas de los sistemas de internet y proteger el patrimonio de información de los usuarios

Del siguiente contexto se extrae: “Las seguridades pueden verse afectadas en tres componentes: el uso indebido de los

dispositivos móviles, la falta de procesos de planificación de seguridad de la información o el desconocimiento de las personas acerca de las distintas medidas de seguridad” (Cárdenas, 2012, pág.95)

- D. Es increíble como las innovaciones actuales que han ido incorporando después del actual estudio, en el cual se midieron las posibles tecnologías que podrían adaptarse a los diferentes medios, en este caso a las aplicaciones móviles con tecnologías *RFID*, dentro de este estudio los lectores de *tags* (Etiquetas) *RFID* podrían permitir una gran variedad de aplicaciones móviles innovadoras y en este caso se permitió estudiar dichos controles.

De la tesis de Trujillo (2012) entendemos como parte fundamental de la investigación el siguiente contexto bajo el resumen de dicha tesis: “Los sistemas *RFID* permiten la identificación rápida y automática de etiquetas *RFID* en través de un canal de comunicación inalámbrica. Estas etiquetas son dispositivos con cierto poder de cómputo y con capacidad de almacenamiento de información. Es por ello que los objetos que llevan una etiqueta *RFID* adherida permiten la lectura de una cantidad rica y variada de datos que los describen y caracterizan”. (pág.143)

- E. Antes de comenzar el estudio y las diferentes indagaciones que motivaron al actual proyecto se buscó una manera referente para el encapsulamiento seguro de los mensajes a enviar. En un comienzo se deseó tercerizar con un servicio de VPN en la cual funcionaria de intermediario y ahorraría los tiempos de entrega del proyecto, fue de gran ayuda optar por leer el estudio de Chamorro, que sirvió para declinar el uso de una tercera herramienta para la transferencia de mensajes.

Del resumen de Chamorro (2011) se extrae el siguiente contexto: “Los elementos de la red móvil que intervienen en el envío de SMS, el tipo de VPN y la encriptación de la

información que atraviesa el enlace. De esta manera, se tendrán los conceptos necesarios sobre los elementos que intervienen en el servicio". (pág.79)

- F. En primer lugar lo que se busca desarrollar es sistema innovadora que este fuera de lo ordinario, dentro de los distintos autores que se estudiaron, la investigación de León ayudo a retomar muchas veces el proyecto, por la fuerte demanda de tiempo y esfuerzo para realizar las pruebas, las matemáticas siempre han sido y serán la base de la ingeniería para un análisis a profundidad y complejidad en el cual se señala lo siguiente.

De acuerdo a la investigación concretamos el siguiente resumen como parte relevante de nuestra investigación: "Los algoritmos de encriptación tienen una base fuertemente matemática y de esto no escapa el *RSA*, poder manejar estos conceptos dentro de este programa no ha sido precisamente de las tareas más sencillas, si no por el contrario demando mucho tiempo no solo en entender el funcionamiento del algoritmo sino también en la implementación y pruebas del mismo" (León, 2010, pág. 214)

- G. Las *VPN`S* siempre fueron la primera herramienta que se utiliza para mejorar los tiempos de entrega del proyecto, pero gracias a diferentes proyectos de investigación, se declinó utilizar las *VPN`S* como canales de seguridad, por distintos motivos, pero más por intentar realizar algo propio y eficiente.

De acuerdo al resumen de Durand (2011) podemos extraer el siguiente contexto: "Se muestra el marco teórico basado en los elementos de la red móvil que intervienen en el envío del SMS, el tipo de VPN y la encriptación de la información que atraviesa el enlace. De esta manera, se tendrán los conceptos necesarios sobre los elementos que intervienen en el servicio". (pág. 194)

H. Las arquitecturas de seguridad es una práctica, de métodos rigurosos en el estudio, de realizar un levantamiento de información previo de la estructura actual y futura, del comportamiento de los procesos de negocio involucrados y como se mencionó anteriormente el objetivo es proteger el patrimonio de los usuarios, Anizar conjeturo esto y más en su proyecto de investigación, las firmas digitales, los módulos de información, las llaves asimétricas e híbridas, identificación en el *login* (ingreso) de los usuarios bajo un cifrado menor de seguridad pero apuntan la dirección a la cual se ingresaba

De la investigación de Anizar (2012) encontramos el siguiente resumen : “En este trabajo, se propone una arquitectura de seguridad para computo móvil, que conjunta diversas tecnologías: cifrado asimétrico, firma digital, usuario y contraseña ; junto con tres módulos de información pertenecientes al usuario: pública, privada y biométrica, creando una identificación digital que podrá ser utilizada en diferentes servicios para la autenticación de usuarios evitando entre diversos problemas, el no repudio y el robo de identidad”. (pág. 167)

I. Cuando modificas o eliminas un archivo del ordenador, lo natural es que tu plataforma tecnológica elimina la referencia “visible” de dicho archivo y toma en cuenta el espacio del disco pueda ser utiliza para nuevos archivos. El caso del desarrollo del módulo de compartir archivos por un canal seguro es diferente a lo nombrado pero gracias a dichas diferencias se pudo crear un modelo agradable para la implementación del proyecto.

En el resumen siguiente encontramos extraordinario el siguiente contexto:” El objetivo del software es crear una red para compartir este tipo de información ¿Cuánto ha pagado un usuario por un objeto? Y de esta forma poder ayudar a futuros viajeros” (Mora, 2012, pág. 89)

J. Los pagos Online siempre causaron incertidumbre y grandes dudas, muchas veces ocasionando dolorosas odiseas al usuario para hacer una transferencia de un monto menor a mayor, en el transcurso que duro el proyecto se quiso incorporar un pequeño módulo de pago de matrícula para los estudiantes pudieran realizarlo cómodamente y en cualquier parte desde su celular, algo que por costos no se pudo incorporar pero si estudiar. Los desarrollos y tecnologías cambiaron, pero los modelos siguen teniendo como base la seguridad de las *apps*, desde las buenas prácticas en sus códigos fuentes como el desarrollo adecuado de una base de datos.

De su investigación se extrae lo siguiente: “El presente trabajo tiene como finalidad desarrollar en toda sus etapas un nuevo canal de transaccional que permita a los clientes de la micro y pequeña realizar sus operaciones con total comodidad y seguridad usando el celular como medio de pago” (Gregorio, 2011, pág. 102).

3.2 MARCO TEÓRICO

3.2.1 Introducción a la seguridad informática

La tecnología avanza rápidamente y así aumentan la transferencia de datos donde se crean nuevas tendencias dentro de la ingeniería informática y se busca reconocer la necesidad de evaluar la vulnerabilidad de nuestra información. Es por ello que se debe tomar como concepto general que dentro de la seguridad de información tiene como objetivo “asegurar la integridad y disponibilidad de la información dentro de los sistemas” (Bruna,2010, pág. 85).

3.2.2 Conceptos básicos de la seguridad informática

A. Criptografía

Dentro de la base de seguridad informática tenemos como elemento de sustentación a la ciencia que estudia la transformación de un determinado mensaje en un código de forma tal que a partir de dicho código solo algunas personas sean capaces de recuperar el mensaje original. En general se utiliza para ello una palabra clave o '*password*' con la cual se cifra el mensaje, el código resultante solamente puede ser descifrado por aquellos que conozcan el *password*. Dentro de la criptografía existen dos tipos de sistema de cifrado:

- Sistema de cifrado simétrico
- Sistema de cifrado asimétrico



Figura 6: Esquema de envío de información criptográfica (Wiki media 2013)

En la figura representa el esquema básico de la transferencia de información con la técnica criptográfica de contraseñas bajo custodia, en la cual bajo ciertos escenarios solo podrán tener acceso a la información las partes autorizadas y señaladas

a. Sistema de cifrado simétrico

Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave para cifrar y descifrar un documento. El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave, por lo tanto también se tiene que buscar un canal de comunicación que sea seguro para el intercambio de la clave.



Figura 7: Esquema de envío de información simétrica (Dit.upm, 2003)

El siguiente esquema muestra el escenario del cifrado simétrico entre el emisor A - B

b. Sistema de cifrado asimétrico

También llamado como sistema de cifrado publico Este sistema de cifrado usa dos claves diferentes. Una es la clave pública y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella. Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el

mensaje. Una vez que lo ha cifrado, solamente con la clave privada del destinatario se puede descifrar, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfectamente la clave pública para que todo aquel que se quiera comunicar con el destinatario lo pueda hacer.

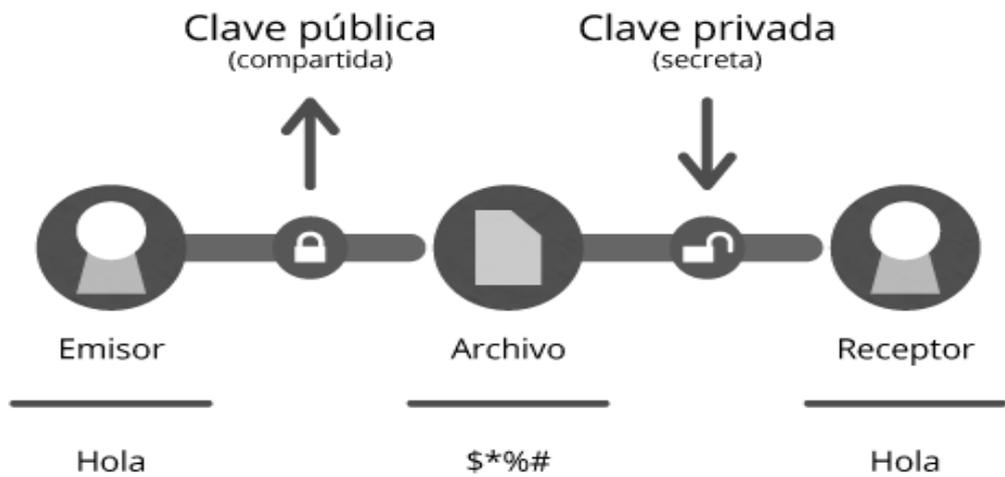


Figura 8: Esquema de envío de información asimétrica (Genbetadev, 2013:01)

Como lo muestra la siguiente figura la criptografía asimétrica se entiende por el uso de 2 claves: (la Pública y la Privada)

c. Sistemas de cifrado híbridos

Dentro del sistema de cifrado híbrido se emplea sistemas de cifrado simétrico como asimétrico, dando soluciones al problema de compartición

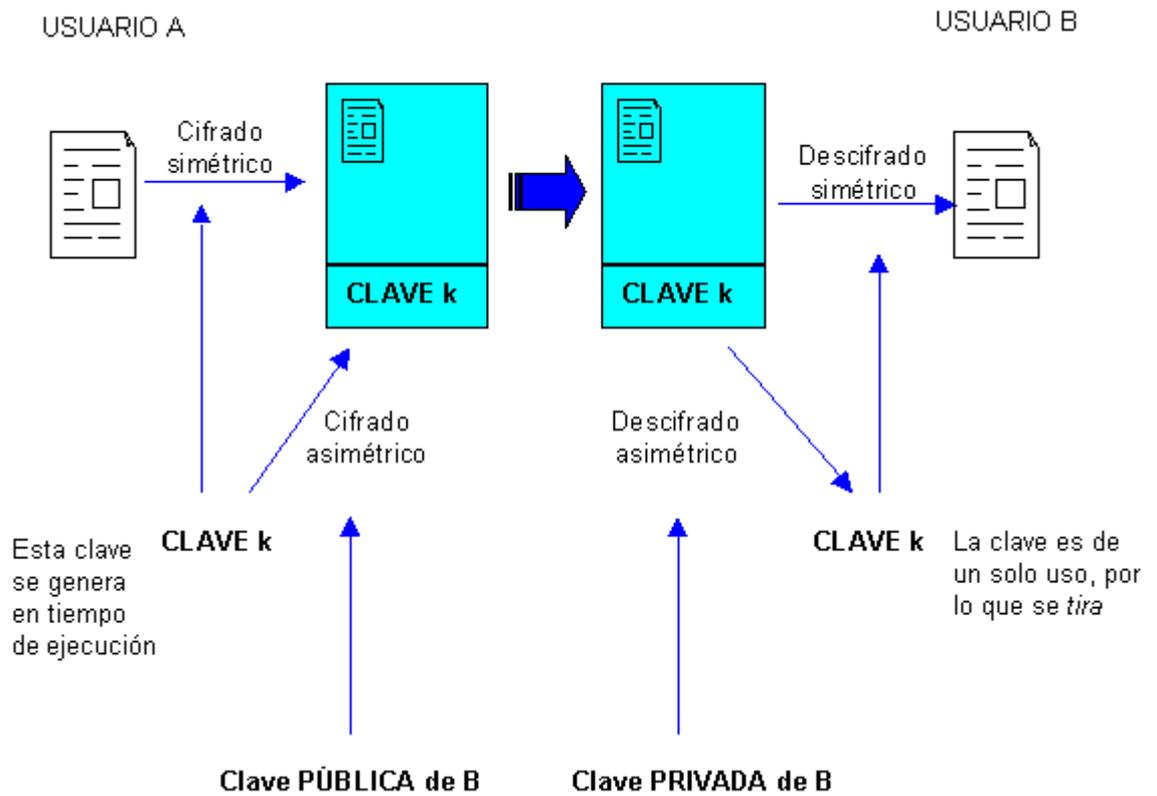


Figura 9: Esquema de envío de información híbrido (Galeón, 2012)

Una vez realizado el intercambio de claves, se proseguirá a utilizar el cifrado asimétrico para dar mayor seguridad y posteriormente utilizar el cifrado simétrico para la comunicación, por motivos de velocidad de respuesta rápida que existen entre los dos cifrados.

El comportamiento de la clave del sistema de cifrado simétrico se procesa, de la siguiente manera:

- El usuario genera clave simétrica para la sesión
- El usuario cifra clave simétrica con la clave pública del destinatario
- Solo el destinatario puede descifrar la clave simétrica que ha recibido

B. Funciones Hash

Las funciones hash son algoritmos que se consiguen a partir de una entrada (texto, contraseña o un archivo), que se realiza una salida alfanumérica donde normalmente se representara un resumen de toda la información vista. Este tipo de funciones no tienen los mismos propósitos que la criptografía asimétrica o simétrica, su cometido es “asegurar que no se ha modificado la información de un archivo dentro del canal de transmisión.” (Gutiérrez, 2013, pág. 110)

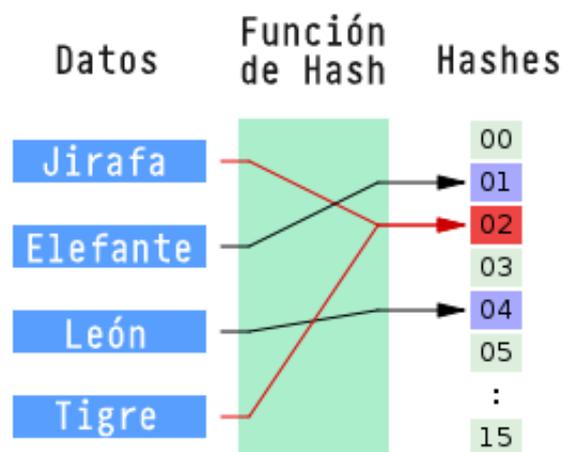


Figura 10: Esquema de funciones hash (Neptalium, 2013)

Entonces podemos definir que las funciones hash existen estrictamente para el resguardo confidencial de la información. Lo que nos indicaría que este sistema criptográfico nos asegura la respuesta (función unidireccional). Puesto nunca podrá saber cuáles han sido los datos enviados.

a. Algoritmos de Hash (MD5 Message Digest Algorithm)

Este algoritmo toma como entrada un mensaje de longitud arbitraria y produce una salida de 128 bits, la cual representa la huella o mensaje resumen de la entrada. Es además, computacionalmente improbable producir dos mensajes que tengan el mismo mensaje.

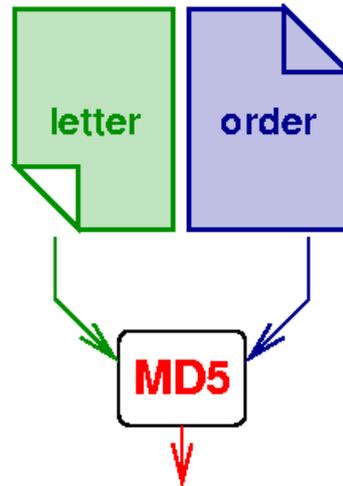


Figura 11: Esquema de algoritmo hash (Mannheim, 2015:10)

En resumen es obtener el mensaje original a partir de un mensaje de resumen. El algoritmo *MD5* fue diseñado específicamente para ejecutarse en ordenadores personales de 32 bits, además de que no requiere grandes tablas de sustitución y puede ser codificado de compacta.

b. Algoritmo de SHA-1 (Secure Hash Algorithm)

El algoritmo *hash*, especifica calcular la representación de un mensaje o archivos de datos. Para un mensaje de una longitud máxima de 264 bits como entrada, *sha-1* produce con salida una cadena de 160 bits llamada (mensaje resumen). El mensaje resumen puede ser introducido a un algoritmo de firma digital, el cual genera e verifica la firma del mensaje. Firmar el mensaje resumen en lugar del mensaje original provee una eficiencia dentro de los procesos, debido que el mensaje resumen es usualmente de menor tamaño que original ayudando a la funcionalidad del sistema.

C. Firma digital

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función *hash*, al contenido. Esta función asocia un valor dentro de un conjunto finito (generalmente los números naturales) a su entrada. “Cuando la entrada es un documento, el resultado de la función es un número que identifica casi unívocamente al texto”. (Infor@firma-electronica.eu-2011).

Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido.

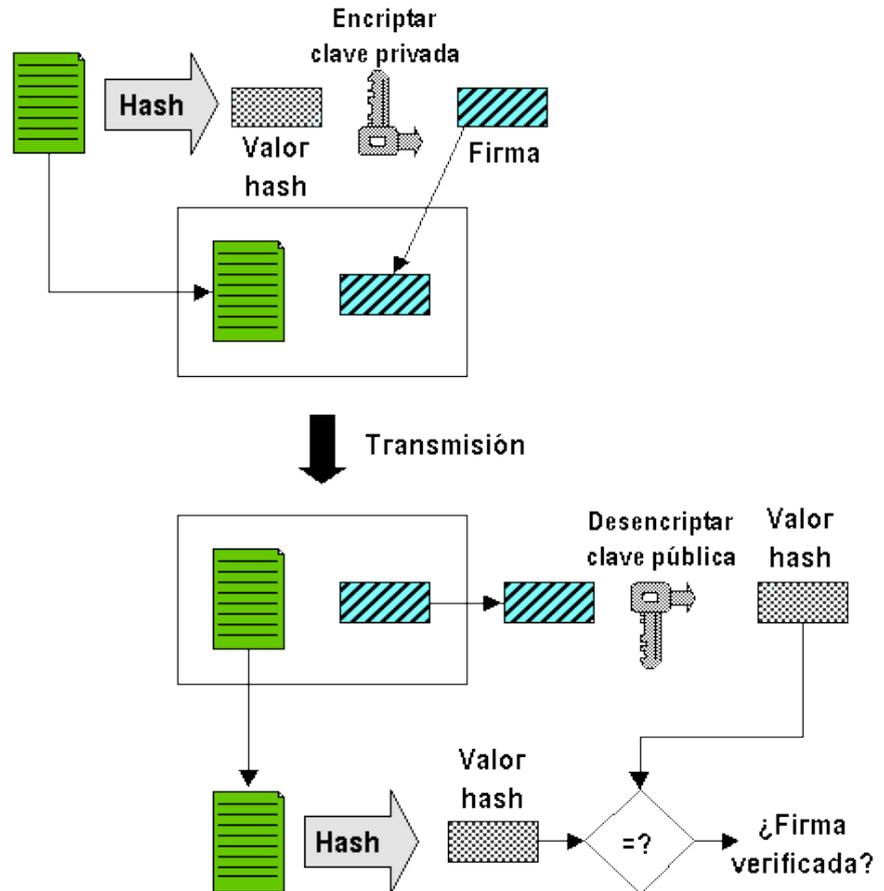


Figura 12: Esquema de envío de información digital (Hfernandezdelpech.com,2013)

De esta forma se ofrecen conjuntamente los servicios de no repudio, ya que nadie excepto el remitente podría haber firmado el documento, y de autenticación, ya que si el documento viene firmado por remitente, podemos estar seguros de su identidad. En último lugar, mediante la firma digital se garantiza además la integridad del documento, ya que en caso de ser modificado, resultaría imposible hacerlo de forma tal que se generase la misma función de resumen.

a. Creación de una firma digital

Es calculado el resumen del mensaje por la aplicación de un algoritmo criptográfico *hashing* (Ej. *MD2*, *MD5*, *SHA1*, etc.). El valor de hash ya calcula representa una secuencia de *bits*, extraídos de alguna forma del mensaje original.

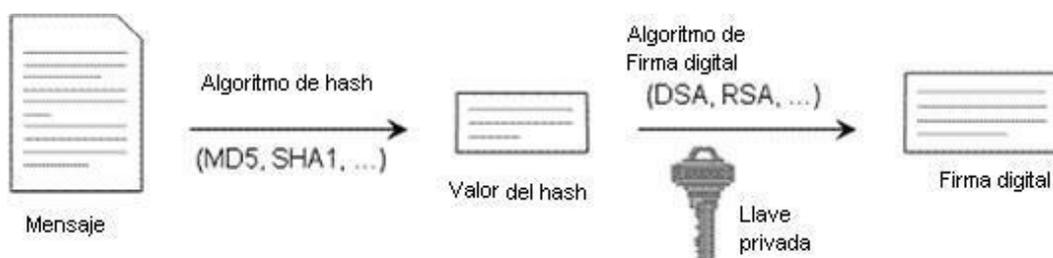


Figura 13: Esquema de creación de firma digital (Cyta,2008:07)

La información obtenida en el primer paso (resumen del mensaje) es cifrada con la llave primaria de la persona que firma el mensaje y así obteniendo el valor que conforma la firma digital.

b. Verificación de la firma digital

La tecnología de la firma digital permite al receptor de un mensaje verificar la integridad e disponibilidad del contenido.

El procesos de verificación buscar determinar si un mensaje fue eliminado por la llave primaria que corresponde a la llave pública.

- Calcular el valor corriente de hash del mensaje firmado: para este cálculo es usado el mismo algoritmo utilizado en el proceso de la generación de la firma digital. El valor obtenido se denominara valor de hash corriente, pues este será creado a partir del estado actual del mensaje.
- Calcular el valor original de hash: La firma digital es descifrada con el mismo algoritmo utilizado durante la generación de la firma digital. El

descifrado es realizado con la llave pública asociada a la llave privada utilizada durante la firma del mensaje. Como resultado se obtendrá el valor original de hash que fue calculado del mensaje original durante el primer paso de la creación de la firma digital.

- Comparar el valor corriente original de hash: comparar el valor corriente de hash obtenido en el primer paso con el valor original del hash. Si los dos valores son idénticos, prueba que el mensaje fue firmado con la llave privada que corresponde a la llave pública usada en la certificación.

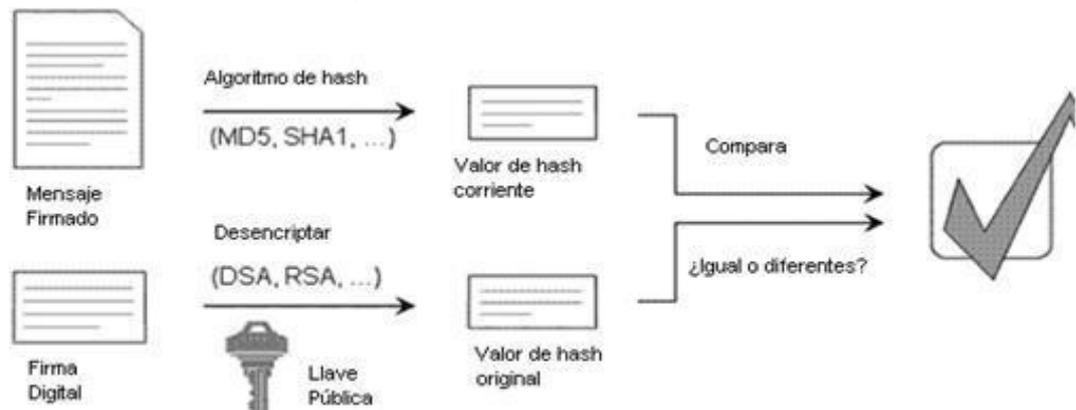


Figura 14: Esquema de verificación de firma digital (Cyta, 2008:07)

No se puede determinar la verificación de una firma digital por tal motivo se debe precisar obtener la llave pública en un canal seguro

c. Certificación de la firma digital

El certificado digital es un documento que contiene datos de identificación de la persona o institución que desea comprobar su propia identidad como así también confirmar la identidad de terceros.

Los certificados digitales vinculan un par de llaves electrónicas que pueden ser usadas para criptografía y firmar información digital.

Usados en conjunto con la criptografía, éstos proveen una solución de seguridad que permiten asegurar la identidad de una o de todas las partes comprometidas en una transacción.

Los certificados digitales evitan tentativas de sustitución de una llave pública por otra. Para evitar que esto ocurra, se hace necesario el uso de certificados digitales de llave pública, ya que estos garantizan seguridad y autenticidad a aquellos que acceden a redes inseguras, previniendo el acceso a datos confidenciales.

D. Firma XML y tipos de firma

a. XML

El extensible *markup language* (*XML*) es una sintaxis estandarizada elaborada por el *World Wide Web* (*WWW*). Este es un subconjunto de *SGML* (*Standard generalizes markup language*), Siendo que el *XML* fue pensado principalmente para estructurar datos intercambiables y servicios aplicados en la web.

Estructurando la información en *XML* se permite a los agentes de software leer e intercambiar datos. Siendo así uno de los primeros pasos hacia la producción de una web semántica legible por los computadores.

b. Firma XML y tipos de firma

La firma XML o XMLDsig. Son firmas digitales pero con una versión más exacta e completa. Esta permite añadir la información relativa a la pura firma de un documento XML. Entre otros campos encontramos el algoritmo de firmado o información sobre la clave.

Cuando se firman datos se utiliza la XMLDsig en lugar de una firma puramente binaria, ya que facilita el proceso de validación.

Dentro de XMLDsig existen tres maneras de generar una firma digital en un documento. El tipo varía dependiendo de la función de la localización de los datos firmados y la firma en el documento XML

- **Detached Signature**

La firma se separa de los datos firmados en dos ficheros diferentes



Archivo



Firma

Figura 16: Detached signature

Un documento firmado tiene una utilidad limitada. Otros usuarios no podrán recuperar el documento original de la versión firmada, e incluso con documentos en ASCII, el documento firmado deberá ser editado para poder recuperar el original (GNU-PRIVACY-2012)

- **Enveloping Signature**

La firma envolvente, consiste en crear un documento XML que contenga la firma y los datos que se han firmado

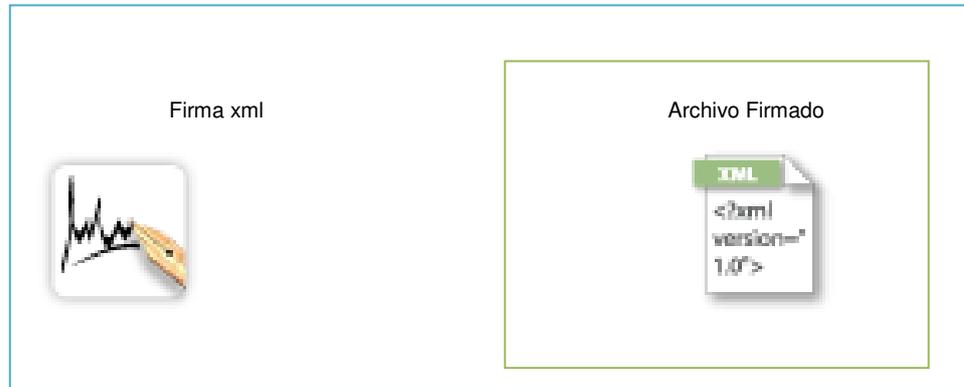


Figura 17: Enveloping signature

- **Enveloped Signature**

La firma envuelta, únicamente permite firmar documentos XML y consiste en incluir dentro del propio documento XML firmado el campo `<Signature>` con la firma XML.

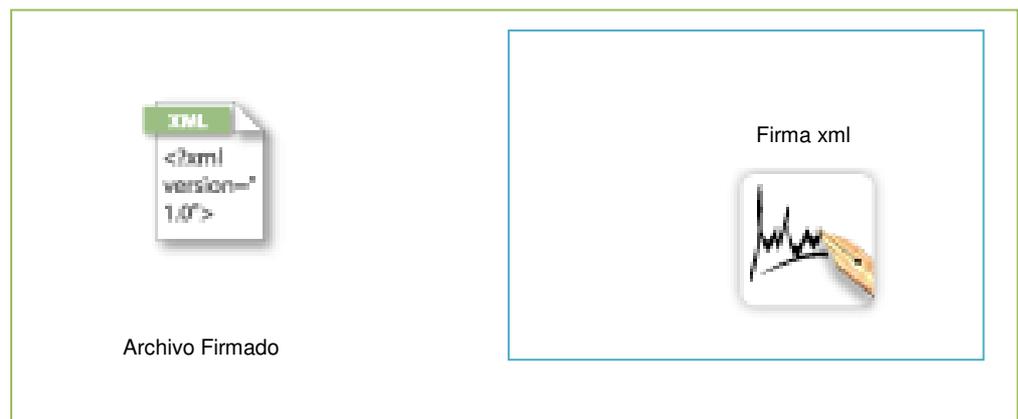


Figura 18: Enveloped signature

E. Encriptación

a. Introducción encriptado

El encriptar significa traducir un mensaje o conjunto de datos a símbolos y códigos variados que no tienen un significado directo, es decir que cualquier medio logre ah acceder al canal de la comunicación y tenga acceso al mensaje (a la señal) no podrá entender cuál es su verdadero significado. En el cual se desarrollada el adecuado filtro de mensajes.

Por ejemplo:

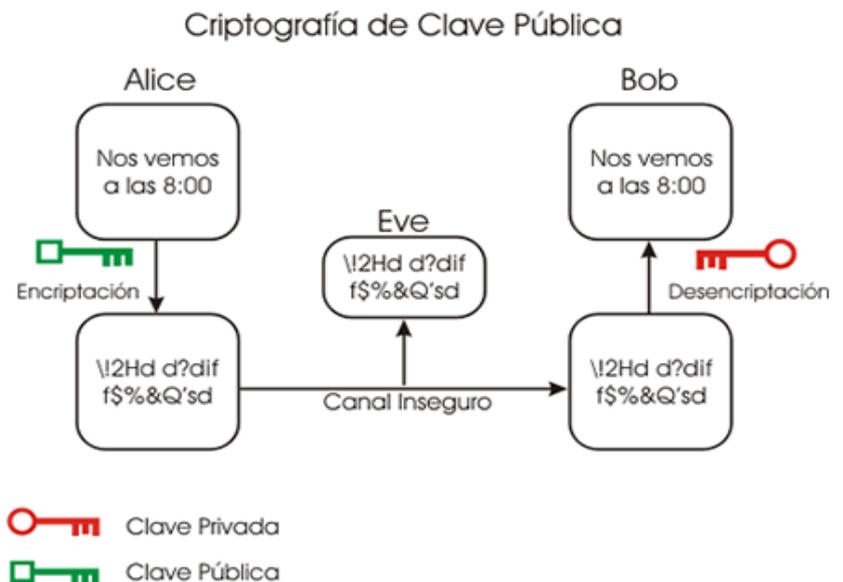


Figura 19: Criptografía esquema clave pública
(Textoscientificos,2005:06)

Como este criterio de decisión se determina la información importante y como tarea inicial. De qué forma se debe respaldar la seguridad y su contenido.

En la actualidad existen métodos modernos criptográficos que pueden ser usados a nivel proveedor o usuario. Tal es el caso de las empresas telefónicas que encriptan los datos de voz; o internet, e se dispone a una tarea de algoritmos criptográficos para garantizar la seguridad de la red patrocinada.

b. Métodos de encriptar

Haremos un repaso de las técnicas más comunes a las más robustas e actualizadas en la actualidad.

- *Blowfish* (llave de 448 bits): Es un algoritmo de encriptación rápido y fuerte. Su creador es Bruce Schneier, uno de los más prestigiosos criptógrafos.
- *Rijndael* (llave de 256 bits): es un algoritmo seguro y eficiente. Sus creadores son Joan Daemen y Vincent Rijmen (Bélgica). Ha sido como uno de los nuevos estándares de encriptación (AES).
- Triples *DES* (llave de 256 bits): Es un algoritmo desarrollado por el gobierno de EE.UU y ha sido evaluado durante años sin descubrirse debilidades, Es una configuración de encriptación en la cual el algoritmos “*DES*” es usado tres veces con tres llaves diferentes
- *Gost* (llave de 256 bits): Es un algoritmo de Rusia y podría ser considerado el análogo de ruso al *DES*. Tiene un diseño conservador y no ha podido ser vulnerado, a pesar de haber sido uno de los más

estudios, durante años, por los mejores expertos de criptoanálisis.

3.2.3 Servidor *web*/HTTP

El servidor web o servidor *HTTP* es el encargado de procesar las peticiones de los usuarios hacen a través de sus navegadores (*browse*) o aplicaciones móviles, proporcionan los recursos solicitados por los mismos para el desarrollo de sus tareas.

Para empezar a exponer el procesamiento de nuestra aplicación recalcaremos que el presente proyecto comprende dos partes bien diferenciadas el servidor y el cliente, que se desarrollaran de forma paralela,

A. *Web service*

Un servicio web (*web service*), es un sistema de software diseñado para soportar la interacción interoperable maquina a máquina sobre una red. Cuenta con una interfaz descrita en un formato procesable por una máquina. Otros sistemas interactúan con el servicio web de una manera prescrita por su descripción usando mensajes *SOAP*, por lo general transmiten por medio de *HTTP*.

Lo que significa que un servicio web es un servicio alojado en un servidor, al cual podemos acceder mediante el uso de la red, a fin utilizar la funcionalidad que el mismo provee.

Para el presente proyecto se decidió utilizar Asp.net. Por el menor consumo de memoria para el dispositivo móvil.

B. Base de datos

La base de datos tiene que ser capaz de almacenar los usuarios de la aplicación móvil y las credenciales de sus respectivos servicios.

Se ha diseñado siguiendo un modelo relacional permitiendo así representar la información de forma lógica y consistente en tablas relacionadas entre sí.

Se debe tomar en presente que cada usuario tendrá su identificador de usuario, que actuara de clave primaria y su identificador de sesión que permitirán acceder a las funcionalidades de los respectivos servicios.

La base de datos que se efectuara a utilizar es *SQL Server Express* por su compatibilidad con ASP.NET.

a. Base de datos mobile

Una base de datos móvil cumple las mismas funciones de una base de datos relacional, pero sus componentes son mucho más compactos y ligeros, a fin de poder operar en un teléfono móvil sin que esto signifique la monopolización de los recursos ni una baja en los niveles de eficiencia y velocidad del dispositivo móvil



Figura 20: Proceso de servidor web

La siguiente arquitectura demuestra el modelo definido por capas y vistas, las tecnologías que se vieron involucrados para su desarrollo

3.2.4 Tecnología móvil

En la actualidad el desarrollo de aplicaciones móviles significa satisfacer a los estándares requeridos y a las diferentes eventualidades tecnológicas futuras, necesarios para los humanos. Existe una gran gama de aplicaciones o servicios que cumplen estos requerimientos, brindando efectividad y adaptabilidad dentro de la plataforma donde se ejecute la aplicación. Por lo cual este trabajo se basa en la tendencia de mensajería instantánea o transferencia de información utilizando encriptación de datos. Creando una comunicación segura y disponible para todo tipo de plataforma de dispositivo móvil.

A. Dispositivo móvil

Para dar una mejor visión de lo investigado, daremos un concepto general de ¿qué son dispositivos móviles?, ¿en que nos benefician? ¿Cuáles son los más utilizados hoy en día? ¿Qué tan seguros son actualmente?

a. Introducción a la movilidad.

Un dispositivo móvil se define como un “aparato de pequeño tamaño con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red con memoria limitada que ha sido diseñado específicamente para una función pero que puede llevar a cabo otras funciones mucho más generales”. (Arturo B.A.2013, pág. 46).

Mediante la descripción, entenderíamos que los dispositivos móviles, son todos los equipos portátiles que tienen acceso a internet mediante una conexión inalámbrica, por ejemplo tendríamos a los populares “teléfonos inteligentes (Smartphone), tablet`s. asistentes personales digitales (PDA), *netbooks*, *iphone*, *iPad!*, etc.

B. Utilidad de dispositivo

Dentro de la gran variedad de dispositivos existentes o en realización, cada uno tiene su propia forma de accesibilidad y herramientas, que los convierte en elementos únicos para cumplir con un requisito, tarea o función. De acuerdo a lo planteado haremos un breve repaso del rendimiento de utilidad que nos brinda estos aparatos adaptables al bolsillo

- **Utilidad en movilidad:** Livianos y transportables, pueden ser utilizados tanto dentro como fuera de nuestro centros de estudios o de labor, permitiendo la búsqueda, selección y procesamiento de la información.
- **Utilidad en la conectividad:** La conexión inalámbrica facilita el acceso a la información, dando como servicio “el no cableado” o la unión de uno o más dispositivos, dando como tarea principal la adaptabilidad y comodidad que todo usuario necesita. Favorece en la comunicación y creación de redes en las comunidades de aprendizaje o sociales.

- **Utilidad de funcionalidad:** Estos dispositivos cuentan con una batería y solo el acceso a red está limitado por la existencia de un lugar de red inalámbrica o *Wifi!* La capacidad de procesamiento de datos facilita la recopilación de información en cualquier contexto

Haciendo una reseña de los repasado, daremos ahora las desventajas que nos limiten el uso y función de efectividad a estos dispositivos.

- **Tamaño no requerido:** Si bien es cierto, el tamaño es una de las características principales dentro de los dispositivos móviles, pero mediante más pequeño sea, también lo será su teclado y pantalla, creando limitaciones para el acceso o uso de funcionalidad dentro del sistema o plataforma a utilizar.
- **Funcionalidad de frontera:** Aun con los mayores esfuerzos de las diferentes industrias para la dotación de resistencia física e fortaleza, no ha dado grandes resultados, en algunos casos resulta ridículo y molestia saber que solo con la uña de tu dedo puede despedir a la pantalla táctil que añoras.

a. Variedad, popularidad y seguridad

A pesar que existe una gran variedad tanto de dispositivos como sus determinadas plataformas, dentro de su propio avance tecnológico recae una gran problemática para el desguardo de data y compartimiento de información se vuelve cada vez más inseguro para los usuarios. Esto es causa de las mismas capacidades de procesamiento, usabilidad y conectividad que se han incrementado

de manera vertiginosa en los últimos años. Tomando de reseña el siguiente contexto para dar apoyo a lo especificado:”...Otro factor que influye en la protección de datos activos comerciales claves es que los dispositivos móviles actuales están cada vez más conectado y sincronizados con un completo ecosistema de servicios de computo en la nube y de escritorio de terceros, lo que sin duda expone más la información importante y privilegiada” (Symantec, 2010, pág. 2). SYMATEC ”

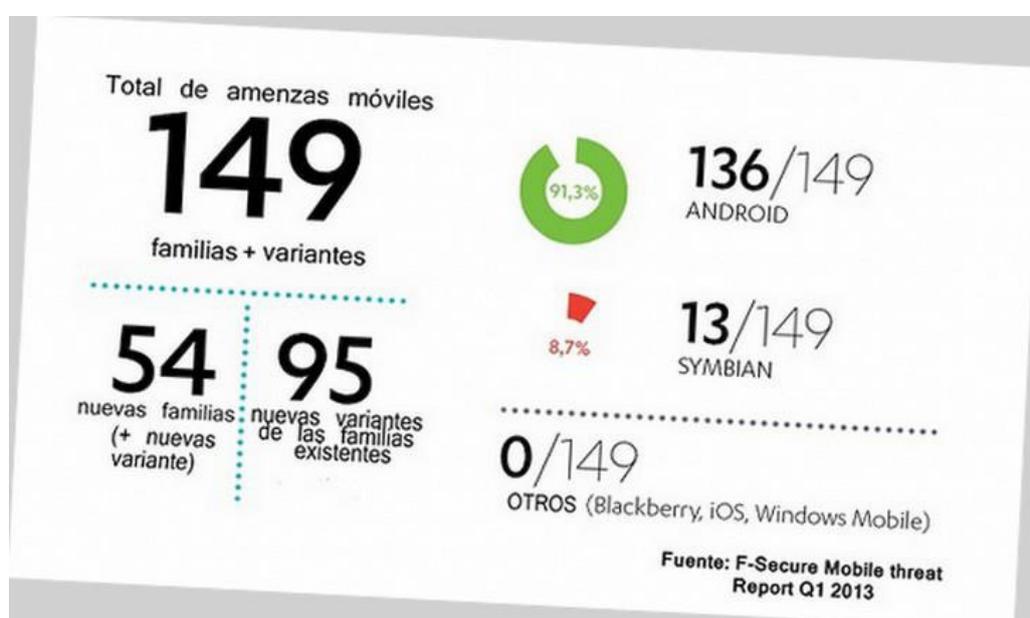


Figura 21: Seguridad de plataformas móviles (F-Secure, 2015)

Dando como visión, la tecnología web y los modelos actuales de seguridad empleados por las plataformas móviles actuales. Evaluando ahora su misma efectividad.

Los actuales escenarios del mundo corporativo han obligado la formación de: “... un sistema informático gestione los recursos de hardware y provee servicios a los aplicativos actuales” (Antonio Calderón 2012) entre en segundo plano dando como prioridad masiva, la creciente demanda de los usuarios

- Administración de perfiles multiusuario, control remoto e accesibilidad de información de cuentas.
- Arquitectura de seguridad (basados en ID o Privilegios)
- Segmentación/fragmentación de versiones
- Gestión y remediación de vulnerabilidades
- Sincronización de aparatos en red (inalámbrica, *bluetooth o wifi*) y comunicación libre

Como podemos observar las limitaciones de seguridad, dentro de la misma arquitectura son basados en permisos y privilegios de nivel usuario que pueden ser fácilmente codificados y *hackeados*. La misma problemática no solo es advertido a nivel de plataforma, si no dentro de las mismas herramientas, funcionalidades de los mismos aplicativos que son sacados al mercado (en algunos casos en versiones de pruebas) que muchas veces no son compatibles en nuestras plataformas y terminan des configurando o malogrando algo que no tenía que ser “tocado”.

“Durante el año 2012 casi 8 de cada 10 ataques contra plataformas móviles se dirigieron hacia *Android*. El sistema operativo es el más popular entre los usuarios de telefonía móvil avanzada pero no tanto como para justificar un número tan elevado.” (Ángel G. j. 2012, pág. 21).

FIGURE 1: NEW MOBILE THREAT FAMILIES AND VARIANTS RECEIVED PER QUARTER, Q1–Q4 2012

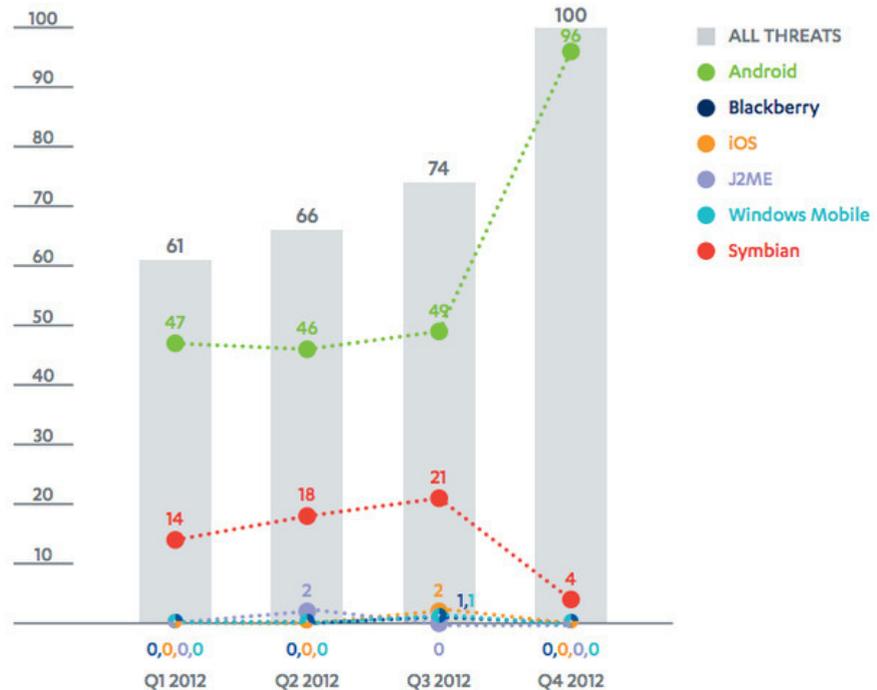


Figura 22: Seguridad de plataforma android (Gizmodo,2013)

Como observamos los dispositivos móviles dejaron de ser únicamente un “Gadget” tecnológico para pasar a formar parte de un fenómeno social y empresarial. Dejando un lado las prioridades de seguridad y dando más coberturas y sincronía entre los dispositivos, una grandiosa idea, pero implementarlo sin tener aun la tecnología de seguridad que pueda acompañar. Mala idea.

D. Tipos de plataformas móviles

Partiendo con lo visto y aprendido, daremos una mejor descripción de los sistemas operativos utilizados dentro de los dispositivos móviles. Dando a entender que la funcionalidad principal de estos mismos sistemas se basan en determinar las capacidades multimedia de los dispositivos, y la forma de estas de interactuar con el usuario

A continuación haremos un repaso de las plataformas más utilizadas o nombradas por el mundo informático

a. Symbian

Es el resultado de la alianza de varias empresas multinacionales de renombre dentro del mercado tales como Nokia, *Sony Ericsson*, *Samsung*, *Siemens*, *Motorola* y otras. Como objetivo principal de su elaboración fue crear un sistema operativo para terminales móviles que pudiera competir con el Palm o el *Windows Phone* de Microsoft y ahora Android de google.Inc

Symbian también es el sistema operativo más extendido dentro de los “*Smartphone*” por lo tanto el que más aplicaciones para su sistema tienen desarrollado. Admite la integración de aplicaciones, ofreciendo protocolos de comunicaciones, control de archivos y los servicios para el correcto funcionamiento de estas aplicaciones.

Dentro de los otros puntos a los cuales destacar. *Symbian* se ha convertido en un sistema que es compatible con los estándares de conectividad y redes *bluetooth*, *GSM*, *GPSR*, *CDMA* Y *WCDMA*

b. Windows phone

Windows Phone, anteriormente llamado Windows Mobile es un sistema operativo desarrollado y diseñado por Microsoft para su correcto en los teléfonos inteligentes (*Smartphone*).

Se basa en el núcleo nativo del sistema operativo CEO y cuenta con un conjunto de aplicaciones para su relieve uso.

Una de las ventajas que se obtiene en *Windows Phone* es que los programadores pueden desarrollar aplicaciones para móviles utilizando los mismos lenguajes y entornos que emplean con *Windows* (PC). Comparando con las aplicaciones de *Symbian* necesitan más esfuerzo dentro de su desarrollo, Otra curiosa característica de *Windows Phone* esta específicamente diseñado para ser similar a las versiones de escritorio de *Windows*.

c. *iOs*

Como historia general, sabemos que *iOS* es conocido mundialmente como el sistema operativo diseñado por Apple en california destinado para sus dispositivos de última generación (*iPod,iPhone,iPad*).

Su mismo desarrollo se basa originalmente del nucleó del sistema operativo Mac Os x (*Darwin BSD*). Pero a diferencia del sistema original, la interfaz como el ambiente grafico fue rediseñado para una mejor adaptación a los dispositivos actuales. Actualmente es uno de los sistemas operativos móviles más rebuscados e utilizados, donde muchos de sus usuarios garantizan la comodidad y adaptabilidad para sus distintas funciones.

d. *Android*

Desde que *google* decidió que era buena idea desarrollar una plataforma basada en *Linux* y *java*. Creo prácticamente un fenómeno para los demás desarrolladores libres y se convirtió como uno de los mayores SO comercializados actualmente.

¿Pero que busca y en qué se diferencia?

El sistema busca un modelo estándar de programación abierta que simplifique las labores de creación de aplicaciones móviles y normalice las herramientas en el caso de la telefonía móvil. Al igual que ocurre con *Symbian*, *Android* apuesta no solo en desarrollar sus creaciones en una sola terminal, si no volverse compatible con diferentes terminales.

Este será el sistema operativo en el que realizaremos las pruebas de conversión y compatibilidad de terminales, desarrollando el *SDK plugin* que provee y posteriormente mandando al rediseño e implementación de nuestra aplicación.

E. Tipos de aplicación

Como habríamos declarado en puntos anteriores, el desarrollo de aplicaciones móviles es actualmente un gran atractivo en demandas específicas y restricciones técnicas bajo el entorno móvil. Tales como dispositivos con capacidades limitada, pero con una evolución continua, existen varios estándares, protocolos y tecnologías, pero la necesidad máxima es de operar sobre distintas plataformas.

La solución ideal a este problema, es crear y mantener una única aplicación, el desarrollo multiplataforma tiene como objetivo mantener la misma base de código sobre distintas plataformas. De esta forma el esfuerzo se minimiza y el costo de desarrollo se reduce notablemente.

apps móviles

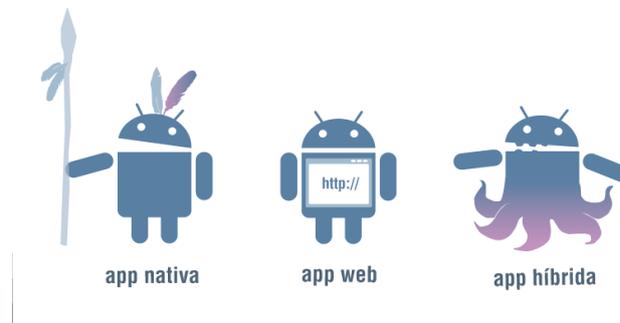


Figura 23: Tipos de aplicaciones (If3socialmedia, 2012:03)

A continuación se presentan 3 enfoques para el desarrollo de aplicaciones para dispositivos móviles: El nativo, web y el híbrido

a. App web

Las aplicaciones web para móviles son diseñadas para ser ejecutadas en el *browser* del dispositivo móvil. Estas aplicaciones son desarrolladas utilizando *HTML, CSS y Java Script*.

Una de las ventajas de este enfoque es su independencia de la plataforma, no necesita adecuarse a ningún entorno operativo. Solo necesita el navegador para su funcionamiento. Por otra parte, esto disminuye la velocidad de ejecución y podría llegar a ser menos atractiva que las aplicaciones nativas



Figura 24: Aplicación web (Testingbaires, 2014)

Una de las herramientas (más no lenguaje de programación) que precisamente nos permiten crear *apps web's* es *HTML5*, que con un solo desarrollo sean accesibles desde cualquier dispositivo

b. App nativa

A diferencia de la *app web*, son desarrolladas para ejecutarse en una plataforma específica, es decir, se debe considerar el tipo de dispositivo, el sistema operativo a utilizar y su versión.

La principal ventaja de este tipo de aplicación es la posibilidad de interactuar con todas las capacidades del dispositivo (cámaras, *GPS*, acelerómetro, agenda entre otras). Además no es necesario poseer acceso a internet para su ejecución rápida, pero si se desea cubrir varias plataformas, se deberá generar una aplicación para cada una de ellas. Esto conlleva a mayores costos de actualización y distribución de nuevas versiones.



Figura 25: Aplicación nativa (Testingbaires, 2014)

Las aplicaciones nativas han sido diseñadas y concebidas bajo las características y los parámetros específicos del dueño de la plataforma tecnológica, que serían *Apple* o *Google* (los más populares de acuerdo a nuestro estudio)

Las aplicaciones híbridas combinan lo mejor de los dos tipos de aplicaciones anteriores, se utilizan tecnologías multiplataforma como *HTML*, *java script* y *CSS*. Pero se puede acceder a buena parte de las capacidades del dispositivo móvil,

Su mayor desventaja es que al utilizar la misma interfaz para todas las plataformas, la apariencia tiene a no ser de una aplicación nativa, finalmente la ejecución será más lenta que la ejecución en una *app* nativa.

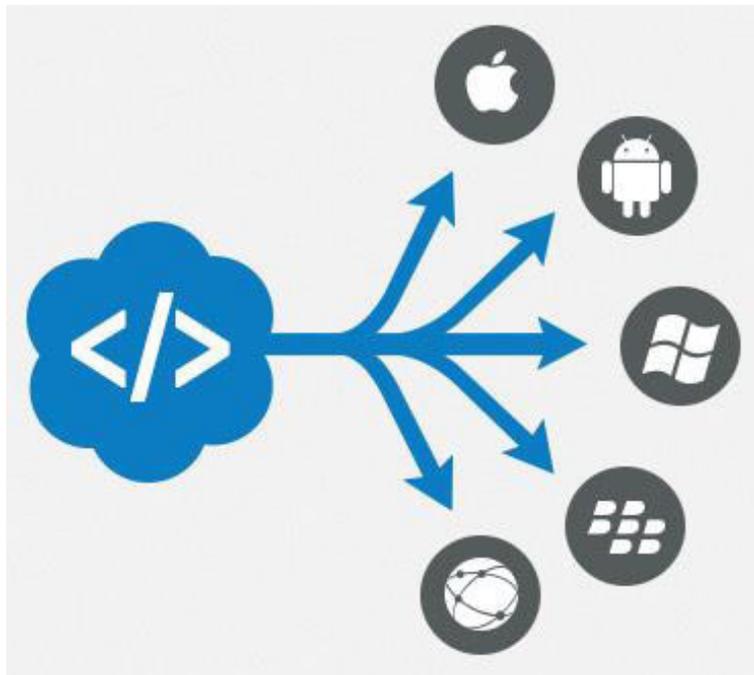


Figura 26: Aplicación híbrida (Testingbaires, 2014)

En resumen, las aplicaciones multiplataforma son desarrolladas utilizando tecnología web y son ejecutadas dentro de un contenedor web sobre el dispositivo móvil, de esta manera se pueden monetizar de gran manera proyectos de aplicaciones Móviles

3.2.5 ¿Qué es mi metodología?

Se entiende como metodología: Como una colección de procedimientos, técnicas, herramientas y documentos auxiliares. Siendo de gran ayuda a la hora de realizar un nuevo sistema de *software*. Por tal motivo la necesidad que los proyectos lleguen al éxito buscado y obtener un producto de gran calidad para los clientes, se generan grandes cambios en las metodologías adoptadas para cumplir sus objetivos. Puntualicemos que unas se adaptan mejor que otras, al contexto del proyecto realizado. Para el desarrollo de este proyecto se analizaran varias de las metodologías usadas con resultados favorables y luego se determinara cuál de ellas se aplicó de acuerdo a las características del propio proyecto.

A. Metodología “tradicional”

El éxito del proyecto dependerá en gran parte de la metodología escogida, ya sea a la clásicas o “tradicional” donde los equipos maximicen su potencial, aumenten su calidad del producto con los recursos y tiempos establecidos.

El desarrollo de las metodologías clásicas o “tradicionales” se focalizan principalmente en: documentación, planificación y procesos. (Plantillas, técnicas de administración, normalizaciones, controles, políticas, modelos, revisiones, roles, burocracia, etc.)

Entre las principales metodologías tradicionales tenemos: *RUP*, *MSF*, *METRICA Vr3*, *OMT*, etc. Entre las cuales su proceso a utilizar *RUP* para el diagrama de negocios y algunos diagramas de sistema para convalidarlos con las historias de usuario

a. **RUP ¿ERES GENIAL PERO ERES PARA MÍ?**

Es una metodología de procesos formales y disciplinarios para asignar diversas tareas y responsabilidades. Su objetivo es asegurar la productividad de *software* de alta gama que satisfaga completamente a los usuarios finales (siempre y cuando respetando el cronograma y no salirse del presupuesto establecido)

Ventajas:

- Seguimiento detallado en cada una de sus fases
- Funciona bien en proyectos grandes e innovadores

Desventajas:

- Excesivas fases para algunos proyectos
- Involucramos a nuestro cliente en una situación muy incómoda. Deberá ser capaz de entender a un gran nivel de detalle para poder acordar un alcance de proyecto con él.

Dejando un lado la extensiva documentación final de arquitectura, la poca flexibilidad, la gestión de incidencias, la estabilización y el despliegue. Lo que se extrajo y ayudo en *RUP* fue su proceso de seguimiento en la fase de negocio, lo cual lo observaremos sus propios diagramas más adelante.

B. Metodología ágil

Como habríamos nombrado al comienzo del capítulo un proyecto de investigación sea exitoso sin importar el tipo de software ya sea para dispositivos móviles, escritorio o web es necesario que el resultado cuente con la calidad esperada por el cliente, usuarios y el desarrollador. La calidad del proyecto se puede definir de acuerdo al desempeño del desarrollador, de las herramientas utilizadas y las metodologías aplicadas, por tal motivo definamos el término “ágil”

El desarrollo “ágil” nace como alternativa ante los procesos disciplinarios y rígidos de las tradicionales. La agilidad de un proyecto es: “sacar adelante un proyecto en el menor tiempo y con la mayor calidad posible”. No importa si no está completo, sacar lo más pronto posible funcional. A diferencia de la tradicional en donde se malgastar tiempo en extensiva burocracia y documentación que a un cliente le sirve poco, puesto lo que desea es una aplicación funcionando pronto y conforme a sus expectativas.

Si bien es cierto, los procesos ágiles mantienen motivado al desarrollador y al cliente, empleando un trabajo en conjunto, gracias a su simplicidad poniendo énfasis a las interacciones entre los individuos del equipo en el desarrollo a base de una planificación activa.

Podemos argumentar que en un método de desarrollo de software funciona mejor cuando se aplica a situaciones con características muy específicas. En la siguiente tabla podemos observar las comparaciones entre las metodologías ágiles y las metodologías tradicionales

Tabla 2: Diferencias metodologías

Área	Metodología Ágil	Metodología Tradicional
Desarrolladores	Colaborativos, unidos, ágiles y entendidos	Orientados al plan con una mezcla de habilidades
Clientes	Son representativos y se les entrega poder	Mezcla de niveles de aptitud
Confianza	Conocimiento táctico interpersonal	Conocimiento explícito documentado
Requerimientos	En gran parte emergentes y con rápidos cambios.	Conocibles tempranamente y bastante estables
Arquitectura	Diseñada para los requerimientos actuales	Diseñada para los actuales y los del futuro próximo
Tamaño	Productos y equipo pequeños	Productos y equipos más grandes

En definitiva el desarrollo ágil de software intenta evitar los tortuosos y burocráticos caminos de las metodologías tradicionales, enfocándose en las personas y los resultados. Promoviendo iteraciones en el desarrollo a lo largo de todo el ciclo de vida del proyecto.

Resumiendo las metodologías ágiles:

- Entregas frecuentes de versiones funcionales en el menor tiempo posible
- Reducir al máximo la complejidad del proceso, lo importante es desarrollar no a el papeleo mediático y sensacionalista
- El progreso se mide según funcione más o menos de la aplicación
- Estamos preparados para cualquier tipo de cambios toscos en el proyecto.

Las metodologías ágiles juegan bien en desarrollo de equipos de más o menos de individuos pero, ¿qué ocurre si lo llevamos a un mundo distinto, de un solo pasajero?,

¿Las metodologías ágiles actuales y favoritas son las recomendables para las *app* móviles?

La realidad que la agilidad no es nada nuevo, ya tiene varias décadas pero no tenía tanta usabilidad como ahora. Existen diversas metodologías de desarrollo ágil que se han empleado para este proyecto desde metodologías híbridas al nuevo mundo de metodologías móviles, los problemas que hemos puntualizado los resolveremos definiendo nuestra propia metodología móvil

a. Todos amamos *SCRUM*

Cuando juntamos agilidad y metodología, lo primero que se nos viene en mente es "*SCRUM*". Porque *SCRUM* es sinónimo de agilidad, presenta un procesos adaptativo, rápido y auto-organizado de desarrollo de productos.

SCRUM se centra en la gestión de proyectos en situaciones en las que es difícil planificar el futuro, con mecanismos de control "proceso empírico", donde los bucles de realimentación constituyen el elemento central. *SCRUM* no es perfecto, existen errores, tenemos que utilizar la retroalimentación ante estos errores o bucles vacíos.

El software es desarrollado por un equipo auto-organizado en incrementos (si lo que llamamos "*sprint*" a todo), empezamos por la planificación y finalizamos con un comentario feliz. Las características que deben existir dentro del sistema (exacto nuestras tarjetas de usuarios) deben registrarse en el "*backlog*". Entonces el dueño del

producto decide que elementos del *backlog* se deben desarrollar en el sprint siguiente.

La coordinación del equipo de trabajo a base del proyecto desarrollado se debe realizar bajo una “reunión diaria” todos los días aproximadamente a la misma hora y durante un periodo de tiempo corto (unos quince minutos es lo ideal donde los miembros comentan sus experiencias, que hicieron el ultimo día, que harán hoy y si tienen algún problema de inspiración o impedimento que lastre su avance)

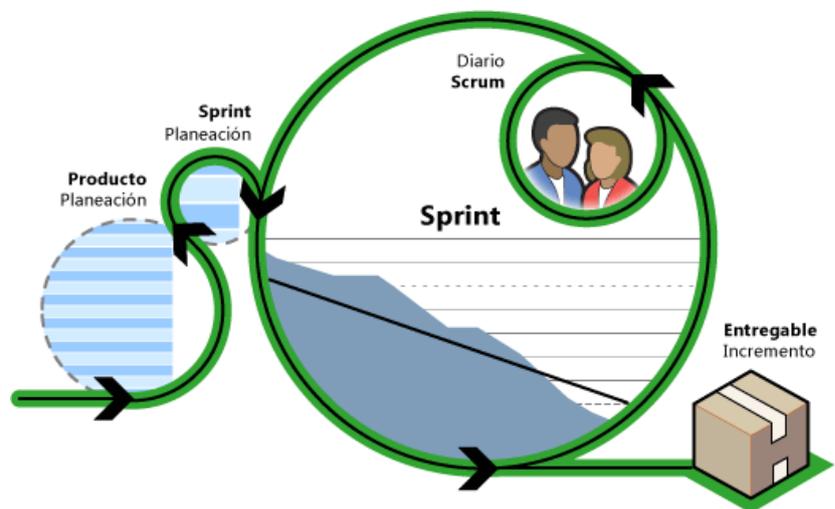


Figura 27: Sprint scrum (Redletterday, 2012)

Siguiendo la ilustración considere la metodología ágil como una manera de habilitar una gran cantidad de requerimientos a través de un proceso incremental que permite llegar a su objetivo

Proseguiremos a definir algunos componentes:

- *Scrummaster* : Es la persona responsable de que el proceso de *scrum* se ejecute correctamente (equivalente al gerente del proyecto)

- *Stakeholders*: Son esas personillas que sin ellas no existiría el proyecto en realidad, “los implicados” en el resultado de desarrollo: “los clientes, vendedores, usuarios finales, etc.”
- *Sprint*: Una iteración del proceso de desarrollo, normalmente de una longitud de una o dos semanas.
- *Sprint review*: Es la presentación del demo del producto al *product owner* las nuevas funcionalidades (las funcionalidades no implementadas no se presentan).
- *Sprint retrospective*: Reflexionamos la realización de los sprint’s – ¿qué fue lo malo y bueno del sprint? – ¿qué cosas se pueden mejorar?
- *Burndown chart* : Podríamos definirlo como el grafico que muestra la cantidad de trabajo restante del sprint en el que estamos desarrollando :
- estima las tareas –el progreso del sprint – la adicción de nuevas tareas

b. Kanban

Kanban tiene un significado profundo al ser una palabra japonesa “tarjetas visuales” (*kan* significa visual, y *ban* tarjeta). Es una técnica que está dentro de la estrategia “Kaizen” “mejora continua la mejor estilo de *Toyota*”.

Kanban permite ver el proceso de producción de un proyecto a través de un tablero en el que se tiene una lista de tareas pendientes y las distintas fases de la cadena por las que tiene que pasar una tarea antes de considerarse completada

Dentro de las ventajas de utilizar *kanban* es que gracias a su representación visual permite identificar rápidamente cuellos de botellas en las distintas fases del proceso. Es decir, si empiezan acumularse las tarjetas (historias de usuarios) en una de las columnas (fases) habría que definir qué sucede en dicha fase y el porqué del retraso (una forma de evitar el estancamiento de HU)



Figura 28: HU Kanban (Dmitryivanov, 2012)

La funcionalidad y aprendizaje de *Kanban* se sumamente simple, se forman tareas pendiente y se ponen en la primera fase, cuando se ha completado dicha fase para la tarea se mueve a la siguiente y así sucesivamente hasta llegar a la final de la cadena, no podemos avanzar si dicha tarea a un no ha finalizado

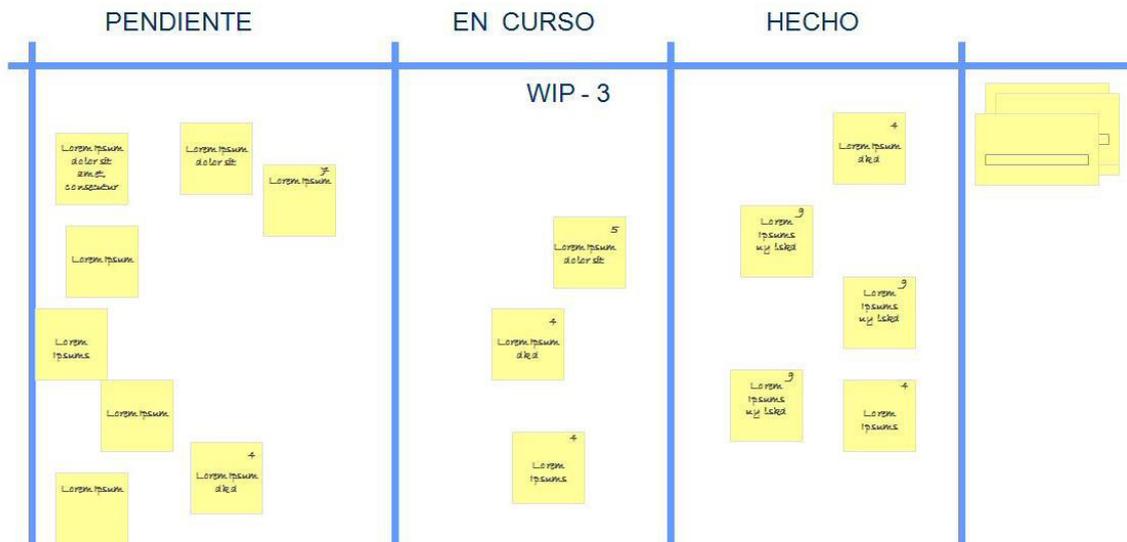


Figura 29: Tablero Kanban (Personalkanban, 2013:11)

Quizás una de las principales ideas de *kanban* es que el trabajo en curso WIP (*Work IN Progress*) debería estar limitado, es decir, que el número máximo de tareas que se pueden realizar en cada fase debe ser algo conocido. Si bien es cierto en *kanban* se puede definir cuantas “tareas” como máximo puede realizarse en cada fase del ciclo de trabajo (ejemplo pueden ser como máximo 11 o 4 tareas en desarrollo, como máximo 2 en pruebas, etc.) a ese número de tareas se le llama límite del “WIP”. La idea es centrarse en realizar todas las tareas y no empezar tareas continuas. Por ello limitar el WIP impide empezar tareas nuevas hasta que se hayan cerrado aquellas en las que se está trabajando.

c. **Scrumban**

Scrumban es una metodología híbrida que mezcla lo mejor de cada una de ellas (*Scrum-kanban*). Esta metodología dependerá de las necesidades de quien implemente la metodología, elementos de *Scrum* y de *Kanban*. *Scrumban* no es una metodología perfectamente definida y por eso puede amoldarse a circunstancias menos comunes tales como equipos de desarrollos unipersonales de un comienzo se

utilizó dicha metodología, pero se pasó a otro tipo de plano a crear nuestra propia metodología a base de flexibilidad de esta.

Lo bueno de la hibridación *scrumban*

- No se requiere el concepto de equipo
- No se requieren sprint, es decir, no hay plazos fijos entre entregas
- No se requiere una reunión diaria de equipo
- No se requiere una retrospectiva

Scrumban Iteration

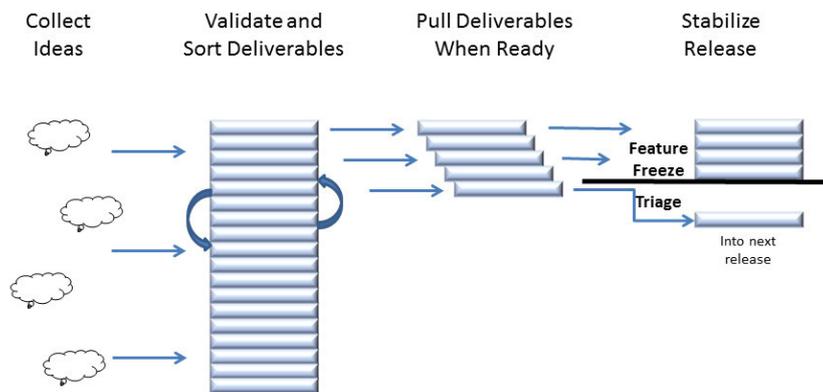


Figura 30: SCRUMBAN (Continuousagile, 2014)

En la figura se muestra el diseño de un proceso *Kanban*, Cada columna representa un paso en el ciclo de vida de tareas o flujo de trabajo.

Aunque se hayan revisado y estudiado diversas metodologías ágiles y tradicionales no llegan a centrarse en los requerimientos tan específicos que el desarrollo móvil necesita. Si bien es cierto las metodologías ágiles poseen ciertas propiedades que las hacen aplicables al dominio del software en los móviles, la dificultad que radica proviene del hecho que los límites de las metodologías ágiles no es tan claramente establecidos, por ejemplo a la

identificación del cliente y la orientación del producto. El cliente puede ser identificado como el distribuidor de *software* en el caso de una metodología ágil, sin embargo, especialmente en el caso de aplicaciones móviles, el problema de la identificación del cliente tiene mayor complejidad

Existen metodologías específicamente para el desarrollo de aplicativos móviles ya sean nativos o multiplataforma, muchas de estas aún se encuentran en etapa experimental se le denomina *Mobile-D – Mobile development process spiral*

C. Metodología móvil

Las metodologías ágiles son una buena alternativa para guiar un proyecto de desarrollo de *software* de tamaño reducido, como es el caso de nuestro proyecto, gracias a su simplicidad y gran facilidad de adaptación que poseen, pero se necesitan ser adaptadas a las características especiales de estos dispositivos con el fin de obtener un producto de calidad.

Dentro de estas características se menciona la gran rapidez con que van cambiando las versiones de los sistemas operativos móviles más populares (en caso de nuestro *android*). La aparición de nuevas prestaciones de hardware, la tendencia de desarrollar aplicaciones en cortos lapsos de tiempo y en la mayoría de casos sacrificando la calidad del producto, precisamente por no seguir una metodología o técnicas de desarrollo propias de la plataforma trabajada.

a. Mobile D

Mobile-D consta de cinco fases: exploración, iniciación, producción, estabilización y prueba del sistema. Cada una de estas fases tiene un número de etapas, tareas y prácticas asociadas. La primera fase debe generar un plan y establecer las características del proyecto (se divide en 3 etapas)

- Definición del alcance : La planificación inicial del proyecto
- Establecimiento de actores : los clientes que forman parte activa en el proceso de desarrollo
- Establecimiento de proyectos : en análisis y recogida de requerimientos

En la segunda fase se establece el entorno técnico como los recursos físicos, tecnológicos y de comunicaciones (incluyendo las reuniones en el equipo de desarrollo)

En la tercera fase, producción existen repeticiones de iteraciones hasta implementar todas las funcionalidades. Se planifica la iteración de trabajo en término de requisitos y tareas a realizar.

La fase de estabilización se lleva a cabo las últimas acciones de integración para asegurar que el sistema completo funciona correctamente. Adicionalmente se puede considerar la producción de documentación.

La última fase (prueba y reparación 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.

b. *Mobile development process spiral*

Como su nombre indica es un modelo de desarrollo en espiral como base, incorpora procesos de evaluación de usabilidad con el fin de garantizar un diseño centrado en el usuario. Esta metodología se encuentra como experimental la nombramos por el énfasis que le otorga en el diseño y la experiencia de usuario (UX) a un modelo de proceso

El proceso de desarrollo se define en cinco iteraciones cada una con tres tareas (definición de requisitos, diseño y prueba). La primera iteración se determina los requisitos del sistema y se identifican usuarios, tareas y contextos en los que se utilizará la aplicación.

Luego, se definen y priorizan los atributos de facilidad de uso. La segunda iteración el equipo recogerá más datos y requisitos, explorada si existen mayores usuarios potenciales, tareas y contextos que se utilizarán en la aplicación. En la tercera iteración los desarrolladores pueden identificar y priorizar los atributos de usabilidad con mayor claridad utilizando los resultados de la iteración anterior, se desarrolla el diseño de todo el sistema y se realiza la versión beta con sus respectivas pruebas.

En la cuarta iteración los resultados de la iteración anterior son utilizados para identificar y dar prioridad a los atributos de facilidad de uso, se desarrolla la versión beta final y se libera para su evaluación por parte del cliente, en la quinta iteración se desarrolla el producto final. Se realiza una evaluación de facilidad de uso, la calificación de la fase anterior, una última alteración en el producto final se realiza sobre la base de los resultados y se libera al producto.

Esta última metodología se consideró como atractiva para el desarrollo del proyecto, por tal motivo la metodología que se desarrolló para este proyecto tomo como base dicha metodología, por las facilidades, el metraje, la distribución de tareas dispersos en procesos puntualizados y ordenados bajo una jerarquía que no lo convierte como una metodología tradicional ni ágil, estamos entrando al mundo del post agilismo, una corriente en la que se consideró varios procesos para este proyecto, acompáñenos.

3.4 Marco legal

Se proseguirá a continuación a tomar el alcance de normas consideradas dentro del presente proyecto:

- Protección clasificada de información
- Derechos de los usuarios
- Derecho a la privacidad, intimidad y a los datos personales
- Implementación de sistemas de seguridad de la información

Decreto Supremo que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N° 681 y ampliatorias

Norma: decreto supremo n° 070-2011-pcm

Nombre entidad Presidencia del Consejo de Ministros (PCM)

Tipo de norma decreto supremo

DESCRIPCIÓN Decreto Supremo que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N° 681 y ampliatorias

FECHA CREACIÓN 27/07/2011

Norma Técnica Peruana N°129-2012-PCM, Técnicas de seguridad. Sistemas de gestión de seguridad de la información, en todas las entidades integrantes del sistema nacional de informática

NORMA: RESOLUCIÓN MINISTERIAL N° 129-2012-PCM

NOMBRE ENTIDAD: PRESIDENCIA DEL CONSEJO DE MINISTROS (PCM/ONGEI)

DESCRIPCIÓN: Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la

Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.

FECHA CREACIÓN: 25/05/2012

Norma técnica Peruana "NTP ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información

Tabla 3: Resolución ministerial gestión seguridad de la información

NORMA: RESOLUCIÓN MINISTERIAL Nº 197-2011-PCM		
m	NOMBRE	PRESIDENCIA DEL CONSEJO DE
a	ENTIDAD	MINISTROS (PCM/ONGEI)
é	TIPO DE NORMA	RESOLUCIÓN MINISTERIAL
i	DESCRIPCIÓN	Establecen fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información"
	FECHA	21/07/2011

a nº 0187-2010-pcm. Ejecución de encuesta de seguridad información en la administración pública

NORMA: RESOLUCIÓN MINISTERIAL Nº 0187-2010-PCM

NOMBRE ENTIDAD: PRESIDENCIA DEL CONSEJO DE MINISTROS (PCM)

TIPO DE NORMA: RESOLUCIÓN MINISTERIAL

DESCRIPCIÓN: Autorizan ejecución de la "Encuesta de Seguridad de la Información en la Administración Pública - 2010"

FECHA CREACIÓN: 15/06/2010

3.5 **ARQUITECTURA DEL SISTEMA O METODOLOGÍA**

En este capítulo se detallara el proceso de la implementación metodológica del proyecto. Empezando por los entornos de desarrollo donde se ha llevado a cabo, las principales tecnologías que han tomado partido para el aplicativo y se mostrara los debidos diagramas UML más relevantes del negocio para comprender mejor la arquitectura interna de nuestro aplicativo

3.5.1 Metodología Mejora Continua de Procesos Móviles (MMCPM)

Mediante las metodologías móviles, ágiles y tradicionales podemos establecer cierto paralelismo dentro del enfoque de un modelo hibrido donde seleccionaremos un conjunto de métricas del rendimientos de los métodos ya mostrados. Por un lado, las métricas cuantitativas que se suelen relacionar con los procesos tradicionales de desarrollo, por el otro lado la filosofía ágil de desarrollo veloz y mejora continúan del software. Esta solución metodológica ofrece un nuevo alcance en distintos trabajos centrados en relacionar el desarrollo ágil con metodologías de gestiones móviles y tradicionales.

A. Alcance de mejora continua de procesos móviles

Tabla 4: Metodología MMCPM



B. Diagrama de procesos MMCPM

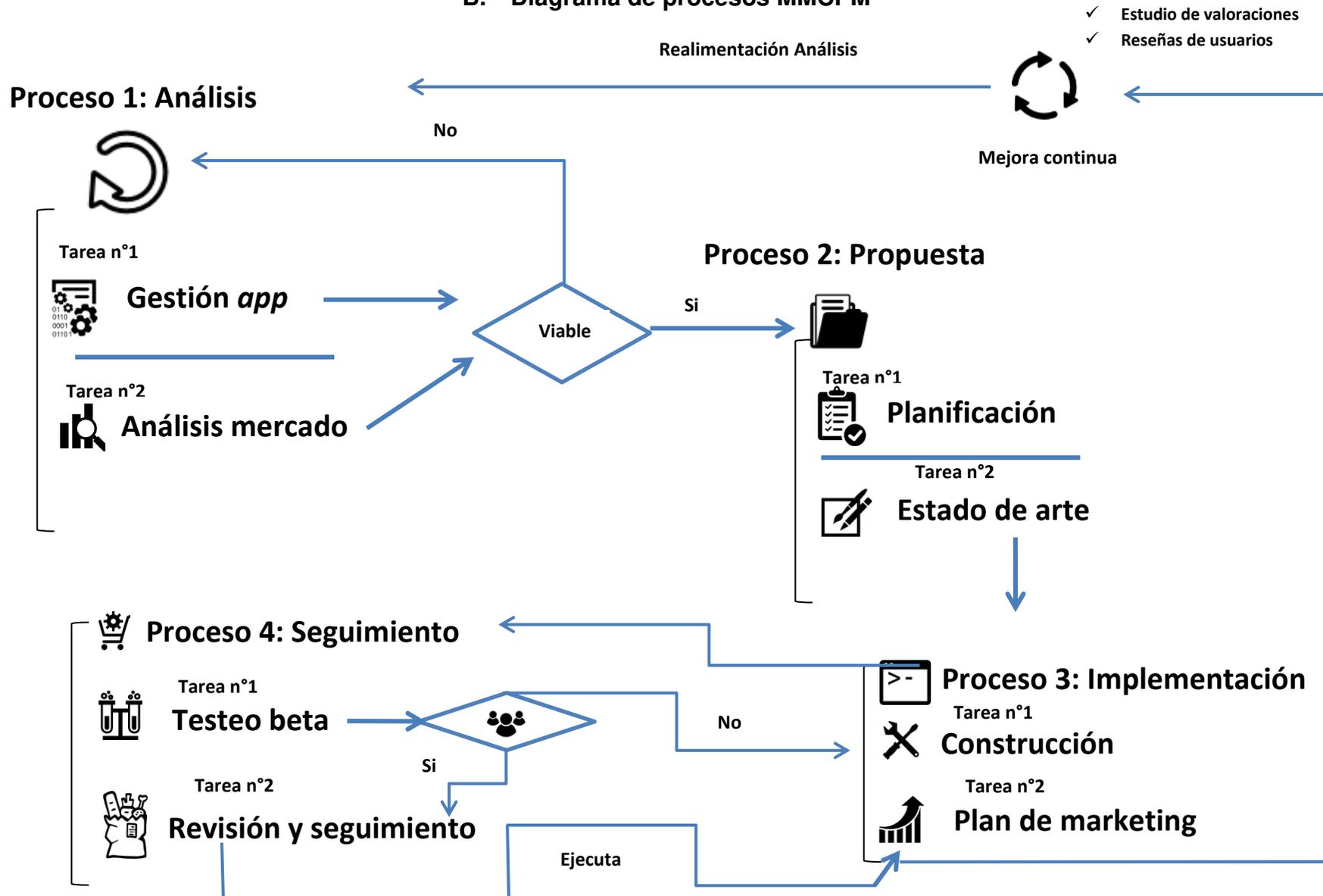


Figura 32: Metodología MMCPM

En la siguiente figura intente ser lo más dinámico posible, para explicar los procesos de mi propia metodología de desarrollo

CAPÍTULO IV:

DESARROLLO DE LA APLICACIÓN

4.1 LEVANTAMIENTO DE INFORMACIÓN

4.1.1 Planificación del proyecto

Como se especificó en el **capítulo III (3.5)** se implementara bajo una metodología hibrida de distintas metodologías, nombrara (MMCPM) para el desarrollo de YAPPO! Como una solución para los alumnos de la Universidad de Ciencias y Humanidades.

Como habríamos descrito el primer proceso se dividirá en dos iteraciones o tareas, la primera fase es analizar que se desea desarrollar de acuerdo a la necesidades actuales, la segunda el estudio propio del mercado de la plataforma y de la *app* si es viable o no el desarrollo, si es aceptable la gestión de la *app* y existe cabida en el mercado se proseguirá al segundo proceso, en el caso contrario se gestionará otro modelo las *app*'s postulantes.

La propia metodología fue estudiara, diseñada, analizada desarrollada y documentada por la persona encargada del proyecto de tesis, la metodología sigue propiamente el ciclo de vida y la corriente creciente *post* ágil utilizando *frameworks* de trabajo, como base e inspiración fue tomada en gran parte la metodología *Mobile Development Process Spiral*.

A. Análisis de mercado

Actualmente el mercado de teléfonos inteligentes en todo el mundo alcanza una nueva marca en lo que fue el último trimestre del 2014, moviéndose más allá de la marca de 300 millones de unidades. De acuerdo con los datos finales de la *international Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker*



Figura 33: Plataformas más utilizadas (Netdreams, 2015)

Existen multitudes de plataformas tecnológicas acompañada de sus respectivos SO (sistema operativo), tanto para las computadoras estacionarias, servidores e incluso para los dispositivos móviles, un dato interesante de la actual grafica que desaparece totalmente los SO móviles más populares del año 2000-2010, *Symbian*, *BlackBerry* y los extintos Web OS, RIM y PALM



Figura 34: SO móviles más vendidos (Netdreams, 2015)

Como podemos observar en las 2 gráficas, las plataformas dominantes, *Android* y *ios*, esta última alejada por un gigantesco nivel de margen, siguen creciendo y no solo en el mundo si no el Perú forma parte también del aficionado robot de google

a. *Android* tiene 88% y los 5% ¿Se acabó la guerra?

Como habríamos comentado *Android* hace su aparición a mediados del 2008 bajo la firma *HTC dream* más adelante obtenida por *google* y sus ideas innovadoras de *Open Source* consiguió obtener millones y millones de ventas dejando atrás la manzana de *Apple*.

El mercado acepto cada día más a *Android* con *Samsung* como su compañero desde el principio de los tiempos. Actualmente controla la mayor parte del mercado desde china hasta Perú por lo cual más posibilidades existen en el financiamiento y

popularidad desarrollar una aplicación bajo *Android* que en iOS, sin mencionar la libertad que existe en dicha terminal. Por el momento *Android* no tiene rival, donde los desarrolladores nos enfocamos en un mercado donde existan mayores posibilidades de usabilidad de nuestro producto, observamos que el mercado *Android* es mucho más extenso que en un mercado de “categoría social”. Por mi parte esta guerra ya finalizo.

- **Aplicaciones más utilizadas**

Desde la aparición de internet, la necesidad de comunicar a personas situadas en cualquier punto del planeta, con el intercambio de archivos e informaciones a través de internet ha sido una de los mayores problemas de los desarrolladores actuales, por cuestiones de seguridad y el compartimiento adecuado.

Hace menos de una década esta funcionalidad estaba limitada por un gran porcentaje de la población, limitada solo al uso de un ordenador y el recordado *msm*. Pero gracias al avance tecnológico de los Smartphone ha sido extrapolada a casi cualquier dispositivo móvil (*smarthphone*, Tablet, ipod, ipad, etc.) acompañado del aumento extraordinario de usuarios que acceden a este tipo de servicios

Según el IV Estudio sobre *Mobile Marketgin* de IAB un 91% de los usuarios utilizan su Smartphone para chatear y correo de los cuales un 72.5% lo hace a diario.

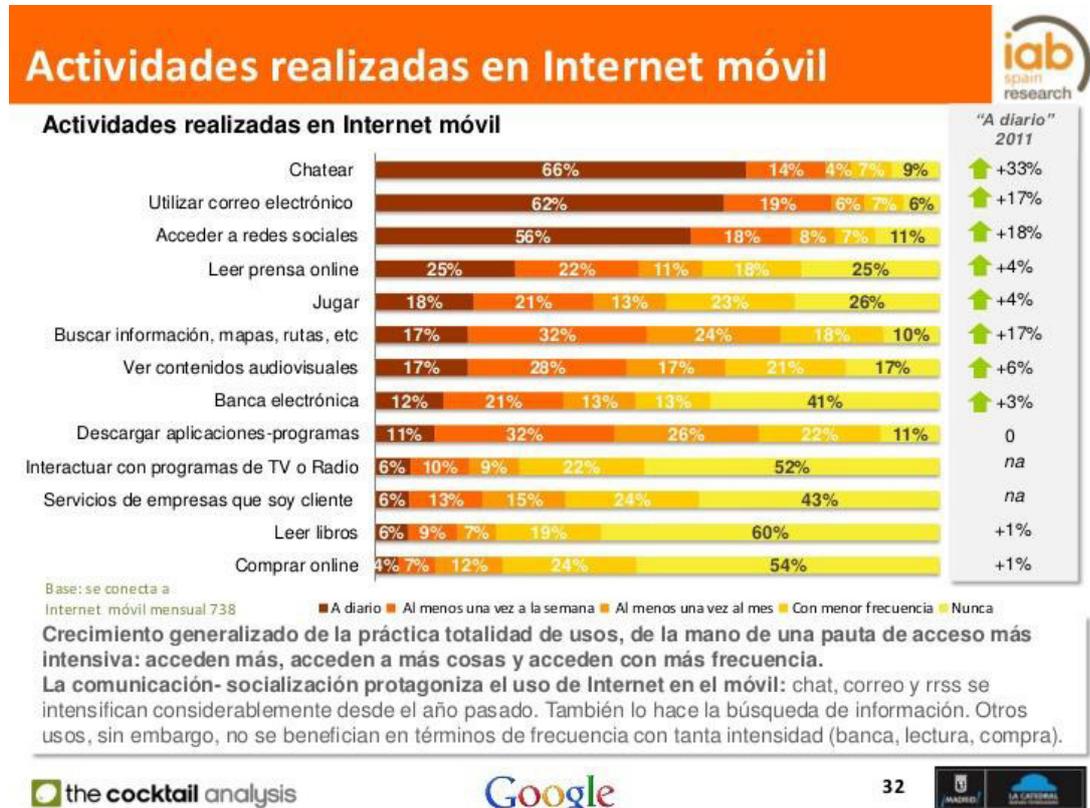


Figura 35: Actividades más realizadas en internet móvil (Sepp.pe, 2015)

Basándonos en las estadísticas anteriores y en su proyección de plataforma en el futuro, podemos afirmar que la mensajería instantánea es una de las herramientas informáticas más utilizadas actualmente, con millones de usuarios en todo el mundo. ¿Pero que hace diferente Yappo de las demás aplicaciones? ¿Qué cosas nuevas trae consigo Yappo y cuál es su enfoque a la nueva era de la mensajería móvil?

- **Aplicaciones de mensajería**

Como habríamos comentado en la actualidad existen gran cantidad de aplicaciones de mensajería instantánea para Smartphone con diferentes matrices y diseño, aunque su funcionalidad básica es en todos la misma: “crear un medio de comunicación flexible entre personas mediante mensajes de texto a través de un Smartphone y una conexión de internet, lo que hace este tipo de servicios la mayor ventaja ofrecer e interactuar en tiempo real con personas sin importar el lugar ni la zona horario en la que estén ubicados algunas tienen mayor éxito que otras, a continuación nombraremos las aplicaciones más populares actualmente, la figura siguiente fue realizada por el jefe de proyecto (yo), las descripciones fueron sacadas de la propia páginas web de las aplicaciones en el transcurso que se desarrolló el proyecto.



Whatsapp Messenger

Whatsapp Inc.

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

Información: Whatsapp fue creada en enero de 2009 y su segunda versión (junio de 2009). Logro tener 250.00 usuarios. Se estima que ha llegado a mover más de 54000 millones de mensajes al día. El año pasado fue comprado por la compañía Facebook por un valor de 19000 millones de dólares

Ventajas:

- Actualmente es la aplicación móvil más famosa del planeta. Por lo tanto, es la que más usuarios tiene por lo que solo usar esta aplicación está casi garantizado comunicarte con la mayoría de personas que conozcas

Desventajas:

- La privacidad se limita a mostrar la última de hora que el usuario escribió un mensaje.
- Seguridad *Whatsapp* es la que ha presentado mayor fallo en esta lista. A lo que tenemos que sumar la desconfianza de muchos usuarios, al saber que Facebook compro dicha aplicación
- Whatsapp ha sufrido repentinos fallos en su conectividad, muchos de ellas muy mediáticos, llegando a privar del servicio de los usuarios en algunos casos durante horas



Line

Naver Japan corp.

<http://line.me/es/>

Información: Era la principal rival de *whatsapp* hasta la aparición del avión de papel de google. Cuenta con más de 300 millones de usuario, supera a whatsapp en algunos países como corea oh Japón. Se diferencia por su interfaz gráfica y la posibilidad de enviar *stickers*

Ventajas:

- Interfaz gráfica amigable y dinámica
- Dispone de servicio de atención al cliente disponible directamente desde la propia aplicación como si fuera un contacto más.

Desventajas:

- Uso excesivo de batería, posiblemente por su interfaz y sus "juegos"
- No permite compartir documentos multimedia

Figura 37: Aplicaciones msm



Viber

Viber Media Inc.

<http://www.viber.com>

Información: Al ser una aplicación de mensajería instantánea, es muy extendida al tener a sus más de 200 millones de usuarios activos, posee prácticamente las mismas funciones de los anteriores. Sin embargo algunos medios recomiendan no usarlo ya que viola los derechos de privacidad de sus usuarios, almacenando información tuya o mía y de nuestros contactos a sus servidores.

Ventajas:

- Es completamente gratuito, actualmente su licencia es de tipo "freeware"
- Sincroniza automáticamente con la agenda del sistema. El usuario no tiene que preocuparse de agregar contactos al programa.

Desventajas:

- Privacidad de datos del usuario : Viber ha sido muy criticado por almacenar data persona en sus servidores
- Dispone de la funcionalidad de hacer video llamadas, aunque se encuentra en fase beta



Telegram

Telegram LLC

<http://www.telegram.org>

Información: Apareció a mediados del 2013 justo cuando comienza el proyecto "YAPPO" y comenzó a crecer por el centro de Europa. Su éxito se basa principalmente en su enfoque de seguridad de los datos. Actualmente cuenta con 35 millones de usuarios en todo el mundo

Ventajas:

- Conversaciones seguras: Telegram nos permite realizar conversaciones seguras. Que no se almacenan en sus servidores
- Interfaz sencilla y poco cargada
- Permite la autodestrucción de mensajes
- Permite enviar archivos de 1GB

Desventajas:

- Sus servidores es código de propietario. Por lo que no se puede confirmar el nivel de seguridad del que presumen.

Figura 38: Aplicaciones msm2

Como se muestra en las figuras se creó una tendencia de los videos llamados, envió de archivos de tipo gifs, stickers, videos, etc. En algunos casos la complementación de juegos internos en la *app* que puede producir calentamiento al procesador si el tiempo es prolongado. Puntos interesantes y atractivos son los mensajes de auto destrucción que si por la época del estudio, el pionero de esta idea fue snapchat, hasta que ingreso un proceso de judicial por los mensajes que desaparecían después de enviarlos, otras dificultades fueron la ubicación geográfica del usuario, el almacenamiento de la lista de contactos de sus usuarios en los servidores de snap-, pero esa es otra historia que debes de investigar.

Aparte de las intromisiones en la privacidad, fallos, agujeros, servicios que caen y se vuelven a levantar después de 4 horas. Podríamos destacar aun cuando estos problemas fueron subsanados (algunos en pendientes). Obliga que los usuarios deseen mejores aspectos en la privacidad y seguridad de sus datos, ya que es un aspecto muy solicitado por los usuarios y que se le ha prestado muy poca atención. Es en este punto de partida donde Yappo comienza a dar servicios de seguridad y privacidad en la comunicación de sus clientes, alumnos de la universidad ciencias y humanidades. Después de ver que el proyecto es viable, ingresa a la planificación. Hemos de demostrar nuestro primer Project nos ayudó mucho en la planificación.

4.1.2 Recopilación de información

A. Herramientas a utilizar para el levantamiento de información

Al ser una metodología hibrida se prosiguió a utilizar las entrevistas como los cuestionarios para el levantamiento de información.

- Entrevistas: Se realizan con un interlocutor que atiende un cuestionario o unos Objetivos de control de interés de conocimiento general del auditor.

- Encuesta: Es un instrumento de investigación que consiste en una serie de preguntas y otras indicaciones con el propósito de obtener información de los consulta

a. Modelos de encuesta

Para el presente proyecto se consideró como universo a la comunidad universitaria de la Universidad Ciencias y Humanidades.



Figura 39: Grafico estadístico de formula población infinita

De este universo fue necesario establecer la muestra conformada por estudiantes de ingeniería de sistemas. Para ello se utilizó la fórmula para establecer proporciones de poblaciones infinitas, en base a una probabilidad de ocurrencia, un nivel de confianza y un error máximo de estimación, obteniendo con ello que la muestra equivaldría 96 estudiantes.

b. Levantamiento de la información

Los datos encontrados por la encuesta fueron procesador utilizando hojas de cálculo de Excel, mismas que brindaron grandes facilidades para gestionar los datos y obtener los gráficos estadísticos presentes.

Las preguntas que conforman los formatos de las encuesta se encuentran en los anexos. A continuación se detallan los resultados de las encuestas aplicadas

Pregunta 1. ¿En algún momento, fuera del horario de clases, ha tenido usted algún comentario o indicación puntual de carácter académico hacia uno o varios estudiantes, y no ha podido comunicársela?

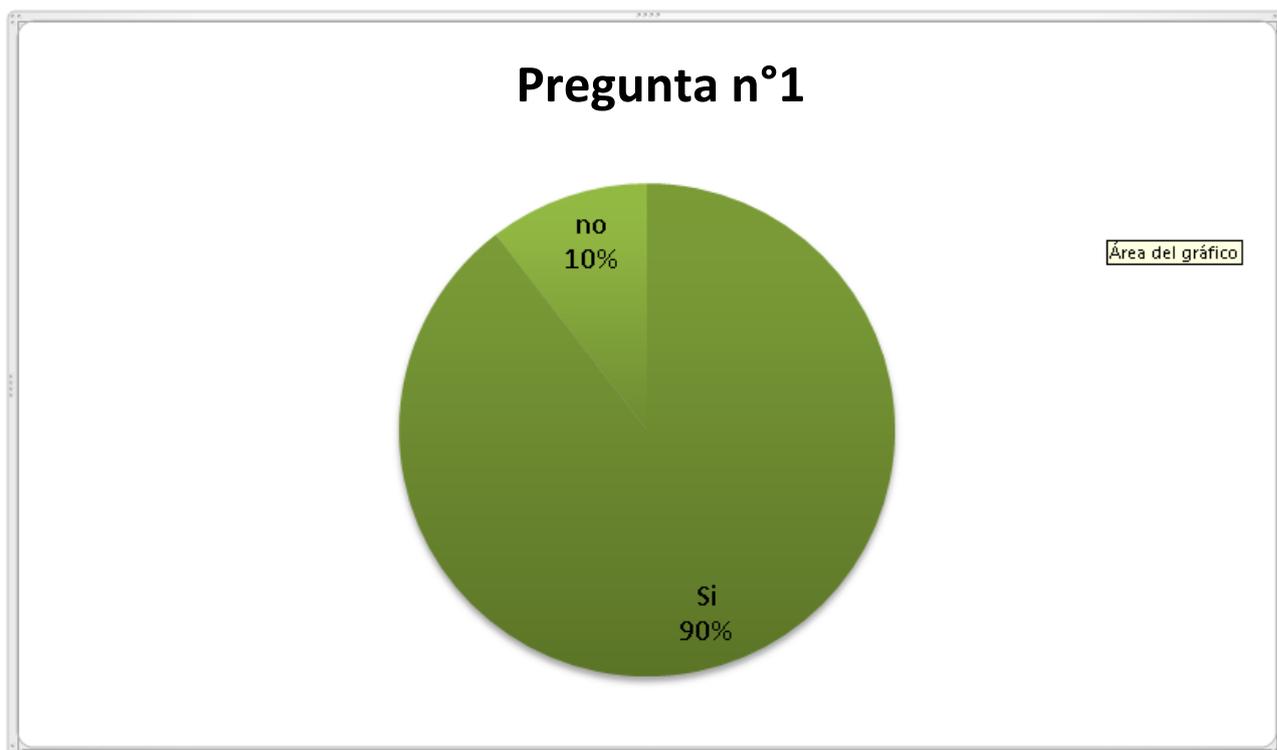


Figura 40: Grafico estadístico de la pregunta 1 a estudiantes

Según la encuesta aplicada a los estudiantes de la universidad ciencias y humanidades, los resultados indican en un grado mayor, la necesidad de realizar una consulta o comentario algún compañero que no se encuentra presente físicamente en la universidad, por ende no han podido realizar su consulta o comentario

Pregunta 2. ¿Tiene usted un teléfono inteligente? (si es no pasarse al nº 4)

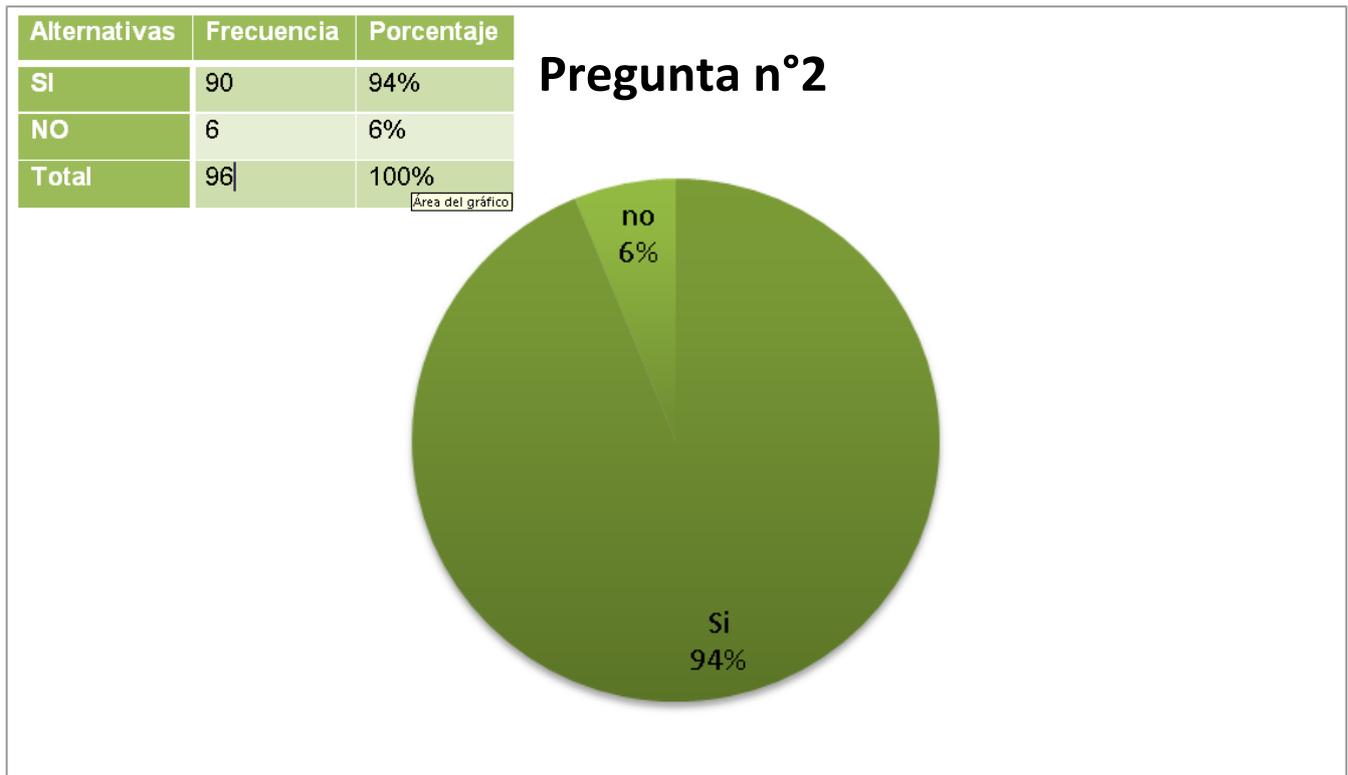


Figura 41: Gráfico estadístico de la pregunta 2 a estudiantes

Se muestra un 94% de dominio de los estudiantes de la universidad Ciencias y humanidades poseen un teléfono inteligente, con funciones más allá de simples llamadas, envío de texto. El reducido 6% restante, con el creciente avance de la tecnología móvil, tenderá a decrecer hasta llegar prácticamente a un 0%

Pregunta 3. ¿Con qué plataforma cuenta su dispositivo móvil?

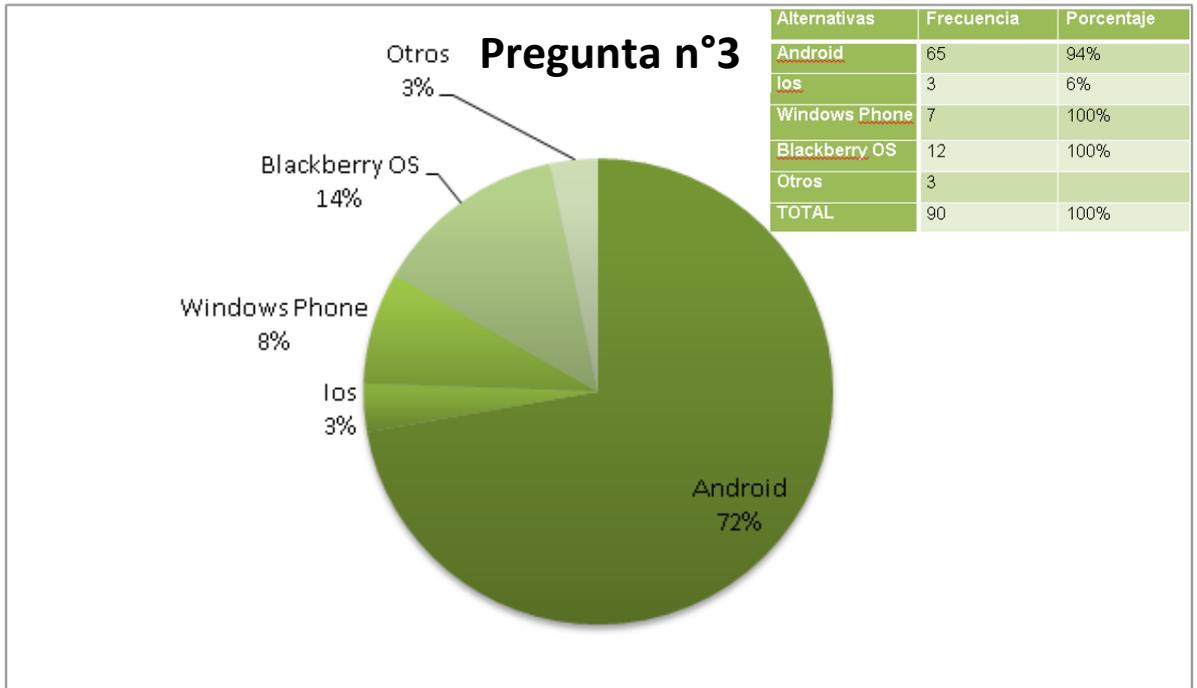


Figura 42: Grafico estadístico de la pregunta 3 a estudiantes

Como se planteaba al comienzo, la plataforma favorita por excelencia dentro y fuera del campus es *Android* y *BlackBerry OS* (cabe recalcar que los estudiantes utilizan los teléfonos móviles que la propia empresa les otorga, mayoritariamente las empresas trabajaban con los *BlackBerry* y muchos de ellos aún no migran). Y bueno como también habríamos comentado *Apple* prácticamente no tiene demasiada influencia en nuestro mercado.

Pregunta 4. ¿Cree usted que el desarrollo de aplicaciones móviles es lo más novedoso en la actualidad?

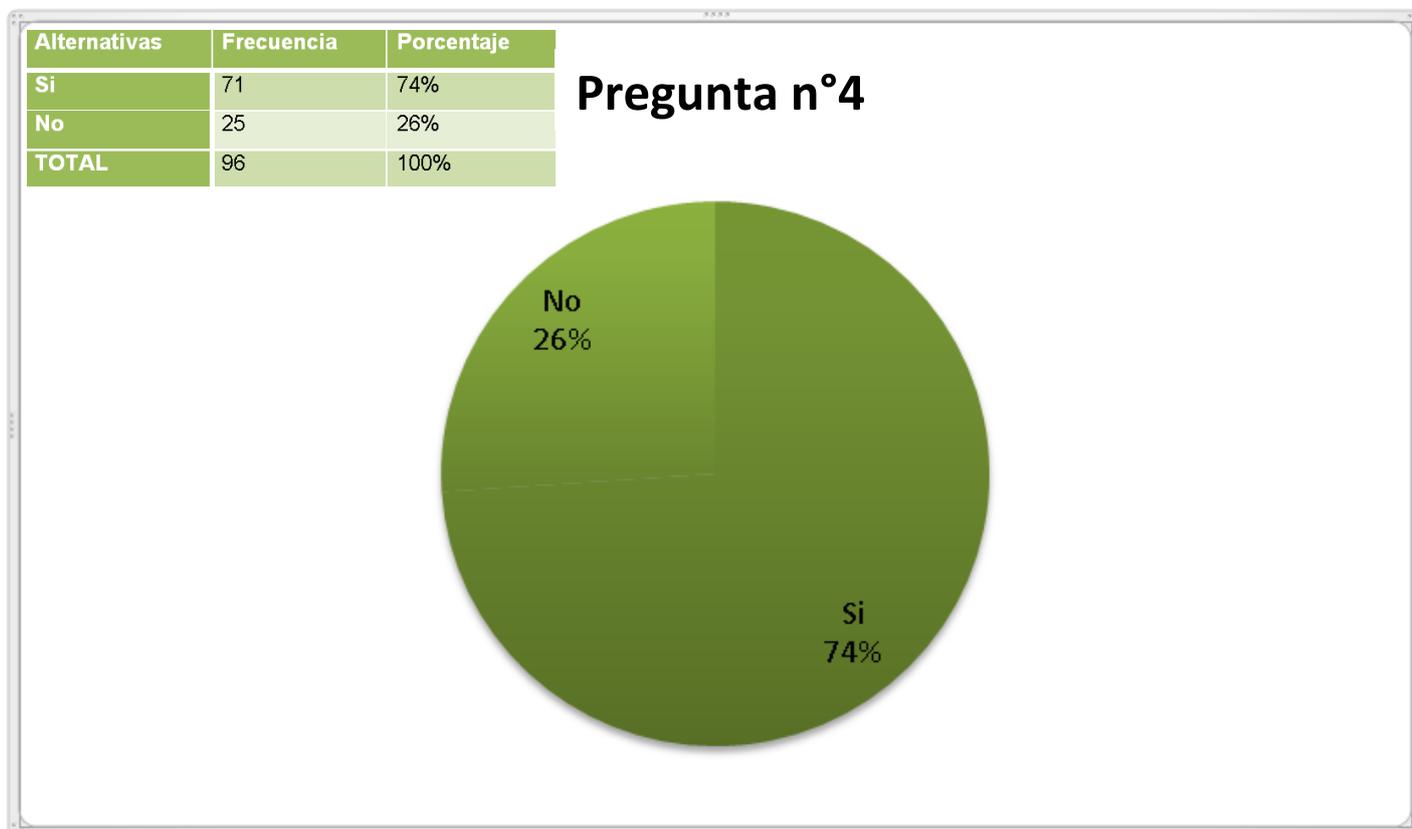


Figura 43: Grafico estadístico de la pregunta 4 a estudiantes

Mediante la pregunta planteada se evidencia que existe un gran porcentaje de interés en el desarrollo de aplicaciones móviles dentro de la misma universidad de los propios estudiantes.

Pregunta 5. ¿Para qué fin utiliza las aplicaciones de su celular?

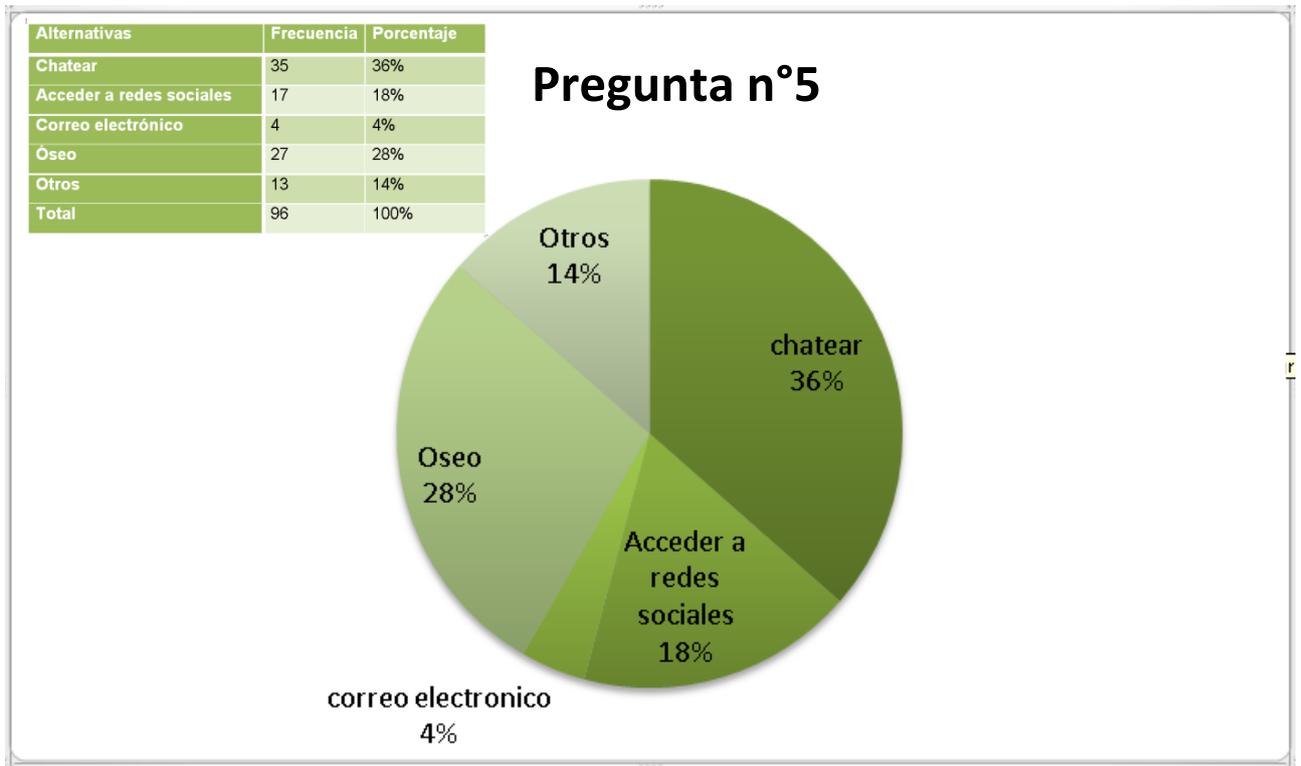


Figura 44: Gráfico estadístico de la pregunta 5 a estudiantes

El nivel de uso más alto respecto a aplicaciones más utilizadas por los alumnos de la universidad ciencias y humanidades es chatear, tanto por la poca carga de datos seguido por las redes sociales lo cual es lo contrario puesto muchas veces coge una cantidad extraordinaria de datos solo para revisar un perfil de un conocido.

Pregunta 6. ¿Qué aplicaciones de mensajería utilizas?

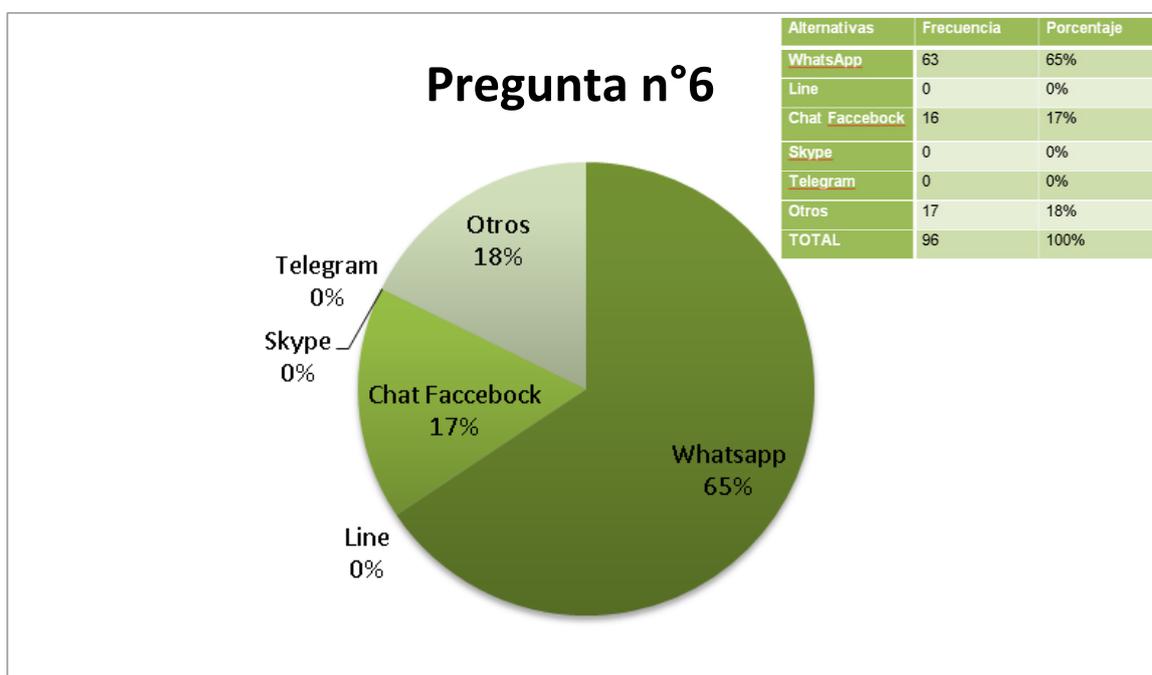


Figura 45: Gráfico estadístico de la pregunta 6 a estudiantes

Como observamos en la gráfica *WhatsApp* es la aplicación por excelencia más utilizada por los estudiantes a la hora de enviar un mensaje a tiempo real. Dando un margen el chat de *Facebook* con 17%.

Pregunta 7. ¿Le gustaría conocer nuevas aplicaciones para mensajería instantánea bajo un entorno seguro y privado sobre un sistema operativo *Android*?

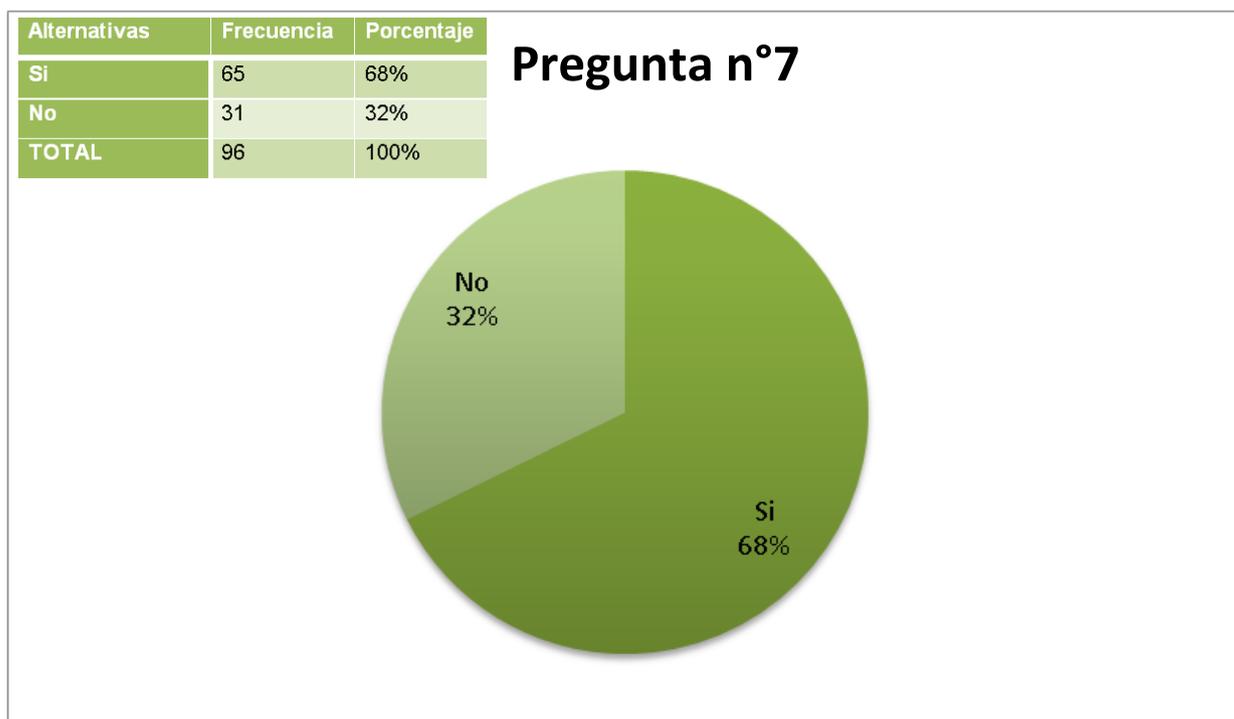


Figura 46: Gráfico estadístico de la pregunta 7 a estudiantes

Los estudiantes de la universidad ciencias y humanidades desean conocer nuevas aplicaciones donde su comunicación sea protegida e íntegra ante la transferencia. Bajo el entorno que ellos utilizan.

Pregunta 8. ¿Si dicha aplicación existiría y fuera gratuita, propia de la universidad la utilizaría?

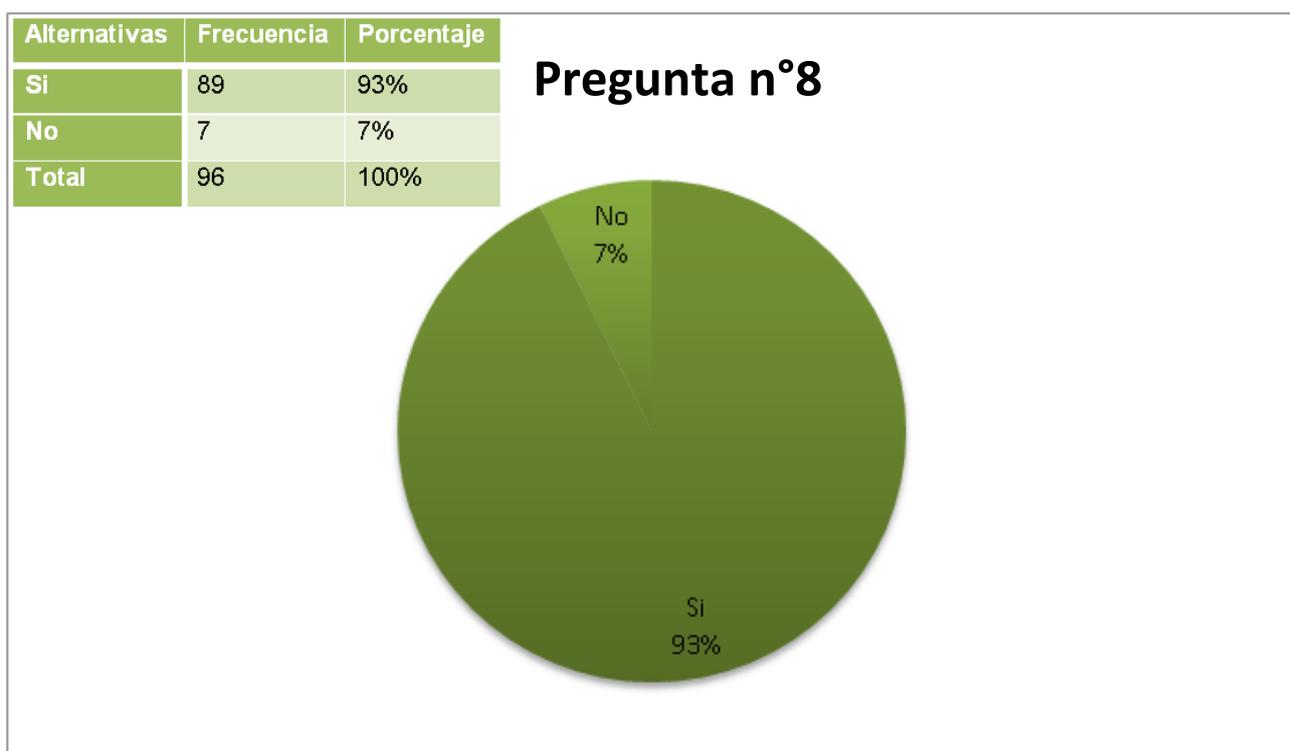


Figura 47: Gráfico estadístico de la pregunta 8 a estudiantes

Se denota que los Alumnos acceden a instalar más fácilmente si la aplicación es gratuita.

Pregunta 9. ¿Con que frecuencia la utilizaría?

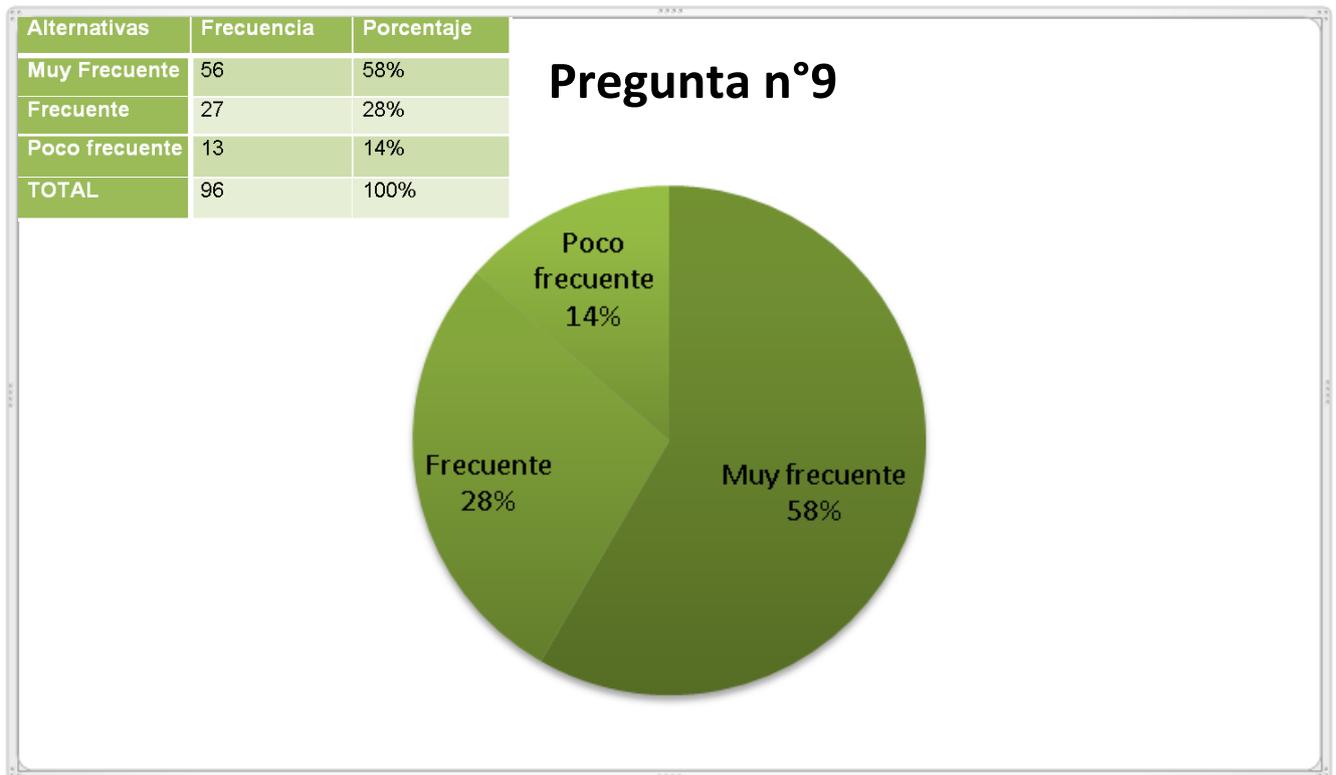


Figura 48: Gráfico estadístico de la pregunta 9 a estudiantes

La aplicación al ser gratuita y de mensajería se utilizaría con mayor frecuencia a lo esperado, dando como resultado que el desarrollo de Yappo! es aceptado por la comunidad estudiantil.

Pregunta 10. De las siguientes razones, seleccione aquellas por las cuales utilizaría la aplicación.

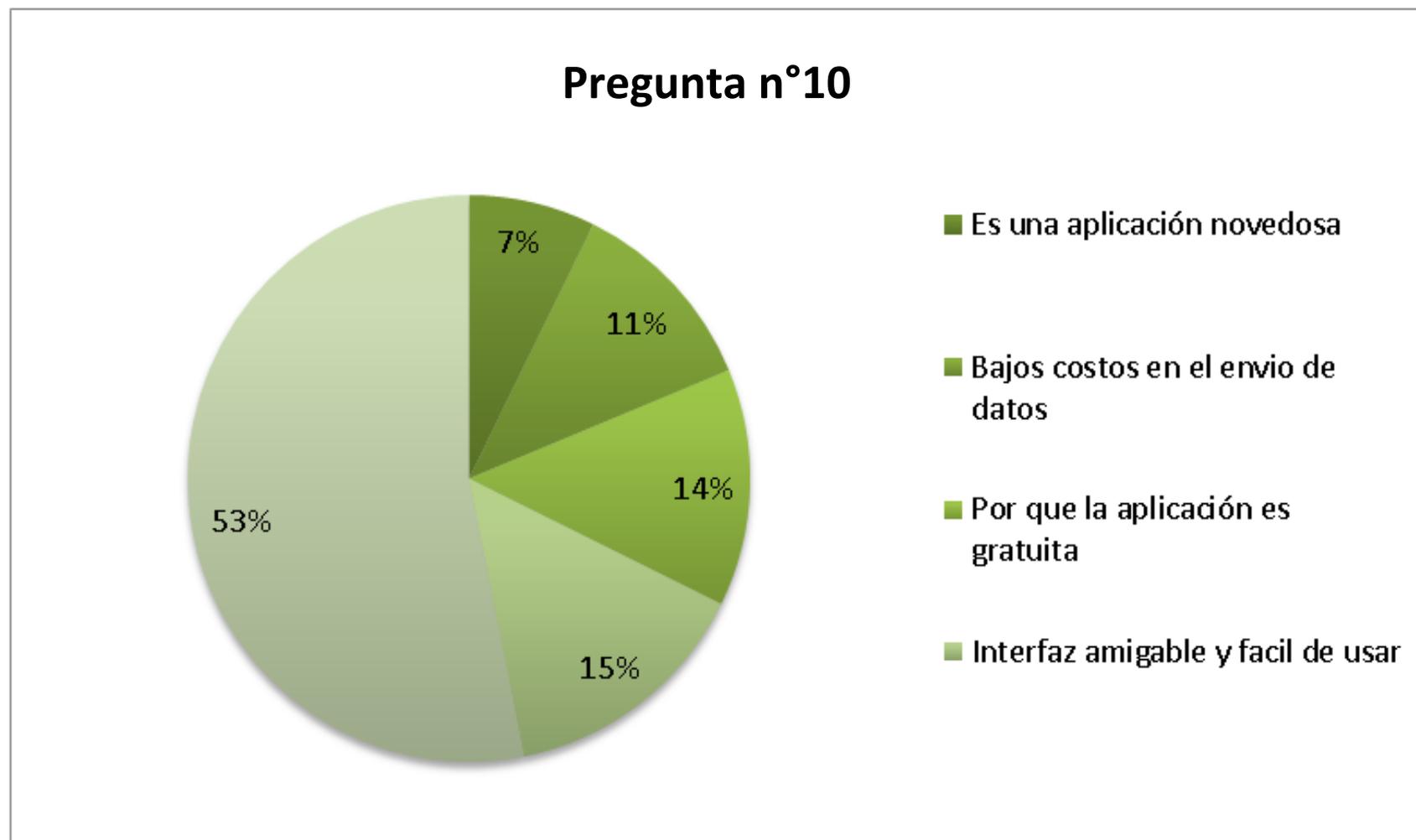


Figura 49: Grafico estadístico de la pregunta 10 a estudiantes

4.2 MODELAMIENTO

4.2.1 Modelo de casos de uso de negocio

A. Lista de actores de negocio

AN_Usuario: Es la persona que desea pertenecer académicamente a la institución.

TN_Pers.Regis.Aca: Personal que se encargara de tramitar la matricula del alumno

TN_Encar.Regis.Aca: Encargado de hacer el proceso administrativo en la atención al estudiante (proceso de matrícula, record de notas, otras actividades en la relación al estudiante)

TN_Direc_Academico: Autoridad encargada de realizar desarrollar difundir y coordinar las iniciativas responsabilidades de la universidad

TN_Dep_Academico: Departamento encargado de hacer la verificación y evaluación de los cursos designados por cada profesor

TN_Dep_Sistemas: Analiza las necesidades informáticas y/o tecnológicas en las áreas de información institucional.

TN_Dep_Produccion: Encargado de brindar información sobre cursos o carreras de especialización

a. Especificaciones del caso de uso del negocio

- Modelo CUN pers.regis.academico

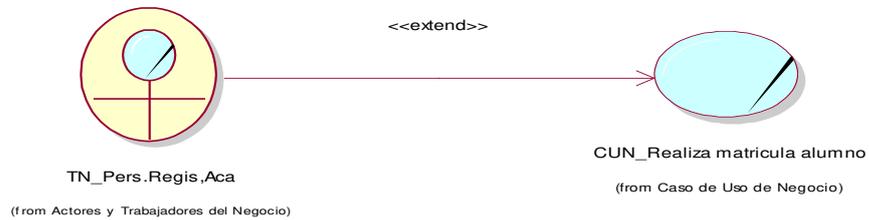


Figura 50: MCUN_registro_academico

Los Modelos CUN (Casos de uso de negocio) servirán para desarrollar la modelación y maquetación del negocio a la cual se basa el proyecto, a continuación se identificarán los numerosos procesos de la Universidad de Ciencias y Humanidades

Tabla 5: MCUN_Registro_Academico

Nombre	Matricula Alumno
Actores	Personal de Registros Académicos
Descripción	Procesos Matricula alumno

- Modelo CUN encar.regis.aca

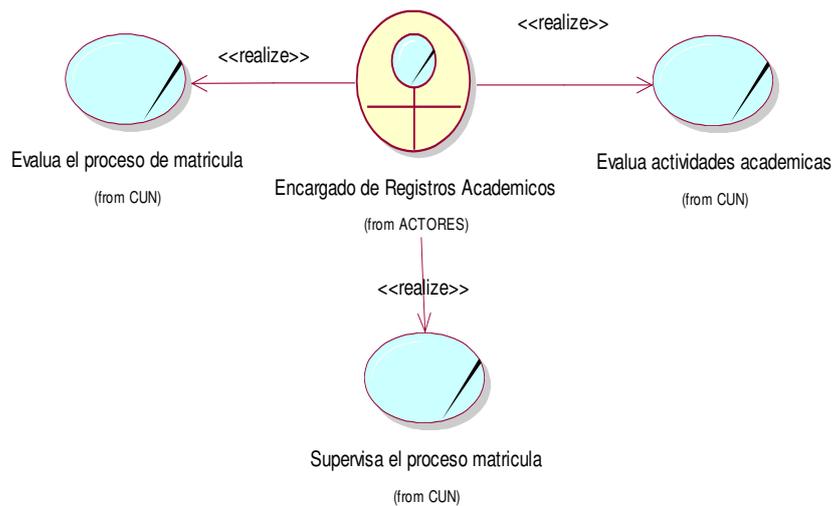


Figura 51: MCUN_encar.regis.aca

Tabla 6: MCUN_Encar.Regis.Aca

Nombre	Unidad Organizativa Encargado Registros Académicos
Actores	Encargado de Registros Académicos
Descripción	Procesos Encargado Registros Académicos

- Modelo CUN dep_academico

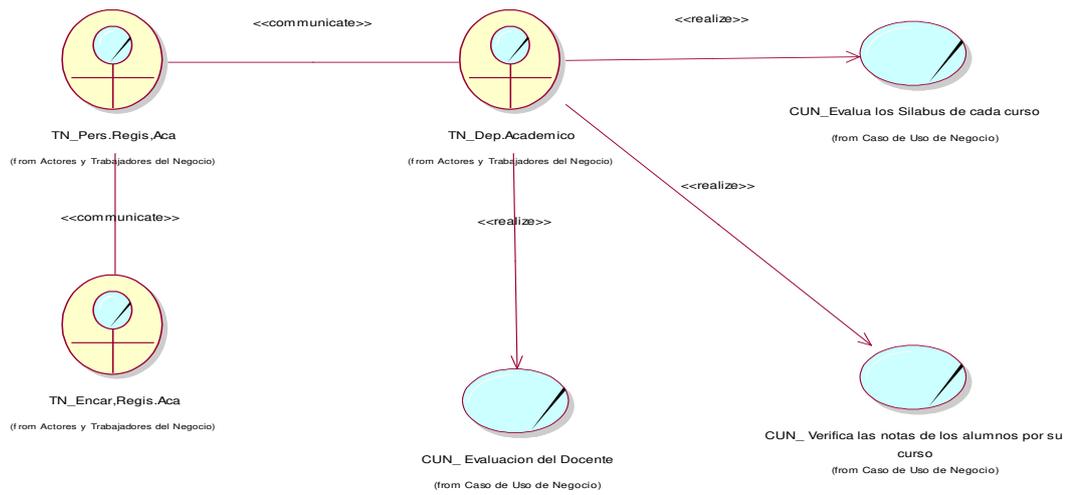


Figura 52: MCUN_dep.academico

Tabla 7: MCUN_Dep.Academico

Nombre	Departamento Académico
Actores	Dep.Aca,Encar.Regis.Aca,Pers_Reg.Ac
Descripción	Proceso del departamento académico

- Modelo CUN dep_produccion

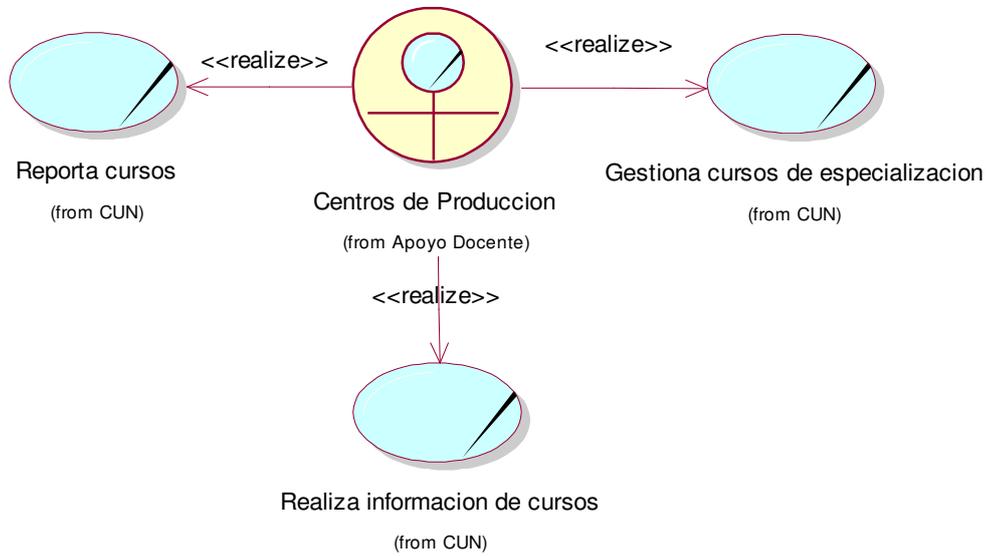


Figura 53: MCUN_dep_produccion

Tabla 8: MCUN_Dep_Produccion

Nombre	Departamento Producción
Actores	Dep.Produccion
Descripción	Proceso del departamento Producción

- Modelo CUN direc_academica

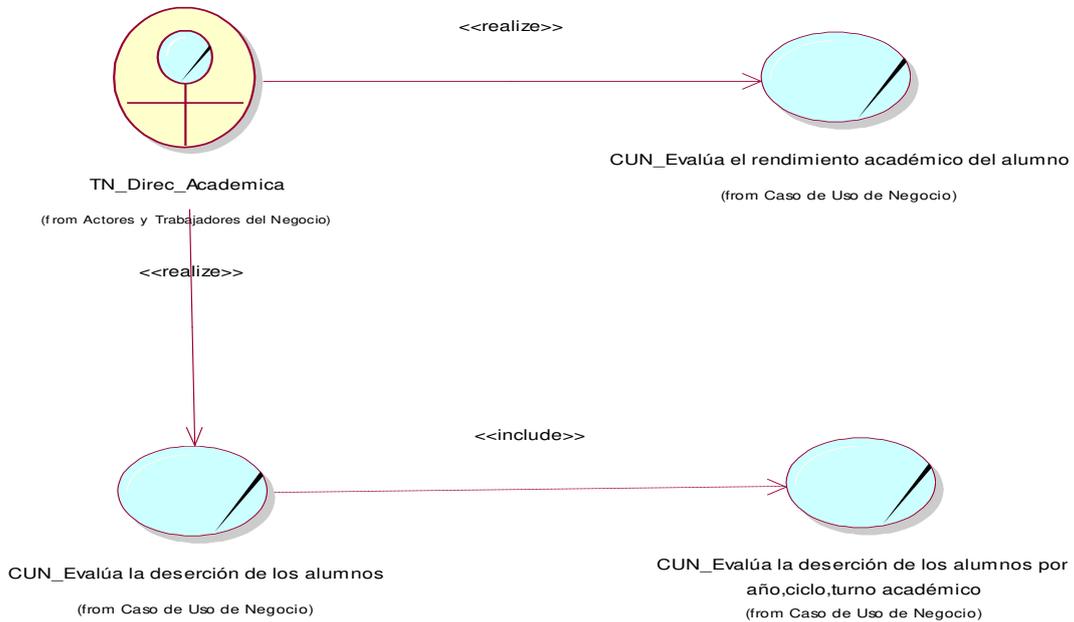


Figura 54: MCUN_direc_academica

Tabla 9: MCUN_Direc_Academica

Nombre	Direc_Academico
Actores	Direc_Academica
Descripción	Proceso del director académica

- Modelo CUN dep_sistemas

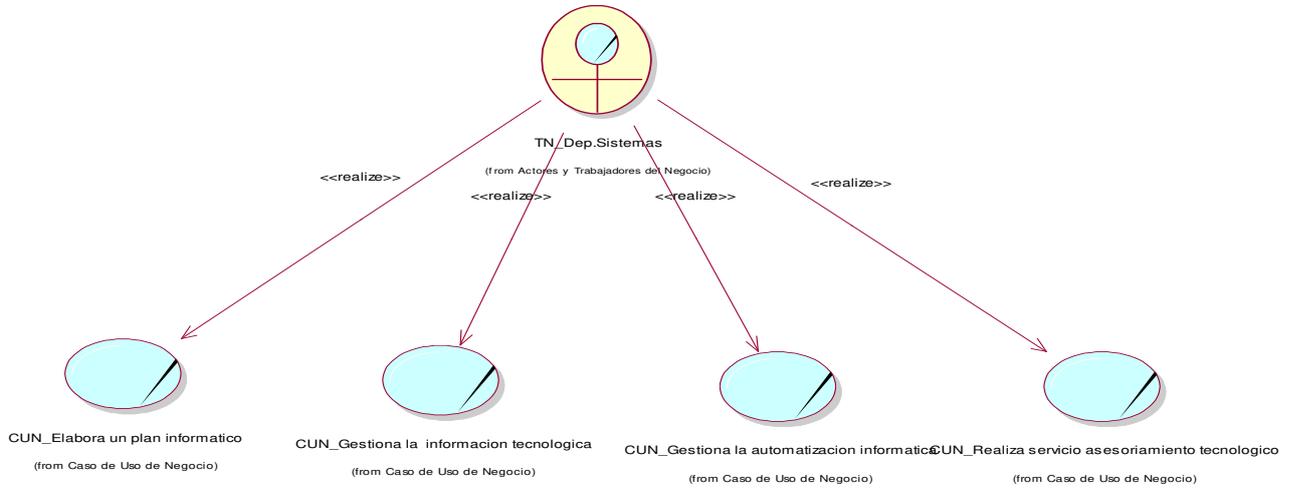


Figura 55: MCUN dep.sistemas

Tabla 10: MCUN_Dep.Sistemas

Nombre	Departamento sistemas
Actores	Departamento de sistemas
Descripción	Proceso del departamento de sistemas

C. Modelo general CUN

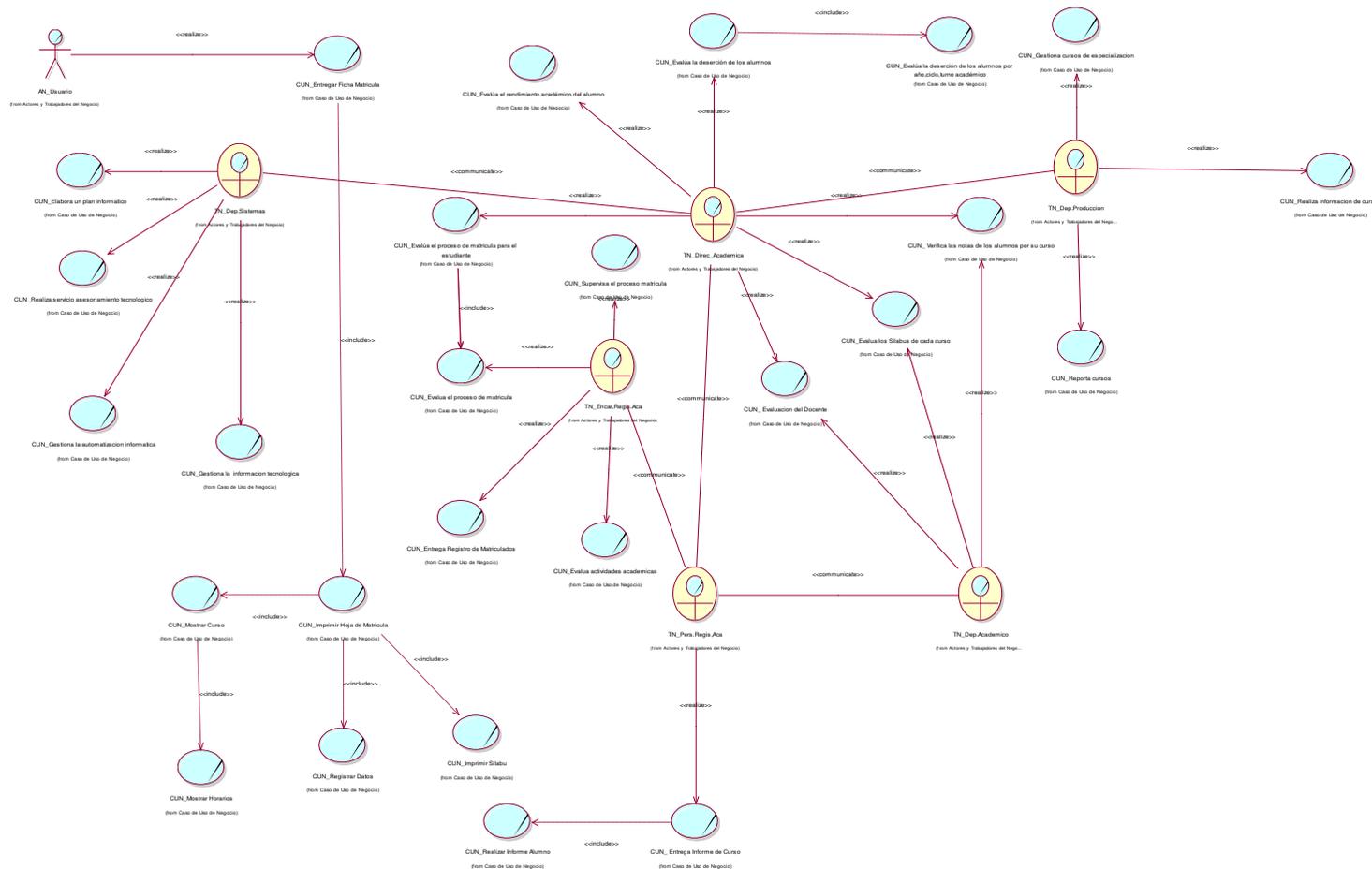


Figura 56: MCUN_general

El modelo general CUN y modelo general de CUS (casos uso de sistema). Son los modelos generales de todos los procesos del negocio y de sistema detallados anteriormente.

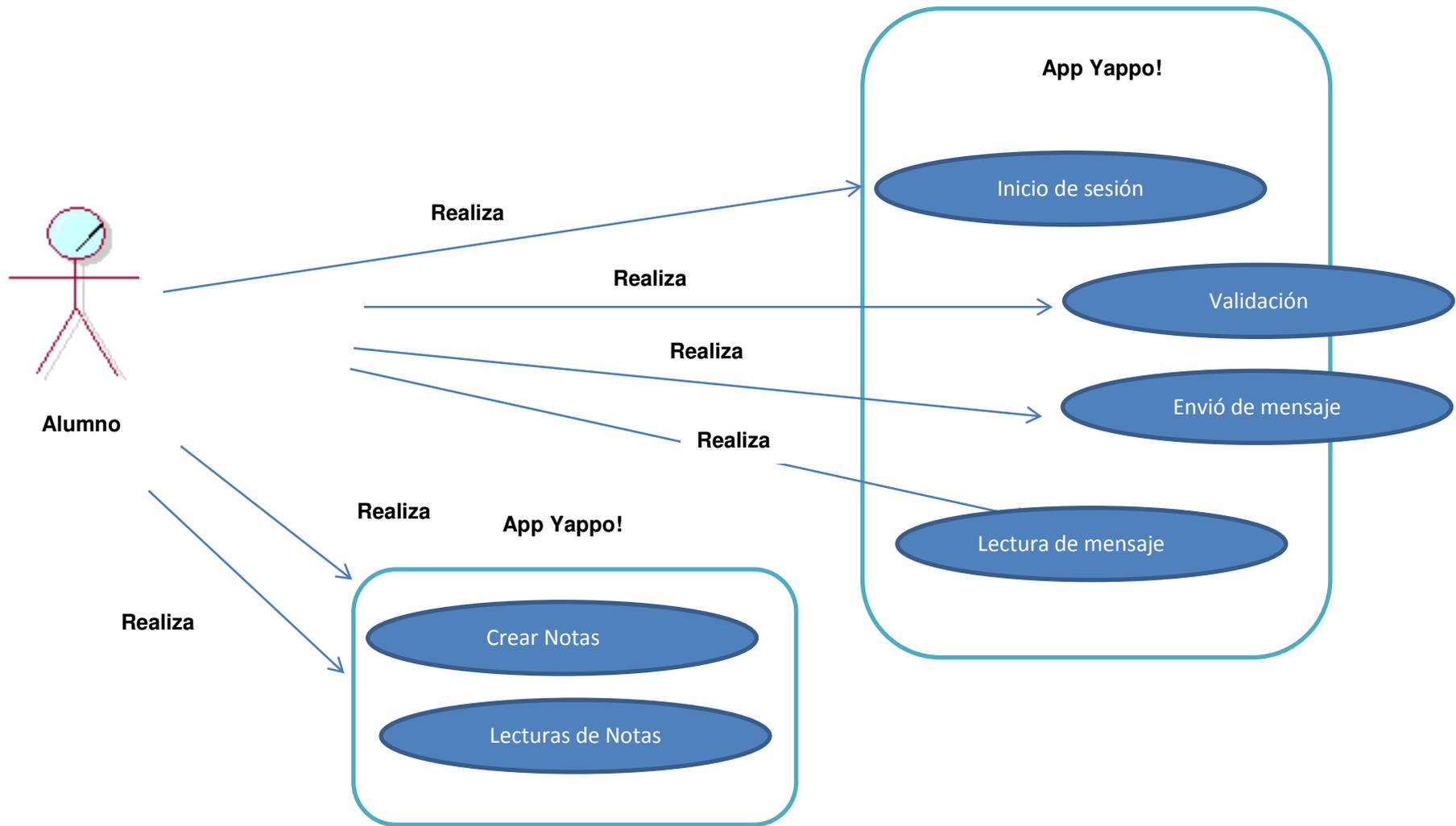


Figura 57: MCUN_GeneralCUS

4.2.2 Planificación del sistema de la aplicación

Se describirá la aplicación que se ha desarrollado junto con las historias de usuario y especificaciones de requisitos de software. No están contempladas en un estándar establecido, pero si en la metodología de desarrollo escogida, MMCP.

Las historias de usuario se definen para conocer rápidamente lo que el usuario quiere para poder completar las metas que quiere alcanzar a través del software.

Finalmente, y conociendo que desea el usuario, se realiza la especificación formal de requisitos funcionales y no funcionales del sistema.

4.3 HISTORIAS DE USUARIO

En esta sección se detallaran las historias de usuario que conforman una especificación ágil de las funcionalidades de la solución, en posteriores secciones del proyecto estas historias se ampliaran con mayor detalle y se transformaran en una especificación formal de requisitos.

Antes de empezar a relatar las historias de usuario es conveniente conocer que es una historia de usuario y que formato se va emplear en este documento para su especificación.

Tabla 11: Backlog con historias de usuario

Identificador	Como...	Quiero...	Para....
US-001	Alumno	Gestionar contactos	Agregar a mis compañeros de aula
US-002	Alumno	Iniciar sesión con mi cuenta de	Aprovechar la cuenta que utilizo para iniciar sesión y comunicarme con mis contactos
US-003	Alumno	Responder a mis mensajes	Atender y comunicarme a tiempo real con mis compañeros matriculados
US-004	Alumno	Tener un listado de mis mensajes recibidos y poder ver cuales he leído y cuales son nuevas	Recibir múltiples mensajes y saber cuáles he respondido y cuales no
US-005	Alumno	Tener una cuenta usuario propia de la universidad	Iniciar sesión y desenlazar mi cuentas
US-006	Alumno	Crear notas	Tener recordatorios de mis exámenes, asesorías, reuniones grupales
US-007	Alumno	Comunicarme con más de 2 compañeros	Iniciar actividades grupales
US-008	Alumno	Adjuntar y enviar distintos tipos de archivos	Tener una mejor comunicación con mis compañeros
US-009	Alumno	Cerrar la aplicación	No tener mis mensajes abiertos
US-010	Alumno	Guardar mis notas	Tenerlas como repositorios de tareas próximas a realizar
US-011	Alumno	Modificar mis notas	Para tener actualizado mis tareas
US-012	Alumno	Listado de notas	Visualizar en orden mis tareas
US-013	Alumno	Recibir mensajes	Para poder comunicarme con mis compañeros

Las historias de usuario recogen una funcionalidad, pero no son especificación de software, si bien es cierto las historias de usuario recogen un requisito de una manera muy breve, cuyo objetivo no es especificar todos sus detalles, si no hacernos recordar que es lo que deseamos desarrollar en cada uno de los prototipos del proyecto

4.3.1 *Product backlog*

Empleando el formato descrito, se procederá en esta sección mostrar el *Product back log* del proyecto

Tabla 12: Backlog_historias_usuario

Identificador	Como...	Quiero...	Para...
US-001	Usuario	Identificarme con mi cuenta de <i>Facebook</i>	Aprovechar la cuenta que utilizo para iniciar sesión y comunicarme con mis profesores



Figura 58: Tablero Kanban

En la foto expuesta demuestra lo dinámico y simple de la funcionalidad e de *Kanban* se sumamente simple, como se comentó (Capítulo III) se forman tareas pendiente y se ponen en la primera fase, cuando se ha completado dicha fase para la tarea se mueve a la siguiente y así sucesivamente hasta llegar a la final de la cadena

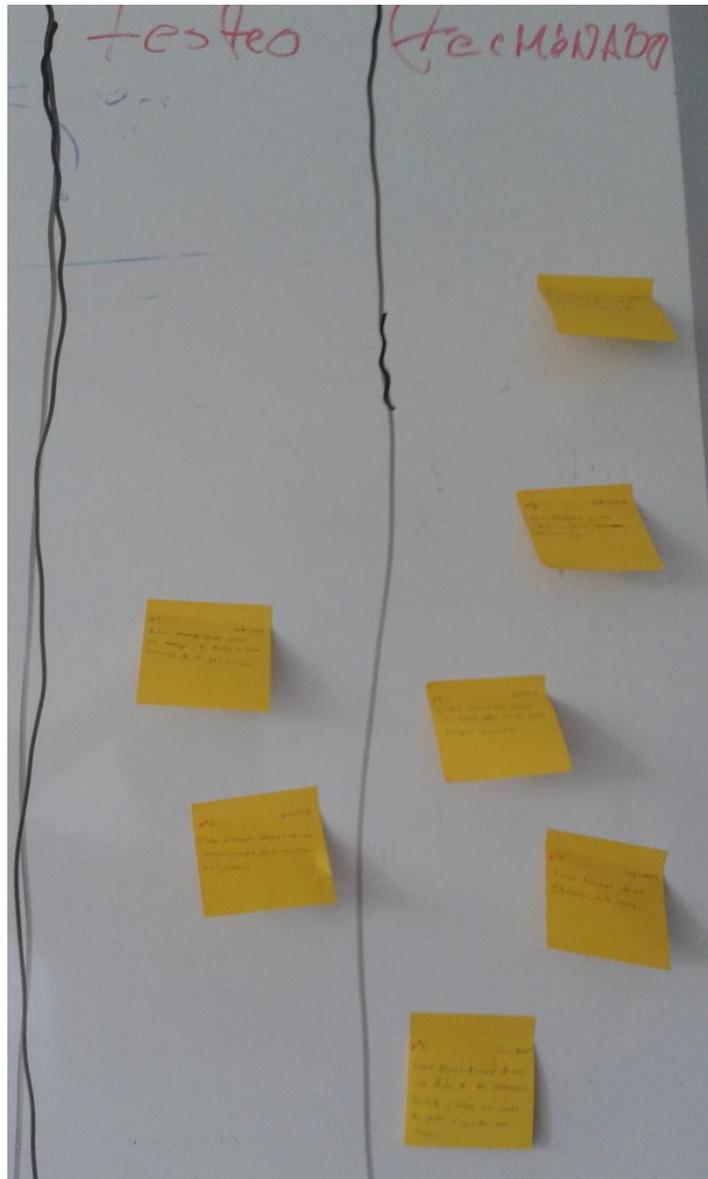


Figura 59: Tablero Kanban-testeo-finalizado

Dentro del desarrollo de los tableros *Kanban*, pueden variar de acuerdo al flujo de trabajo que la organización o el jefe de proyecto haya decidido y/o que más se acomode a sus necesidades, en la imagen se definen las historias de usuarios que han llegado a la etapa de “prueba” y las que han logrado ingresar etapa “Finalizado”

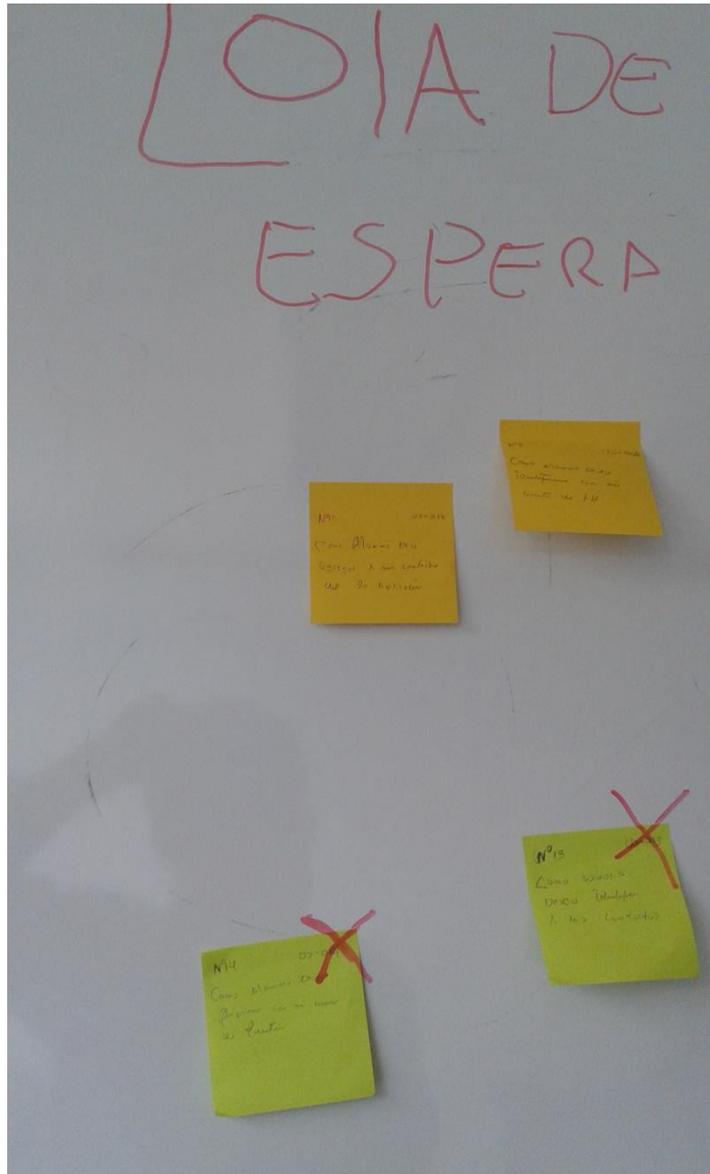


Figura 60: Tablero Kanban-cola-de-espera

La cola de espera define las historias de usuario (HU) que debido a su nivel de complejidad se tuvieron que volver analizar, las historias marcadas en "X" son las (HU) que tuvieron que retirarse debido al tiempo de desarrollo y no pertenecían a los objetivos del proyecto.

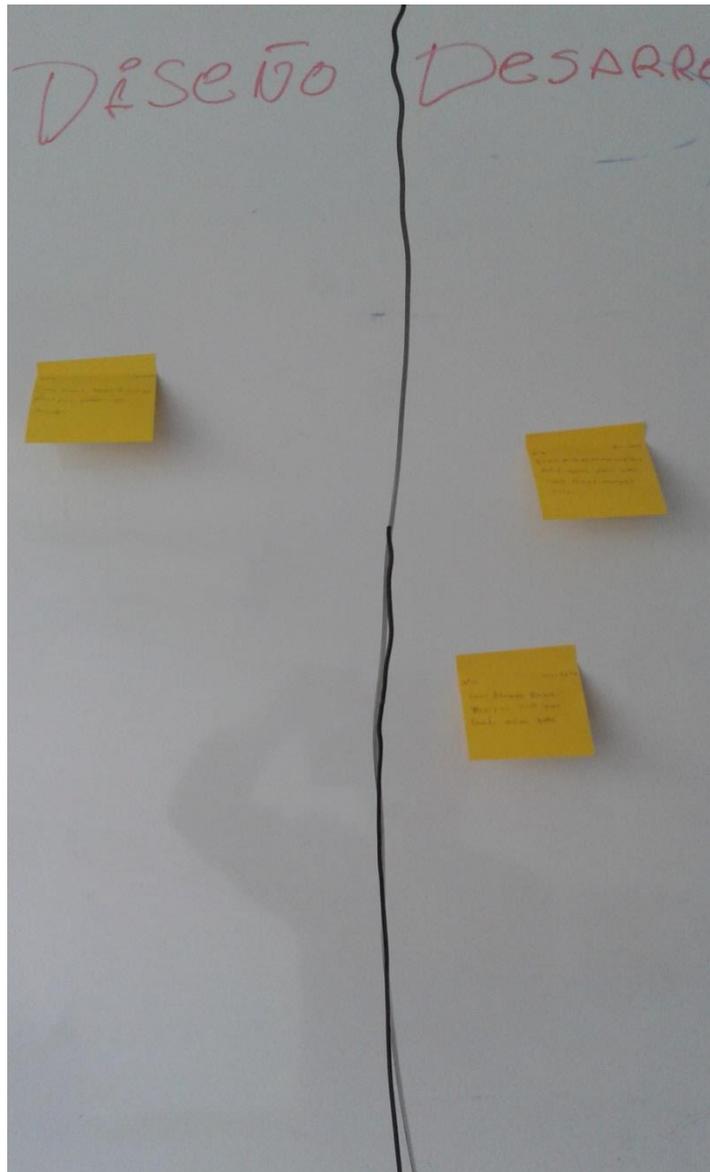


Figura 61: Tablero *Kanban*-diseño-desarrollo

Desde la perspectiva inicial, *Kanban* pareciese tomar un ciclo de vida en cascada, pero todo lo contrario, al ser una herramienta que se integra con SCRUM y distintas metodologías ágiles, se crea una retroalimentación en el desarrollo de las historias de usuario.

4.3.2 Especificación de requisitos

En el siguiente catalogo se describen todos los requisitos que forman parte de una especificación completa a partir de la cual diseña la solución al problema planteado al inicio de la tesis.

A. Formato de requisitos

A continuación se describen los campos que definen cada uno de los requisitos.

- **Identificador:** Código que identifica de manera única al requisito. Tendrá el siguiente formato REQ-XX donde REQ representa el tipo de requisito que se define
- **Nombre :** Descripción de la función del requisito de forma abreviada
- **Historias de usuario :** Código identificador de la historia de usuario de la que proviene este requisito

Tabla 13: Plantilla para la definición de requisitos

Parámetro	Descripción
Identificador	REQ-XXX
Nombre	Nombre del requisito
Prioridad	Alta-Media- Baja
Estabilidad	Estable – inestable
Necesidad	Esencial – Deseable –Opcional
Verificabilidad	Alta – Media – Baja – N/A
Historia de Usuario	US-XXX

4.3.3 Catálogo de requisitos

A continuación se exponen todos los requisitos a los que la solución debe responder para ser validado. El catalogo se subdivide en requisitos funcionales (que especifican los servicios y funcionalidades de la aplicación) y en requisitos no funcionales, que especifican las restricciones que deben existir en el producto ya desarrollado, no durante el proceso de desarrollo.

A. Requisitos Funcionales

Mediante este cuadro se describirán todas y cada una de las funcionalidades que debe poseer la solución

Tabla 14: Requisito RF-001-agregar contactos

Parámetro	Descripción
Identificador	RF-001
Nombre	Agregar contactos
Descripción	Los usuarios podrán agregar nuevos contactos. Un nuevo contacto se creara a partir de los siguiente datos : <ul style="list-style-type: none">• Código del usuario• PIN de usuario• Cuenta de FB que emplea el usuario
Historia de usuario	US-001

Tabla 15: Requisito RF-002-identificacion con FB

Parámetro	Descripción
Identificador	RF-002
Nombre	Identificación con FB
Descripción	Los usuarios deben ser capaces de identificarse en la aplicación usando una cuenta de usuario de FB
Historia de usuario	US-002

Tabla 16: Requisito RF-003-responder mensajes

Parámetro	Descripción
Identificador	RF-003
Nombre	Responder mensajes
Descripción	Los usuarios deben poder responder mensajes que reciban en sus dispositivos mediante el propio dispositivo, seleccionando el chat deseado, durante todo el tiempo que su sesión este abierta
Historia de usuario	US-003

Tabla 17: Requisito RF-004-listar mensajes recibidos

Parámetro	Descripción
Identificador	RF-004
Nombre	Listar mensajes y notas
Descripción	Los usuarios deben poder ver los mensajes que han recibido en una lista de tipo de bandeja de entrada donde puedan distinguir que mensajes han sido leídas y cuáles son las nuevas. Deben asimismo tener la posibilidad de seleccionar la que crean oportuna y así acceder al mensaje propiamente descrito
Historia de usuario	US-004

Tabla 18: Requisito RF-005-iniciar nueva sesión

Parámetro	Descripción
Identificador	RF-005
Nombre	Iniciar nueva sesión
Descripción	Los usuarios podrán tener nuevas sesiones. Una nueva sesión se creara a partir del correcto <i>login</i> del usuario, a partir de los siguiente datos : <ul style="list-style-type: none">▪ Código de usuario (Alum/Pro)▪ <i>Password</i>
Historia de usuario	US-005

Tabla 19: Requisito RF-006 crear tarea nueva

Parámetro	Descripción
Identificador	RF-006
Nombre	Crear tarea nueva
Descripción	Los usuarios podrán crear nuevas notas/tareas. Una nueva tarea se creara a partir de los siguientes datos : <ul style="list-style-type: none">▪ Título de la nota▪ Descripción de la nota
Historia de usuario	US-006

Tabla 20: Requisito RF-007-modificar tarea

Parámetro	Descripción
Identificador	RF-007
Nombre	Modificar Tarea
Descripción	Los usuarios podrán modificar tareas/notas. Una nota/tarea puedan modificarse los siguientes datos :: <ul style="list-style-type: none">▪ Título de la nota▪ Descripción de la nota
Historia de usuario	US-006

Tabla 21: Requisito RF-008-borrar tarea/nota

Parámetro	Descripción
Identificador	RF-008
Nombre	Borrar nota
Descripción	Los usuarios podrán modificar borrar notas existentes
Historia de usuario	US-006

Tabla 22: Requisito RF-009-crear grupo de conversación

Parámetro	Descripción
Identificador	RF-009
Nombre	Crear grupo de conversación
Descripción	Los usuarios podrán tener conversaciones en su menú principal con más de 2 usuarios en tiempo real. Se necesitaran los siguientes datos <ul style="list-style-type: none">• Código de usuarios
Historia de usuario	US-007

Tabla 23: Requisito RF-010-envio de ficheros

Parámetro	Descripción
Identificador	RF-010
Nombre	Envío de ficheros
Descripción	Los usuarios podrán enviar distintos tipos de ficheros a sus compañeros.
Historia de usuario	US-008

Tabla 24: Requisito RF-0011-cerrar sesiones

Parámetro	Descripción
Identificador	RF-011
Nombre	Cerrar sesiones
Descripción	Los usuarios podrán cerrar sesiones existentes
Historia de usuario	US-009

Tabla 25: Requisito RF-0012-recibir mensajes

Parámetro	Descripción
Identificador	RF-012
Nombre	Recibir mensajes
Descripción	Los usuarios deben poder recibir en sus dispositivos los mensajes que lancen sus demás contactos. Si tienen la aplicación abierta, cuando reciban un mensajes, esta deberá parpadear de color inmediatamente para su pronta lectura
Historia de usuario	US-013

B. Requisitos no funcionales

En esta sección se describen los requisitos que debe cumplir la solución pero que no son funcionalidades si no aspectos a los que el producto final debe ajustarse

Tabla 26: Requisito RNF-001-dispositivos soportados

Parámetro	Descripción
Identificador	RNF-001
Nombre	Dispositivos soportados
Descripción	La solución debe funcionar en los dispositivos que funcionen con la plataforma Android, ya sean teléfonos móviles o <i>tablet's</i>
Prioridad	Alta
Estabilidad	Estable
Necesidad	Esencial
Verificabilidad	Alta
Historia de usuario	N/A
Norma	ISO/IEC 25010

Tabla 27: Requisito RNF-002-version-minima-de-la-plataforma

Parámetro	Descripción
Identificador	RNF-002
Nombre	Versión mínima de la plataforma Android
Descripción	La versión mínima de la plataforma Android sobre la que funcionara es la versión 2.3
Historia de usuario	N/A
Norma	ISO/IEC 25010

Tabla 28: Requisito RNF-003-interfaz adaptativa

Parámetro	Descripción
Identificador	RNF-003
Nombre	Interfaz adaptativa
Descripción	La interfaz de usuario debe adaptarse a los distintos tamaños de pantalla de los teléfonos y <i>tablet</i> 's
Historia de usuario	N/A
Norma	ISO/IEC 25010

4.3.4 Trazabilidad de requisitos – historias de usuario

Tabla 29: TR_HU

	US-001	US-002	US-003	US-004	US-005	US-006	US-007	US-008	US-009	US-010	US-011	US-012	US-013
RF-001	X												
RF-002		x											
RF-003			x										
RF-004				x								x	
RF-005					x								
RF-006						x					x		
RF-007						x							
RF-008						x				x			
RF-009							x						
RF-010								x					
RF-011									x				
RF-012													x

4.3.6 Especificación de casos de uso

En esta parte del documento se elaborara una especificación de los casos de uso del sistema con mayor relevancia. Se mostrara el grafico UML y a continuación se procederá a realizar la descripción textual.

Para la descripción textual se empleara una tabla con los siguientes campos:

- **Identificador:** Identifica a cada caso de uso. El formato utiliza es el siguiente "CU-XX", donde cada "x" se corresponde con un numero comprendido entre 0 y 9
- **Nombres :** Se corresponde con el nombre asignado al caso de uso
- **Actores:** Son los distintos roles de usuarios que encontraremos en el sistema. Es cualquier entidad externa al sistema que está relacionada con este y que le demanda una funcionalidad
- **Objetivo :** Se corresponde con la finalidad que se pretende obtener tras realizar el caso de uso
- **Curso típico de eventos :** Se corresponde con la descripción del caso de uso referido
- **Pre-condición :** Se corresponde con las condiciones iniciales que deben cumplir para que se realice dicho caso de uso
- **Post- condición :** Se corresponde con las condiciones finales que se cumplirán tras realiza dicho caso de uso

A. Diagrama caso de Uso

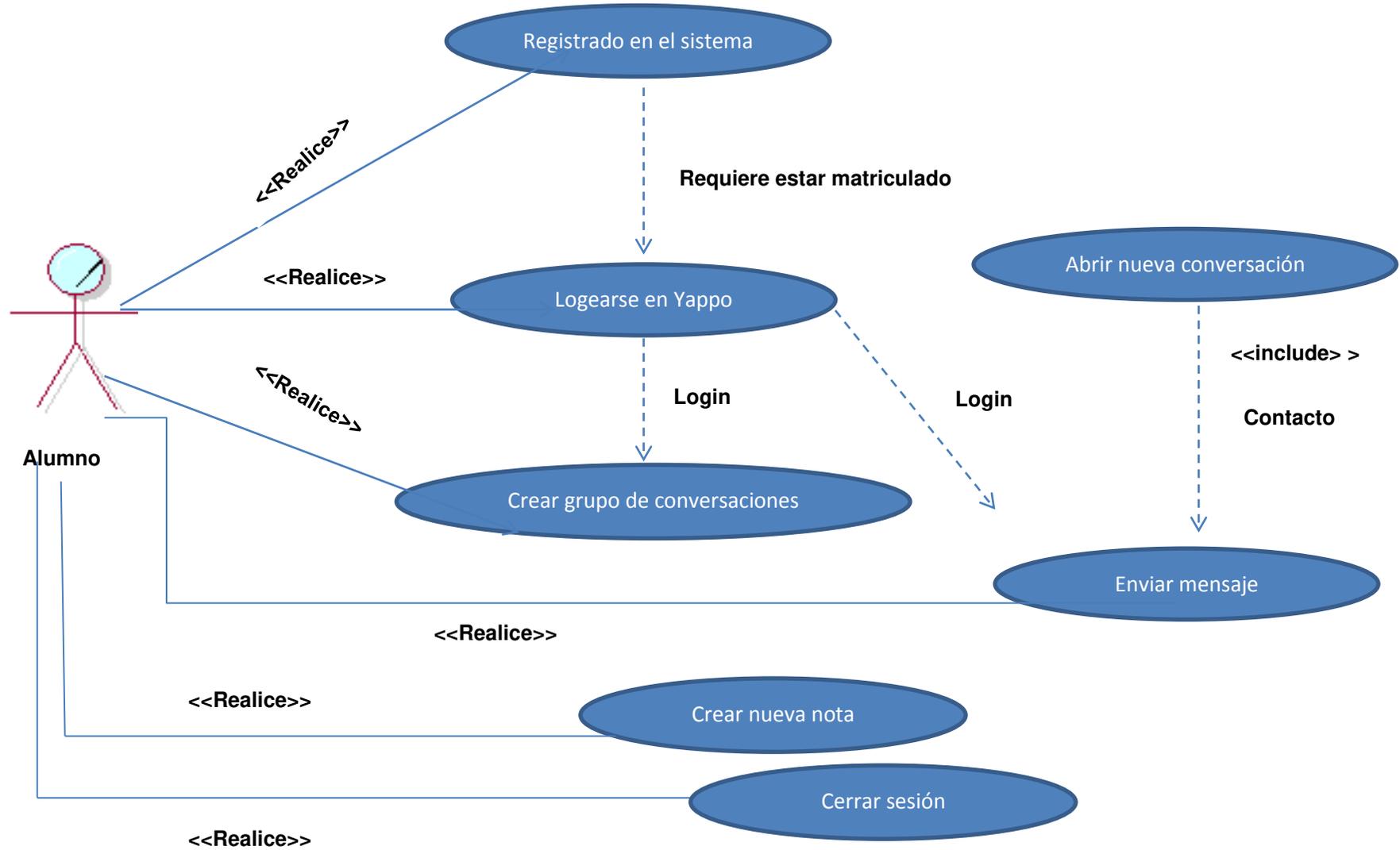


Figura 60: DiagramaCUS

B. Descripción caso de uso

- Proceso Inicio de sesión

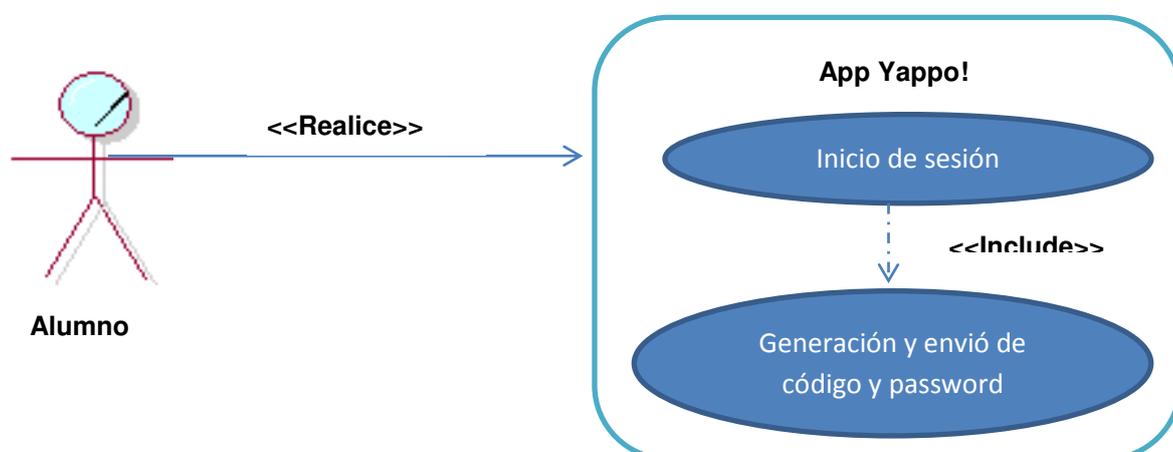


Figura 61: Pr_inicio_sesion CUS

Tabla 30: Descrip_Inic

Nombre	Iniciar sesión
Actores	Alumno
Objetivo	El alumno desea iniciar una nueva sesión
Curso Típico de eventos	<ol style="list-style-type: none"> 1. El alumno abre la aplicación <ol style="list-style-type: none"> 1.1 Se ejecuta el <i>splash</i> Yappo 2. El alumno ingresa su código y <i>password</i> <ol style="list-style-type: none"> 2.1 Mensaje de validación de datos 3. El alumno inicia sesión caso contrario se genera un mensaje de error
Descripción	<ul style="list-style-type: none"> • El alumno ingresa sus respectivas credenciales (su código de alumno y <i>password</i> de la Universidad Ciencias y humanidades • La aplicación realiza la respectiva validación con la información almacenada en la base de datos • Si la información concuerda se generada automáticamente el ingreso a la aplicación, caso contrario se genera un mensaje de error • Si el usuario olvido su contraseña, deberá comunicarse con el área de sistemas

Pre-Condición	<ul style="list-style-type: none"> • La aplicación debe estar instalada • El alumno debe de haber abierto la aplicación • Debe existir conexión a internet
Post-Condición	<ul style="list-style-type: none"> • Queda registrado el inicio de sesión

- Proceso validación

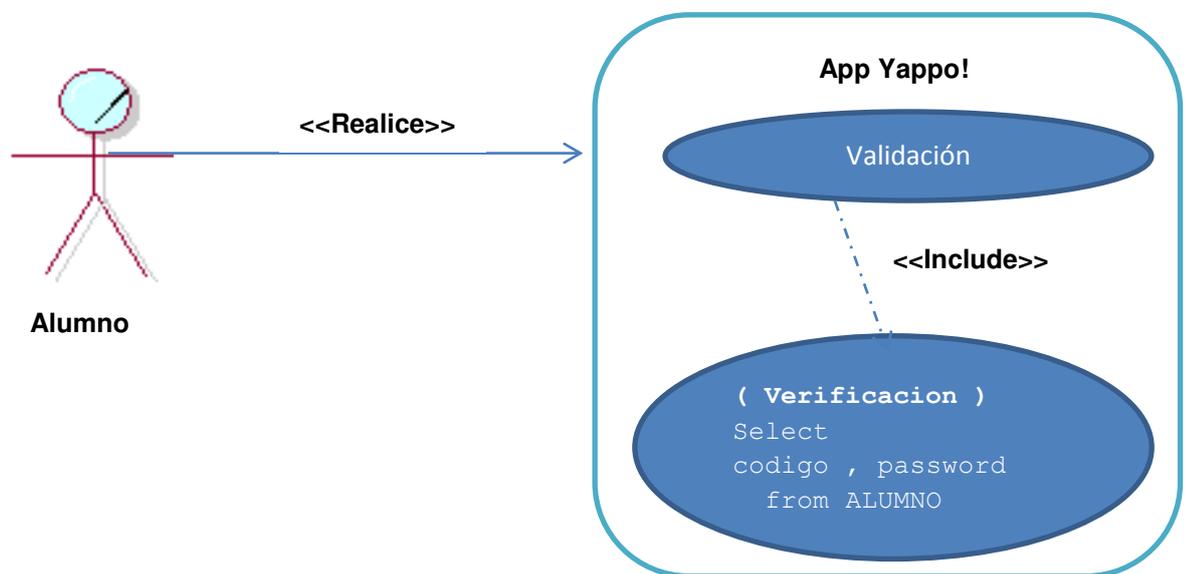


Figura 62: Pr_validacion

Tabla 31: Descrip_ validacion

Nombre	Validación
Actores	Alumno
Curso de eventos	<ol style="list-style-type: none"> 1. El alumno abre la aplicación 1.1 Se ejecuta el <i>splash</i> Yappo 2. El alumno ingresa su código y <i>password</i> 3. Se verifica el código y <i>password</i> del alumno en la base de datos, si concuerda se inicia sesión caso contrario se genera mensaje de error
Descripción	<ul style="list-style-type: none"> • El alumno ingresa el código y <i>password</i> recibido de registros académicos • La aplicación realiza la respectiva validación del código y <i>password</i> de verificación con la información almacenada en la base de datos • Si la información concuerda se generada automáticamente el ingreso a la aplicación, caso contrario se genera un mensaje de error
Pre-Condición	<ul style="list-style-type: none"> • La aplicación debe estar instalada • El alumno debe de haber abierto la aplicación • Debe existir conexión a internet
Post-Condición	<ul style="list-style-type: none"> • Queda registrado el inicio de sesión

- Proceso envió de mensaje

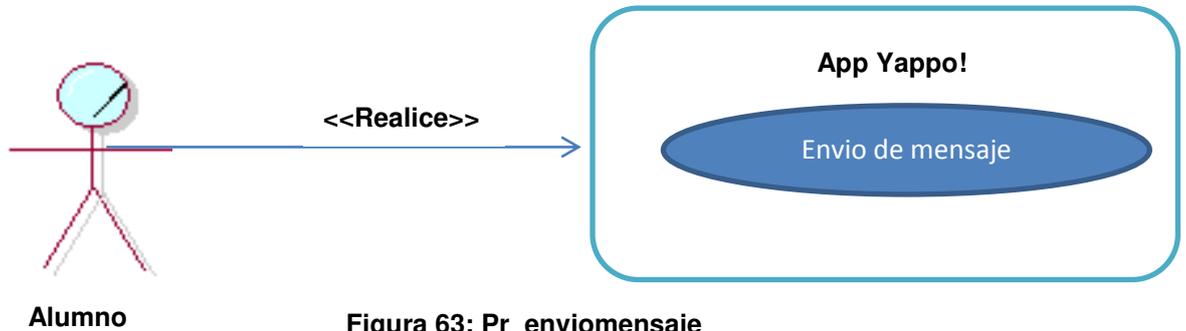


Figura 63: Pr_enviomensaje

Tabla 32: Descrip_ EnvioMensaje

Nombre	Envió de mensaje
Actores	Alumno
Curso de eventos	<ol style="list-style-type: none"> 1. El alumno abre la aplicación <ol style="list-style-type: none"> 1.1 Se ejecuta el <i>splash</i> Yappo 2. El alumno ingresa su código y password <ol style="list-style-type: none"> 2.1 Validación del registro 3. El alumno selecciona el botón nuevo mensaje en el menú principal 4. El alumno se encuentra con la pantalla de nuevo mensaje 5. El alumno escribe/selecciona al contacto que desea enviar el mensaje, se redacta el asunto, mensaje, aprieta el botón enviar
Descripción	<ul style="list-style-type: none"> • El alumno selecciona la opción de enviar un nuevo mensaje según el contacto que desee • El alumno selecciona el o los receptores del mensaje que se dispone a realizar • El usuario ejecuta el botón “enviar” para realizar el envió del mensaje
Pre-Condición	<ul style="list-style-type: none"> • La aplicación debe estar instalada • El alumno debe de haber abierto la aplicación • El alumno debe de haber agregado al menos un contacto • Debe existir conexión a internet
Post-Condición	<ul style="list-style-type: none"> • EL sistema envía y procesa el mensaje, marca la fecha de envió del mensaje

- Proceso de lectura del mensaje

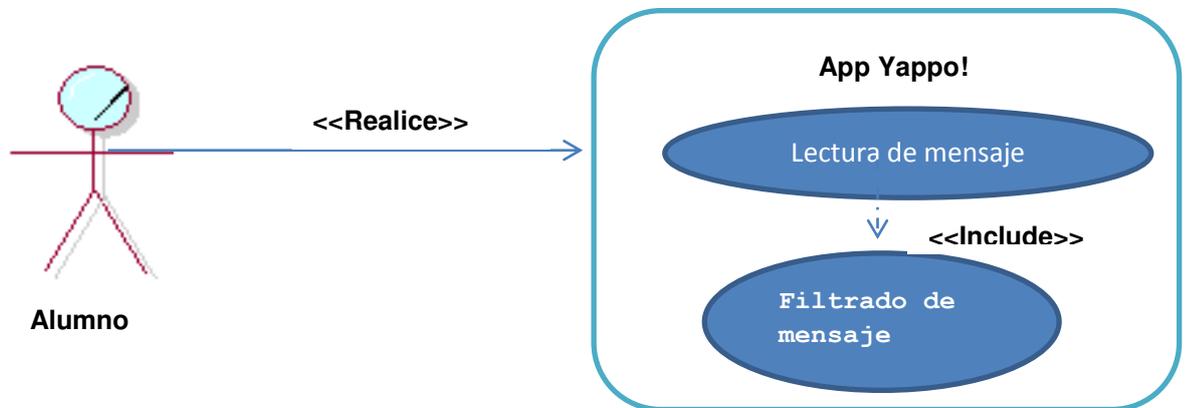


Figura 64: Pr_lecturamensaje

Tabla 33: Descrip_ LecturaMensaje

Nombre	Lectura de mensaje
Actores	Alumno
Curso de eventos	<ol style="list-style-type: none"> 1. El alumno recibe un nuevo mensaje en su dispositivo 2. Se muestra el nuevo mensaje, el alumno la lee y elige una de las opciones disponibles (eliminar, contestar
Descripción	<ul style="list-style-type: none"> • El alumno puede revisar el mensaje de acuerdo a la notificación enviada de la <i>app</i> “nuevo mensaje”, selecciona dicha opción de lectura de mensaje. • Se realiza el respectivo filtrado y presentación de mensajes enviados y recibidos por el usuario, presentándolos de forma cronológica descendente
Pre-Condición	<ul style="list-style-type: none"> • La aplicación debe estar instalada • El alumno debe de haber abierto la aplicación

- El alumno debe de haber agregado al menos un contacto
- Debe existir conexión a internet

Post-Condición

- EL sistema recibe y procesa el mensaje y marca la fecha de envío del mensaje

- Proceso Creación de nota

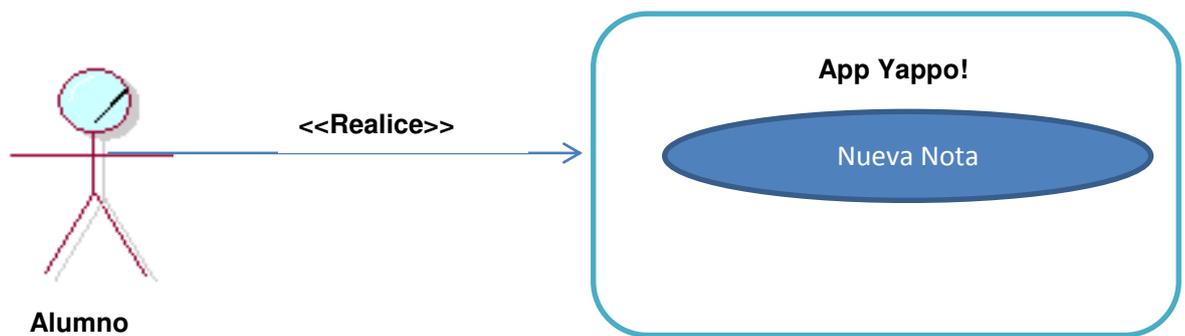


Figura 65: Pr creacion tarea

Tabla 34: Descrip_ CreacionTarea

Nombre	Creación de tarea
Actores	Alumno
Descripción	<ul style="list-style-type: none">• El alumno selecciona la opción de nueva nota y redacta la nueva tarea dentro de su módulo “Notas”• El alumno ingresara el título y resumen de la nota que pretende realizar• El usuario ejecuta el botón “listo” para finalizar la reacción de su nueva nota y verlo en su bandeja de entrada de notas

- Proceso de lectura de notas

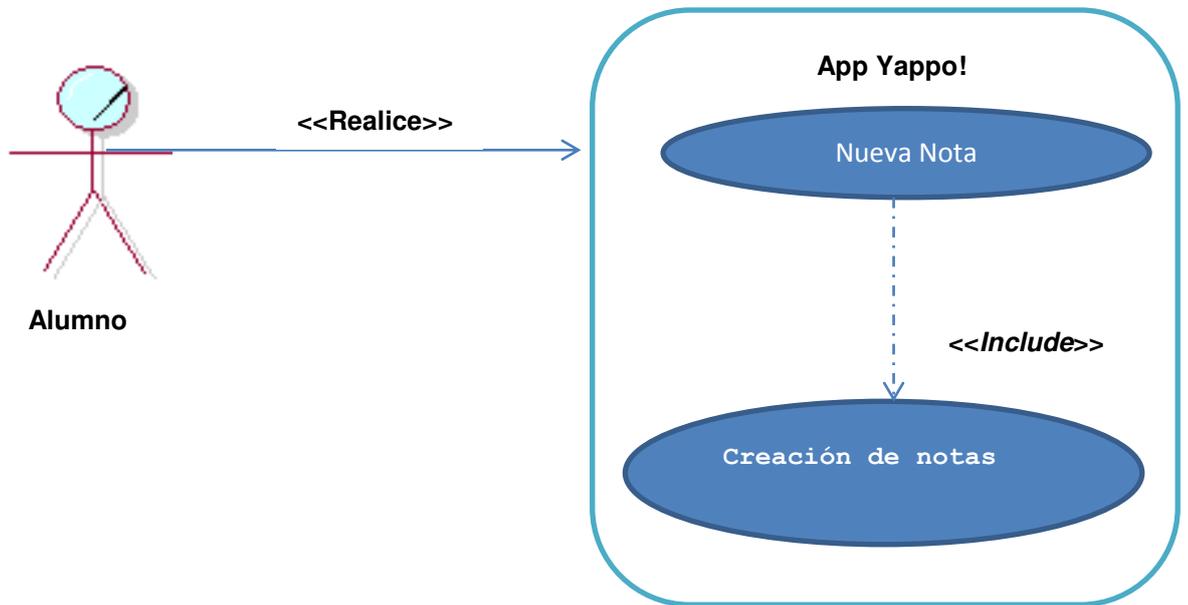


Figura 66: Pr_lectura_tareas

Tabla 35: DescriLectura_Tareas

Nombre	Lectura de nota
Actores	Alumno
Descripción	<ul style="list-style-type: none"> • El alumno selecciona la nota que desea revisar de acuerdo a su bandeja de entrada de notas ya creadas • Se realiza el respectivo filtrado y presentación de nota creada previamente para la disposición del alumno

C. Trazabilidad requisitos – casos de uso

En esta sección se muestra la correspondencia entre casos de uso y requisitos

Tabla 36: TR_RQ_CU

	CU-001	CU-002	CU-003	CU-004	CU-005	CU-006
RF-001	X					
RF-002	X					
RF-003	X					
RF-004		X				
RF-005		X				
RF-006			X			
RF-007			X			
RF-008				X		
RF-009					X	
RF-010						X

4.4 DESARROLLO

4.4.1 Diseño de la BD

A. Modelo conceptual

Para implementar la base de datos en el usuario (cliente), lo primero que debemos hacer es definir las tablas independientemente del sistema de bases de datos a utilizar

Tabla 37: Diseño_Tablas_Yappo

Tbl_Contactos	Tbl_Mensaje
idContacto : (bigint)	IdMensaje : (bigint)
idUsuarioContacto: (Varchar(8))	idUsuarioRecibe : (bigint)
Activo : (int)	idUsuarioEnvia : (bigint)
Código : (Varchar(8))	FechaEnvio : (datetime)
Password: (Varchar(48))	FechaRecibe: (datetime)
	Mensaje_leido: (varchar(300))

IdMensaje → *Primary Key*

idContacto → *Primary Key*

La base de datos tiene que ser capaz de almacenar los usuarios de la aplicación móvil y las credenciales de sus respectivos servicios. La tabla Tbl_usuarios almacenara el perfil del usuario y su ID será la clave principal, mientras para el logeo será su código UCH de ocho dígitos.

La tabla Tbl_mensajes almacena los mensajes tanto los enviados como los recibidos, introducimos un campo ID como clave principal ya que usaremos recibe-envía-mensaje como clave principal, un usuario A/E no podría enviar un usuario B dos mensajes con el mismo contenido

La tabla Contactos almacenara el código de todos los usuarios agregados, por lo que no se podrá tener dos contactos con el mismo código.

Una vez diseñada las tablas principales de la base de datos se implementa en nuestro sistema. En primer lugar diseñamos el prototipo de lo que será nuestra aplicación donde en su primer paso no tendrá ningún tipo de restricción.

B. Modelo dimensional

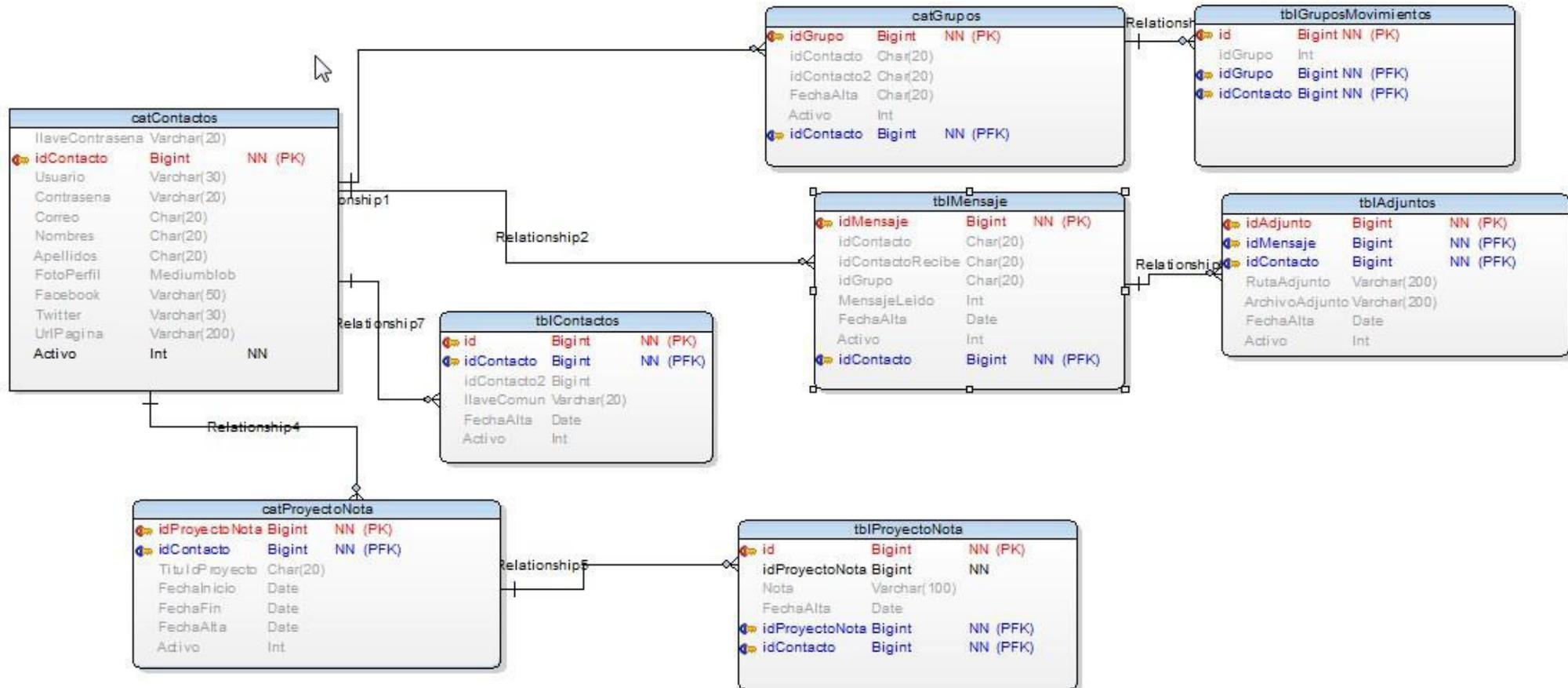


Figura 67: Diagrama_RE_BD

- **Script del modelo dimensional**

-- Create tables section -----

-- Table catContactos

```
CREATE TABLE catContactos
(
  llaveContrasena Varchar(20),
  idContacto Bigint NOT NULL AUTO_INCREMENT,
  Usuario Varchar(30),
  Contrasena Varchar(20),
  Correo Char(20),
  Nombres Char(20),
  Apellidos Char(20),
  FotoPerfil Mediumblob,
  Facebook Varchar(50),
  Twitter Varchar(30),
  UrlPagina Varchar(200),
  Activo Int NOT NULL DEFAULT 1,
  PRIMARY KEY (idContacto)
)
;
```

-- Table catContactos

```
CREATE TABLE catContactos
```

```
(  
)  
;
```

-- Table tblMensaje

```
CREATE TABLE tblMensaje
```

```
(  
  idMensaje Bigint NOT NULL AUTO_INCREMENT,  
  idContacto Char(20),  
  idContactoRecibe Char(20),  
  idGrupo Char(20),  
  MensajeLeido Int DEFAULT 0,  
  FechaAlta Date,  
  Activo Int DEFAULT 1,  
  idContacto Bigint NOT NULL,  
  PRIMARY KEY (idMensaje,idContacto)  
)  
;
```

-- Table tblAdjuntos

```
CREATE TABLE tblAdjuntos
```

```
(  
  idAdjunto Bigint NOT NULL AUTO_INCREMENT,  
  idMensaje Bigint NOT NULL,  
  idContacto Bigint NOT NULL,  
  RutaAdjunto Varchar(200),  
  ArchivoAdjunto Varchar(200),  
  FechaAlta Date,  
  Activo Int DEFAULT 1,  
  PRIMARY KEY (idAdjunto,idMensaje,idContacto)  
)  
;
```

-- Table catGrupos

```
CREATE TABLE catGrupos
(
  idGrupo Bigint NOT NULL,
  idContacto Char(20),
  idContacto2 Char(20),
  FechaAlta Char(20),
  Activo Int DEFAULT 1,
  idContacto Bigint NOT NULL
)
```

```
ALTER TABLE catGrupos ADD PRIMARY KEY (idGrupo,idContacto)
```

-- Table tblGruposMovimientos

```
CREATE TABLE tblGruposMovimientos
(
  id Bigint NOT NULL AUTO_INCREMENT,
  idGrupo Int,
  idGrupo Bigint NOT NULL,
  idContacto Bigint NOT NULL,
  PRIMARY KEY (id,idGrupo,idContacto)
)
```

-- Table catProyectoNota

```
CREATE TABLE catProyectoNota
(
)
```

-- Table tblProyectoNota

```
CREATE TABLE tblProyectoNota
(
  id Bigint NOT NULL AUTO_INCREMENT,
  idProyectoNota Bigint NOT NULL,
  Nota Varchar(100),
  FechaAlta Date,
```

```
idProyectoNota Bigint NOT NULL,  
idContacto Bigint NOT NULL,  
PRIMARY KEY (id,idProyectoNota,idContacto)  
)  
;
```

-- Table catProyectoNota

```
CREATE TABLE catProyectoNota  
(  
idProyectoNota Bigint NOT NULL AUTO_INCREMENT,  
idContacto Bigint NOT NULL,  
TituloProyecto Char(20),  
FechaInicio Date,  
FechaFin Date,  
FechaAlta Date,  
Activo Int DEFAULT 1,  
PRIMARY KEY (idProyectoNota,idContacto)  
)  
;
```

-- Table tblContactos

```
CREATE TABLE tblContactos  
(  
id Bigint NOT NULL AUTO_INCREMENT,  
idContacto Bigint NOT NULL,  
idContacto2 Bigint,  
llaveComun Varchar(20),  
FechaAlta Date,  
Activo Int DEFAULT 1,  
PRIMARY KEY (id,idContacto)  
)  
;
```

-- Create relationships section -----

```
ALTER TABLE catGrupos ADD CONSTRAINT Relationship1 FOREIGN KEY  
(idContacto) REFERENCES catContactos (idContacto) ON DELETE NO  
ACTION ON UPDATE NO ACTION
```

```
;
```

```
ALTER TABLE tblMensaje ADD CONSTRAINT Relationship2 FOREIGN KEY  
(idContacto) REFERENCES catContactos (idContacto) ON DELETE NO  
ACTION ON UPDATE NO ACTION
```

```
;
```

```
ALTER TABLE tblGruposMovimientos ADD CONSTRAINT Relationship3  
FOREIGN KEY (idGrupo, idContacto) REFERENCES catGrupos (idGrupo,  
idContacto) ON DELETE NO ACTION ON UPDATE NO ACTION
```

```
;
```

```
ALTER TABLE catProyectoNota ADD CONSTRAINT Relationship4 FOREIGN  
KEY (idContacto) REFERENCES catContactos (idContacto) ON DELETE NO  
ACTION ON UPDATE NO ACTION
```

```
;
```

```
ALTER TABLE tblProyectoNota ADD CONSTRAINT Relationship5 FOREIGN  
KEY (idProyectoNota, idContacto) REFERENCES catProyectoNota  
(idProyectoNota, idContacto) ON DELETE NO ACTION ON UPDATE NO  
ACTION
```

```
;
```

```
ALTER TABLE tblAdjuntos ADD CONSTRAINT Relationship6 FOREIGN KEY  
(idMensaje, idContacto) REFERENCES tblMensaje (idMensaje, idContacto) ON  
DELETE NO ACTION ON UPDATE NO ACTION
```

```
;
```

```
ALTER TABLE tblContactos ADD CONSTRAINT Relationship7 FOREIGN KEY  
(idContacto) REFERENCES catContactos (idContacto) ON DELETE NO  
ACTION ON UPDATE NO ACTION
```

4.4.2 Diseño de la interfaz del sistema

A. Diseño de los prototipos

El diseño del sistema hace que se puedan extraer tres modelos de datos conceptuales a almacenar

- El usuario de la aplicación
- Credenciales para realizar operaciones
- Credenciales para realizar servicios de las *web services*

En el desarrollo de la arquitectura y diseño del proyecto, la aplicación tenía otro tipo de enfoque, dejando un poco de lado de ser una *app* de comunicación instantánea segura a tener mayores facultades para sea más atractiva para el usuario

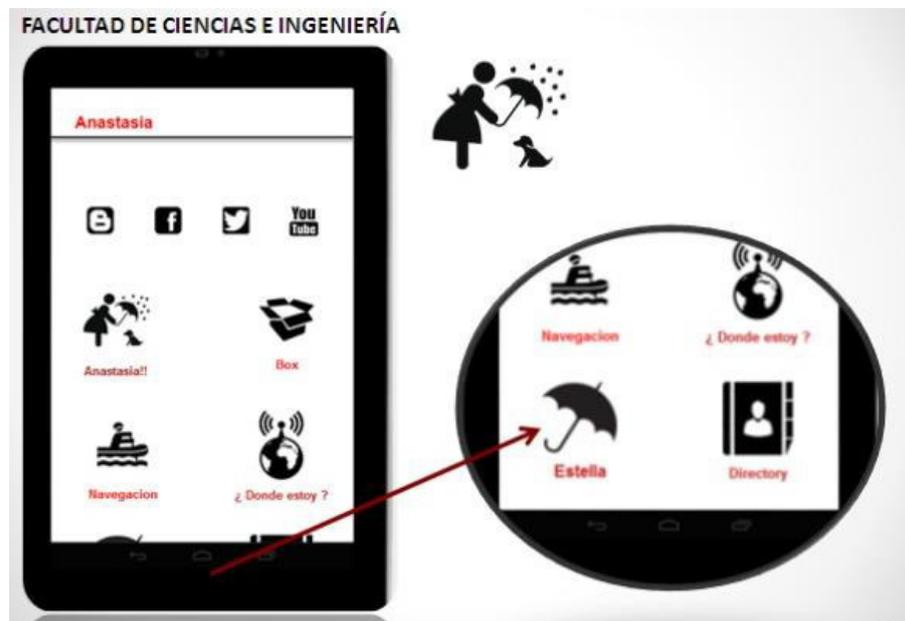


Figura 68: Prototype_Menu

Se presenta el otro Menú de la aplicación "Anastasia" donde observamos el modulo llamado "Estella" es donde se decidiría dar el comienzo del proyecto la aplicación instantánea



Figura 69: Prototype_Anastasia

En el icono anastasia se demuestra la información de dicha aplicación

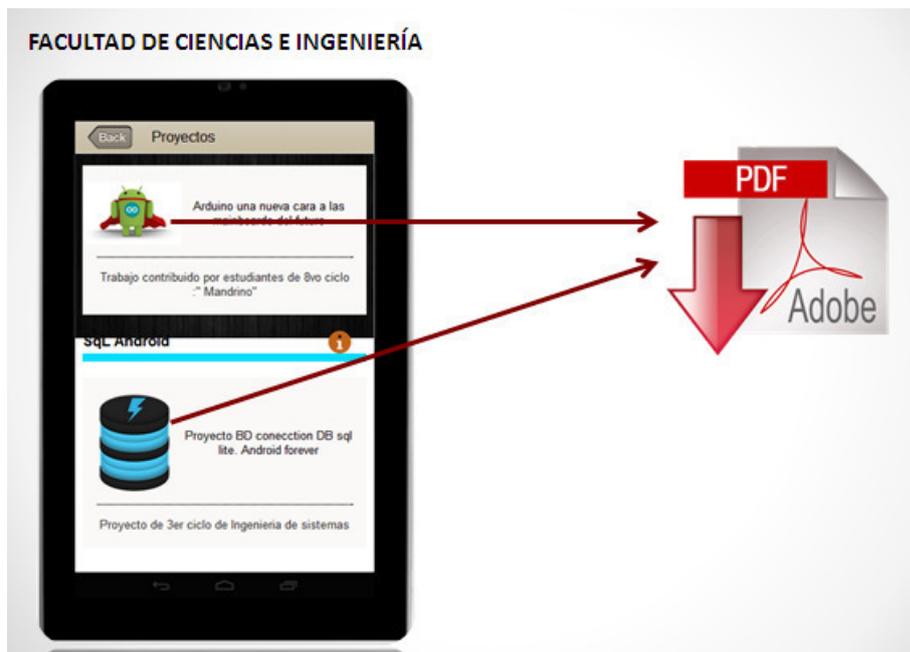


Figura 70: Prototype_Proyectos

El box fue uno de los módulos más ambiciosos de toda la aplicación “anastasia” donde los alumnos podrán acceder a documentación PDF como un máximo de 30 Mb, este servicio servirá para subir y compartir archivos entre los estudiantes de ingeniería de sistema, más adelante este modelo se fusiona dentro de las funciones del chat.

7.-Desarrollo:

FACULTAD DE CIENCIAS E INGENIERÍA

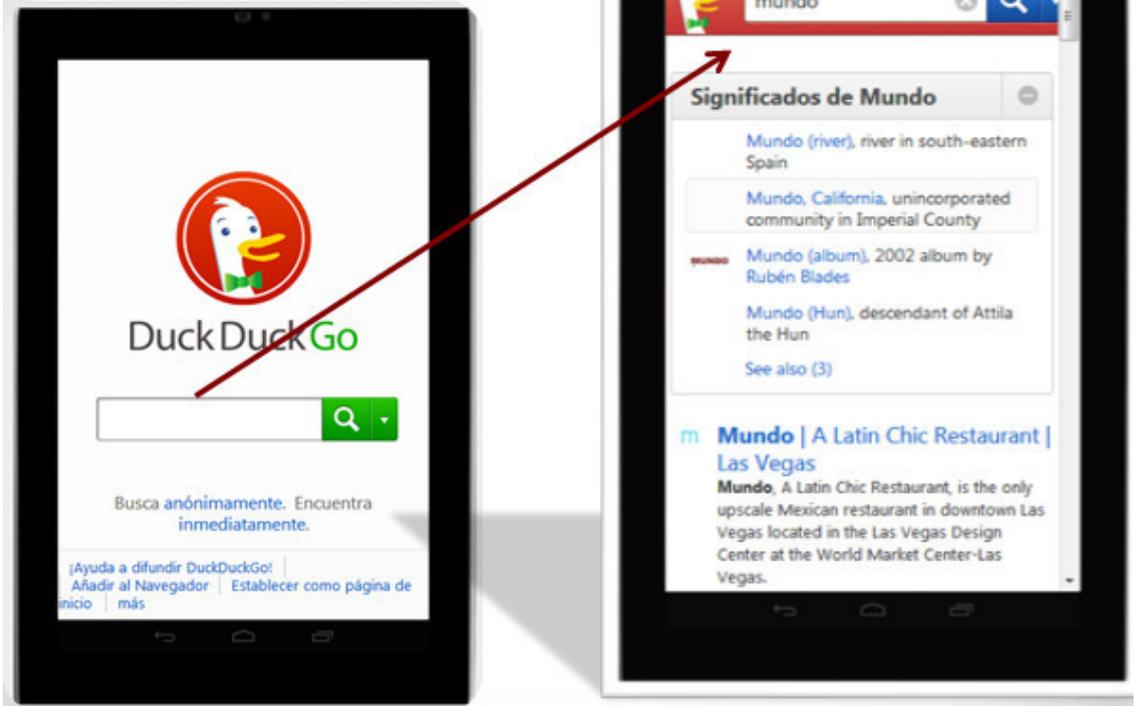


Figura 71: Prototype_search

En el módulo de Navegación el usuario podría navegar mediante una plataforma segura, donde todo su historial de búsqueda no sería enviado a un servidor externo y/o público como lo que conocemos de google. Este módulo se decidió abandonar puesto daba preferencia a un solo buscador dando conflicto contra las políticas de yappo!

7.-Desarrollo:

FACULTAD DE CIENCIAS E INGENIERÍA

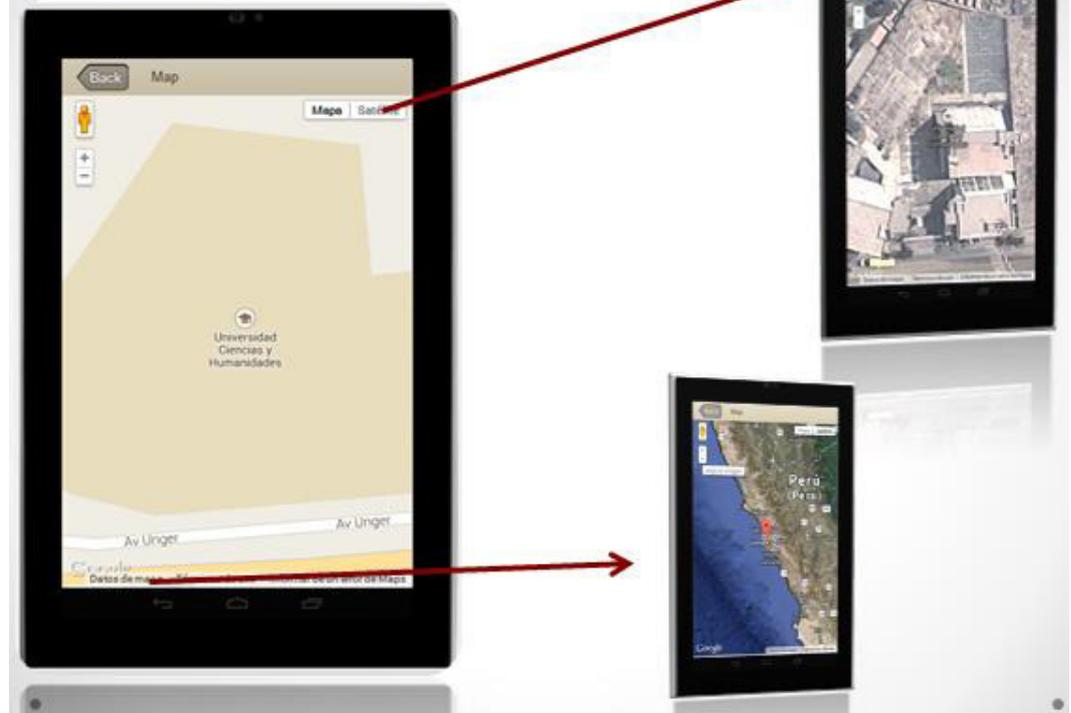


Figura 72: Prototype_DondeEstoy

Otros de los servicios de "anastasia es donde estoy un GPS que debe estar implementado en su dispositivo móvil, haría una búsqueda en donde se encuentra el alumno.

Al probarse dicha función consumía enormes recursos para los actuales Smartphone que poseen los usuarios, por lo cual se tuvo de abandonar.



Figura 73: Prototype_Inicio

Estella propone una comunicación abierta dentro de un círculo en donde los alumnos podrán tener comunicación entre los de su mismo ciclo, como también los *friend's* un canal en donde el alumno podrá agregar modificar o eliminar a un contacto, necesariamente no de su ciclo o facultad, pero sí de la universidad.



Figura 74: Prototype_Lista_Contactos

Interfaz de la *app* Estella donde podemos observar las diferentes opciones que tiene el alumno en su lista de contactos

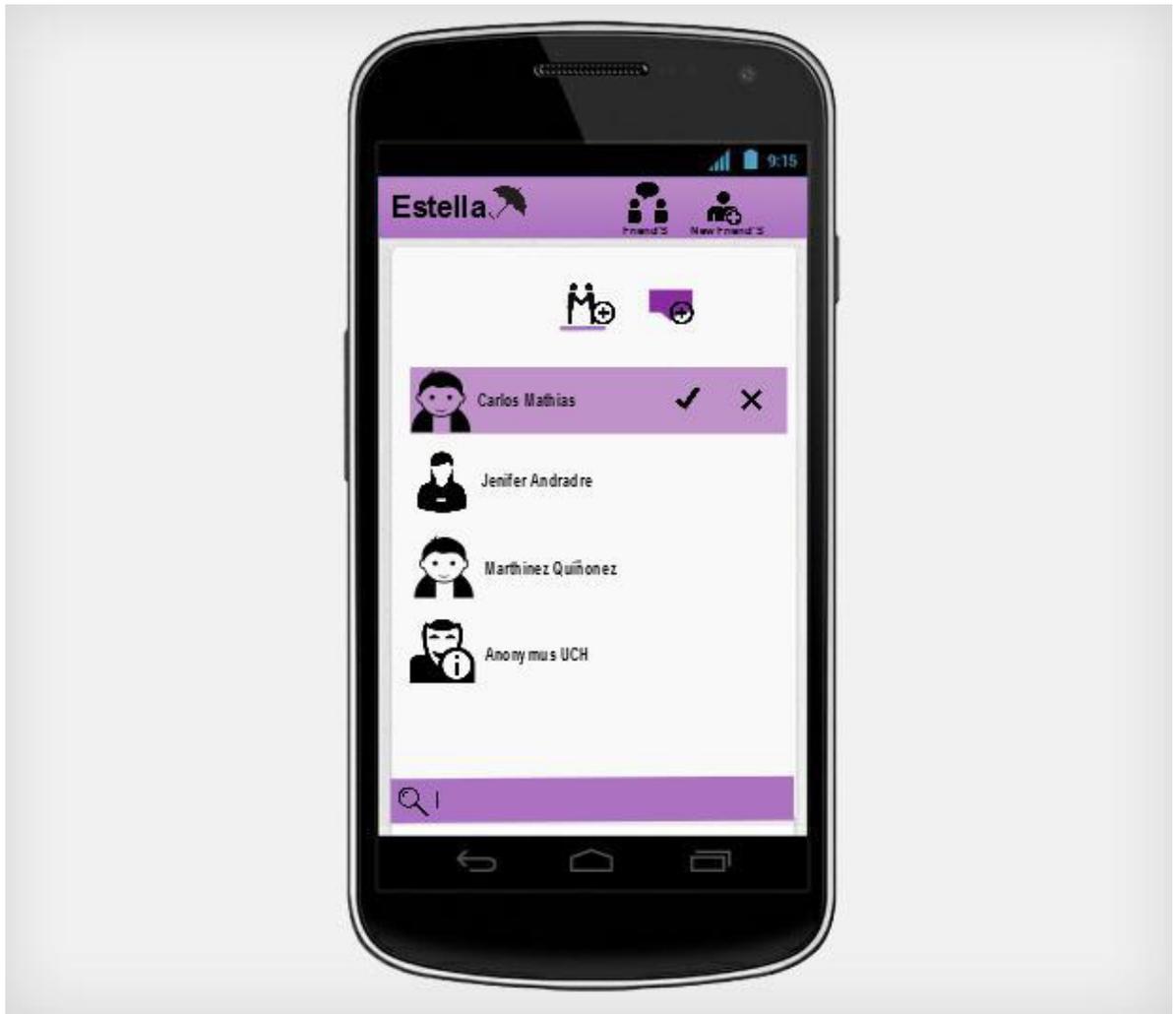


Figura 75: Prototype_Lista_solicitudes

El alumno no solo puede aceptar una solicitud de amistad como también de rechazar.



Figura 76: Prototype Lista Mensajes No Leídos

Se muestra una advertencia de los mensajes no leídos por el alumno

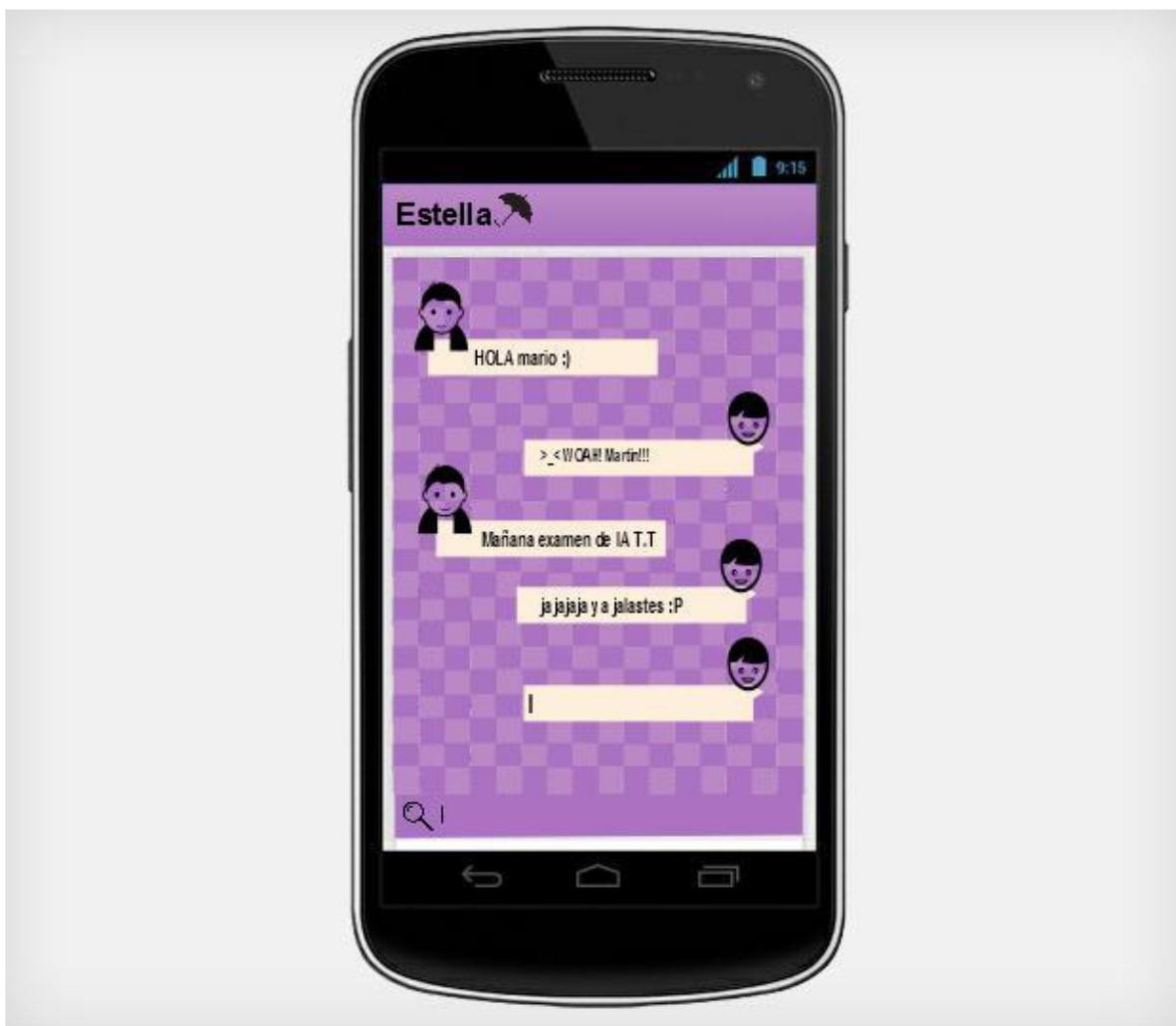


Figura 77: Prototipo_Interfaz_Chat

El alumno puede agregar a un usuario mediante su código de 8 dígitos, como es única sobre la base de datos busca dicha clave única sin tener que buscar nombres, apellidos, ciclo, etc.



Figura 78: Prototype_Interfaz_Chat

Este como las anteriores ventanas es el prototipo del diseño de la aplicación, hasta el momento, se observa una completa comunicación, pero no existe encriptamiento en los mensajes.



Figura 79: Prototype_Agregar_Amistad

Enviar una solicitud de amistad a un usuario registrado, mediante el código del estudiante.



Figura 80: Prototype_Agregar_Amistad

Creación de un nuevo grupo y elección del icono que llevara su nuevo grupo, en mi caso soy un alumno de 1er ciclo y creare un grupo llamado "actividad 1" para después agregar a la lista de alumnos que se encuentran en mi ciclo y unirlos los que se encuentren en mi grupo de trabajo de actividad 1

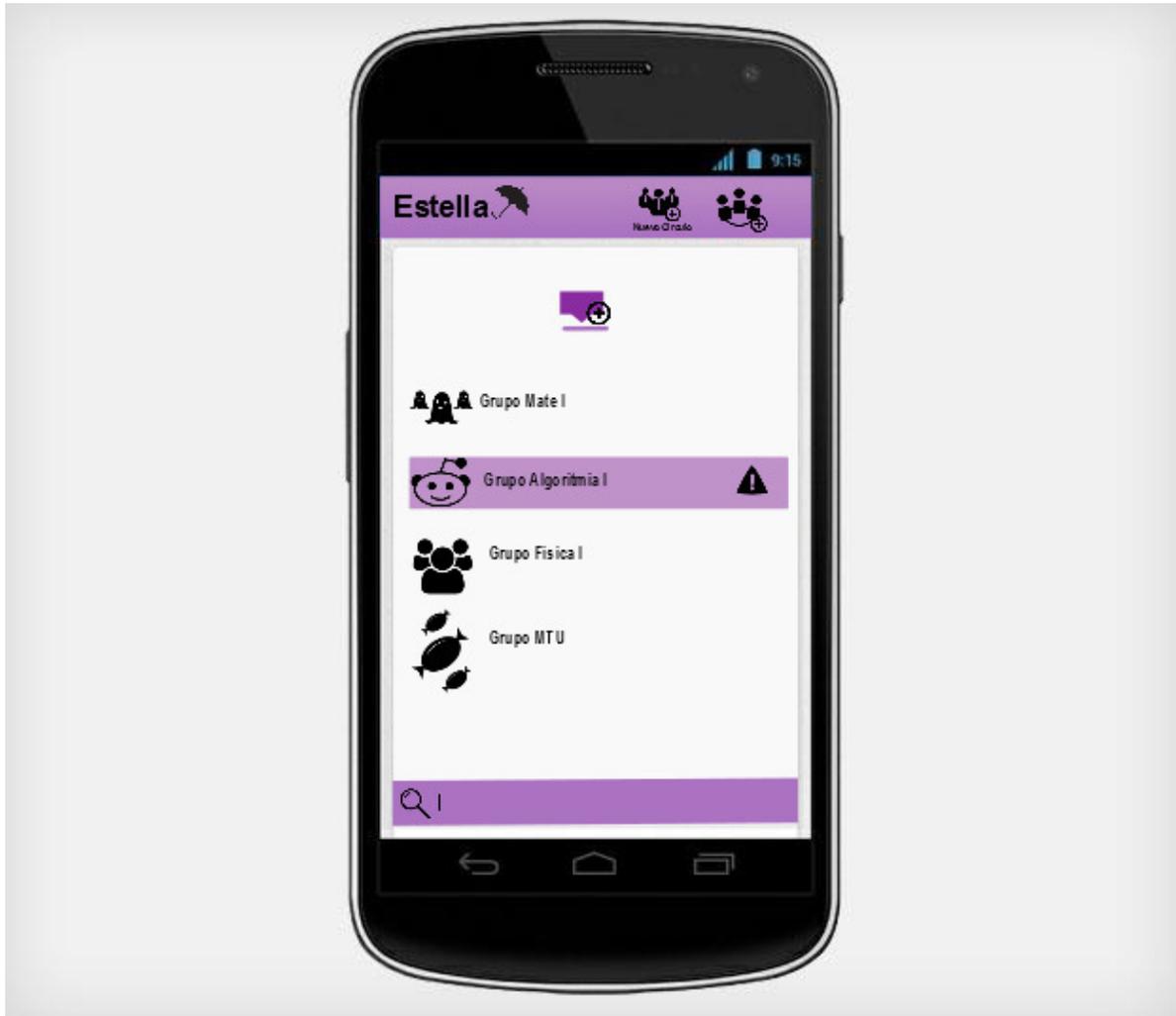


Figura 81: Prototype_Grupos

La creación de grupos, es esencialmente un grupo de chat con todas las personas que compartan la misma conversación, en un inicio dentro de los prototipos se pensó realizar un grupo por cada materia del estudiante, algo realmente tedioso, para anexar el al invitado al grupo de chat es suficiente buscarlo por el código y/o nombre del estudiante. Pero más eficiente siempre será el código

4.5 APLICACIÓN

Utilizaremos Eclipse y el SDK de *Android* para hacer posible la convergencia y desarrollo de la aplicación.

A. Inicio del proyecto

a. Seleccionamos un dispositivo virtual para arrancar Yappo!

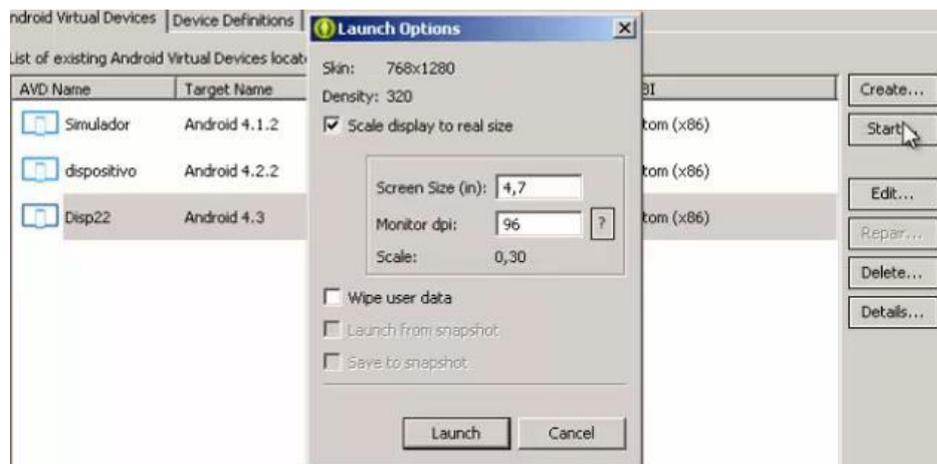


Figura 82: Launch_Dis22

Dentro del panel “*Android Virtual Device Manager*”, donde se podrán crear los dispositivos Virtuales, La figura muestra el arranque de un dispositivo *Android* virtual con la versión de *Android Jelly Bean*.

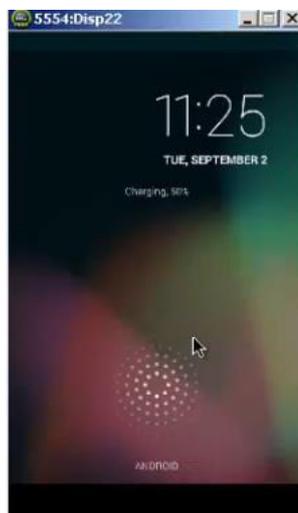


Figura 83: Disp22_Ignition

Un detalle interesante que la inicialización del dispositivo de prueba es de 30 segundos considerando las características del procesador, memoria del anfitrión.

- Ejecutamos Yappo

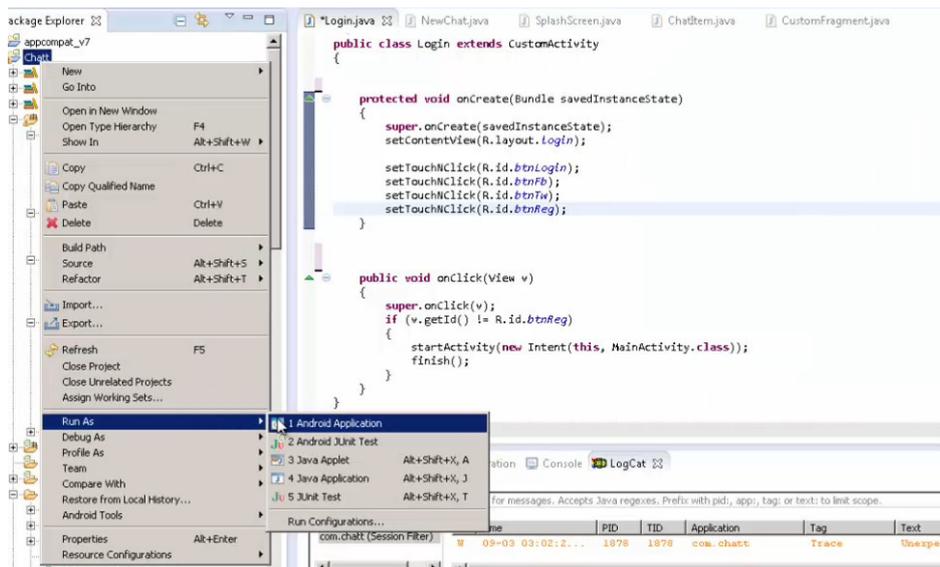


Figura 84: RunAs_Yappo

La dirección de ejecutar el proyecto > *Run as* > *Android Aplicacion* En aquellos tiempos donde armar un proyecto de “*Javita-Android*” era desde la consola y descargando el *ADT Plugin* desde el repositorio.



Figura 85: Splash_Yappo

El “*Splash-Screen*”. La pantalla de presentación o de inicio de la aplicación es un detalle muy importante (Aun si algunos piensan que es innecesario), con ello conseguimos mejorar la presentación e interés del usuario.

- Ingresamos nuestras credenciales

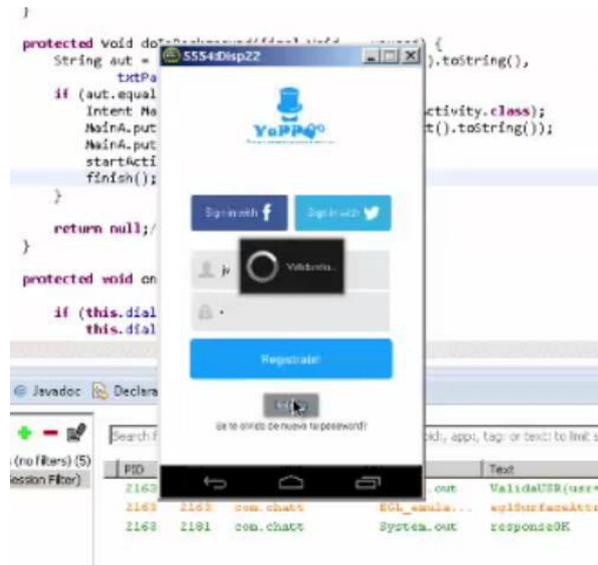


Figura 86: Login_Yappo

El Gestión de usuarios y el *login* son los pasos donde mayor análisis se tomó, por la privacidad de datos y no comprometer información útil del usuario, los contenidos de seguridad, el cifrado de la contraseña y otras buenas prácticas.

b. Interfaces del usuario

- Interfaz principal



Figura 87: Interf Yappo

- Interfaz de chats

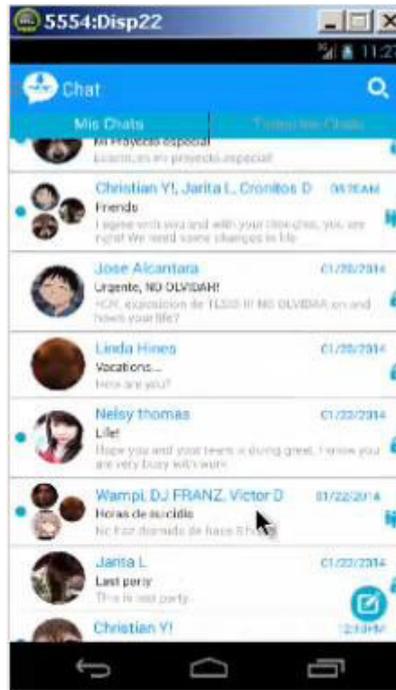


Figura 88: Interf_Chats

Las próximas figuras se mostrarán los procesos más relevantes de la aplicación desarrollada, desde el *screen* de inicio de sesión hasta el cierre de sesión del usuario, las interfaces de chat, el panel de notas y el interfaz de proyectos

- Interfaz de conversación



Figura 89: Interf_Conver

- Interfaz de notas

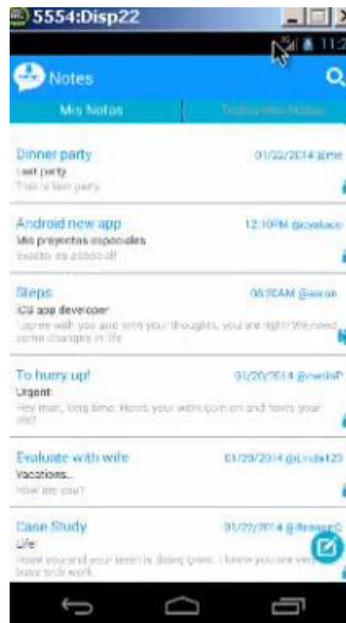


Figura 90: Interf_Notes

- Interfaz de proyectos

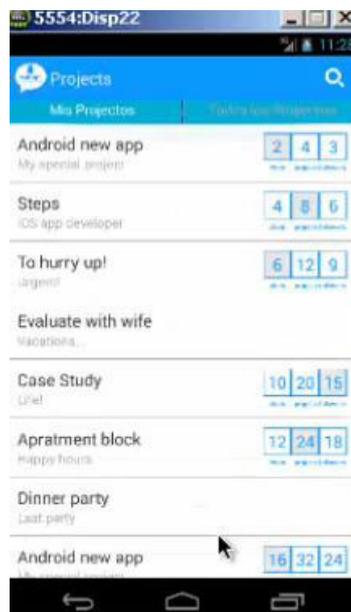


Figura 91: Interf_Projects

- Interfaz de “acerca de Yappo...”



Figura 92: About_Yappo

- Interfaz cerrar sesión

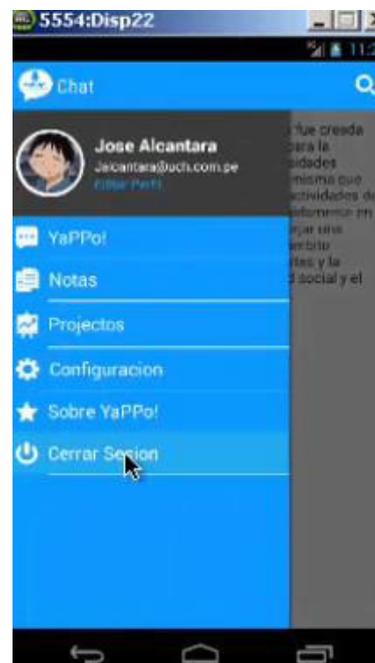


Figura 93: Cerrar_Yappo

4.6 IMPLEMENTACIÓN

4.6.1 Instalación y configuración de YAPPO!

A. Instalar y configurar *SDK (Android)* y *JDK (JAVA)*

a. Configuración y levantamiento de Yappo

- Verificamos los paquetes que utilizaremos para la aplicación estén instalados

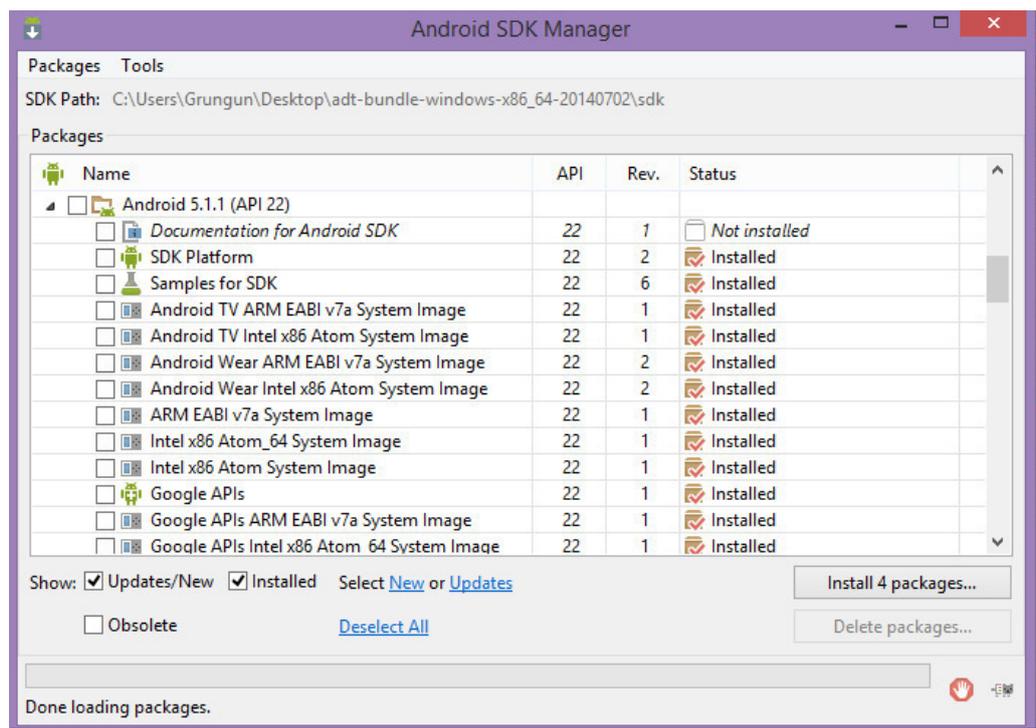


Figura 94: Anb_Sdk_Manager

Dentro del panel *Android SDK manager*, es la herramienta donde se descargara lo necesario para preparar y realizar las pruebas correspondientes para los dispositivos móviles virtuales, la aplicación se probó bajo un escenario mínimo de compatibilidad del “*Gingerbread*”- “*Jelly Bean*” hasta el Marshmallow robótico, a continuación se mostrara el proceso de configuración del proyecto.

- En caso contrario que no estén instalados pasamos a instalarlos y aceptamos las licencias de los repositorios

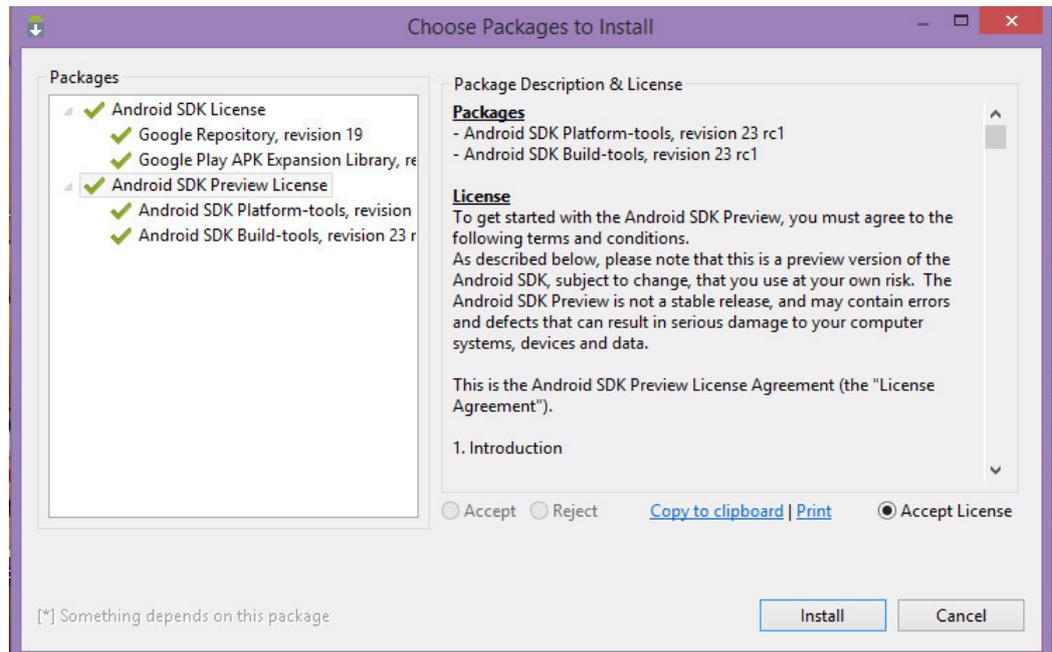


Figura 95: Package_Install

- Verificamos nuestra versión de JDK de java

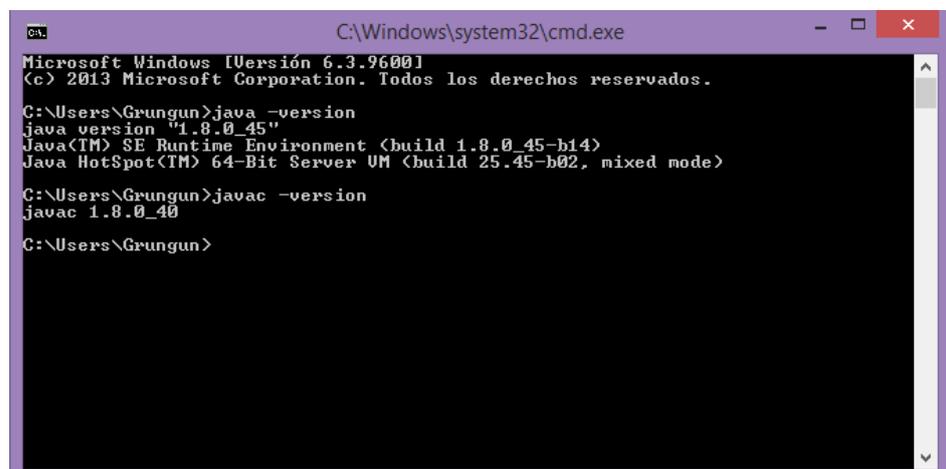


Figura 96: Jdk Jvers

Windows normalmente busca en el listado de los directorios en la variable de entorno "PATH" para programas ejecutables, como el JDK (Compilador de Java) normalmente estos residen en la carpeta de su instalación bajo sub carpeta llamada "/bin". Algunas veces los comandos "javac -versión" no son reconocidos oh envían mensajes de error de directorio para ello tenemos editar la variable y entorno "PATH" (Equipo > Propiedades > Cambiar configuración >Opciones Avanzadas> Variables de entorno).Listo tarea finalizada.

b. Instalar y configurar los *web service* en el servidor

- Habilitamos las características de IIS de Windows 8.1

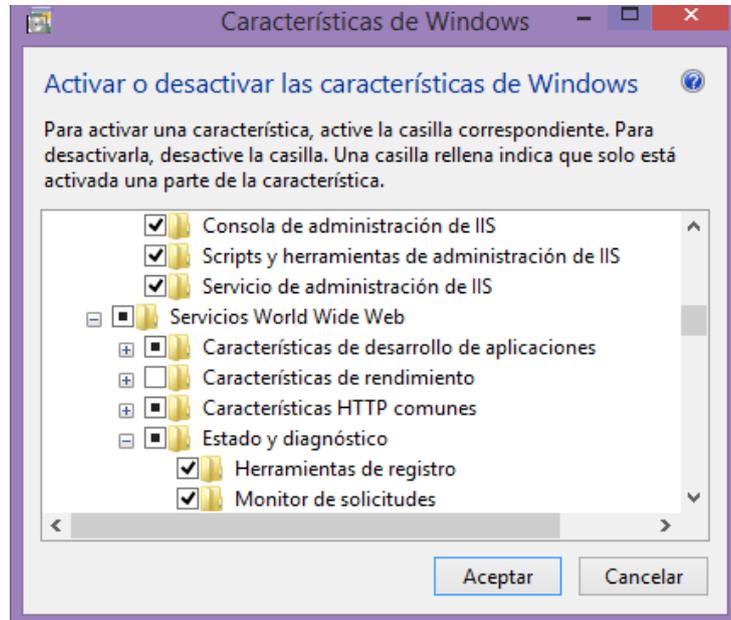


Figura 97: Installer_IIS

- Verificamos si la instalación fue correcta, abrimos una nueva instancia en el navegador y escribimos en la barra de direcciones <http://localhost>

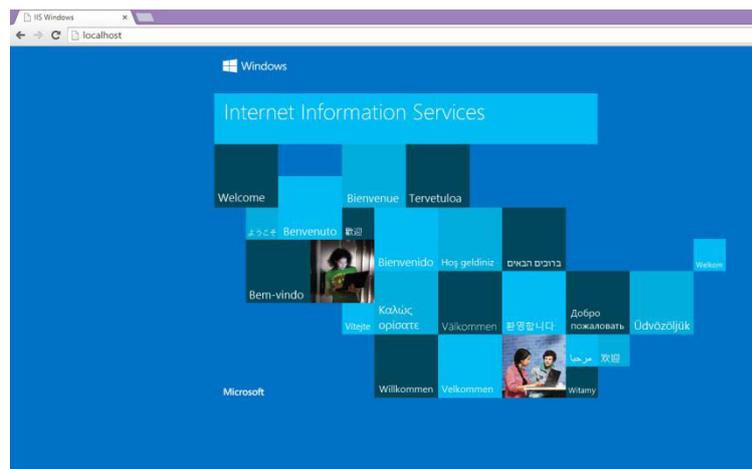


Figura 98: Localhost_IIS

- Procedemos a la configuración de *IIS Manager*. Ejecutando:” inetmgr”

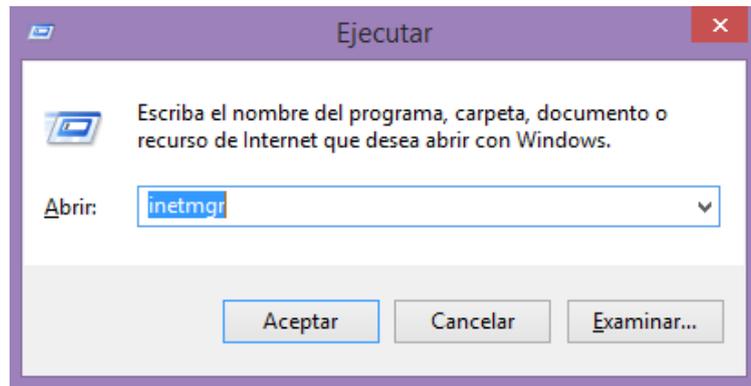


Figura 99: Inges_IIS_Manager

- Ingresamos a la interfaz de Il service (IIS)

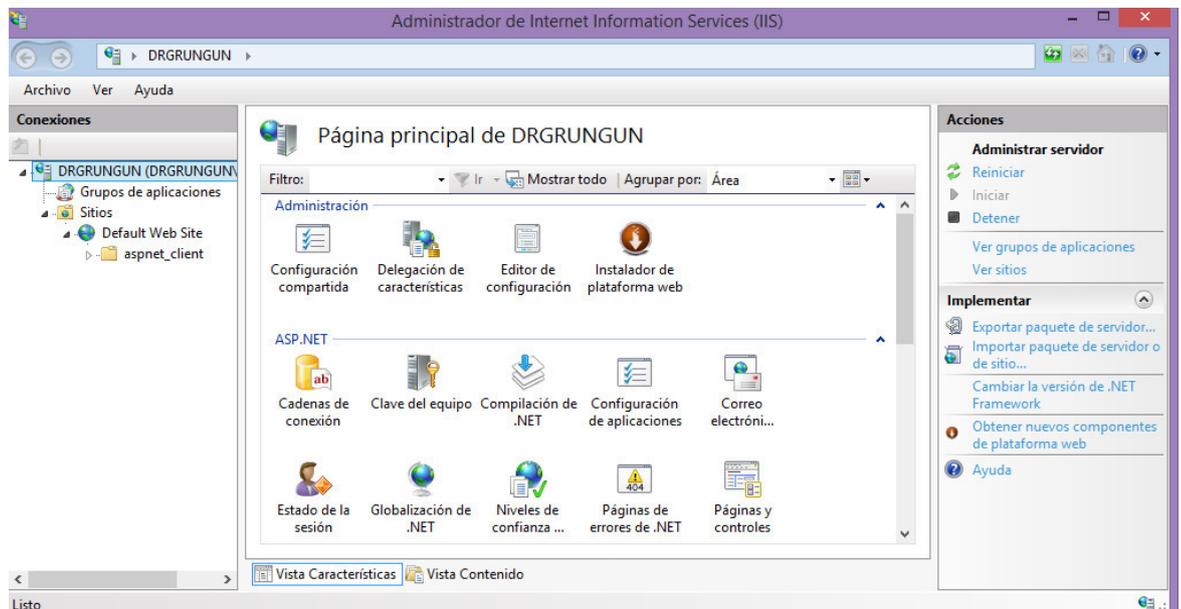


Figura 100: Adm_IIS

- Seleccionamos donde tenemos nuestros *web service*

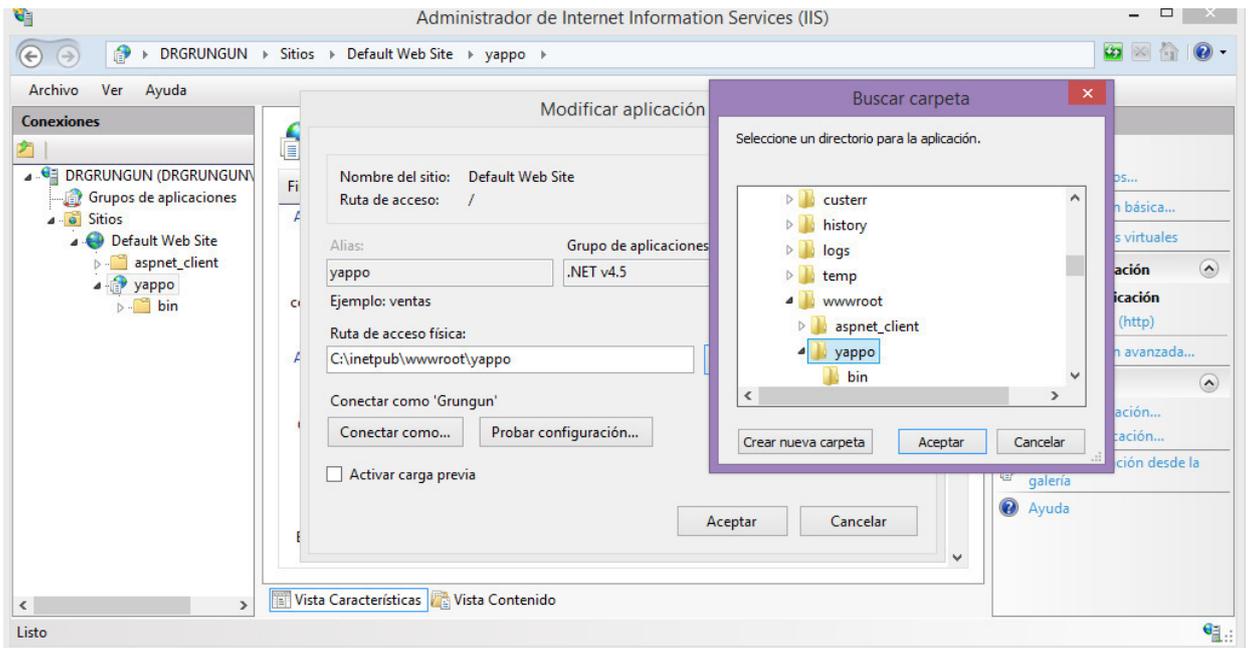


Figura 101: Ingres_IIS_Ma_Yappo

- Hacemos una prueba si está correctamente configurado

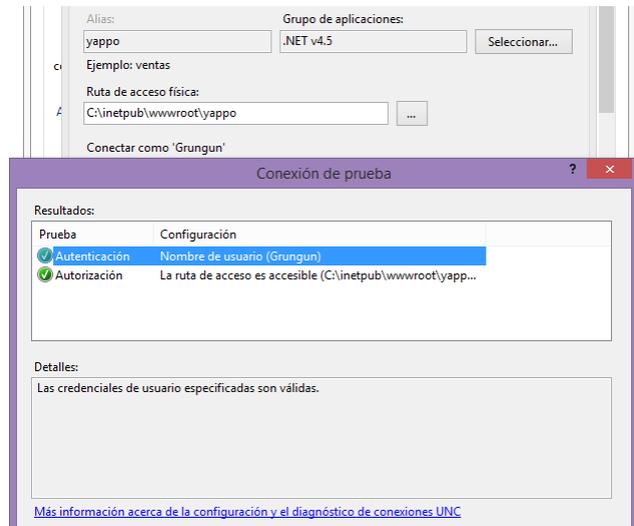


Figura 102: Test_IIS_Mang_YAPPO

- Abrimos una nueva instancia del explorador para revisar nuestros *Web service*

localhost - /yappo/

[\[To Parent Directory\]](#)

08/06/2015	15:48	<dir>	bin
05/12/2012	17:30	94	Service1.asmx
08/06/2015	15:57	393	Web.config

Figura 103: Local_Host_Yappo

- Ingresamos “service1.asmx” para verificar los ws

Service1

Las operaciones siguientes son compatibles. Para una definición formal, revise la [descripción de servicios](#).

- [EnviarMensaje](#)
- [LeerMensajes](#)
- [MarcarMensajeComoLeido](#)
- [ValidaUSR](#)

Figura 104: Serv_Yappo

Las *web services* permiten crear diversas funcionalidades que estas mismas permitirán obtener datos actualizados en tiempo real, esto convierte que se vuelva dinámico al incorporar el uso de lenguajes web para la gestión de los protocolos. Las siguientes figuras señalaran el recorrido de cómo se termina consumiendo las *web services* y las respuestas de los archivos XML

- Hacemos una prueba de “envió” de mensaje

Service1

Haga clic [aquí](#) para obtener una lista completa de operaciones.

EnviarMensaje

Prueba

Haga clic en el botón 'Invocar', para probar la operación utilizando el protocolo HTTP POST.

Parámetro	Valor
idUsuarioEnvia:	<input type="text"/>
idUsuarioRecibe:	<input type="text"/>
FechaEnvio:	<input type="text"/>
Mensaje:	<input type="text"/>

SOAP 1.1

A continuación se muestra un ejemplo de solicitud y respuesta para SOAP 1.1. Es necesario reemplazar los marcadores de posición que aparecen con valores reales.

```

POST /yappo/Service1.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://yappo.no-ip.org/yappo/EnviarMensaje"
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <EnviarMensaje xmlns="http://yappo.no-ip.org/yappo/">
      <idUsuarioEnvia>string</idUsuarioEnvia>
      <idUsuarioRecibe>string</idUsuarioRecibe>
      <FechaEnvio>string</FechaEnvio>
      <Mensaje>string</Mensaje>
    </EnviarMensaje>
  </soap:Body>
</soap:Envelope>

HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <EnviarMensajeResponse xmlns="http://yappo.no-ip.org/yappo/">
      <EnviarMensajeResult>string</EnviarMensajeResult>
    </EnviarMensajeResponse>
  </soap:Body>
</soap:Envelope>

```

Figura 105: Enviar_Mensaje

This XML file does not appear to have any style information associated with it. The document tree is shown below

```

<?xml version="1.0" encoding="utf-8"?>
<ArrayOfMensaje xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://yappo.no-ip.org/yappo/">
  <Mensaje>
    <idUsuarioEnvia>1</idUsuarioEnvia>
    <idUsuarioRecibe>jvc</idUsuarioRecibe>
    <Mensaje>hola, primer mensaje</Mensaje>
    <Fecha>30/09/2014 19:06:20</Fecha>
  </Mensaje>
</ArrayOfMensaje>

```

Figura 106: Res_Mensaje

- Prueba “leer mensaje”

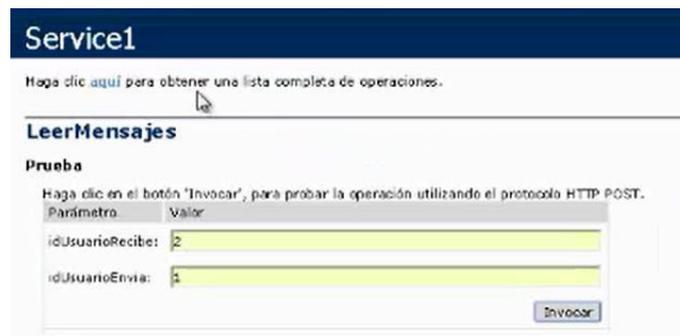


Figura 107: Leer_Mensaj



Figura 108: XML_Leer_Mens

Los archivos XML señalan como se gestionó el envío y recepción de mensajes, tanto las fechas y horas en las que se envió entre el emisor y receptor

- Validar usuario

Service1

Haga clic [aquí](#) para obtener una lista completa de operaciones.

ValidaUSR

Prueba

Haga clic en el botón 'Invocar', para probar la operación utilizando el protocolo HTTP POST.

Parámetro	Valor
usr:	<input type="text" value="a"/>
clave:	<input type="text" value="a"/>

SOAP 1.1

A continuación se muestra un ejemplo de solicitud y respuesta para SOAP 1.1. Es necesario reemplazar los marcadores de posición que aparecen con valores reales.

```
POST /yappo/Service1.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://yappo.no-ip.org/yappo/ValidaUSR"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsd="http://www.w3.org/2001/XMLSchema-instance" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ValidaUSR xmlns="http://yappo.no-ip.org/yappo/">
      <username>a</username>
      <password>a</password>
    </ValidaUSR>
  </soap:Body>
</soap:Envelope>
```

HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsd="http://www.w3.org/2001/XMLSchema-instance" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ValidaUSRResponse xmlns="http://yappo.no-ip.org/yappo/">
      <ValidaUSRResult>OK</ValidaUSRResult>
    </ValidaUSRResponse>
  </soap:Body>
</soap:Envelope>
```

SOAP 1.2

A continuación se muestra un ejemplo de solicitud y respuesta para SOAP 1.2. Es necesario reemplazar los marcadores de posición que aparecen con valores reales.

```
POST /yappo/Service1.asmx HTTP/1.1
Host: localhost
```

Figura 109: Valid_User

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<string xmlns="http://yappo.no-ip.org/yappo/">OK</string>
```

Figura 110: XML_User

- Configuramos nuestro *router* para re direccionar al puerto 80 desde nuestro PC. Para eso verificamos nuestra direcciona IP

```

Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . . . : fe80::53d:45a4:16d1:2234%3
Dirección IPv4. . . . . : 192.168.0.10
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.0.1

```

Figura 111: Direc_IP

Mientras los comandos del CMD se puede conocer cuáles son los puertos ocupados y las direcciones IPV4 que actualmente están en uso

- Escribimos nuestra dirección IP dentro de las configuraciones del *router*

The screenshot shows the Cisco configuration interface. At the top, there are navigation tabs: System, Signal, Status, Log, Provisioning, Setup (selected), and Advanced. Below the tabs, the page title is "Setup" and the sub-page is "Advanced Settings - Port Forwarding". A small text note says "This page allows you to configure port forwarding for local IP addresses." The main content is a table titled "Port Forwarding" with the following data:

Local IP Addr	Start Port	End Port	Protocol	Enable
192.168.0.10	80	80	Both	<input checked="" type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>

At the bottom of the table, there are "Apply" and "Back" buttons.

Figura 112: Port_Forwar

Al conocer nuestra dirección IP, declaramos en nuestro *router* que se liberen y re direccionamiento de dichos puertos a la IP escrita.

- Ingresar a No-IP

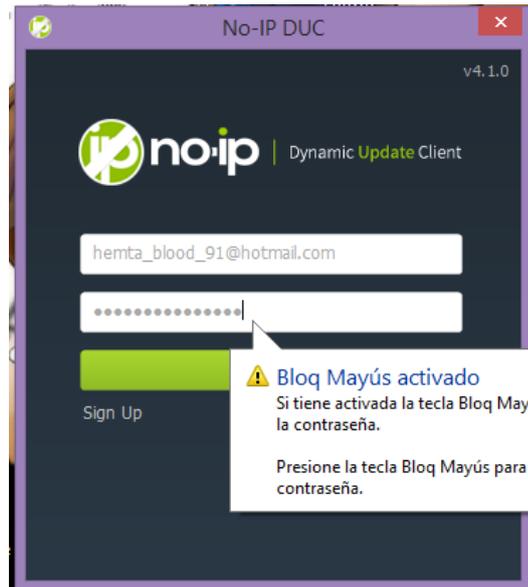


Figura 113: Login_NOIP

Como sabrán se necesitaba un *host* puesto al poner nuestra IP dinámica que se cambia y te la asigna aleatoriamente tu *router* y/o proveedor de internet como que no es muy buena práctica (risas) y las dificultades que se traerá consigo, entonces la primera opción era *dyndns* pero en el tiempo que se desarrolló el actual proyecto ya no era gratuito, adiós *dyndns* hola “No-ip”.

- Después de ingresar con nuestra cuenta configuramos nuestro *hosting*

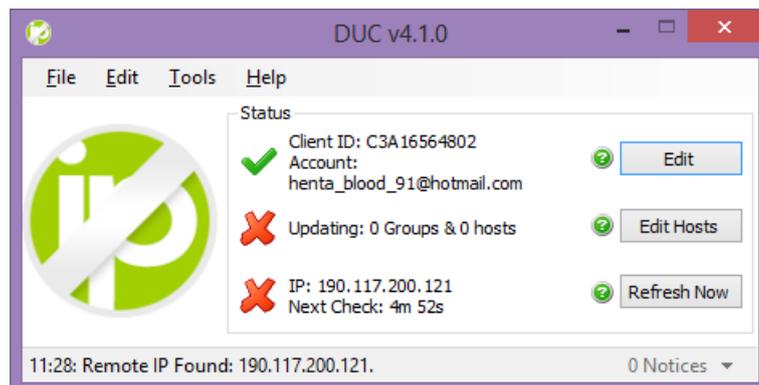


Figura 114: DUC_NOIP

A continuación se verá la secuencia de figura que forma parte de configurar No-ip en la PC en donde se ejecutara los “servicios web”.

- Seleccionamos nuestro host creado de NO-IP

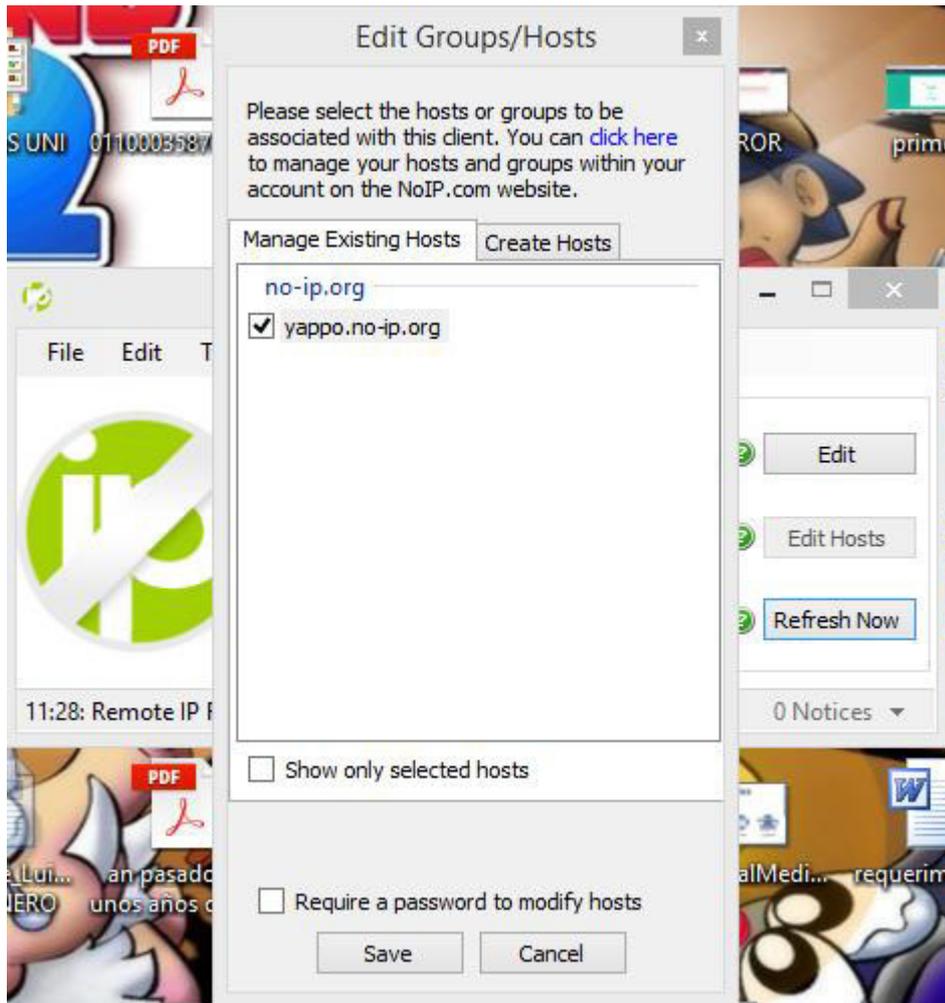


Figura 115: EDIT_HOSTS_NOIP

- Esta correctamente configurado

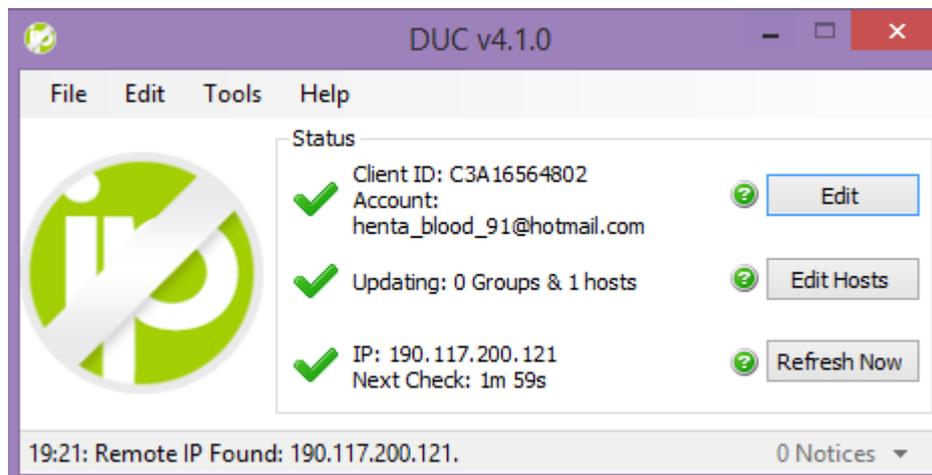


Figura 116: EDIT_HOSTS_NOIP

4.6.2 Manual de la aplicación

A. Requisitos del equipo móvil para instalar Yappo :

- Versión mínima de Android : 2.3.3
- Acceso a internet.

Debido a que la transferencia de mensajes es mediante servicio de internet, la velocidad de la aplicación dependerá de la velocidad de conexión de internet que se tenga en el equipo

B. Introducción

El proyecto Yappo! ofrece la oportunidad para la integración de los estudiantes y profesores de una manera segura y dedicada. Facilitando una enseñanza generalizada y sin llegar a propalar información delicada de los usuarios.

Paso N°1: Instalar Yappo



Paso N°3: Otros terceros no pueden descifrar nuestra conversación

Figura 118: Res_Yappo

La actual figura muestra de forma simple los procesos que se ven involucrados en la instalación y el funcionamiento de esta misma, a continuación se verán las figuras que forman parte para la instalación y ejecución de la aplicación.

- b. Información general de la aplicación
Yappo! Tiene como finalidad asegurar y proteger los procedimientos relacionados en el envío y recepción de mensajes instantáneos.

Resultados:

- Envío de mensajes
- Recepción de mensaje leído
- Marcar mensajes como leído
- No recupera mensajes
- Manual de la aplicación

- c. Instalar *Yappo!*

En el momento en que ya tengamos en nuestro poder el archivo *APK*, entonces lo tendremos que transferir al dispositivo *Android*, y para ello nos valdremos de un cable *USB* correspondiente oh mediante servicios *cloud* como *dropbox, mega, etc*

b1. Paso 1

Conectamos al dispositivo móvil a la PC en el momento en el que el sistema lo solicite, activamos el **modo de almacenamiento masivo**. También podremos montar la tarjeta SD como hace con un USB



Figura 119: Alm_Usb

b2. Paso 2

En el siguiente paso procedemos a copiar el archivo *APK* a la tarjeta, para ello lo arrastramos a la misma. En este punto es aconsejable crear una carpeta dentro de la SD con el objeto de hacer más fácil recordar su ubicación

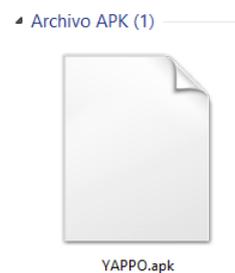


Figura 120: Apk_Yappo

b3.Paso 3

Ahora es cuando tenemos que indicarle a *Android* que permita la instalación de programas fuera de *Google Play*, para ello nos desplazamos hasta “**Ajustes > seguridad > orígenes desconocidos**”



Figura 121: Orig_Desc

b4.Paso 4

Cuando finalizamos con este proceso, estaremos en condiciones de instalar la aplicación. Abrimos nuestro administrador de archivos preferido, buscamos el archivo en la carpeta que creamos o donde copiamos en la tarjeta SD y lo ejecutamos

El procedimiento de instalación no puede producir ninguna clase de problemas puesto la *APK* de Yappo es de fuentes confiables y seguras

- Ingreso Yappo!

Después de instalar *Yappo!* Ingresamos con nuestro código de alumno y contraseña que utilizamos para el intranet: <http://www.uch.pe/>



Figura 122: Login_Yappo

- Contenido de Yappo!

En la parte superior izquierda de la pantalla se muestran el menú de opciones

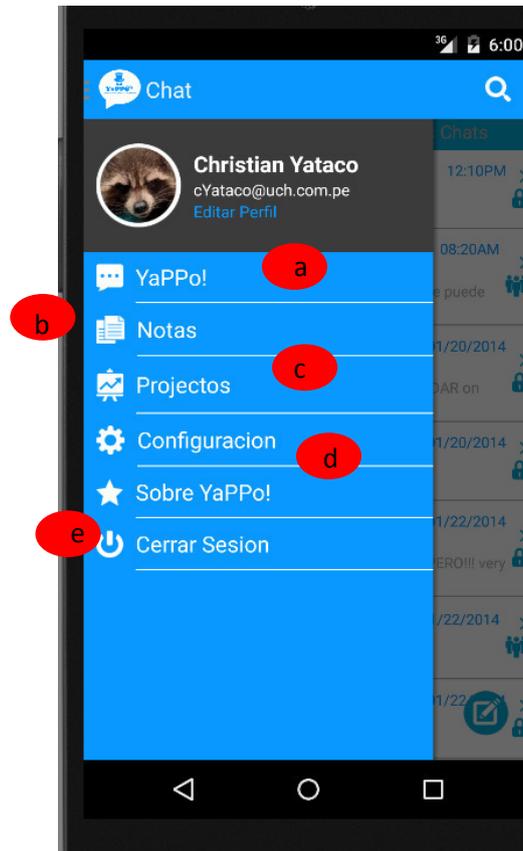


Figura 123: Yappo!_Ingreso

A continuación se nombrar la función de cada módulo de Yappo, esto no define la funcionalidad directa de los módulos si no como una breve descripción y para diferenciar los módulos se utilizara como viñeta temporal: a),b) – e)

- a) Permite ingresar a la bandeja de entrada de chats
- b) Permite ingresar a la lista de notas
- c) Permite ingresar a la lista de proyecto (en desarrollo)
- d) Permite ingresar a la información de Yappo
- e) Cierra la aplicación

d. Ingreso bandeja de chat

Esta opción nos muestra un listado de nuestras conversaciones convirtiéndolo en una bandeja de entrada de chats, dando la opción de enviar un nuevo mensaje en el botón derecho inferior de una lápiz o contestar seleccionando el chat que se desee.

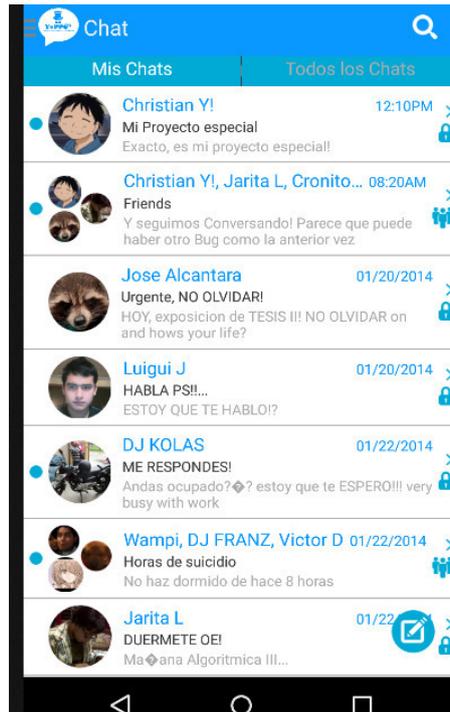


Figura 124: Yappo!_BE_chat

- Seleccionar contacto



Figura 125: Yappo!_contac

- Nuevo mensaje



Figura 126: Yappo!_Chat

- Diccionario inteligente

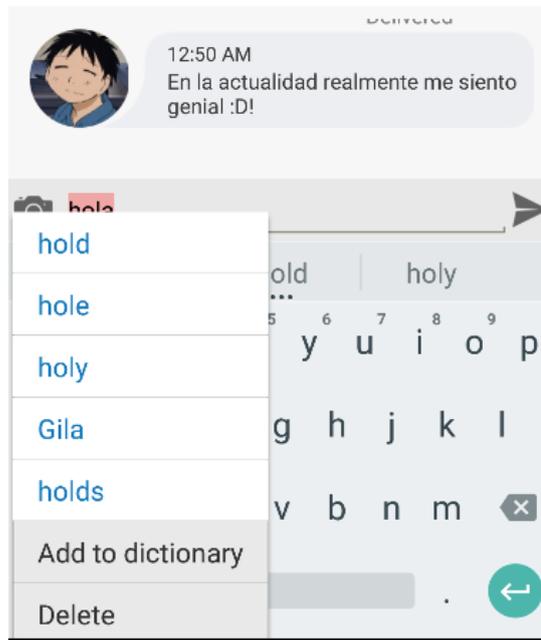


Figura 127: Yappo!_Chatt2

- Respuesta de chat



Figura 128: Yappo!_Chat_3

C. Ingreso bandeja de notas

Esta opción nos muestra un listado de nuestras notas en un listado, dando la opción de crear una nueva nota en el botón derecho inferior de un lápiz.

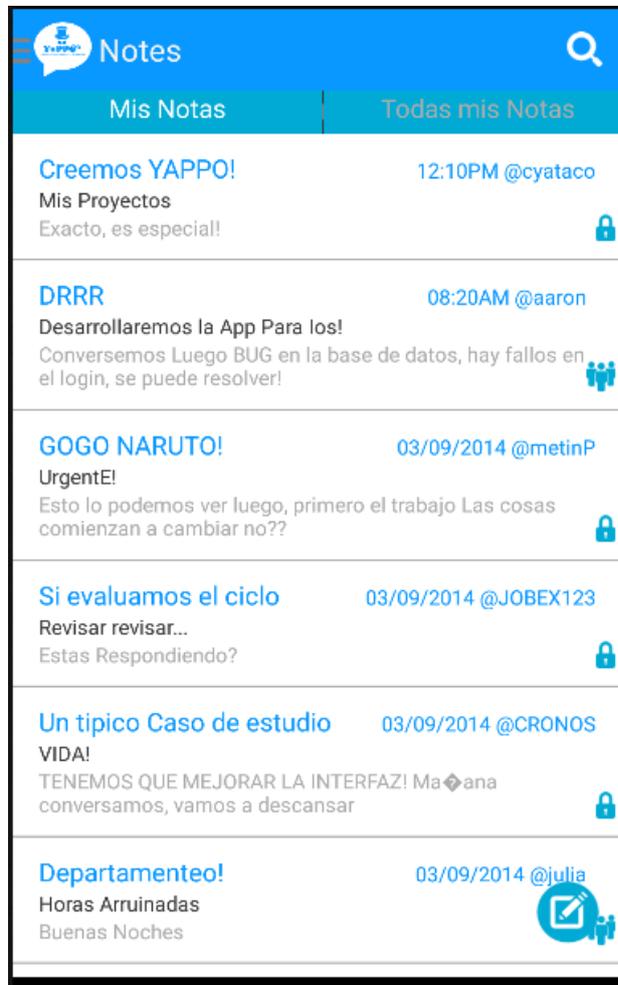


Figura 129: Yappo!_Note

D. Ingreso bandeja de proyectos

Proyectos con metodología *Kanban* aun esta en desarrollo esta etapa no está dentro de los objetivos de Yappo! Si no un agregado que se tendrá listo para comienzos de octubre

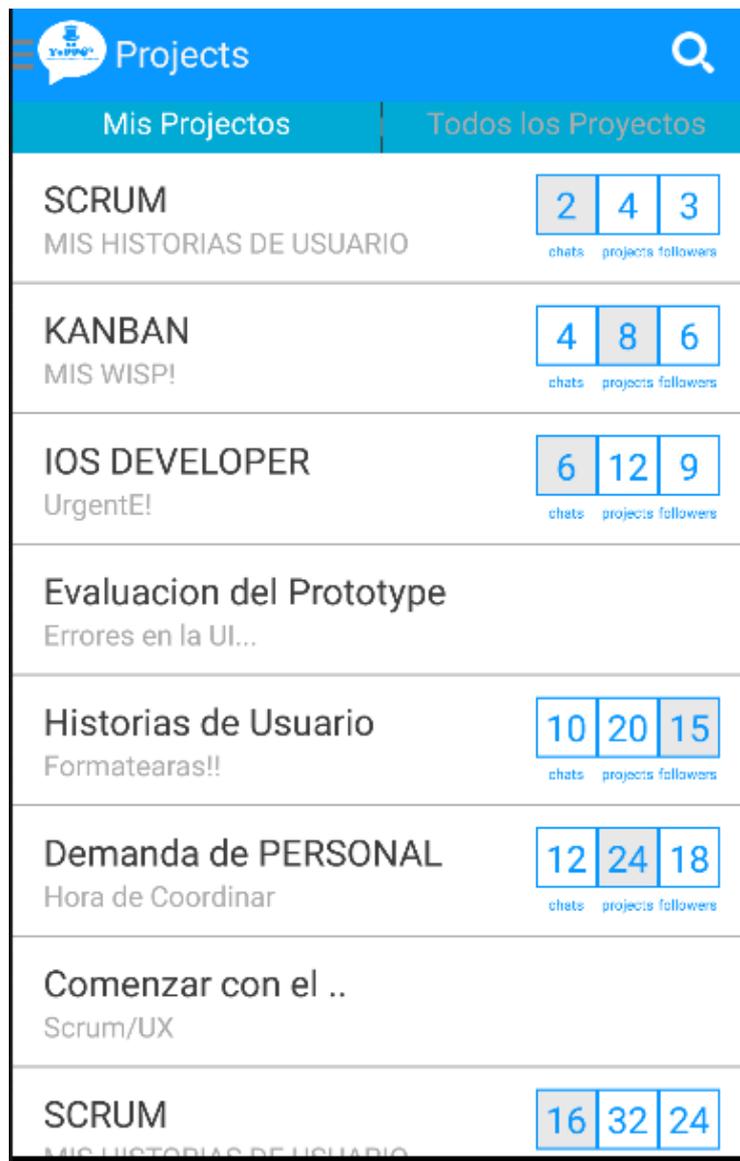


Figura 130: Yappo!_Project

E. Sobre Yappo!

Información de la aplicación respecto a la universidad de Ciencias y humanidades

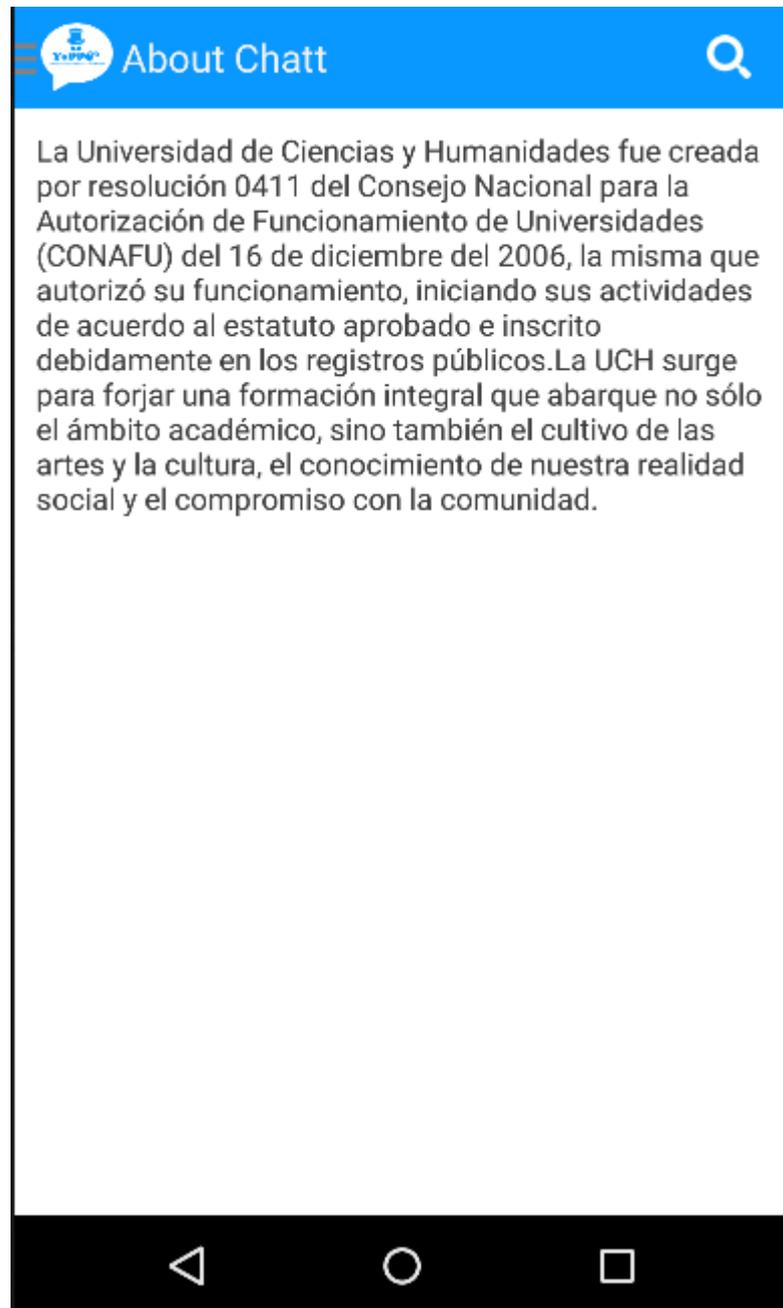


Figura 131: Yappo!_AboutYappo

F. Cerrar la aplicación

Cierra sesión del usuario

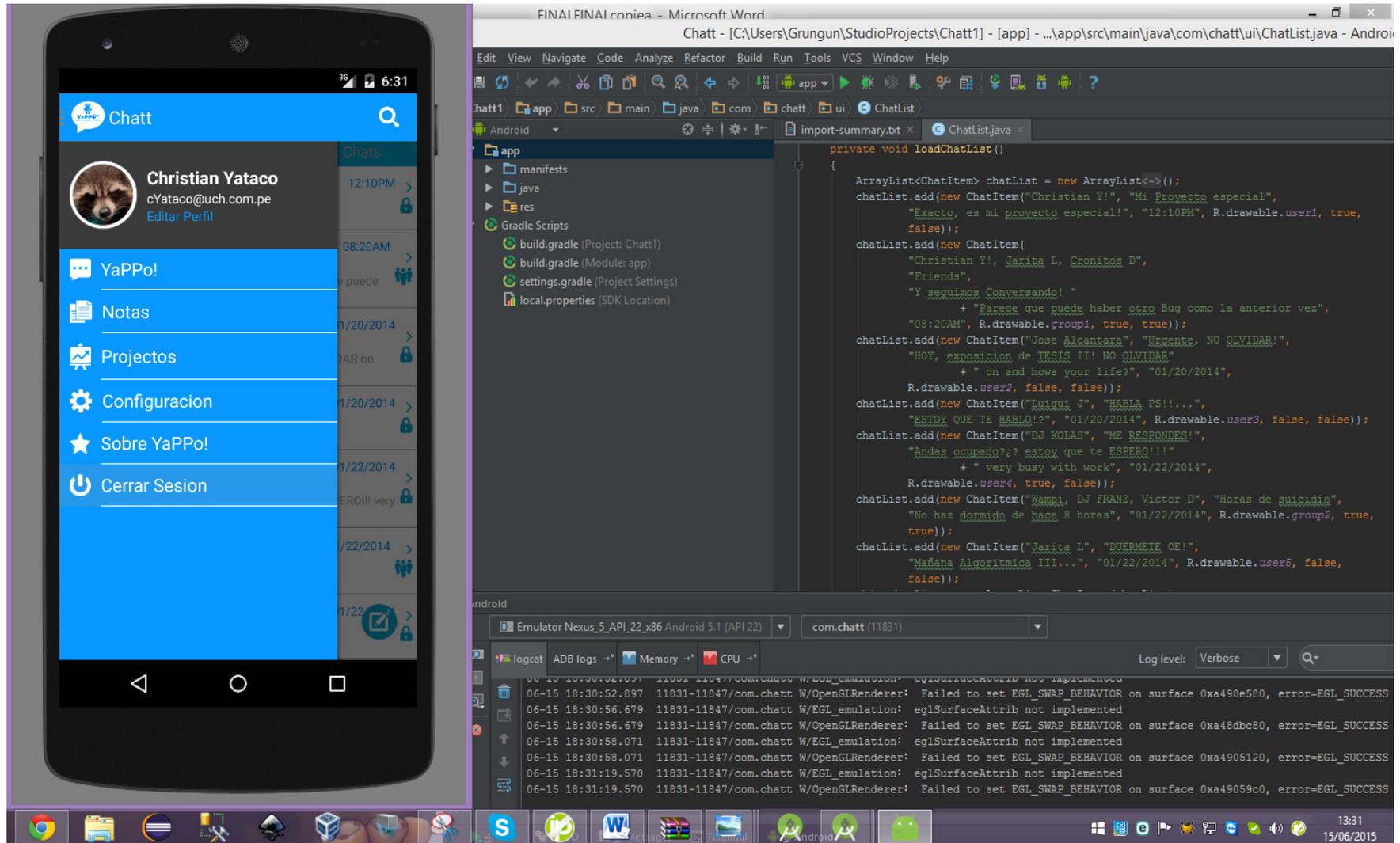


Figura 132: Yappo!_CerrarYappo

4.6.3 Capacitación a los usuarios

- Propósito

Capacitar al usuario en el manejo de la solución: implementación de una aplicación mensajería instantánea *Android* con funciones de encriptamiento y privacidad de datos orientada a la seguridad de datos estudiantil en la UCH

- Descripción

La capacitación pretende desarrollar, en los usuarios finales, el conocimiento, competencias y habilidades suficientes para su manejo.

Esta comprende los siguientes reportes de la implementación de la solución de Yappo!

A. Personal a capacitar

A continuación se presenta la lista del personal a capacitar tanto de las áreas funcionales como técnicas, asimismo se describen las competencias a desarrollar por cada reporte de la solución.

Usuarios capacitar:

- Tutoría.
- Alumnos UCH

Tabla 38: Capacitación de usuario

Área	Acción	Competencias a desarrollar
Tutoría	<ul style="list-style-type: none"> • Envío de mensajes • Selección de destinatarios • Destinatario • Texto del mensaje • Fecha y hora de envío 	<ul style="list-style-type: none"> • Envía el mensaje al rellenar el campo de lectura, escribir el texto del mensaje dentro de “mensaje nuevo” y pulsar sobre el botón “enviar” • Incluye los destinatarios al pulsar sobre los contactos que se hayan añadido • Identifica por nombre a su destinatario • Para ver el texto íntegro de un mensaje bastara con hacer un clic sobre él. Pulsar el botón volver para regresar a la bandeja de mensajes • Muestra la fecha en la que el mensaje fue enviado
Alumnos	<ul style="list-style-type: none"> • Envío de mensajes • Selección de destinatarios • Destinatario • Texto del mensaje • Fecha y hora de envío 	<ul style="list-style-type: none"> • Envía el mensaje al rellenar el campo de lectura, escribir el texto del mensaje dentro de “mensaje nuevo” y pulsar sobre el botón “enviar” • Incluye los destinatarios al pulsar sobre los contactos que se hayan añadido • Identifica por nombre a su destinatario • Para ver el texto íntegro de un mensaje bastara con hacer un clic sobre él. Pulsar el botón volver para regresar a la bandeja de mensajes • Muestra la fecha en la que el mensaje fue enviado

B. Actividades de capacitación

La capacitación, para los usuarios, abarcará los tópicos siguientes:

- Presentación de Yappo!, exponiendo sus alcances.
- Descripción de estándares y requisitos de Yappo!
- Descripción detallada del funcionamiento de cada opción de Yappo!
- Presentación de pantallas.
- Descripción de pantallas y destinatarios.

C. Recursos necesarios

a. Infraestructura / Ambientes del Capacitación

La capacitación se realizará en las instalaciones de la Universidad de Ciencias y Humanidades determine las mismas que deberán ofrecer las condiciones mínimas de equipamiento y materiales descritas en el presente plan.

b. Materiales y equipamiento

Los ambientes de capacitación deberán contar como mínimo, con lo siguiente:

- PC (*Team viewer/Vnc/RDS*)
- Una (01) PC / Laptop por participante.
- Carpetas, mesas y sillas de acuerdo al número de asistentes.
- Micrófono (si fuera posible) para el expositor.
- Pizarra acrílica blanca y plumones.

c. Formato de asistencia

Tabla 39: Formato de Asistencia

	"IMPLEMENTACIÓN DE UNA APLICACIÓN MENSAJERÍA INSTANTÁNEA ANDROID CON FUNCIONES DE ENCRIPCIÓN Y PRIVACIDAD DE DATOS ORIENTADA A LA SEGURIDAD DE DATOS ESTUDIANTIL EN LA UNIVERSIDAD CIENCIAS Y HUMANIDADES"		
Lugar	Lima -Olivos		
Nombre del Proyecto	IMPLEMENTACIÓN DE UNA APLICACIÓN MENSAJERÍA INSTANTÁNEA ANDROID CON FUNCIONES DE ENCRIPCIÓN Y PRIVACIDAD DE DATOS ORIENTADA A LA SEGURIDAD DE DATOS ESTUDIANTIL EN LA UNIVERSIDAD CIENCIAS Y HUMANIDADES	Periodo de la capacitación	Junio 2015
Fecha Inicio	12/06/2015	Fecha Fin	30/06/2015

Se utilizó el siguiente formato para las capacitaciones realizadas durante el **mes de Junio del 2015**, comprendido entre el **12/06/2015 al 30/06/2015**, correspondiente a la implementación de una aplicación mensajería instantánea Android con funciones de

encripta miento y privacidad de datos orientada a la seguridad de datos estudiantil en la universidad ciencias y humanidades

Tabla 40: Formato de usuarios

Nombre de las personas presentes en la capacitación		Área	
Fecha inicio capacitación		Hora Inicio	
Descripción de la Capacitación			
Fecha fin capacitación		Hora Fin	
Responsable capacitación		E- mail	
Firma persona presente en la capacitación		Firma persona responsable capacitación	

4.7 MONITOREO

4.7.1 Desarrollo de pruebas en producción

A. Nivel de prueba

Los niveles de prueba definidos son:

- Pruebas Funcionales
- Pruebas de Sistema

B. Propósito

El propósito del Plan de Pruebas, es explicitar el alcance, enfoque, recursos requeridos, responsables y manejo de riesgos de un proceso de pruebas.

C. Casos de prueba

Esta sección detalla las pruebas planeadas a utilizar para comprobar Yappo! y garantizar la consecución de sus objetivos con los que fue diseñado. Para realizar estas pruebas se debe llevar a cabo las configuraciones necesarias en el entorno de prueba, cada caso de prueba puede requerir un conjunto de especificaciones determinadas.

Los casos de prueba constan de 2 secciones:

- Caso de Prueba
- Resultado de la Prueba

a. Caso de prueba

Tabla 41: Casos de Prueba

ID	Acción a realizar	Resultado esperado	Resultado obtenido
1	Instalación de Yappo!	Carga y proceso de instalación	CORRECTO
2	Ingresar Usuario y Contraseña.	a. Ingreso exitoso	CORRECTO
3	Lista de bandejas	Listado general de las bandejas de Yappo!	CORRECTO
4	Selección de envío y recepción de mensaje	<p>Luego de ingresar a Yappo! donde se encuentra lista de contactos, seleccionamos el contacto que necesitamos.</p> <p>a. Envío de mensaje "Para enviar un mensaje bastara con rellenar el campo "mensaje nuevo", escribir el texto del mensaje dentro del campo y pulsar sobre el botón enviar"</p> <p>b. Selección destinatarios "Para incluir destinatarios deberás pulsar sobre los contactos que hayas añadido"</p> <p>c. Ver mensaje nuevo: "Para ver el texto integrado de un mensaje bastara con hacer clic sobre él. Pulsa volver para regresar a la bandeja de mensajes</p>	CORRECTO

b. Resultado de la prueba

Tabla 42: Resultado de Prueba

Proyecto	Implementación de una aplicación mensajería instantánea <i>Android</i> con funciones de encriptamiento y privacidad de datos orientada a la seguridad de datos estudiantil en la Universidad Ciencias y Humanidades	
ID del Caso de Prueba	CP_001	
Nombre del Caso de Prueba	1	
Ejecución N°	1	
Descripción	Se procede a realizar las pruebas a los usuarios finales ya sean tutoria y/o alumnado	
Criterios generales para la aprobación	Conforme	
Persona que realiza la prueba	Tutoria /alumnado	
Fecha y hora de inicio	2:00pm	
Sistema Operativo usado	WINDOWS	
Software Remoto	Team viewer	
Comentarios	Prueba satisfactoria	
Estado del Caso de Prueba	Culminado	
N° total de pasos		3
N° de pasos completados con estado "Correcto"		3
N° de pasos completados con estado "Fallido"		0
Prueba completada al		100%
Porcentaje de error		0%

4.7.2 Lista y control de cambios

- Control de Cambios para la implementación de una aplicación mensajería instantánea *Android* con funciones de encriptamiento y privacidad de datos orientada a la seguridad de datos estudiantil en la Universidad Ciencias y Humanidades
- Usuarios
 - Se creará un usuario por cada perfil del intranet
 - Los roles y Perfiles serán manejados de acuerdo a como están registrados dentro de su intranet
 - Los profesores o docentes podrá participar en la aplicación si lo amerita

Tabla 43: Control de cambios

Opciones / Reportes	ALUMNO	Tutoría
Envío de mensaje	X	X
Recepción de mensaje	X	X
Instalación de Yappo!	X	
Ingreso de Yappo!	X	
Lectura de mensaje	X	X

Los cambios de un proyecto tienden a re programarse en el desarrollo de levantamiento de información, definiciones de roles, etc. La siguiente tabla puntualiza los records y cambios que se dieron entre la asesoría interna y las márgenes de prueba tomadas por los alumnos.

Tabla 44: Reajuste de usuario final

REAJUSTES DEL SISTEMA	RESPUESTA DEL REQUERIMIENTO			
	FECHA	ESTADO	Rpta.	Responsable
IMPLEMENTACIÓN DE UNA APLICACIÓN MENSAJERÍA INSTANTÁNEA ANDROID CON FUNCIONES DE ENCRIPAMIENTO Y PRIVACIDAD DE DATOS ORIENTADA ALA SEGURIDAD DE DATOS ESTUDIANTIL EN LA UNIVERSIDAD CIENCIAS Y HUMANIDADES				
NINGUNO	15/06/2015	Cerrado	Validado	Tutoría

4.7.3 Reajustes y aprobación del usuario final

A. Usuarios aprobar: tutoría

Tabla 45: Usuario aprobar

Usuarios	Sistema	Estado
Tutoría	Implementación de una aplicación mensajería instantánea <i>Android</i> con funciones de encripta miento y privacidad de datos orientada a la seguridad de datos estudiantil en la Universidad Ciencias y Humanidades	Validado

CAPITULO V
ANÁLISIS DE COSTO Y BENEFICIO

5.1 ANÁLISIS DE COSTOS

5.1.1 Costos de implementación

A. Recursos humanos

Tabla 46: RRHH

DESCRIPCIÓN DE ACTIVIDAD	Personal	Horas	Precio Unitario	Monto
Análisis del Negocio	1	10	80,00	800,00
Lista de Requerimiento	1	5	80,00	400,00
Desarrollador VB	1	10	80,00	800,00
Desarrollador SQLSERVER	1	5	60,00	300,00
Desarrollador <i>java- Android</i>	1	30	60,00	1800,00
Desarrollador API PHP	1	10	60,00	600,00
Desarrollo BD <i>MYSQL</i>	1	5	40,00	200,00
Desarrollo de la solución	1	12	75,00	900,00
TOTAL				5800,00

B. Recursos de hardware

Tabla 47: RR Hardware

COSTOS DE HARDWARE

DESCRIPCIÓN DEL EQUIPO	CANTIDAD	Precio Unitario	Monto
Servidor	1	4095	4095
<i>Switch</i> Link 12 puertos	1	95	95
Laptop Toshiba I5	1	2500	2500
Mouse Óptico <i>Genius</i>	1	30	30
Teclado USB	1	30	30
Tablet Toshiba <i>Exite Write</i>	1	1400	1400
<i>One Plus One</i> 64gb	1	1300	1300
TOTAL			9450.00

C. Recursos de *software*

- Costo de *Software*

Tabla 48: RR Software

DESCRIPCIÓN DEL SOFTWARE	DESCRIPCIÓN	CANTIDAD	Precio unitario	Monto
SQL Server EXPRESS	Licencia	1	0.00	0.00
NOIP	Licencia	1	0.00	0.00
IDE ECLIPSE	Licencia	1	0.00	0.00
XAMPP	Licencia	1	0.00	0.00
Teamviewer	Licencia	1	0.00	0.00
visual studio express 2012	Licencia	1	0.00	0.00
Windows 7 Ultimate 64 Bits	Licencia	1	832.00	832.00
Microsoft Office 2010	Licencia	1	403,00	403.00
TOTAL SOFTWARE				1235,00

Tabla 49: Costos de implementación

DESCRIPCIÓN DE ACTIVIDAD	Monto
TOTAL DE SOFTWARE	1.235,00
TOTAL DE HARDWARE	9.450,00
TOTAL DE MANO DE OBRA	5.800,00
TOTAL MANO DE OBRA	16.485,00

5.1.2 Costos de mantenimiento

Tabla 50: Costos de variables

DESCRIPCIÓN DEL MANTENIMIENTO	CANTIDAD	Precio Unitario	Monto
Mantenimiento de servicio <i>outsourcing</i>	1	1200.00	1200.00
Mantenimiento de servidor	1	750.00	750.00
		TOTAL MANO DE OBRA	1950.00

5.1.3 Otros gastos

Tabla 51: Costos de otros gastos

COSTOS VARIABLES	Monto
Pagos de Luz	120,00
Costos de Papel A4	60,00
Servicio de Internet 4 Mbps	140,00
TOTAL DE SUELDO	320,00

5.2 ANÁLISIS DE BENEFICIOS

5.2.1 Beneficios cuantitativo

Tabla 52: BE cuantitativos

DESCRIPCIÓN	Hora	Monto	Total
Beneficios TANGIBLES			
Comunicación interna segura	1	40	480
Transferencia de datos	1	20	240
Creación de notas/tareas	1	20	240
Reporte por profesor	1	20	240
Reporte deserción académica	1	20	240

5.2.2 Beneficios cualitativos

Tabla 53: BE cualitativos

Beneficios Cualitativos			Total
ahorro de pago de tutores para el seguimiento del Rendimiento Académico del estudiante	80	10	8000
Ahorro de publicidad	00.00	00.00	2000
calidad de servicio al alumno	00.00	00.00	2500

Tabla 54: Beneficios tangibles e intangibles

DESCRIPCIÓN	HORA	MONTO/HORA	TOTAL
Beneficios TANGIBLES			
Comunicación interna segura	1	40	480.00
Transferencia de datos	1	20	240.00
Creación de notas/tareas	1	20	240.00
Reporte por profesor	1	20	240.00
Reporte deserción académica	1	20	240.00
Beneficios Cualitativos			
ahorro de pago de tutores para el seguimiento del Rendimiento Académico del estudiante	80	10	800.00
Ahorro de publicidad	00.00	00.00	2000.00
calidad de servicio al alumno	00.00	00.00	2500.00
TOTAL INGRESOS			6740.00

5.3 Análisis de sensibilidad

5.3.1 Desarrollo de flujo de caja

Tabla 55: Desarrollo flujo de caja

Cuadro de recuperación de la inversión

Descripción	0	1	2	3	4	5	6	7	8
Beneficio	-----	6740.00	13480	20220	26960	33700	40440	47180	53920
Costo de mantenimiento	-----	2270.00	2270.00	2270.00	2270.00	2270.00	2270.00	2270.00	2270.00
Utilidad	-----	18.755,00	21.025,00	23.295,00	25.565,00	27.835,00	30.105,00	32.375,00	34.645,00
Ingreso Neto	-----	4470	4470	4470	4470	4470	4470	4470	4470
Inversión	16485.00	-1201,5	-754,5	-307,5	139,5	586,5	1033,5	1480,5	1927,5

Como se muestra en el grafico la inversión la obtenemos en el 4to mes, algo interesante puesto se tenía prevista obtener ganancias en el mes 8

9	10	11	12	13	14	15	16	17	18
60660	67400	74140	80880	87620	94360	101100	107840	114580	121320
2270.00	2270.00	2270.00	2270.00	2270.00	2270.00	2270.00	2270.00	2270.00	2270.00
36.915,00	39.185,00	41.455,00	43.725,00	45.995,00	48.265,00	50.535,00	52.805,00	55.075,00	57.345,00
4470									
2374,5	2821,5	3268,5	3715,5	4162,5	4609,5	5056,5	5503,5	5950,5	6397,5

19	20	21	22	23	24
128060	134800	141540	148280	155020	161760
2270.00	2270.00	2270.00	2270.00	2270.00	2270.00
59.615,00	61.885,00	64.155,00	66.425,00	68.695,00	70.965,00
4470	4470	4470	4470	4470	4470
68445	72915	77385	81855	86325	90795

5.4 Análisis de VAN

VAN (Valor Actual Neto): Es un método cuya principal aplicación es determinar la rentabilidad de la inversión. Como su nombre lo indica trata de determinar el valor que ahora (actual) tiene la inversión sobre la base de los importes que se percibirán en unos plazos determinados. Se calcula sobre los flujos netos de caja que generara la inversión: El VAN, es el valor monetario que resulta de restar a la inversión inicial la suma de los flujos de caja esperados, ajustados con cierta tasa de descuento.

Tabla 56: Análisis VAN

PROMEDIO DE INVERSIÓN (2 AÑOS)	
TIR	27%
VAN	S/. 32,970.00

5.4.1 Análisis del TIR

TIR (Tasa Interna de Retorno): Es un indicador de la rentabilidad de un proyecto, la tasa % de rendimiento anual acumulado que genera la inversión. Su formulación busca una tasa de rendimiento interno que iguale los flujos netos de caja con la inversión inicial. Suele definirse como la tasa de descuento que iguala el VAN a cero y suele presentarse complementando al VAN

Tabla 57: Análisis TIR

PROMEDIO DE INVERSIÓN (2 AÑOS)	
TIR	27%
VAN	S/. 32,970.00

5.4.2 Análisis del ROI

Tabla 58: Análisis ROI

PROMEDIO DE INVERSIÓN (2 AÑOS)	
TIR	27%
VAN	S/. 32,970.00
Total de Inversión a 2 años	
	70.965,00
Total de Beneficios a 2 años	
	161.760,00
ROI	128%

Como se refleja en la propuesta tabla Análisis ROI.

El **VAN** al ser superior a 0 antes de cumplir el primer año, supera la inversión aplicada en el año 2 nos demuestra un monto **S/. 32,970.00** superiores a lo invertido, justificando la viabilidad del proyecto.

En cambio el porcentaje del **TIR** ya en el primer año su porcentaje es **13.5%** dando como indicador un rentabilidad mayor al 20% para el segundo año (**27%**), concluyendo por el TIR que el proyecto no generara perdidas

Respecto al **ROI** como punto crucial a lo invertido evaluamos que tan eficiente es el gasto,

Considerar que el $ROI = (Ganancias - Inversión) / Inversión$

Es decir, comparamos los costos que hemos realizado y las ganancias que hemos obtenido para calcular de manera económica si el proyecto realizado tuvo el éxito como se esperaba, dando una proyección del 128% obtenida, la rentabilidad es positiva.

Conclusiones

- **Resumen General**

De acuerdo a los objetivos específicos definidos para el presente proyecto se realizó el análisis de las siguientes etapas:

1. Estudio implementación
2. Implementación de la aplicación móvil de mensajería

- **Conclusiones de implementación**

- Gracias al cifrado y políticas de seguridad que se integraron al proyecto se logró satisfactoriamente incrementar el rendimiento de seguridad en el envío y transferencia de datos, de este modo mejoro en creces los procesos de comunicación entre estudiantes de la universidad Ciencias y Humanidades.
- El envío de mensajes y recepción aun estando bajo un nivel de seguridad no garantiza que la data no sea expuesta por el emisor o receptor de los mensajes. La información del usuario como lista de contactos, mensajes se encuentra propiamente en el dispositivo móvil, en sus historiales.
- Se logró reconocer el nivel de disposición al uso y desarrollo de una aplicación móvil propia de la universidad ciencias y humanidades

- **Conclusiones de la implementación de la aplicación móvil**

Como resultado del estudio implementación se puede concluir que los estudiantes de la Universidad de Ciencias y Humanidades están cediendo ante el creciente apoderamiento del mercado de la telefonía móvil por parte de los dispositivos móviles bajo la plataforma Android.

De igual manera se puede concluir que teóricamente estudiantes de la UCH están dispuestos en un 90% a la adopción de nuevas herramientas tecnológicas bajo un estándar colaborativo, seguro y privado dentro de su proceso educativo bajo una plataforma

android, con el fin de mejorar los canales de comunicación académica entre docentes y estudiantes.

Por otro lado, el objetivo de este proyecto era la creación de un aplicativo multi plataforma móvil con funcionalidades de privacidad y seguridad para móviles. Para poder realizar dicho aplicativo (Yappo!). Fue necesario valorar si las herramientas de desarrollo y tecnologías multiplataforma o CPT (*Cross-Plataform Tools*) eran viables para la comunidad universitaria de la Universidad Ciencias y Humanidades (UCH).

El resultado final mediante el levantamiento de información demuestra un alto índice de popularidad y variedad en una sola plataforma (Android). No solo para el público universitario si no del país y Latinoamérica. Definiendo el anterior concepto se decidió realizar puramente Yappo! como una *app* móvil nativa por tener un mayor rendimiento que una aplicación web y/o multiplataformica. De acuerdo a los estándares actuales y requeridos por los propios estudiantes.

Recomendaciones

Las tecnologías móviles están en un constante cambio por mejoras continuas y por diseños que buscan la experiencia del usuario, aplicaciones que apuestan por las corrientes como *design thinking*, *user experience* entre muchas otras. Por lo cual Yappo! puede ser mejorado en distintos aspectos y el alumno ofrece algunas alternativas para mejorarlo en un futuro. Son mejoras que no tenían cabida en el presente trabajo, dirigidas específicamente al área de sistemas y/o soporte de la Universidad Ciencias y Humanidades

- Almacén de credenciales: Actualmente el servidor almacena el par usuario contraseña en una tabla de su base de datos. Se recomienda que sería mucho más seguro modificar este sistema y que cada usuario, en lugar de ser un registro en la base de datos del servidor.
- Transferencia de archivos: El envío y recepción de archivos es una función muy importante en casi cualquier sistema de mensajería. Se propone como posible mejora una ampliación del sistema actual incorporando un sistema de envío y recepción de archivos de cualquier tipo.
- Multiplataformica. : Actualmente Yappo! es una aplicación 100% nativa desarrollada en *android*. Se recomienda que en vez de migrar la aplicación a una web se desarrolle una aplicación con lenguaje nativo para las distintas terminales nombradas en este trabajo.
- En los que respecta al análisis de rendimiento y monitorización sería conveniente tener acceso a otros dispositivos Android con diferentes especificaciones de hardware en cuanto a pantalla, memoria y CPU. Distintas versiones del sistema operativo. Además, llevar cabo dicho procedimiento en un ambiente controlado

Referencias

Giménez, L. (2014) *Android tiene problemas de seguridad*. Recuperado el 03/04/2014 de <http://es.gizmodo.com/tiene-android-un-problema-de-seguridad-451495756>

Calderón, A. (2012). *Definición de sistema operativo*. Recuperado el 02/05/2014 de <http://www.antonicalderonch.com>

Arturo, A., Ferreira, A. y Rodríguez, M. (2013) *Dispositivos Móviles*. Recuperado el 13/06/2013 de <http://156.35.151.9/~smi/5tm/09trabajos-sistemas/1/Memoria.pdf>

Fecha de acceso: 13/06/2013

Anizar. (2012) *.Arquitectura de seguridad basada en identificación para cómputo móvil*. México: Editorial. Grijalbo México

Carmen P. y Aguilera M. (2011), *Sistema de Información para el registro y control de los procesos de gestión de higiene ocupacional. Caso: gerencia de ambiente e higiene ocupacional, división Faja Del Orinoco Pdvsa-San Tomé*. Tesis de Licenciatura no publicada, Universidad de Oriente, Venezuela

Bruna L, I. (2004) *La seguridad informática evoluciona*. Recuperado el 12/05/2013 de <http://www.belt.es.com>.

Fecha de acceso: 12/05/2013. Lima Perú

- Cárdenas, (2012). *Análisis de seguridad de la información en los dispositivos móviles Smartphone*. Tesis de Licenciatura no publicada, Universidad Central de Ecuador, Ecuador
- Carrillo, F. (1986) *Como hacer la tesis y el trabajo de Investigación Universitario*. Lima, Perú: Editorial Horizonte.
- Chamorro, (2011). *Análisis de factibilidad del marketing móvil vis SMS para servicios de valor agregado en la ciudad de Lima*. Lima, Perú: Editorial Horizonte
- Cujano R. (2010). *Diseño e implementación de un sistema de control electrónico para bloquear/desbloquear automóviles mediante SMS encriptados*. Tesis de Licenciatura no publicada Universidad Central de Ecuador, Ecuador
- Continuousagile. (2014) Metodologías Agiles. Recuperado el 05/09/2015 de <http://www.continuousagile.com/>
- Cyta. (2008) *Firma Digital*. Recuperado el 21/11/2008 de www.cyta.com.ar "firma digital"
- Dan Lesna, H. (2004) *Metodología de la Investigación*. Bogotá, Colombia: Editorial Diente de León
- Dmitrivivanov. (2012) *Portabilidad Kanban*. Recuperado el 08/11/2012 de <http://dmitryivanov.net/>

- Ferrer. (2012) *Seguridad informática y software Libre*. Recuperado el 12/05/2014 de <http://es.tldp.org/Informes/informe-seguridad-SL/informe-seguridad-SL.pdf>.
- Fsecure, (2015) *Seguridad informática*. Recuperado el 08/04/2015 de http://www.f-secure.com/en/web/labs_global/
- Fukushima J. (2010). *Análisis, diseño e implementación de un sistema de control de inventarios para empresas de almacenamiento de hidrocarburos*. Tesis de Licenciatura no publicada, Universidad Pontificia Católica del Perú, Lima.
- Galeón. (2013) *Envoltorio Digital*. Recuperado el 08/10/2013 de www.galeon.com-“Envoltorio digital”
- Genbetadev. (2013) *Móvil vs Escritorio*. Recuperado el 13/08/2013 de <http://www.genbetadev.com>
- Gerardo C. (2011) *Implementation of Cryptosystem of elliptic curve in mobile environments*. Madrid, España: Editorial VINCULOS
- Gizmodo, (2013) *Los Smartphone más utilizado*. Recuperado el 12/11/2013 de <http://es.gizmodo.com>
- Gregorio, R. (2013) *Nuevo canal transaccional móvil para empresarios de micro y pequeña empresa*. Tesis de Licenciatura no publicada, Universidad Peruana de Ciencias Aplicadas, Perú.

GNU *Privacy*. (2012) Making and verifying signatures. Recuperado el 12/04/2012 de <http://gnupg.org/gph/en/manual/x135.html>

Guadarrama, P. (2009) *Dirección y Asesoría de la Investigación Científica*
Bogotá: Editorial Magisterio

Gutiérrez P. (2013) *Sistemas asimétricos*. Recuperado el 15/01/2013
<http://www.genbetadev.com>

Hernández Samperio, R., Fernández Collado, C., & Baptista Lucio, P. (2010).
Metodología de la investigación. México: Mc Graw Hill.

Hernández Fernández, (2013) *Derechos de autor*. Recuperado el 02/05/2013
www.hfernandezdelpech.com.ar

Honores Chuchuca L.J. (2014). *Estudio estadístico comparativo entre sensores Android y Windows pone aplicado en la detección de movimientos telúricos*. Tesis de Licenciatura no publicada, Escuela Superior Politécnica de Chimborazo Riobamba. Ecuador

Hurtado de Barrera J. (2004) *Como Formular objetivos de Investigación*. 1ª ed.
Bogotá: Cooperativa Editorial magisterio.

I3SocialMedia, (2012:03) *Apps Móviles*. Recuperado el 05/03/2012 de
<http://if3socialmedia.blogspot.com/>

Infor@firma-electronica-eu (2011) *Firma Electrónica*. Recuperado el 11/07/2011 de <http://www.firma-electronica.eu/2.html>

Martínez, F. (2014) *Evaluación de la Calidad de Sistemas de Información*. Recuperado el 21/04/2014 de <http://es.scribd.com/doc/63814241/Sistemas-de-Informacion>, [Lima, Peru](#)

Manheim. (2015) *Esquema de MD5*. Recuperado el 15/08/2015 th.informatik.uni-mannheim-“esquema MD5”

Meneses, A. (2011). *Diseño de un sistema de control de activos para el almacén de electrónica de la Pontificia Universidad Católica del Perú utilizando RFID*. Tesis de Licenciatura no publicada, Universidad Católica del Perú, Perú

Mora. (2012). *Desarrollo de aplicativo Mobile multiplataformica-Cataluña*. Recuperado de <http://www-03.ibm.com/software/products/es/category/mobile-application-development>. Fecha de acceso 25/05/2015, España.

Muñoz, C. (1998) *Como Elaborar y Asesorar una Investigación de Tesis*. 1ª ed. México: Prentice Hall.

Netdreams. (2015) *Los sistemas Operativos Móviles más utilizados*. Recuperado el 05/06/2015 <http://netdreams.pe/>

- Neptarium. (2013) *Funciones Hash*. Recuperado el 05/08/2013
www.neptarium.com
- Oblitas Guadalupe. (1987) *Metodología de la Investigación*. Lima, Perú: Caribe.
- PersonKanban. (2013) *Metodología Kanban* recuperado el 05/07/2013
<http://www.personalkanban.com/>
- Peña Llopis, J. (2006). *Sistemas de Información Geográfica aplicados a la gestión del territorio*. Madrid España 2ª ed. Club Universitario España
- Pino Gotuzzo R., Pino Gotuzzo I. (2002) *Metodología de Investigación*. Lima, Perú: Ed. San Marcos
- Redletterday. (2012) *A Simple Case for Hybrid Mobile App Development*
Recuperado de <http://redletterday.ch/>. Fecha de acceso: 10/06/2012
- Serrano, A. (2010). *Desarrollo de un Sistema de Gestión y Control Administrativo para la Coordinación de Servicio Comunitario de la Universidad de Oriente*, Tesis de Licenciatura no publicada, Universidad del Oriente, México
- sepp.pe. (2015) *Desarrollo de aplicaciones*. Recuperado el 08/11/2015 de
<http://sepp.pe/>
- Symantec. (2015) *Una ventana a la seguridad de dispositivos móviles*.
Recuperado el 04/10/2015 de
<http://www.symantec.com/es/mx/theme.jsp?themeid=mobile-security-study>

Tafur P. Raúl. (1995) *La Tesis Universitaria*. Lima: Editorial Mantaro.

TestingBaires.(2014) *Testing Aplicaciones Móviles* recuperado el 10/12/2014 de
<http://testingbaires.com/>

Texto-Científico. (2006:11) *Funciones de del protocolo móvil*. Recuperado el
08/12/2006 de: www.textoscientificos.com-“Introducción”

Web.dit. (2003) *Cifrado digital asimétrico*. Recuperado el 08/05/2013 de
<http://web.dit.upm.es>-

Wikimedia. (2013) *Firma digital asimétrica*. Recuperado el 09/08/2013 de
<http://upload.wikimedia.org>-

Glosario

Dentro de este marco definiremos a continuación los términos básicos de la cual llevaremos a cabo para aclarar y entender mejor el contenido de la aplicación:

- a) **Acceso no autorizado a datos:** Acceso a datos almacenados en el sistema o intento de obtención de información del sistema bien mediante escucha del tráfico de usuario o del sistema, bien, suplantado a un elemento de la red a fin interceptar datos
- b) **Arquitectura:** El diseño de la estructura y las relaciones de sus elementos
- c) **Ataques:** tipos y naturaleza de inestabilidad en la seguridad
- d) **Autenticación de entidad:** Corroboración de la identidad de una entidad
- e) **Autorización legal:** Permiso otorgado por una LEA bajo ciertas condiciones para interceptar determinadas telecomunicaciones requiriendo la cooperación con un operador de red o proveedor de servicios
- f) **Clasificación de datos:** El procesos de determinar la sensibilidad y criticidad de la información
- g) **Clonación:** Proceso de cambio de la identidad de una entidad por otra entidad del mismo tipo, de forma que existan dos entidades del mismo tipo con la misma identidad.
- h) **Control de acceso:** El acceso a la red puede iniciarse tanto desde la parte móvil como desde la parte fija de la red.

- i) **Confidencialidad:** Propiedad de aquella información no accedida por usuarios/ entidades no autorizados.
- j) **Disponibilidad:** Es la característica de disponer requerimientos a procesos e aplicaciones, dentro del acceso completo de la información por personas autorizadas en el momento que requieran.
- k) **Dirección particular:** Dirección IP asignado por un periodo de tiempo largo a un nodo móvil. Esta dirección permanece inalterable independientemente de lugar donde el móvil se conecte.
- l) **Evidencia:** Información que por sí misma o en relación con otros datos, se utiliza para establecer pruebas sobre un evento o acción
- m) **Evitar:** El riesgo evitado es cuando la organización rechaza aceptarlo, no permite ningún tipo de exposición de peligro.
- n) **Exposición:** Áreas que son vulnerables a un impacto por parte de una amenaza
- o) **Filtro de mensajes:** La función realiza el filtro de aquellos mensajes no autorizados o no solicitados.
- p) **Gestión de claves:** Administración y uso de la generación, registro, certificación, de registro, distribución, instalación, almacenamiento, archivo, revocación, derivación y destrucción de claves de acuerdo con una política de seguridad.
- q) **Integridad:** Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- r) **Índice de Parámetro de Seguridad:** Índice identificativo de un contexto de seguridad, de los definidos de una asociación de seguridad entre dos nodos.

- s) **Negación de servicio:** Impedir el acceso a servicios de red de otra entidad
- t) **No repudio:** Es la confirmación de la identidad del autor de la firma, si el descifrado se realiza satisfactoriamente con la clave pública del firmante por las propiedades de la criptografía asimétrica, implica que la firma ha sido realizada con su clave privada.
- u) **Normas:** Establecer los límites permisibles de acciones y procesos para cumplir con las políticas.
- v) **Política:** Declaración de alto nivel sobre la intención y la dirección de la gerencia.
- w) **Protocolo:** Son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación y dispositivos.
- x) **Repudio:** Negación del uso de un servicio, de una recepción o transmisión de datos
- y) **Sincronización:** Procedimiento de establecimiento de opciones de protocolo entre cliente y servidor
- z) **Vulnerabilidades:** Deficiencias que pueden ser explotadas por amenazas

Anexos

Anexo A: Modelo de encuesta



Estimado(a) alumno:

La finalidad de la presente encuesta es recabar información necesaria para el desarrollo e implementación de una aplicación móvil de mensajería instantánea, bajo entorno colaborativo y desguardo de privacidad de información, para estudiantes de la UCH.

Instrucciones:

Esta encuesta consta de 11 preguntas con las siguientes características:

- Preguntas cerradas en las que se debe contestar SI o NO
- Preguntas que requieren que escojas más de una opción

Recomendaciones:

- Se recomienda responder las preguntas en el orden presentado
- En caso de no conocer el significado de alguna palabra, por favor consultar con el encuestador

Nota: Entienda por aplicación de mensajería instantánea cualquier aplicación que pueda utilizar en su teléfono inteligente para comunicarse con otras personas, llámese esta WhatsApp, Line, Twitter, etc.

Entienda por comunicación bajo entorno seguro y colaborativo, aquella que está comprometida a la privacidad de sus datos y seguridad, que permita el intercambio de texto, imágenes, entre otros.

Gracias por su colaboración.

Genero del encuestado: Masculino Femenino

Edad: 22 años

Código: 091015

1. ¿En algún momento, fuera del horario de clases, ha tenido usted algún comentario o indicación puntual de carácter académico hacia uno o varios estudiantes, y no ha podido comunicársela?

a) Si

b) No

2. ¿Tiene usted un teléfono inteligente? (si es no pasarse al nº 4)

a) Si

b) No

3. ¿Con qué plataforma cuenta su dispositivo móvil?

- a) Android
- b) ios
- c) Blackberry OS
- d) Windows Phone
- e) Otros

4. ¿Cree usted que el desarrollo de aplicaciones móviles es lo más novedoso en la actualidad?

a) Si

b) No

5. ¿Para qué fin utiliza las aplicaciones de su celular?

- a) Chatear
- b) Acceder a redes sociales
- c) Correo electrónico
- d) Oseo (juegos, música, etc)
- e) Otros

6. ¿Qué aplicaciones de mensajería utilizas?

- a) Whatsapp
- b) Line
- c) Chat Facecebook
- d) Skype
- e) telegram
- f) otros

7. ¿Le gustaría conocer nuevas aplicaciones para mensajería instantánea bajo un entorno seguro y privado sobre un sistema operativo Android?

- a) Si
- b) No

8. ¿Si dicha aplicación existiera y fuera gratuita, propia de la universidad la utilizaría?

- a) Si
- b) No

9. ¿Con que frecuencia la utilizaría?

- a) Muy frecuente
- b) Frecuente
- c) Poco frecuente

10. De las siguientes razones, seleccione aquellas por las cuales utilizaría la aplicación.

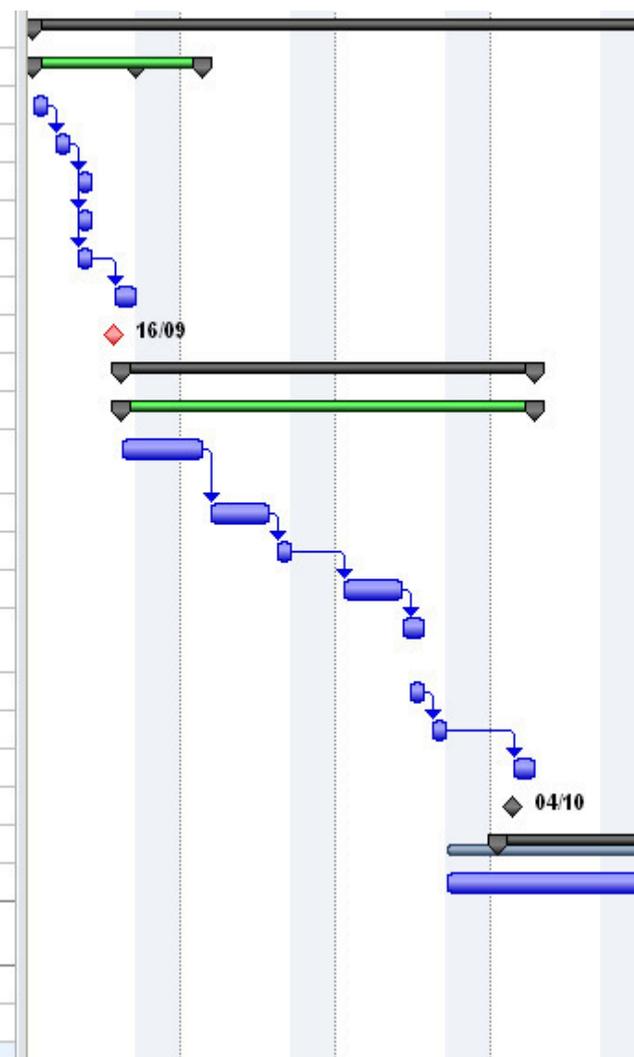
- a) Es una aplicación novedosa
- b) Bajos costos en el envío de datos
- c) Porque la aplicación es gratuita
- d) Interfaz amigable y fácil de usar
- e) Para tener comunicación académica con mis docentes y compañeros

Anexo B: Análisis sin el sistema y con el sistema.

Antes del Sistema	Después del Sistema
1. Se utiliza aplicaciones de terceros para comunicación de estudiantes, incluso mensajes de texto que realiza una recarga adicional al presupuesto del estudiante	1. Se utiliza aplicación propia de la universidad, dando facilidades de encontrar dentro de la libreta de contactos y comunicarse propiamente con ellos, sin realizar un costo adicional al estudiante
2. Se realiza perdidas comunicación entre estudiantes y profesorado, los estudiantes utilizan medios convencionales como correos electrónicos, mensajes, etc.	2. La comunicación se mejora, el alumno se contacta con mayor facilidad al tener a su docente como contacto en una aplicación privada.
3. Las aplicaciones convencionales no difieren y otorgan medios de seguridad en sus canales dejando agujeros enormes donde se puedan captar y robar información propia del estudiante (véase que dicha aplicación fue desarrollada antes que las aplicaciones modernas impusieran modelos de seguridad).	3. La aplicación ofrece un medio base de canal seguro al ser privada la información se mantiene en la sociedad corporativa que pertenece
4. Los primeros ciclos se particularizan al ser alumnado nuevo, esto ocasiona tiempo de comunicación congelado oh perdido por la inseguridad que los cachimbos no saben socializarse.	4. La aplicación da mayor facilidad de tener como contacto a tus nuevos compañeros ya sean pertenecientes del ciclo oh de diferente facultad, dando mayor sociabilidad a la comunidad universitaria

Anexo C: Diagrama de gantt

1 PROYECTO DE SISTEMA DE INFORMACION	69.75 días?
1.1 FASE I	6 días
1.1.1 Reunión inicial con las Areas sistemas y registros academicos	1 día
1.1.2 Crear el perfil del Proyecto	1 día
1.1.3 Definir los objetivos del proyecto	1 día
1.1.4 Definir el alcance y Beneficios del nuevo sistema	1 día
1.1.5 Anastasia Version 0.1 beta	1 día
1.1.6 Entrega del perfil del Proyecto	1 día
1.1.7 Fase I completada	0 días
1.2 FASE II	12.75 días?
1.2.1 Investigacion Inicial	12.75 días?
1.2.1.1 Recopilacion datos generales Universidad de Ciencias y Humanidades	2 días
1.2.1.2 Revision del Plan Estrategico	3 días
1.2.1.3 Desarrollo de la Cadena de Valor	1 día
1.2.1.4 Desarrollo del Modelo de Negocio	2.75 días?
1.2.1.5 Identificacion de los Stakeholders (Estudiantes,Empleados,Profesores,telefonica,telemex)	1 día
1.2.1.6 Estructura organizacional de la Empresa	1 día
1.2.1.7 Asignacion del estudio de Logística de Entrada	1 día
1.2.1.8 Entrega de la documentacion	1 día
1.2.2 Fase II completada	0 días
1.3 FASE III	20 días
1.3.1 Requerimiento de Personal	6 días
1.3.2 Tecnologia movil, Across Manager ,plugin, jQuery mobile ,css ,html ,javascript ,Soap ,jdbc ,PKI	9 días
1.3.3 Metodologia SCRUM y (Norma ISO/IEC IS 27005)	3 días
1.3.4 Evaluacion del avance del proyecto	2 días
1.3.5 Fase III completada	0 días



Anexo D: Matriz de investigación

Título: DISEÑO E IMPLEMENTACIÓN DE APLICACIÓN MULTIPLATAFORMA MÓVIL CON FUNCIONES DE ENCRIPTA MIENTO Y PRIVACIDAD DE DATOS ORIENTADA A LA SEGURIDAD ESTUDIANTIL DE LA UNIVERSIDAD CIENCIAS Y HUMANIDADES, OLIVOS – 2014

PROBLEMÁTICA	PREGUNTA DE INVESTIGACIÓN	OBJETIVO GENERAL	PREGUNTAS DE INVESTIGACIÓN	OBJETIVOS ESPECÍFICOS	ACCIONES	MARCO TEÓRICO
<p>En los últimos años las aplicaciones móviles han evolucionado llegando a significar un factor innovador e importante para la comodidad y adaptabilidad dentro del desarrollo de comunicaciones integrales de cualquier institución, empresa o entidad corporativa, implementando una aplicación móvil de comunicación segura, bajo un entorno colaborativo es la adaptación a las necesidades específicas que existen dentro de la actual comunidad universitaria. Dando como resultado un crecimiento vertiginoso dentro de las tecnologías de la información y la comunicación TIC'S. El objetivo del trabajo será diseñar e implementar una aplicación con funciones de cifrado, encriptado de datos y privacidad de comunicación, a base de una comunicación colaborativa, flexible y rápida que garantice la seguridad de este tipo de comunicación de forma no intrusiva en la confidencialidad del estudiante.</p> <p>CAUSAS: La falta de una herramientas tecnologica que mejore la comunicacion de los grupos estudiantiles bajo un canal seguro</p>	<p>¿El diseño e implementación de una aplicación móvil con funciones de cifrado, encriptado de datos y privacidad de comunicación podrá garantizar la correcta seguridad de transferencia de información para plataformas móviles?</p>	<p>Implementar aplicación para dispositivos móviles en Android que apoyen el resguardo de transferencia de información, con funciones de cifrado, encriptación de datos y privacidad de comunicación para la optimización de seguridad de la información hacia los estudiantes de la Universidad de Ciencias y Humanidades.</p>	<p>PE1:¿La solución de una aplicación móvil con funciones de seguridad podrá mejorar el rendimiento en la transferencia o transacciones de envío de datos? .</p>	<p>•O.E.1: Incrementar el rendimiento de seguridad en él envío y transferencia de envió de datos para mejorar los procesos de comunicaciones móviles a estudiantes de la UCH</p>	<p>Acc 1 - O. E. 1</p> <ul style="list-style-type: none"> • Desarrollar la arquitectura de una base de datos mediante modelos de seguridad y buenas practicas <p>Acc 2 - O. E. 1</p> <ul style="list-style-type: none"> • Identificar los campos criticos de informacion del usuario para evitar errores de seguridad <p>Acc 3 - O. E. 1</p> <p>identificar el proceso critico para la transferencia de mensajes y informacion</p>	<p>M.T. Acc 1 - O. E.1</p> <p>Normalizar la base de datos e incluir procesos de seguridad</p> <p>M.T. Acc 2 - O. E. 1</p> <p>Determinar los campos criticos y utilizar un nivel de ciframiento</p> <p>M.T. Acc 3 - O. E. 1</p> <p>Conocer como diseñar un prototipo aplicación movil</p>
			<p>PE2:¿La aplicación permitirá que la comunicación sea de tipo no intrusiva en la confidencialidad del estudiante?</p>	<p>•O.E.2: La aplicación será capaz de enviar mensajes a otros usuarios de la aplicación sin dejar marcas de conexión, sin exponer información intrusiva al emisor, como la recepción del mensaje, o su estado en línea.</p>	<p>Acc 1 - O. E. 2</p> <ul style="list-style-type: none"> • Investigar el modelo ciframientos y algoritmos en encriptamiento <p>Acc 2 - O. E. 2</p> <ul style="list-style-type: none"> • Identificar la arquitectura y tecnologicas involucradas para un de modelos transaccional de datos seguros <p>Acc 3 - O. E. 2</p> <ul style="list-style-type: none"> • Investigar metodologias Moviles 	<p>M.T. Acc 1 - O. E. 2</p> <p>Definicion del algoritmo y nivel de encriptacion ah utilizar</p> <p>M.T. Acc 2 - O. E. 2</p> <p>Conocer y determinar las herramientas encensarias para el desarrollo de la aplicacion</p> <p>M.T. Acc 3 - O. E. 2</p> <p>Conocer las caracteristicas y ventajas de las demas metodologias</p>
			<p>PE3: ¿Cuál es el nivel de disposición hacia la aplicación móvil de comunicación, por parte de los estudiantes de la universidad ciencias y humanidades?</p>	<p>•O.E.3: Reconocer el nivel de disposición al uso de la aplicación móvil de comunicación, por parte de estudiantes de la Universidad de Ciencias y Humanidades</p>	<p>Acc 3 - O. E. 3</p> <p>Conocer que se quiere optimizar</p> <p>Acc 2 - O. E. 3</p> <p>Conocer cual es indice de popularidad de las aplicaciones moviles en el grupo estudiantil</p> <p>Acc 3 - O. E. 3</p> <p>identificar las plataformas mas utilizadas en el eruoio estudiantil</p>	<p>M.T. Acc 1 - O. E. 3</p> <p>Definicion de optimizar.</p> <p>M.T. Acc 2 - O. E. 3</p> <p>Conocer cuadros teoricos de aplicación mas utilizadas</p> <p>M.T. Acc 3 - O. E. 3</p> <p>Estudio del mercado nacional e internacional de las plataformas mas utilizadas</p>

DESARROLLO	EVALUACION	CONCLUSIONES	RECOMENDACIONES
<ul style="list-style-type: none"> • Diseño del modelo conceptual, lógico de la B.D. • Diseño de las tablas, campos con PK y FK, las relaciones y restricciones de la BD. • Diseño del modelo físico en software libre soporte para distintas plataformas 	<p>La aplicación tiene la capacidad de poder incluir servicios de GPS, invitaciones mediante redes sociales y pagos ah terceros</p>	<p>Se desarrollo la base de datos, se cifro los campos criticos del usuarios, esto conlleva replantear un modelo mas seguro en los registros de la aplicacion</p>	<p>Actualmente el servidor almacena el par usuario contraseña en una tabla de su base de datos. Se recomienda que sería mucho más seguro modificar este sistema y que cada usuario, en lugar de ser un registro en la base de datos del servidor.</p>
<ul style="list-style-type: none"> • Diseño y desarrollo de algoritmo de encriptacion • Diseño y desarrollo de las herramientas involucradas ah utilizar para la aplicacion • Diseño y desarrollo de una propia metodologias de desarrollo 	<p>Se identifico las herramientas mas actuales ah utilizar para un modelo mas seguro y estable, se procedio ah investigar y recopilar diferentes metodologias de desarrollo, hasta realizar una propia metodologia adaptable al proyecto propuesto</p>	<p>Fue necesario valorar si las herramientas de desarrollo y tecnologías multiplataforma o CPT (Cross-Plataform Tools) eran viables para la comunidad universitaria de la Universidad Ciencias y Humanidades (UCH).</p>	<p>El envío y recepción de archivos es una función muy importante en casi cualquier sistema de mensajería. Se propone como posible mejora una ampliación del sistema actual incorporando un sistema de envío y recepción de archivos de cualquier tipo.</p>
<ul style="list-style-type: none"> • Diseño de proceso, flujos y entrevistas a los usuarios. • Conocer el nivel de atencion del grupo de estudiantil • Realizar un propio levantamiento de informacion a los grupos de usuarios 	<p>Teóricamente los estudiantes de la UCH están dispuestos en un 90% a la adopción de nuevas herramientas tecnológicas bajo un estándar colaborativo, seguro y privado dentro de su proceso educativo bajo una plataforma android, con el fin de mejorar los canales de comunicación académica entre docentes y estudiantes.</p>	<p>El resultado final mediante el levantamiento de información demuestra un alto índice de popularidad y variedad ah una sola plataforma (android). No solo para el público universitario si no del país y Latinoamérica. Definiendo el anterior concepto se decidió realizar puramente Yappo! como una app móvil nativa por tener un mayor rendimiento que una aplicación web y/o multipltaformica. De acuerdo a los estándares actuales y requeridos por los propios estudiantes.</p>	<p>☑ En los que respecta al análisis de rendimiento y monitorización sería conveniente tener acceso a otros dispositivos Android con diferentes especificaciones de hardware en cuanto a pantalla, memoria y CPU. Distintas versiones del sistema operativo. Además, llevar cabo dicho procedimiento en un ambiente controlado</p>

Anexo E: Acta de constitución

	"IMPLEMENTACIÓN DE UNA SOLUCION DE INTELIGENCIA DE NEGOCIO PARA LA MEJORA DEL PROCESO DE FORMACIÓN ACADEMICA EN LA UNIVERSIDAD DE CIENCIAS Y HUMANIDADES"	UCH
---	--	------------

Cliente	UCH	Lugar	Lima – Olivos
Nombre del Proyecto	"DISEÑO Y IMPLEMENTACION DE APLICACIÓN MULTIPLATAFORMA MOVIL CON FUNCIONES DE ENCRIPITAMIENTO Y PRIVACIDAD DE DATOS ORIENTADA A LA SEGURIDAD ESTUDIANTIL DE LA UNIVERSIDAD CIENCIAS Y HUMANIDADES"	Fecha de Entrega	JUNIO 2015

Datos Generales del Informe.

Apellidos y Nombres:	Jose Luis Alcantara
Cargo:	Jefe de Proyecto
Fecha:	22/06/2015

Actividades a la Fecha:

Mediante la presente hacemos entrega formal de la documentación correspondiente a la totalidad de entregables definidos en los Términos de Referencia, del proyecto referido, para el "Entregable 1". Adicionalmente se hace entrega, a través de un medio físico (DVD), de cada uno de ellos en formato digital.

Se detalla a continuación las actividades llevadas a cabo, en la etapa de planificación obtenidos en el periodo del 05/11/2014

Funcional:

- Definición del Alcance del proyecto
- Identificación de los roles que desempeñara cada área y/o persona en el proyecto
- Se presentó al usuario un cronograma de actividades (Elaboración del Ms Project)
 - Fases por etapa del proyecto
 - Tiempo por etapa del proyecto

Atte.



José Alcantara
Jefe de Proyecto



Coordinador de la carrera de
Ingeniería sistemas

Anexo F: Acta de conformidad

Acta de Conformidad – Despliegue

Proyecto:	“Servicio de Desarrollo del Sistema de Registro de IPRESS, Registro de IAFAS y Regulación”
Preparado por:	Jose Luis Alcantara
Fecha:	16/06/2015
Cliente:	Universidad de Ciencias y Humanidades
Contrato:	06-2015-001/Alcantara

Declaración formal de la Aceptación

Por medio de la presente se deja constancia de la aceptación por parte de la UNIVERSIDAD CIENCIAS Y HUMANIDADES, del despliegue del Sistema del “Diseño e implementación de aplicación multiplataforma móvil con funciones de encriptamiento y privacidad de datos orientada a la seguridad estudiantil de la universidad ciencias y humanidades”

En este punto se da la conformidad a satisfacción del cliente la UNIVERSIDAD CIENCIAS Y HUMANIDADES el despliegue del sistema proyecto, quien constata su finalización.

Resumen de Actividades Realizadas y/o Entregables Presentados

Ítem	Actividad/Entregable
01	Despliegue del Sistema de Registro de IPRESS, Registro de IAFAS y Regulación

Acta firmada por

Nombre	Cargo / Rol	Organización	Firma
Miguel Angel Jara	Especialista en Gestión de Tecnologías de la información	UNIVERSIDAD CIENCIAS Y HUMANIDADES	
Jose Luis Alcantara	Jefe del Proyecto	Yappo.	

