

**ESCUELA MILITAR DE INGENIERÍA**  
**MCAL. ANTONIO JOSÉ DE SUCRE**  
**BOLIVIA**

## **TRABAJO DE GRADO**



### **APLICACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA EN LOS CERTIFICADOS PARA EL SEGUIMIENTO Y CONTROL DE EMBARCACIONES**

**CASO: DIRECCIÓN GENERAL DE INTERESES MARÍTIMOS,  
FLUVIALES, LACUSTRE Y MARINA MERCANTE**

**LUIS RICARDO RIVAS GIWENCER**

**LA PAZ, 2020**

**ESCUELA MILITAR DE INGENIERÍA  
MCAL. ANTONIO JOSÉ DE SUCRE  
BOLIVIA**

**TRABAJO DE GRADO**

**APLICACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA EN LOS  
CERTIFICADOS PARA EL SEGUIMIENTO Y CONTROL DE  
EMBARCACIONES**

**LUIS RICARDO RIVAS GIWENCER**

**Modalidad:** Proyecto de Grado  
presentado como requisito para optar  
al Título de Licenciatura en  
Ingeniería de Sistemas

**TUTOR: LIC. CYNTHIA RODRIGUEZ CANAVIRI**

**LA PAZ, 2020**

# DOCUMENTACIÓN



CITE : ING. DE SISTEMAS N° 57/2020  
OBJETO : Aprobación de Temario del Trabajo de Grado  
ANEXOS: Temario 2 Hojas

La Paz, 6 de abril de 2020

Señor  
Luis Ricardo Rivas Giwencer  
Presente.

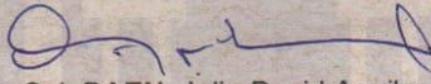
De mi consideración:

En atención a su solicitud y de conformidad a lo dispuesto por el Reglamento RAC – 02 "GRADUACIÓN DE GRADO", CAPITULO VII "DESARROLLO DEL TRABAJO DE GRADO Y TRABAJO DE GRADO TÉCNICO" Arts. 55, 56º, 64º y Art. 66º, tengo a bien comunicar a usted que ha sido aprobado el Temario para su Trabajo de Grado, cuyo título es: "APLICACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA EN LOS CERTIFICADOS PARA EL SEGUIMIENTO Y CONTROL DE EMBARCACIONES CASO: DIRECCIÓN GENERAL DE INTERESES MARÍTIMOS, FLUVIALES, LACUSTRE Y MARINA MERCANTE".

El plazo para la presentación del mencionado Trabajo de Grado es de (2) dos Semestres Académicos a partir del inicio del 10mo. (Décimo) Semestre, vencido dicho plazo el tema quedará caduco y sin efecto.

El trabajo deberá ser presentado, de conformidad a las "Normas para la Presentación de Trabajos de Grado" de la Escuela Militar de Ingeniería, sujetándose a las disposiciones vigentes.

Con este motivo, saludo a usted atentamente.

  
Cnl. DAEN. Julio David Aguilar Pérez ·  
DIRECTOR UNIDAD ACADÉMICA LA PAZ  
ESCUELA MILITAR DE INGENIERÍA



<b>CITE</b>	: ING. DE SISTEMAS	Nº 57/2020
<b>OBJETO</b>	Aprobación de Temario	
<b>ANEXOS</b>	del Trabajo de Grado	
	Temario 2 Hojas	

<b>CARRERA</b>	: INGENIERÍA DE SISTEMAS
<b>TEMA</b>	: "APLICACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA EN LOS CERTIFICADOS PARA EL SEGUIMIENTO Y CONTROL DE EMBARCACIONES CASO: DIRECCIÓN GENERAL DE INTERESES MARÍTIMOS, FLUVIALES, LACUSTRE Y MARINA MERCANTE".
<b>OCENTE TUTOR</b>	: Lic. Cynthia Rodriguez Canaviri
<b>PROPONENTE</b>	: Sr. Luis Ricardo Rivas Giwencer
<b>FECHA</b>	: 6 de abril de 2020

## TEMARIO

### **CAPÍTULO I. GENERALIDADES**

- 1.1 INTRODUCCIÓN
- 1.2 ANTECEDENTES
- 1.3 PLANTEAMIENTO DEL PROBLEMA
- 1.4 OBJETIVOS
- 1.5 JUSTIFICACIÓN
- 1.6 ALCANCES

### **CAPÍTULO II. MARCO TEÓRICO**

- 2.1 INGENIERÍA DE SISTEMAS
- 2.2 INGENIERÍA DE SOFTWARE
- 2.3 SEGURIDAD DE SISTEMAS
- 2.4 CRIPTOGRAFÍA
- 2.5 CRIPTOGRAFÍA ASIMÉTRICA
- 2.6 METODOLOGÍA DE DESARROLLO

### **CAPÍTULO III. MARCO PRÁCTICO**

- 3.1 ANÁLISIS DE SITUACIÓN ACTUAL
- 3.2 IMPLEMENTACIÓN DEL ALGORITMO ASIMÉTRICO
- 3.3 DESARROLLO DEL SISTEMA
- 3.4 PRUEBAS DEL SISTEMA
- 3.5 IMPLEMENTACIÓN DEL SISTEMA

CITE : ING. DE SISTEMAS N° 57/2020

OBJETO : Aprobación de Temario  
del Trabajo de Grado

ANEXOS: Temario 2 Hojas

PROPONENTE: Sr. Luis Ricardo Rivas Giwencer

CARRERA: INGENIERÍA DE SISTEMAS

#### **CAPITULO IV: ANÁLISIS COSTO BENEFICIO**

- 4.1 DETERMINACIÓN DE COSTOS
- 4.2 ESTIMACIÓN DE BENEFICIOS
- 4.3 RELACIÓN COSTO-BENEFICIO

#### **CAPITULO V: CONCLUSIONES Y RECOMENDACIONES**

- 5.1 CONCLUSIONES
- 5.2 RECOMENDACIONES

**BIBLIOGRAFÍA**  
**GLOSARIO**  
**ANEXOS**

My. DIM. Yusef Aparicio Romay  
**JEFE DE CARRERA**  
**INGENIERÍA DE SISTEMAS**

Cnl. DAEN. Julio David Aguilar Pérez  
**DIRECTOR**  
**UNIDAD ACADÉMICA LA PAZ**



Pág. 2

## **DEDICATORIA**

Este Trabajo está dedicado a:

A mis padres que en todo momento se  
preocuparon por mi y de mis estudios, siempre  
me apoyaron y dieron lo que necesite

## **AGRADECIMIENTOS**

A: Mis padres Luis y Mónica que me ayudaron en todo momento y pese a cualquier circunstancia, ellos me dieron la oportunidad de estudiar lo que me gusta y salir adelante, dándome algo con que enfrentar a la vida y siempre me apoyaron incondicionalmente.

A: Mis hermanos Alejandra y Mateo los que siempre me sacaron una sonrisa y me dieron aliento para seguir adelante, una de las principales razones por la cual jamás desistí.

A: Mi abuelita Luz la cual fue una madre mas para mi que me apoyo y siempre se preocupo por todo, gracias a ella empecé en la universidad.

A: Mis abuelitos David, Miriam y Carmen los cuales siempre estuvieron presentes con palabras de aliento y apoyo, aconsejándome con la experiencia que ellos tienen los quiero mucho, gracias por estar siempre.

A: Mis tíos José Antonio, Erika y mis primos Pamela y Pablo ellos son como mi otra familia la cuales siempre están a mi lado en todo momento, gracias por las palabras y por estar ahí cuando lo necesito, siempre me sacan una sonrisa.

A: Mi familia que se encuentra dispersa y es inmensa siempre me daba fuerzas para seguir adelante y motivarme.

A: Mi tutora Cynthia Rodríguez que a pesar de todo ella me apoyo y defendió, me guio hasta el final de este camino el cual tuvo sus tropiezos, pero siempre me animó a levantarme.

A: Mis mejores amigos José, Jhonatan, Christian, Gabriela, Sergio, Henry, Andrés, Daniela, Jorge y Echalar que a lo largo de esta etapa estuvieron ahí para mi apoyándome en todo, aconsejándome en las decisiones que tomé, pasé momentos inolvidables con todos, y sin ellos no hubiera llegado tan lejos.

A: Alejandra Espinoza la cual fue una persona que en el poco tiempo que conocí estuvo prácticamente en todo este proceso, brindándome su cariño y apoyo incondicional, se preocupó por mi en todo momento y me dio las fuerzas para seguir adelante, un logro más conseguido y vamos por más.

A: Mis amigos compañeros de universidad, los cuales son varios que siempre me estuvieron apoyando en todas las etapas de la universidad y pase momentos inolvidables con ellos, supieron ser parte de mi vida y siempre se los agradeceré.

# ÍNDICES



## ÍNDICE

### **CAPÍTULO I: GENERALIDADES**

<b>1.1</b>	<b>INTRODUCCIÓN.....</b>	1
<b>1.2</b>	<b>ANTECEDENTES .....</b>	2
1.2.1	Antecedentes Institucionales .....	2
1.2.2	Antecedentes Académicos .....	4
<b>1.3</b>	<b>PLANTEAMIENTO DEL PROBLEMA .....</b>	6
1.3.1	Problema Principal .....	7
1.3.2	Problemas Secundarios.....	7
<b>1.4</b>	<b>OBJETIVOS.....</b>	8
1.4.1	Objetivo General.....	8
1.4.2	Objetivos Específicos .....	8
<b>1.5</b>	<b>JUSTIFICACIÓN .....</b>	8
1.5.1	Justificación Técnica .....	9
1.5.2	Justificación Económica .....	9
1.5.3	Justificación institucional .....	9
<b>1.6</b>	<b>ALCANCES .....</b>	10
1.6.1	Alcance Geográfico .....	10
1.6.2	Alcance Temporal.....	11
1.6.3	Alcance Temático .....	11
1.6.4	Alcance Funcional .....	11

### **CAPÍTULO II MARCO TEÓRICO**

<b>2.1</b>	<b>INGENIERÍA DE SISTEMAS.....</b>	12
2.1.1	Ingeniería .....	13
2.1.2	Sistema .....	14
<b>2.2</b>	<b>INGENIERÍA DE SOFTWARE .....</b>	14
2.2.1	Modelos de Desarrollo de Software .....	15
2.2.1.1	Modelo en V .....	15
2.2.1.2	Modelo Evolutivo .....	16

2.2.1.3	Modelo en espiral .....	17
2.2.2	Lenguaje de Modelado Unificado (UML).....	18
2.2.3	Gestor de Base de Datos .....	21
2.2.3.1	SQL Server.....	21
2.2.3.2	MySQL .....	22
2.2.3.3	PostgreSQL.....	23
2.2.4	Framework .....	24
2.2.4.1	Laravel .....	24
2.2.5	COCOMO II.....	25
<b>2.3</b>	<b>SEGURIDAD DE SISTEMAS</b> .....	26
2.3.1	Pilares de la seguridad de la información .....	27
<b>2.4</b>	<b>CRPTOGRAFÍA</b> .....	29
2.4.1	Objetivos de la Criptografía .....	30
2.4.2	Conceptos Básicos de Criptografía .....	31
<b>2.5</b>	<b>CRPTOGRAFÍA ASIMÉTRICA</b> .....	32
2.5.1	Ventajas .....	33
2.5.1.1	Método Wigginton.....	33
2.5.2	Algoritmo RSA.....	34
2.5.3	Algoritmo DSA.....	38
2.5.4	Algoritmo DPH.....	38
<b>2.6</b>	<b>METODOLOGÍA DE DESARROLLO</b> .....	39
2.6.1	Técnicas de Recolección de Datos.....	40
2.6.1.1	Entrevistas.....	40
2.6.2	Metodología Ágil.....	41
2.6.2.1	RUP.....	43
2.6.2.2	Extreme Programming (XP).....	43
2.6.2.3	Metodología Design Sprint .....	44
2.6.2.4	Fases .....	45
<b>CAPÍTULO III MARCO PRÁCTICO</b>		
<b>3.1</b>	<b>ANÁLISIS DE LA SITUACIÓN ACTUAL</b> .....	56
3.1.1	Contexto de la organización .....	56

3.1.2	Identificación del personal .....	57
3.1.3	Consulta de información .....	58
3.1.4	Análisis de procesos.....	59
3.1.4.1	Registro de embarcaciones .....	59
3.1.4.2	Inspección de embarcaciones .....	62
3.1.5	Determinación de Requerimientos del Sistema .....	64
3.1.6	Definición de módulos del sistema .....	66
<b>3.2</b>	<b>IMPLEMENTACIÓN DEL ALGORITMO ASIMÉTRICO</b> .....	<b>67</b>
3.2.1	Determinación del Algoritmo a Implementar .....	68
3.2.2	Generación de llaves .....	70
3.2.3	Determinación de Información a Encriptar .....	71
3.2.4	Generación de código QR .....	72
<b>3.3</b>	<b>DESARROLLO DEL SISTEMA</b> .....	<b>73</b>
3.3.1	Sprint 1 Módulo de Gestión de Usuarios .....	74
3.3.1.1	Lista de requerimientos Sprint 1 .....	74
3.3.1.2	Especificación de Procesos Sprint 1 .....	75
3.3.1.3	Diseño de Procesos Sprint 1 .....	77
3.3.1.4	Diseño de Interfaces Sprint 1 .....	79
3.3.1.5	Diseño de Navegacional Sprint 1.....	81
3.3.1.6	Construcción de Interfaces Sprint 1 .....	82
3.3.1.7	Código Sprint 1 .....	84
3.3.1.8	Prueba Unitaria Sprint 1 .....	85
3.3.2	Sprint 2 Módulo de Registro de Embarcaciones .....	86
3.3.2.1	Lista de Requerimientos Sprint 2 .....	86
3.3.2.2	Especificación del Proceso Sprint 2.....	88
3.3.2.3	Diseño de Procesos Sprint 2 .....	90
3.3.2.4	Diseño de Interfaces Sprint 2 .....	92
3.3.2.5	Diseño Navegacional Sprint 2.....	94
3.3.2.6	Construcción de Interfaces Sprint 2 .....	94
3.3.2.7	Código Sprint 2.....	96
3.3.2.8	Prueba Unitaria Sprint 2 .....	97

3.3.3	Sprint 3 Módulo de Inspección de Embarcaciones .....	97
3.3.3.1	Lista de Requerimientos Sprint 3.....	97
3.3.3.2	Especificación del Proceso Sprint 3.....	99
3.3.3.3	Diseño de Procesos Sprint 3 .....	101
3.3.3.4	Diseño de Interfaces Sprint 3 .....	103
3.3.3.5	Diseño Navegacional Sprint 3.....	105
3.3.3.6	Construcción de Interfaces Sprint 3 .....	106
3.3.3.7	Código Sprint 3.....	107
3.3.3.8	Prueba Unitaria Sprint 3 .....	108
3.3.4	Sprint 4 Módulo Verificación de Documentos .....	109
3.3.4.1	Lista de Requerimientos Sprint 4.....	109
3.3.4.2	Especificación del Proceso Sprint 4.....	111
3.3.4.3	Diseño de Procesos Sprint 4 .....	113
3.3.4.4	Diseño de Interfaces Sprint 4 .....	115
3.3.4.5	Diseño Navegacional Sprint 4.....	115
3.3.4.6	Construcción de Interfaces Sprint 4 .....	116
3.3.4.7	Código Sprint 4.....	117
3.3.4.8	Prueba Unitaria Sprint 4 .....	118
3.3.5	Sprint 5 Módulo de Reportes .....	119
3.3.5.1	Lista de Requerimientos Sprint 5.....	119
3.3.5.2	Especificación del Proceso Sprint 5.....	120
3.3.5.3	Diseño de Procesos Sprint 5 .....	121
3.3.5.4	Diseño de Interfaces Sprint 5 .....	122
3.3.5.5	Diseño Navegacional Sprint 5.....	123
3.3.5.6	Construcción de Interfaces Sprint 5 .....	124
3.3.5.7	Código Sprint 5.....	125
3.3.5.8	Prueba Unitaria Sprint 5 .....	126
<b>3.4</b>	<b>PRUEBAS DEL SISTEMA .....</b>	<b>127</b>
3.4.1	Pruebas de Integración.....	127
<b>3.5</b>	<b>IMPLEMENTACIÓN DEL SISTEMA .....</b>	<b>129</b>
3.5.1	Instalación del sistema .....	130

3.5.2 Revisión de funcionamiento.....	132
<b>CAPÍTULO IV ANÁLISIS COSTO BENEFICIO</b>	
<b>4.1 DETERMINACIÓN DE COSTOS .....</b>	134
4.1.1 Costos Fijos.....	135
4.1.1.1 Costos de Software .....	135
4.1.1.2 Costos de Hardware.....	136
4.1.1.3 Costos de Desarrollo .....	137
4.1.2 Costos Variables .....	142
4.1.3 Costo Total .....	143
<b>4.2 DETERMINACIÓN DE BENEFICIOS.....</b>	144
4.2.1 Beneficios Cualitativos .....	144
4.2.2 Beneficios Cuantitativos .....	145
<b>4.3 RELACIÓN COSTO BENEFICIO.....</b>	146
<b>CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES</b>	
<b>5.1 CONCLUSIONES.....</b>	150
<b>5.2 RECOMENDACIONES .....</b>	151
BIBLIOGRAFÍA	
GLOSARIO	
ANEXOS	

## **ÍNDICE DE FIGURAS**

FIGURA 1: ORGANIGRAMA DE LA DGIMFLMM .....	3
FIGURA 2: UBICACIÓN DGIMFLMM .....	10
FIGURA 3: MODELO EN ESPIRAL .....	17
FIGURA 4: PILARES DE LA SEGURIDAD DE LA INFORMACIÓN .....	28
FIGURA 5: FASES DESIGN SPRINT .....	45
FIGURA 6: PRUEBA UNITARIA .....	48
FIGURA 7: ORGANIGRAMA DEL PERSONAL DE DGIMFLMM .....	57
FIGURA 8: DIAGRAMA DE CASO DE USO DE ALTO NIVEL.....	66
FIGURA 9: PONDERACIONES DE CHECKLIST.....	67
FIGURA 10: IMPLEMENTACIÓN DE ALGORITMO ASIMÉTRICO.....	68
FIGURA 11: GENERACIÓN DE PARES DE LLAVES.....	70
FIGURA 12: LLAVE ENcriptada EN BASE64 .....	71
FIGURA 13: OBTENCIÓN DE MENSAJE A ENcriptar .....	71
FIGURA 14: PROCESO DE GENERACIÓN DE CÓDIGO QR.....	72
FIGURA 15: CÓDIGO QR AÑADIDO A CERTIFICADO .....	73
FIGURA 16: DIAGRAMA E-R SPRINT 1.....	75
FIGURA 17: DIAGRAMA DE CASO DE USO (GESTIÓN DE USUARIOS).....	76
FIGURA 18: DIAGRAMA DE CLASES SPRINT 1 .....	77
FIGURA 19: DIAGRAMA RELACIONAL SPRINT 1 .....	78
FIGURA 20: DIAGRAMA DE ACTIVIDADES (SPRINT 1).....	79
FIGURA 21: BOCETO DE INICIO DE SESIÓN.....	80
FIGURA 22: BOCETO DE REGISTRO DE USUARIO .....	80
FIGURA 23: BOCETO DE MODIFICACIÓN DE USUARIO.....	81
FIGURA 24: DIAGRAMA DE COMPONENTES (GESTIÓN DE USUARIOS) .....	82
FIGURA 25: PANTALLA INICIO DE SESIÓN .....	83
FIGURA 26: PANTALLA DE REGISTRO DE USUARIO .....	83
FIGURA 27: PANTALLA DE EDICIÓN DE USUARIOS .....	84
FIGURA 28: CÓDIGO PARA GESTIÓN DE USUARIOS .....	85
FIGURA 29: PRUEBA UNITARIA MOCK (GESTIÓN DE USUARIOS) .....	86

FIGURA 30: DIAGRAMA E-R SPRINT 2.....	88
FIGURA 31: DIAGRAMA DE CASO DE USO (REGISTRO) .....	89
FIGURA 32: DIAGRAMA DE CLASES SPRINT 2 .....	90
FIGURA 33: DIAGRAMA RELACIONAL SPRINT 2 .....	91
FIGURA 34: DIAGRAMA DE ACTIVIDADES (SPRINT 2).....	92
FIGURA 35: BOCETO DE REQUISITOS.....	93
FIGURA 36: BOCETO DE REGISTRO .....	93
FIGURA 37: DIAGRAMA DE COMPONENTES (REGISTRO) .....	94
FIGURA 38: PANTALLA DE REQUISITOS DE REGISTRO .....	95
FIGURA 39: PANTALLA DE REGISTRO DE EMBARCACIÓN.....	95
FIGURA 40: CÓDIGO PARA REGISTRO DE EMBARCACIÓN.....	96
FIGURA 41: PRUEBA UNITARIA MOCK (REGISTRO DE EMBARCACIÓN) .....	97
FIGURA 42: DIAGRAMA E-R SPRINT 3.....	99
FIGURA 43: DIAGRAMA DE CASO DE USO (INSPECCIÓN).....	100
FIGURA 44: DIAGRAMA DE CLASES SPRINT 3 .....	101
FIGURA 45: DIAGRAMA RELACIONAL SPRINT 3 .....	102
FIGURA 46: DIAGRAMA DE ACTIVIDADES (SPRINT 3).....	103
FIGURA 47: BOCETO DE REALIZAR INSPECCIÓN .....	104
FIGURA 48: BOCETO DE BARRA DE PROGRESO .....	104
FIGURA 49: BOCETO DE FORMULARIO DE INSPECCIÓN .....	105
FIGURA 50: DIAGRAMA DE COMPONENTES (INSPECCIONES) .....	106
FIGURA 51: PANTALLA PARA ACCEDER A INSPECCIÓN .....	106
FIGURA 52: PANTALLA DE FORMULARIO DE INSPECCIÓN .....	107
FIGURA 53: CÓDIGO PARA INSPECCIONES.....	108
FIGURA 54: PRUEBA UNITARIA MOCK (GESTIÓN DE USUARIOS) .....	109
FIGURA 55: DIAGRAMA E-R SPRINT 4.....	111
FIGURA 56: DIAGRAMA DE CASO DE USO (VERIFICACIÓN).....	112
FIGURA 57: DIAGRAMA DE CLASES SPRINT 4 .....	112
FIGURA 58: DIAGRAMA RELACIONAL SPRINT 4 .....	113
FIGURA 59: DIAGRAMA DE ACTIVIDADES (SPRINT 4).....	114
FIGURA 60: BOCETO DE VERIFICACIÓN DE DOCUMENTO .....	115

FIGURA 61: DIAGRAMA DE COMPONENTES (VERIFICACIÓN).....	116
FIGURA 62: PANTALLA DE VERIFICACIÓN DE DOCUMENTO .....	117
FIGURA 63: CÓDIGO PARA VERIFICACIÓN DE DOCUMENTOS .....	118
FIGURA 64: PRUEBA UNITARIA MOCK (VERIFICACIÓN) .....	119
FIGURA 65: DIAGRAMA DE CASO DE USO (REPORTES) .....	121
FIGURA 66: DIAGRAMA DE ACTIVIDADES (SPRINT 5) .....	122
FIGURA 67: BOCETO DE REPORTE .....	123
FIGURA 68: DIAGRAMA DE COMPONENTES (REPORTES) .....	124
FIGURA 69: REPORTE .....	125
FIGURA 70: CÓDIGO PARA REPORTE .....	126
FIGURA 71: PRUEBAS UNITARIAS MOCK (REPORTES) .....	127
FIGURA 72: EXAMEN DE USABILIDAD.....	128
FIGURA 73: PRUEBAS MOCK DEL SISTEMA.....	129
FIGURA 74: CREACIÓN DE PROYECTO HEROKU .....	131
FIGURA 75: SUBIDA DE ARCHIVOS A HEROKU .....	132
FIGURA 76: SISTEMA SUBIDO A LA PLATAFORMA HEROKU .....	133
FIGURA 77: ESQUEMA DE COSTO-BENEFICIOS.....	134

## ÍNDICE DE TABLAS

TABLA 1: DIAGRAMAS UML.....	19
TABLA 2: EJEMPLO DE USO DE RSA .....	37
TABLA 3: COMPARACIÓN DE METODOLOGÍA.....	41
TABLA 4: DESCRIPCIÓN DE ENTREGABLES .....	47
TABLA 5: DESARROLLO DEL MARCO PRÁCTICO .....	49
TABLA 6: COMPARACIÓN INSPECCIONES DE EMBARCACIONES .....	64
TABLA 7: TABLA DE REQUERIMIENTOS .....	65
TABLA 8: COMPARACIÓN DE ALGORITMOS ASIMÉTRICOS .....	69
TABLA 9: DOT VOTING DE ALGORITMO VS PERSONAL.....	69
TABLA 10: LISTA DE REQUERIMIENTOS GESTIÓN DE USUARIOS .....	74
TABLA 11: REQUERIMIENTOS MÓDULO DE INSPECCIONES .....	87
TABLA 12: REQUERIMIENTOS MODULO DE INSPECCIONES .....	98
TABLA 13: REQUERIMIENTOS MÓDULO DE SEGURIDAD .....	110
TABLA 14: REQUERIMIENTOS MÓDULO DE REPORTES.....	120
TABLA 15: COMPARACIÓN HEROKU VS AWS .....	130
TABLA 16: TABLA DE COSTOS DE SOFTWARE (CLIENTES).....	135
TABLA 17: TABLA DE COSTOS DE SOFTWARE (SERVIDOR) .....	136
TABLA 18: TABLA DE COSTOS DE HARDWARE (CLIENTE) .....	136
TABLA 19: TABLA DE COSTOS DE HARDWARE (SERVIDOR) .....	137
TABLA 20: LÍNEAS DE CÓDIGO DESARROLLADAS .....	139
TABLA 21: COEFICIENTES DE DESARROLLO .....	140
TABLA 22: COSTOS VARIABLES .....	142
TABLA 23: COSTOS TOTALES DE DESARROLLO DEL PROYECTO .....	143
TABLA 24: BENEFICIOS CUANTITATIVOS .....	146
TABLA 25: FLUJO DE CAJA .....	148

## **ÍNDICE DE ECUACIONES**

ECUACIÓN 1: CÁLCULO DEL ESFUERZO .....	138
ECUACIÓN 2: CÁLCULO DEL TIEMPO .....	138
ECUACIÓN 3: CÁLCULO DE CANTIDAD DE PERSONAS .....	138
ECUACIÓN 4: CÁLCULO DE COSTO DE DESARROLLO DE SOFTWARE .....	139

## **ÍNDICE DE ANEXOS**

- ANEXO A: ÁRBOL DE PROBLEMAS
- ANEXO B: ÁRBOL DE OBJETIVOS
- ANEXO C: FORMULARIO DE INSPECCIÓN
- ANEXO D: FOTO DE EMBARCACIÓN
- ANEXO E: CERTIFICADO DE SEGURIDAD
- ANEXO F: REGISTRO DE EMBARCACIONES
- ANEXO G: EMISIÓN DE CERTIFICADO DE REGISTRO
- ANEXO H: REGLAMENTO NACIONAL DE REGISTRO
- ANEXO I: TAREAS DEL PERSONAL DE UNIDAD DE MARINA MERCANTE
- ANEXO J: PROCESO DE REGISTRO DE EMBARCACIONES
- ANEXO K: PROCESO DE INSPECCIÓN DE EMBARCACIONES
- ANEXO L: EJECUCIÓN DE LA INSPECCIÓN TÉCNICA
- ANEXO M: DETERMINACIÓN DE MENSAJES A ENcriptar
- ANEXO N: COTIZACIÓN DE SERVIDORES PARA BASES DE DATOS
- ANEXO O: COTIZACIÓN DE SERVIDOR PARA APLICACIÓN
- ANEXO P: CARTA DE ACEPTACIÓN DE CASO DE ESTUDIO
- ANEXO Q: CARTA DE CONFORMIDAD DE CASO DE ESTUDIO

# RESUMEN EJECUTIVO



## **RESUMEN EJECUTIVO**

El presente Trabajo de Grado tiene por objetivo aplicar criptografía asimétrica en los certificados que emite la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, para realizar el seguimiento y control durante las inspecciones, verificando la autenticidad de la información en los mismos.

La aplicación de criptografía asimétrica en los documentos previamente mencionados generara un par de llaves (llave publica y llave privada), las cuales están relacionadas matemáticamente. La llave publica se incluirá a cada certificado que la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante emita (inmersa en un código QR) de manera que por la misma se pueda verificar la integridad de la información.

El sistema desarrollado almacena la información de las embarcaciones registradas en el presente caso de estudio. Automatiza el proceso de inspecciones de las mismas y ofrece la posibilidad de generar de manera automática el certificado de registro y seguridad de la navegación que son extendidas.

El presente documento se divide en cinco capítulos, los cuales detallan los pasos seguidos para lograr el objetivo planteado, para lograr el desarrollo se aplicado una metodología ágil.

En el primer capítulo se define la problemática a solucionar, se plantearon los objetivos, además de las justificaciones y alcances.

En el segundo capítulo se establecieron los fundamentos necesarios para la consolidación teórica del proyecto, la metodología y el algoritmo asimétrico elegido.

En el tercer capítulo se realiza el desarrollo del sistema web, se realiza la implementación de criptografía, se realizó el análisis de las características técnicas de los algoritmos asimétricos, determinando la implementación del algoritmo RSA debido

a que presenta ventajas al momento de encriptar y desencriptar los datos, y se centraliza la información de las embarcaciones. Se realizó este proceso siguiendo la metodología ágil Design Sprint.

En el cuarto capítulo se realizó el análisis de costo beneficio, en el cual se identificaron los costos fijos y variables incurridos para el desarrollo del sistema. También realizó el flujo de caja a partir del cual se determinó la viabilidad del proyecto desarrollado.

Por último, en el capítulo cinco se determinaron las conclusiones después del proceso de desarrollo y pruebas, además de las recomendaciones para mejoras futuras.

## ABSTRACT

The objective of this Degree Project is to apply asymmetric cryptography in the certificates issued by the General Directorate of Maritime, Fluvial, Lacustrine and Merchant Marine Interests, to carry out monitoring and control during inspections, verifying the authenticity of the information in them.

The application of asymmetric cryptography in the previously mentioned documents will generate a pair of keys (public key and private key), which are mathematically related. the public key It will be included in each certificate issued by the General Directorate of Maritime, River, Lake and Merchant Marine Interests (embedded in a QR code) so that the integrity of the information can be verified.

The developed system stores the information of the vessels registered in the present case study. It automates the inspection process of the same and offers the possibility of automatically generating the certificate of registration and navigation security that are extended.

This document is divided into five chapters, which detail the steps followed to achieve the proposed objective, to achieve the development, an agile methodology was applied.

In the first chapter, the problem to be solved is defined, the objectives, as well as the justifications and scope, were raised.

In the second chapter, the necessary foundations for the theoretical consolidation of the project, the methodology and the asymmetric algorithm chosen were established.

In the third chapter, the development of the web system is carried out, the implementation of cryptography is carried out, the analysis of the technical characteristics of the asymmetric algorithms was carried out, determining the

implementation of the RSA algorithm due to the fact that it presents advantages when encrypting and decrypting the data, and the information of the vessels is centralized. This process was carried out following the agile Design Sprint methodology.

In the fourth chapter, the cost benefit analysis was carried out, in which the fixed and variable costs incurred for the development of the system were identified. I also carry out the cash flow from which the viability of the developed project was determined.

Finally, chapter five determined conclusions after the development and testing process, as well as recommendations for future improvements.

# CAPÍTULO I

## GENERALIDADES



# **CAPÍTULO I**

## **GENERALIDADES**

### **1.1 INTRODUCCIÓN**

La criptología es la disciplina que se encarga del estudio de la escritura secreta, la cual está compuesta de cuatro áreas: el criptoanálisis (romper las codificaciones realizadas por terceros), la esteganografía (la ocultación de mensajes dentro de canales inseguros de manera que pasen desapercibidos), estegoanálisis (detectar los mensajes ocultos mediante esteganografía).

Finalmente, se define a la criptografía como el estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información dotando de seguridad a las comunicaciones además de a las entidades que se comunican. Esta última además tiene como objetivo diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad, posee las siguientes propiedades: confidencialidad, integridad, vinculación y autentificación.

La criptografía ha hecho cambiar el curso de conflictos como la Segunda Guerra Mundial y el criptoanálisis se ha convertido en una potente arma que muchos gobiernos usan para conseguir ventaja táctica y acceder a fuentes de información de lo más diversa. La misma es una necesidad derivada de realizar comunicaciones por escrito creada para preservar la privacidad de la información que se transmite, garantizando que una persona que no esté autorizada no pueda leer el contenido del mensaje. Actualmente existen tres tipos de esta: simétrica, asimétrica e híbrida, en el actual trabajo nos centraremos en el uso de la asimétrica.

La criptografía asimétrica (o criptografía de llave pública) permite establecer una conexión segura entre dos partes, autenticando mutuamente a las partes y permitiendo el traspaso de información entre los dos. El sistema utiliza dos llaves para cifrar un mensaje: una llave pública y otra privada. Para encriptar un mensaje, se utiliza la llave pública del receptor (que se conoce a priori) y la privada del emisor. Para desencriptar se utiliza la llave pública del emisor (que se envía junto al mensaje cifrado) y la llave privada del receptor. La llave privada es secreta y es la única que permite descifrar los mensajes.

La idea es que ninguna tercera parte pueda descifrar la información en caso de que lograse interceptar el mensaje. Estas llaves son generadas por cada usuario y son únicas. Incluso si se generan a partir de los mismos datos, las claves serán distintas.

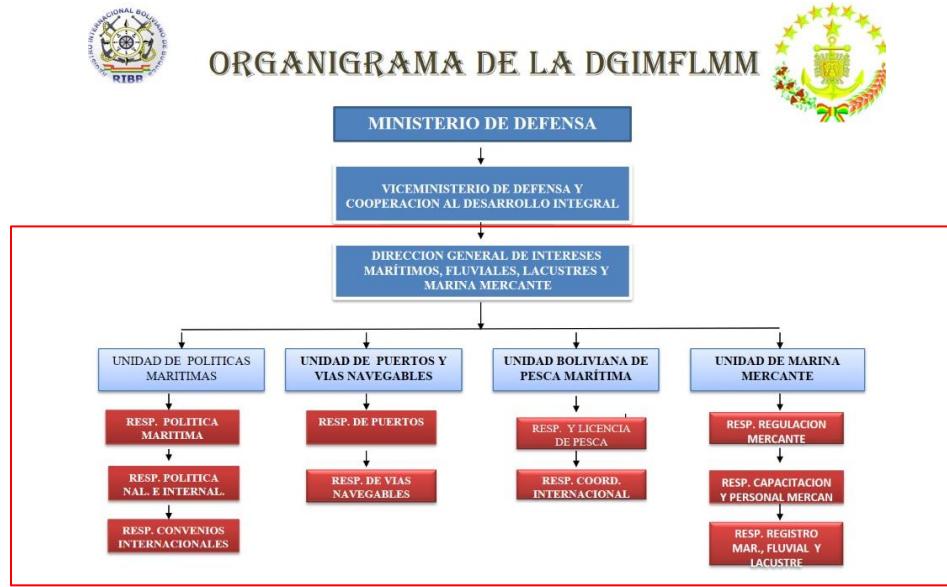
## **1.2 ANTECEDENTES**

Para realizar el presente Trabajo de Grado se consultó la información básica de la Dirección de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, como su objetivo, misión, visión dependencias y su ubicación. De la misma manera también se consultaron Trabajos de Grado y Tesis, los cuales sirvieron de referencia.

### **1.2.1 Antecedentes Institucionales**

Actualmente la Dirección de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante es una Unidad de la Armada Boliviana, pero esta es dependiente del Viceministerio de Defensa y Cooperación al Desarrollo Integral, y este a su vez es dependiente del Ministerio de Defensa como se muestra en la Figura 1. Esta es responsable de la regulación, control y seguridad de las actividades relacionadas con la navegación, marina mercante, puertos, muelles, atracaderos el transporte acuático y actividades conexas.

**FIGURA 1: ORGANIGRAMA DE LA DGIMFLMM**



**Fuente:** Ministerio de Defensa

En la Figura 1 se pudo observar el organigrama de la DGIMFLMM, el cual se subdivide en: Unidad de Políticas Marítimas, Unidad de Puertos y Vías Navegables, Unidad de Pesca Marítima y Unidad de Marina Mercante.

La Dirección General de Intereses Marítimos, Fluviales, Lacustres y Marina Mercante (DGIMFLMM), dependiente del Ministerio de Defensa, se constituye en la Autoridad Marítima, Fluvial y Lacustre del Estado Plurinacional de Bolivia, siendo responsable de la regulación, control y seguridad de las actividades relacionadas con la navegación, marina mercante, puertos, muelles, atracaderos de transporte acuático y actividades conexas.

La misión de la Dirección de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante es la de ejercer la autoridad marítima fluvial y lacustre mediante la regulación, control y vigilancia de todas las actividades que se desarrollan en el ámbito acuático y portuario del Estado, a fin de contribuir a la protección y

administración de los intereses marítimos fluviales y lacustres del Estado Plurinacional de Bolivia (DGIMFLMM, 2020).

La visión de la Dirección de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante es la de ser reconocida como la autoridad marítima, fluvial y lacustre a nivel nacional e internacional como entidad gestora de los Intereses marítimos fluviales lacustres y de la Marina mercante, mediante una administración moderna, eficaz, eficiente y sostenible al servicio de la comunidad que desarrolla actividades en el ámbito acuático en pro del desarrollo del poder marítimo del Estado Plurinacional de Bolivia (DGIMFLMM, 2020).

### **1.2.2 Antecedentes Académicos**

Para el siguiente Trabajo de Grado, se consultaron distintos antecedentes académicos. Se revisaron trabajos Nacionales, Departamentales e Internacionales, los cuales se detallarán a continuación.

Tesis de Grado “**SEGURIDAD EN TRANSACCIONES EN LÍNEA CON TARJETA DE DEBITO MEDIANTE MÉTODOS DE ENCRIPCIÓN HIBRIDA**”, por el Licenciado Arturo Ricardo Mirabal Alvarado (2010), Universidad Mayor de San Andrés, La Paz, Bolivia. Su propósito es: Criptografía sobre el uso de tarjetas bancarias, pero se hace referencia a criptografía hibrida y criptografía tradicional.

La diferencia con el actual Trabajo de Grado es que solamente se hace el uso de criptografía asimétrica para la implementación de firma digital, al implementar una única forma de encriptación (asimétrica) el nivel de seguridad es mayor, la criptografía hibrida presenta tanto, vulnerabilidades de la criptografía simétrica y asimétrica.

Trabajo de Grado “**IMPLEMENTACIÓN DE UN MODELO SIMPLIFICADO DE FIRMA DIGITAL BASADO EN LA TECNOLOGÍA PKI Y LA INVOCACIÓN POR PROTOCOLOS CASO DE ESTUDIO: MUNICIPALIDAD DE MIRAFLORES**”.

Elaborado por Ing. Gino Brehan Aguilar Alcarráz elaborado en el año 2016, en la Universidad Mayor de San Andrés, el cual tiene como objetivo implementar un modelo simplificado de firma digital basado en tecnología PKI, el cual utiliza algoritmos de cifrado que son conocidos y están accesibles para todos.

La diferencia con el actual Trabajo de Grado, es la implementación de tecnología PKI, este utiliza algoritmos de cifrado accesibles para cualquier persona existiendo la posibilidad de ser vulnerado con mayor facilidad, implementando un algoritmo asimétrico que genere las claves a partir de ecuaciones matemáticas, elevará el nivel de seguridad en la información que se pretende proteger, debido a que las ecuaciones que se usan no son accesibles para cualquier personal y no son de fácil entendimiento.

Tesis “**ENCRIPCIÓN RSA DE ARCHIVOS DE TEXTO**”. Elaborado por Magister Katia Regina Leon Lomparte elaborado en el año 2005, en la Pontificia Universidad Católica de Perú, el cual tiene como objetivo implementar el algoritmo RSA para encriptar archivos de texto al momento de la transmisión de los mismos.

La diferencia con el actual Trabajo de Grado es, que la Tesis antes mencionada realiza el uso del algoritmo RSA para encriptar todo un archivo de texto, se hará uso de este mismo algoritmo de manera que se encripte información correspondiente a una embarcación, posteriormente siendo plasmada en un certificado.

Tesis “**SEGURIDAD EN REDES Y CRIPTOGRAFÍA**”. Elaborado por el Ing. Dante Iván González Sánchez en el año 2004 en Instituto Tecnológico y de Estudios Superiores de Monterrey (México), el cual tiene como objetivo proponer varias soluciones informáticas por medio de encriptación, políticas, técnicas y herramientas para así elevar la seguridad en varias configuraciones de sistemas de cómputo.

La diferencia con el actual Trabajo de Grado es que se hace el uso de criptografía híbrida para elevar la seguridad en sus dispositivos de red, al implementar

criptografía asimétrica no se presentan tantas vulnerabilidades como con la antes mencionada, debido a que esta cuenta tanto con vulnerabilidades de criptografía asimétrica y simétrica.

### **1.3 PLANTEAMIENTO DEL PROBLEMA**

Actualmente la Dirección de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, es una unidad perteneciente a la Armada Boliviana, y a su vez es dependiente del Ministerio de Defensa. Esta unidad se encarga de ejercer autoridad marítima fluvial y lacustre mediante la regulación, control y vigilancia de todas las actividades que se desarrollan en el ámbito acuático y portuario del Estado. Su principal función es la de registrar cualquier embarcación a nivel nacional, emitiendo certificados de registro.

Para realizar el registro de una embarcación, previamente el propietario debe presentar requisitos solicitados por esta unidad (fotocopia de c.i., factura de la embarcación, depósito bancario, etc.), para que posteriormente estos sean registrados y almacenados de manera semimanual. Estos documentos se almacenan en carpetas, junto a su formulario de inspección inicial, como se observa en el Anexo C, fotos de la embarcación, como se observa en el Anexo D, y su certificado de seguridad, como se observa en el Anexo E. Para este proceso de registro, se asigna a un Inspector de Buques se presenta de manera presencial, juntamente con solicitudes de registro y formularios de registro de modo que registre la información correspondiente y almacenarla en medios ofimáticos.

Una vez finalizado este proceso y habiéndose verificado la autenticidad de todos estos, se procede a la emisión del certificado de registro, el cual tiene tanto los datos técnicos de la embarcación como los datos del propietario, como se observa en el Anexo F. Estos certificados cuentan con dos normas de seguridad, físicas únicamente, el papel en los que son impresos y los altos relieves que presenta este, dicho motivo puede ocasionar duplicidad y copias no autorizadas, como se observa en el Anexo G.

Para el seguimiento de embarcaciones, la Dirección de Intereses Marítimos, Fluviales; Lacustre y Marina Mercante realiza inspecciones anualmente, en las cuales se consulta la información histórica de estas. La dificultad dentro de este proceso se encuentra en que la información que se tiene almacenada actualmente no se encuentra centralizada, generando tiempos de consulta más extendidos y ocupación de una mayor cantidad de personal para realizar esta tarea.

En el proceso antes explicado se realiza el control de los certificados de seguridad anteriormente emitidos, si es que las observaciones que presenta han sido subsanadas, en el caso de que todo este correcto se le emite un nuevo certificado de seguridad con una validez de un año (hasta que se realice la próxima inspección), caso contrario la embarcación no tendrá el permiso para navegar. El no contar con este certificado causa una infracción a leyes 2976 “Ley de capitanías de puertos”, ley 165 “Ley general de transporte” y Decreto Supremo 3073.

### **1.3.1 Problema Principal**

El actual proceso que usa la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, en la verificación de la información de los certificados de embarcaciones se realiza de manera semimanual, provocando dificultad al momento de realizar el seguimiento y control de estas, durante las inspecciones.

### **1.3.2 Problemas Secundarios**

- Actualmente se almacena la información de los registros de las embarcaciones en medios físicos y en listados digitales, lo que causa una posible pérdida de la misma por parte del personal a cargo.
- La disponibilidad de la información de las embarcaciones se ve limitada debido a que se encuentra en medios físicos, lo que causa dificultad al momento de realizar el seguimiento y control durante las inspecciones.

- Los mecanismos que actualmente se utilizan en la verificación y emisión de los certificados de embarcaciones, ocasiona posible duplicidad en los mismos debido a que no tiene un método por el cual verificar su veracidad.

## **1.4 OBJETIVOS**

Luego de analizar y observar los inconvenientes que se presentan la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante se toman en cuenta los siguientes objetivos.

### **1.4.1 Objetivo General**

Aplicar criptografía asimétrica en los certificados que emite la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, para realizar el seguimiento y control durante las inspecciones, verificando la autenticidad de la información en los mismos.

### **1.4.2 Objetivos Específicos**

- Centralizar la información obtenida acerca de las embarcaciones registradas, para poder optimizar el tiempo en el que se entrega la certificación de las embarcaciones.
- Proporcionar al personal a cargo de las inspecciones información detallada de cada embarcación mediante una plataforma web, para realizar un adecuado seguimiento y control de las mismas.
- Implementar el algoritmo asimétrico que permita generar los certificados digitales, para verificar la autenticidad de la información en los mismos minimizando la posibilidad de duplicidad.

## **1.5 JUSTIFICACIÓN**

A continuación, se detallará las siguientes justificaciones.

### **1.5.1 Justificación Técnica**

Se justifica el presente Trabajo de Grado técnicamente, debido a que la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante cuenta con la tecnología y el personal capacitado, para automatizar el proceso de registro de embarcaciones, además de mejorar el seguimiento y control de las mismas garantizando la integridad de la información emitida en sus certificados.

Se aplicará criptografía asimétrica en los certificados que esta unidad emite, al momento de emitirse los certificados correspondientes estos contendrán una clave pública generada por el sistema de manera aleatoria, la misma les permitirá corroborar la información emitida en el certificado y asegurarse que la información se encuentra almacenada en la base de datos de esta unidad.

### **1.5.2 Justificación Económica**

Económicamente se reducen los costos que se realizan en la compra de insumos materiales, los cuales coadyuvaban al registro y almacenamiento de información de embarcaciones. El acceso a la misma será inmediato, al momento de realizar consultas, no existirá la necesidad de recurrir a medios físicos. Automatizar los procesos de registro y emisión de certificados reducirán los recursos que actualmente se emplean en estos procesos, permitiendo que el personal estipulado pueda cumplir con una mayor cantidad de deberes que se les son asignado.

### **1.5.3 Justificación institucional**

El presente proyecto se desarrollará de acuerdo a los requerimientos presentados por la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante:

- Centralizar la información: Recolectar la información que se encuentra dispersa en diversos medios físicos y digitales acerca de las embarcaciones. Esta será

centralizada y digitalizada en una base de datos la cual permitirá realizar consultas de las mismas cuando se realicen las inspecciones anuales, o en algún caso externo.

- Automatizar el proceso de registro: Contar con una plataforma web la cual nos ayudará a registrar una embarcación nueva, sin la necesidad de formularios físicos. La información que se mande acerca de esta será almacenada de manera digital.
- Implementación de normas de seguridad: Se aplicará criptografía asimétrica como norma de seguridad en los certificados que esta unidad emite, de modo que al momento de realizar inspecciones se pueda verificar la autenticidad de la información.

## 1.6 ALCANCES

A continuación, se detallarán los alcances del presente Trabajo de Grado.

### 1.6.1 Alcance Geográfico

La Dirección General de Intereses Marítimos, Fluviales, Lacustres y Marina Mercante se encuentra ubicada en Intendencia Central, ubicada en la Avenida Saavedra, cerca al Estadio Hernando Siles como se observa en la Figura 2

**FIGURA 2: UBICACIÓN DGIMFLMM**



**Fuente:** <https://www.google.com/maps/@-16.5005351,-68.1228222,17z>

En la Figura 2 se puede observar la dirección exacta de la DGIMFLMM obtenida gracias a la aplicación Google Maps.

#### **1.6.2 Alcance Temporal**

La elaboración del presente trabajo de investigación se desarrollará de acuerdo al calendario académico de la Escuela Militar de Ingeniería de la gestión 2020, donde se encuentran marcadas las fechas de presentación y defensa de trabajo.

Se trabajará con la información disponible desde la gestión 2015 hasta la actualidad.

#### **1.6.3 Alcance Temático**

El desarrollo del presente Trabajo de Grado aborda información sobre el área general de Ingeniería de Sistemas, utilizando conceptos de Ingeniería Web particularmente.

Área General: Ingeniería de Sistemas.

Área Específica: Seguridad de Sistemas, Ingeniería de Software

Área Temática: Criptografía

#### **1.6.4 Alcance Funcional**

Los alcances funcionales definidos son los siguientes:

- Gestionar los usuarios que ingresarán y harán uso del sistema.
- Automatizar el proceso de registro de embarcaciones.
- Generar reportes acerca de los usuarios y embarcaciones
- Automatizar el proceso por el cual se realizan las inspecciones a las distintas embarcaciones

## CAPÍTULO II

### MARCO TEÓRICO



## **CAPÍTULO II**

### **MARCO TEÓRICO**

#### **2.1 INGENIERÍA DE SISTEMAS**

La Ingeniería de Sistemas es aquella que se encarga del diseño, programación, implementación y mantenimiento de sistemas. Es una ciencia interdisciplinaria, que requiere de varios conocimientos para plasmar diseños de manera práctica, permitiendo transformar una necesidad operativa en una descripción de parámetros de un sistema.

A continuación, revisaremos algunas definiciones de Ingeniería de Sistemas:

La Ingeniería de Sistemas puede definirse como «la aplicación de técnicas científicas y de ingeniería para transformar una necesidad operativa en la descripción de los parámetros de prestaciones de un sistema y en su configuración mediante la utilización de un proceso iterativo de definición, síntesis, análisis, diseño, prueba y evaluación; integrar los parámetros técnicos relacionados y asegurar la compatibilidad de todas las interrelaciones físicas, funcionales y del programa de forma que se consiga la mejor definición y diseño del sistema completo; e integrar los aspectos de fiabilidad, mantenibilidad, seguridad, supervivencia, de personal y otros similares en el proceso global de ingeniería para conseguir los objetivos técnicos, de coste y de calendario fijados. (Blanchard, 1995, p.19)

“Ingeniería de Sistemas es una tecnología por la que el conocimiento de investigación se traslada a aplicaciones que satisfacen necesidades humanas

mediante una secuencia de planes, proyectos y programas de proyectos” (Hall, 1962).

En base a las definiciones mencionadas se enfocará a la ingeniería de sistemas como aquella rama de la ingeniería, que nos permitirá resolver necesidades humanas, tomando en cuenta la dimensión temporal, comenzando en la idea inicial del sistema hasta la retirada del mismo, y la dimensión lógica, en la que se realiza el planteamiento del problema y se toman acciones para poder dar solución a este.

### **2.1.1 Ingeniería**

La Ingeniería es una profesión, la cual nos permite aplicar conocimientos científicos y tecnológicos para solucionar las distintas dificultades que se presentan en el diario vivir de la mejor manera posible. Esta a su vez nos permite generar conocimiento que será de utilidad, conforme se van realizando investigaciones, desarrollando y mejorando de técnicas y herramientas que son utilizadas para satisfacer necesidades y resolver problemas.

A continuación, revisaremos algunas definiciones de Ingeniería:

“Ingeniería es la ciencia que, con la técnica y el arte, aplicando la matemática, crea y desarrolla sistemas, elementos y obras físicas mediante el empleo de la energía para proporcionar a la humanidad, con eficiencia y sobre bases económicas” (Sobrevilla, 2008, p.7).

Ingeniería es la aplicación de los conocimientos científicos a la invención, perfeccionamiento y utilización de la técnica industrial en todas sus ramas. Estudios que permiten fijar las mejores orientaciones para la realización óptima de una obra o un programa de inversiones. (Larousse, 2009)

Para el presente Trabajo de Grado se tomará a la Ingeniería como el conocimiento de las matemáticas, de modo que se puedan aplicar para desarrollar formas de utilizar económicamente los materiales para beneficiar a la humanidad.

## **2.1.2 Sistema**

Un sistema es un conjunto de elementos que tienen características comunes y se interrelacionan para lograr un fin. Estos poseen elementos de entrada con los cuales trabajan, posteriormente estos pasan por un proceso interno de modo que se pueda proveer información de salida.

Los sistemas son estudiados con el objetivo de comprender su funcionamiento, los límites que estos poseen, entender los objetivos que persiguen y la forma en estos interactúan con otros sistemas externos.

A continuación, revisaremos algunas definiciones de Sistema:

Un sistema es un conjunto o aglomerado de elementos y procesos que se encuentran relacionados y cuyo comportamiento satisface las necesidades de un cliente u operacionales y que permite que se pueda brindar soporte a los productos a lo largo de su ciclo de vida. (IEEE,1998)

“Un sistema es una unión de partes o componentes, conectados en una forma organizada. Las partes se afectan por estar en el sistema y se cambian si lo dejan” (Van Glinch, 1987).

## **2.2 INGENIERÍA DE SOFTWARE**

La Ingeniería de Software es una de las ciencias de la computación que se encarga de estudiar la creación de software confiable y calidad. Esta incluye el análisis previo de la situación, el diseño del proyecto, el desarrollo del software, las pruebas necesarias para confirmar su correcto funcionamiento y la implementación del sistema.

A continuación, revisaremos algunas definiciones de Ingeniería de Software:

“La Ingeniería de Software es una disciplina o área de la informática, que ofrece técnicas y métodos para desarrollar y mantener software de calidad que resuelva todo tipo de problemas” (Pressman, 2010, pág. 11).

“Es la aplicación de un enfoque sistemático, disciplinado y cuantificable al desarrollo, operación y mantenimiento del software; es decir, la aplicación de la Ingeniería de Software” (IEEE, 1993).

En base a las definiciones mencionadas se enfocará a la Ingeniería de Software como la aplicación de técnicas y métodos para desarrollar y mantener el software propuesto en el actual Trabajo de Grado.

### **2.2.1 Modelos de Desarrollo de Software**

Para el desarrollo de cualquier producto de software se debe realizar una serie de tareas entre la idea inicial y el producto final. Un modelo de desarrollo establece el orden en el que se realizaran las tareas en un proyecto, se determina las entradas y salidas para cada actividad.

El ciclo de vida de un proyecto nos ayuda a controlar las actividades que son programadas, y el modelo de desarrollo nos ayuda en el cómo se construye el producto. Entre los modelos de desarrollo se tiene: Modelo Cascada, Modelo en V, Prototipo y Modelo Espiral.

#### **2.2.1.1 Modelo en V**

“El Método-V fue desarrollado para regular el proceso de desarrollo de software, describe las actividades y los resultados que se producen durante el desarrollo del software.” (Administración Federal Alemana, 1990)

En el desarrollo de software, la V-modelo representa un proceso de desarrollo que puede ser considerado una extensión del modelo de cascada, y es un ejemplo de

la más V-modelo general . En lugar de mover hacia abajo en una forma lineal, las etapas de procedimiento se doblan hacia arriba después de la codificación de fase, para formar la forma típica V.

### Ventajas

- Optimización de la comunicación entre las partes involucradas a través de términos y responsabilidades claramente definidos.
- Minimización de riesgos y mejor planificación a través de roles, estructuras y resultados fijos y predeterminados.
- Mejora de la calidad del producto gracias a medidas de control de la calidad firmemente integradas.
- Ahorro de costes gracias al procesamiento transparente a lo largo de todo el ciclo de vida del producto.

### Desventajas

- El modelo en cuatro niveles puede ser demasiado simple para mapear todo el proceso de desarrollo desde el punto de vista de los desarrolladores. Está sobre todo centrado en la gestión de proyectos.
- Su estructura relativamente rígida permite una respuesta poco flexible a los cambios durante el desarrollo, y, por lo tanto, promueve un curso lineal del proyecto. Sin embargo, si el modelo se entiende y se utiliza correctamente, es posible utilizar el modelo V para el desarrollo ágil.

#### **2.2.1.2 Modelo Evolutivo**

Dentro la principal característica tenemos que “los modelos evolutivos son iterativos, se caracterizan por la manera en la que permiten desarrollar versiones cada vez más completas del software.” (Sommerville,2005)

Entre las principales características se puede mencionar:

- La especificación puede desarrollarse de forma creciente.
- Los usuarios y desarrolladores logran un mejor entendimiento del sistema. Esto se refleja en una mejora de la calidad del software.
- Es más efectivo que el modelo de cascada, ya que cumple con las necesidades inmediatas del cliente.

### 2.2.1.3 Modelo en espiral

“Es un modelo de proceso de software evolutivo donde se conjuga la naturaleza de construcción de prototipos con los aspectos controlados y sistemáticos del modelo lineal y secuencial” (Bohen, 1976).

Proporciona el potencial para el desarrollo rápido de versiones incrementales del software que no se basa en fases claramente definidas y separadas para crear un sistema, como se puede observar en la Figura 4.

**FIGURA 3: MODELO EN ESPIRAL**



Fuente: <http://b-one-informatica.blogspot.com/2016/02/la-triada-cid-seguridad-informatica.html>

En la Figura 4, se puede observar las fases que aplica cualquier modelo espiral, estos se van repitiendo según se va desarrollando el sistema, de manera que se mejora el producto que se elabora en cada iteración.

Se plantea el uso de un modelo de desarrollo en espiral debido a que existirá una integración continua de los distintos requerimientos que se tiene, pasando por las cuatro fases que presenta esta, además se tendrá un trabajo continuo con pasos pequeños.

### **2.2.2 Lenguaje de Modelado Unificado (UML)**

Es un lenguaje de modelado para especificar, describir métodos o procesos. Este lenguaje gráfico permite visualizar, especificar, construir y documentar un sistema. Además, incluye aspectos conceptuales como procesos, funciones del sistema, y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y compuestos reciclados.

“El Lenguaje de Modelado Unificado (UML) permite a través de sus elementos gráficos representar flujos de trabajo diversos para proyectos de tecnología informática, hardware, electrónica, etc., de cualquier nivel en una organización sin importar su tamaño o naturaleza” (Castañeda, 2015).

UML ofrece un estándar para describir una organización del sistema, incluyendo aspectos conceptuales tales como procesos de negocio y funciones del sistema, y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y componentes reutilizables.

Para el actual Trabajo de Grado se incluirá el Lenguaje de Modelo Unificado, de manera que el mismo nos ayude en la representación de distintos procesos identificados en la parte de desarrollo.

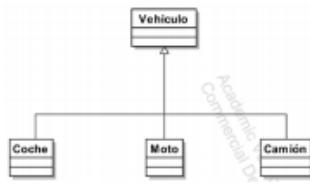
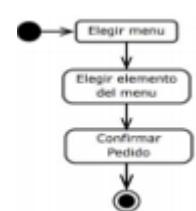
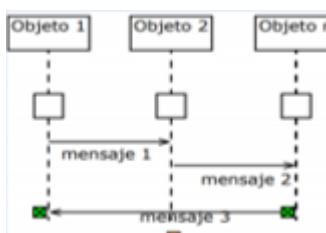
#### **2.2.2.1 Diagramas UML**

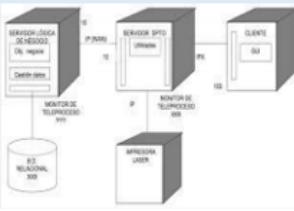
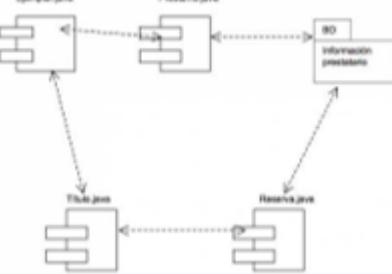
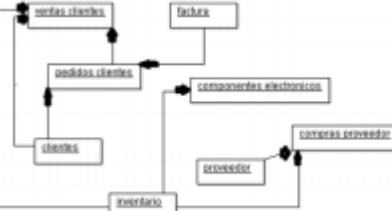
Para la representación de diferentes procesos, actores y actividades se utilizan distintos diagramas que posee UML, cada diagrama tiene un propósito específico, como se puede apreciar en la Tabla 1.

Los diagramas UML ayudan a realizar la documentación al momento de desarrollar el sistema, de modo que se tenga una mejor comprensión tanto de los participantes de un proceso, como de los procesos en sí.

“UML ofrece un estándar para describir un “plano” del sistema, incluyendo aspectos conceptuales tales como procesos de negocio y funciones del sistema, y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y componentes reutilizables” (Fowler, 1999).

**TABLA 1: DIAGRAMAS UML**

Diagrama	Descripción	Prioridad
Diagrama de clases	 <p>Muestra una colección de elementos de modelado declarativo (estáticos), tales como clases, tipos y sus contenidos y relaciones</p>	Alta
Diagrama de actividades	 <p>Representa los procesos de negocios de alto nivel, incluidos el flujo de datos. También puede utilizarse para modelar lógica compleja y/o paralela dentro de un sistema</p>	Alta
Diagrama de secuencias	 <p>Un diagrama que representa una interacción, poniendo el foco en la secuencia de los mensajes que se intercambian, junto con sus correspondientes ocurrencias de eventos en las líneas de vida</p>	Alta

<p><b>Diagrama de despliegue físico</b></p> 	<p>Un diagrama de despliegue físico muestra cómo y dónde se desplegará el sistema. Las máquinas físicas y los procesadores se representan como nodos y la construcción interna puede ser representada por nodos o artefactos embebidos.</p>	<p>Media</p>
<p><b>Diagrama de casos de uso</b></p> 	<p>Un diagrama que muestra las relaciones entre los actores y el sujeto (sistema), y los casos de uso</p>	<p>Media</p>
<p><b>Diagrama de componentes</b></p> 	<p>Representan los componentes que conforman una aplicación, sistema o empresa. Los componentes, sus relaciones, iteraciones y sus interfaces públicas</p>	<p>Media</p>
<p><b>Diagrama de objetos</b></p> 	<p>Un diagrama que presenta los objetos y sus relaciones en un punto en el tiempo. Un diagrama de objetos se puede considerar como un caso especial de diagrama de clases o un diagrama de comunicaciones</p>	<p>Baja</p>

**Fuente:** Sena,2009, p.5

Para el presente Trabajo de Grado se usará UML de modo que ayude a representar flujos de trabajo, especificar los procesos que el sistema realizará y documentar el mismo.

### **2.2.3 Gestor de Base de Datos**

Un sistema gestor de base de datos es un conjunto de programas que permiten el almacenamiento, modificación y extracción de la información en una base de datos. A continuación, se dará un concepto de este.

En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. Actualmente y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital, siendo este un componente electrónico, por tanto, se ha desarrollado y se ofrece un amplio rango de soluciones al problema del almacenamiento de datos (Silberschatz,1987).

Entre los gestores de bases de datos más reconocidos tenemos a: SQL Server, MySQL y PostgreSQL.

#### **2.2.3.1 SQL Server**

Microsoft SQL Server es un sistema de gestión de base de datos relacionales (SGBD) basado en el lenguaje Transact-SQL, y específicamente en Sybase IQ capaz de poner a disposición de muchos usuarios grandes cantidades de base de datos simultánea.

Los clientes o usuarios buscan soluciones para sus problemas de negocios. La mayoría de las “soluciones” de bases de datos solamente traen múltiples niveles de costos y complejidad, la estrategia de Microsoft es la de hacer que SQL Server sea la base de datos más fácil de utilizar para construir, administrar e implementar aplicaciones de negocios. Esto significa tener que poner a disposición un modelo de programación rápido y sencillo para desarrolladores, eliminando la administración de base de datos para

operaciones estándar, y suministrando herramientas sofisticadas para operaciones más complejas (Worl,2009).

Dentro de las principales características de SQL Server se puede mencionar:

- Integración con internet gracias a un motor de base de datos.
- La capacidad de escalar a medida que incrementa la información, y la disponibilidad con los distintos dispositivos electrónicos.
- Facilidad de instalación, distribución y utilización ya que incluye un conjunto de herramientas administrativas y de desarrollo.
- Almacenamiento de datos ya que incluye herramientas para extraer y analizar datos de resumen para el procesamiento analítico en línea de SQL Server.

#### **2.2.3.2 MySQL**

El software MySQL ofrece un multiusuario muy rápido y robusto de servidor de base de datos SQL (Structured Query Language), “el servidor MySQL está diseñado para sistemas de producción de misión crítica y de alta carga, así como para integrarse en software para ser distribuido, es una marca registrada de Oracle Corporation y no podrá ser utilizada por clientes sin la autorización expresa por escrito de Oracle” (MySQL, 2010).

MySQL tiene una doble licencia, sin embargo, los usuarios pueden acceder por el uso del software MySQL como un producto código abierto bajo los términos de la Licencia Pública General de GNU, dentro de sus características se tiene:

- MySQL es un sistema de administración de base de datos.
- MySQL es un sistema de administración relacional de bases de datos permitiendo tener velocidad y flexibilidad en las consultas y peticiones a las bases de datos.
- MySQL es un software de fuente abierta lo significa que es posible para que cualquier persona lo pueda usar y modificar.

### **2.2.3.3 PostgreSQL**

PostgreSQL es un sistema para gestionar bases de datos de muy alto nivel, completamente de software libre y con una licencia BSD, compatible con cualquier uso, ya sea personal o comercial. A continuación, se revisara una definición de este, dado por su grupo de desarrollo,

PostgreSQL es un servidor de base de datos objeto relacional libre, ya que incluye características de la orientación a objetos, como puede ser la herencia, tipos de datos, funciones, restricciones, disparadores, reglas e integridad transaccional, liberado bajo la licencia BSD. Como muchos otros proyectos open source, el desarrollo de PostgreSQL no es manejado por una sola compañía, sino que es dirigido por una comunidad de desarrolladores y organizaciones comerciales las cuales trabajan en su desarrollo, dicha comunidad es denominada el PGDG (PostgreSQL Global Development Group).

PostgreSQL, también llamado Postgres, es un sistema de gestión de bases de datos relacional orientado a objetos y de código abierto, publicado bajo la licencia PostgreSQL.

Dentro de las características se puede mencionar:

- Modelo orientado a objetos
- Tiene capacidad para alta concurrencia
- Acceso encriptado a SSL

## **2.2.4 Framework**

“Un Framework es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.” (Dirk,2000)

El propósito de un framework es mejorar la eficiencia de la creación de un nuevo software. Los framework pueden mejorar la productividad del desarrollador y mejorar la calidad, la fiabilidad y robustez del nuevo software. La productividad del desarrollador se ha mejorado al permitir a los desarrolladores centrarse en las necesidades únicas de su aplicación, en lugar de pasar tiempo en la infraestructura de aplicaciones.

### **2.2.4.1 Laravel**

“Laravel es un framework de código abierto para desarrollar aplicaciones y servicios web con PHP 5 y PHP 7. Su filosofía es desarrollar código PHP de forma elegante y simple” (Taylor Otwell, 2018).

El framework Laravel trabaja con una arquitectura de carpetas avanzada, de modo que promueve la separación de los archivos con un orden correcto y definido. Entre sus principales características podemos mencionar:

- Un sistema de rutas, mediante las cuales es fácil crear y mantener todo tipo de URLs amistosas a usuarios y buscadores, rutas de API, etc.
- Varias configuraciones para envío de email, con proveedores diversos
- Un sistema de notificaciones a usuarios, mediante email, base de datos y otros canales
- Una abstracción del sistema de archivos, mediante el cual podemos escribir datos en proveedores cloud, y por supuesto en el disco del servidor, con el mismo código.

- Sistema de autenticación, con todo lo necesario como recordatorios de clave, confirmación de cuentas, recordar un usuario logueado, etc.
- La posibilidad de acceder a datos en tiempo real y recibir notificaciones cuando éstos se alteran en la base de datos

Para el presente Trabajo de Grado se usará el framework Laravel en su versión 7, la cual es la más reciente, esto debido a los requerimientos establecidos por el caso de estudio incluyendo los beneficios mencionados.

### **2.2.5 COCOMO II**

A continuación, se revisará una definición de COCOMO II:

COCOMO II es un modelo que permite estimar el coste, esfuerzo y tiempo cuando se planifica una nueva actividad de desarrollo software. Consta de tres submodelos que se denominan (Boehm, 2000).

Este modelo trata de estimar, de una manera rápida y más o menos burda, la mayoría de los proyectos pequeños y medianos. Se consideran tres modos de desarrollo en este modelo: orgánico, semi orgánico y empotrado.

- Este modelo nos permite calcular valores aproximados referentes al desarrollo de un sistema. Entre las cuales podemos mencionar.
- Esfuerzo: El esfuerzo empleado al momento de realizar el desarrollo del proyecto, el mismo se encuentra expresado en personas /mes.
- Tiempo: El tiempo que calcula para poder completar a cabalidad con el proyecto desde el análisis de este, hasta la entrega, para esta parte se toma en cuenta que las personas trabajaran una jornada laboral de 8 horas durante cinco días a la semana.
- Personas: La cantidad de personas necesarias, o sugeridas para que el proyecto se cumpla en el plazo establecido.

- Costo: El costo total del desarrollo de software tomando en cuenta los parámetros previamente mencionados.

Dentro del COCOMO, además se debe determinar el tipo de proyecto al cual se lo clasifica, se tienen tres tipos según COCOMO:

- Orgánico: En esta clasificación se encuentran proyectos desarrollados en un ambiente familiar y estable. El producto para elaborar es relativamente pequeño y requiere pocas innovaciones tecnológicas en lo que refiere a algoritmos, estructuras de datos e integración de hardware.
- Semiacoplado: Es un modelo para productos de software de tamaño y complejidad media. Tiene un nivel intermedio de experiencia y conocimiento del sistema en desarrollo. Está conformado por algunas personas con vasta experiencia y otras inexpertas en el campo de aplicación. Está constituido por personas con amplios conocimientos sólo en algunos aspectos.
- Empotrado: En esta clasificación están incluidos proyectos de gran envergadura que operan en un ambiente complejo con altas restricciones de hardware, software y procedimientos operacionales, tales como los sistemas de tráfico aéreo. Se espera que el software no sólo conforme las especificaciones sino también que sea estable frente a cambios y dificultades producidas en el ambiente. Es decir, estos proyectos no tienen opción de negociar cambios y/o arreglos provocados por modificaciones en los requerimientos y/o en las especificaciones de interfase.

## **2.3 SEGURIDAD DE SISTEMAS**

La Seguridad de Sistemas hace referencia al proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica la protección contra intrusos, el uso de recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

De la misma manera está presente el estándar ISO/IEC 27002, el cual colabora en las buenas prácticas para la gestión de la seguridad de la información enfocado a todo tipo de empresas, independientemente del tamaño, naturaleza, se encuentra organizado en base a los 14 dominios, 35 objetivos de control y 114 controles.

La Seguridad de Sistemas se define como toda aquella medida que impide la realización de operaciones no autorizadas sobre un sistema o red informática, donde sus efectos pueden conllevar severos daños en la información, tanto como comprometer su confidencialidad, autenticidad e integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema (Gómez, 2006).

“La Seguridad de Sistemas es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema.” (Fisher, 1998)

Para el presente Trabajo de Grado se usarán las medidas de Seguridad de Sistemas, de modo que se impida la realización de operaciones no autorizadas, por parte de terceras personas.

### **2.3.1 Pilares de la seguridad de la información**

La gestión de la información se basa en tres pilares fundamentales que son: confidencialidad, integridad y disponibilidad, como se puede apreciar en la Figura 5. La seguridad de la información aplica barreras y procedimientos que resguardan el acceso a los datos y sólo permite acceder a las personas autorizadas para realizarlo.

- Confidencialidad: es la garantía de acceso a la información de los usuarios que se encuentran autorizados para tal fin.
- Integridad: es la preservación de la información completa y exacta.

- Disponibilidad: es la garantía de que el usuario accede a la información que necesita en ese preciso momento.

**FIGURA 4: PILARES DE LA SEGURIDAD DE LA INFORMACIÓN**



Fuente: <https://rosarioherediaproyectodesoftware.wordpress.com/2017/09/10/espiral-de-proyectos/>

Como se puede ver en la Figura 4, la confidencialidad, la integridad y la disponibilidad son los pilares de la seguridad de la información

Una vez revisados los conceptos de Seguridad de Sistemas, se hará énfasis en el pilar de la “Integridad”, debido a que se verificará la información emitida en los certificados en las inspecciones que se realicen. Consultando la norma ISO/IEC 27002, esta misma proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad”.

Para el presente Trabajo de Grado se tomarán en cuenta los dominios de adquisición desarrollo y mantenimiento de sistemas, de modo que garanticemos la seguridad de la información sea parte integral del sistema en todo el ciclo de vida, también se hará uso de controles del dominio de organización de la seguridad de la información, estableciendo un marco para iniciar y controlar la implementación de la seguridad de la información.

## 2.4 CRIPTOGRAFÍA

La criptografía es, en líneas generales, el arte y la técnica de crear mensajes codificados con procedimientos o claves secretas con el objeto de que no pueda ser descifrado salvo por la persona a quien está dirigido o que detenta la clave. En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para modificarlos y hacerlos incomprensibles. El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, llamado texto simple. Siendo preciso garantizar que el receptor del mensaje pueda descifrarlo cuando lo reciba.

“La criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican” (Pastor, 1998).

Para el presente Trabajo de Grado se aplicará algoritmos criptográficos (algoritmos de criptografía asimétrica), mediante la plataforma web, de modo que se pueda dotar seguridad a la información de los distintos certificados que emite la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante. También se hará énfasis en el dominio de “Criptografía”, presente en la norma ISO/IEC 27002, la cual tiene como controles “Controles criptográficos”, el cual garantiza el uso adecuado y eficaz de criptografía para proteger la integridad de la información, y “Administración de claves”, desarrollando e implementando claves criptográficas.

#### **2.4.1 Objetivos de la Criptografía**

El objetivo principal de la criptografía es el cifrado de la información. Existen también otros objetivos que se derivan en gran parte de esa posibilidad del cifrado.

El objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad. Por tanto, el tipo de propiedades de las que se ocupa la criptografía son: Confidencialidad. Es decir, garantiza que la información sea accesible únicamente a personal autorizado. Para conseguirlo utiliza códigos y técnicas de cifrado. Integridad. Es decir, garantiza la corrección y completitud de la información. Para conseguirlo puede usar por ejemplo funciones hash criptográficas MDC, protocolos de compromiso de bit, o protocolos de notarización electrónica. Vinculación. Permite vincular un documento o transacción a una persona o un sistema de gestión criptográfico automatizado. Cuando se trata de una persona, se trata de asegurar su conformidad respecto a esta vinculación de forma que pueda entenderse que la vinculación gestionada incluye el entendimiento de sus implicaciones por la persona. Antiguamente se utilizaba el término "No repudio" que está abandonándose, ya que implica conceptos jurídicos que la tecnología por sí sola no puede resolver. En relación con dicho término se entendía que se proporcionaba protección frente a que alguna de las entidades implicadas en la comunicación, para que no pudiera negar haber participado en toda o parte de la comunicación. Para conseguirlo se puede usar por ejemplo firma digital. En algunos contextos lo que se intenta es justo lo contrario: Poder negar que se ha intervenido en la comunicación. Por ejemplo, cuando se usa un servicio de mensajería instantánea y no queremos que se pueda demostrar esa comunicación. Para ello se usan técnicas como el cifrado negable. Autenticación. Es decir, proporciona mecanismos que permiten verificar la identidad del comunicador. Para conseguirlo puede usar por ejemplo función hash criptográfica MAC o protocolo de conocimiento cero. Soluciones a problemas de la falta de simultaneidad en la telefirma digital de contratos. Para conseguirlo puede usar por ejemplo protocolos de transferencia inconsciente. (Menezes, 1996)

Para el presente Trabajo de Grado se tomarán en cuenta las propiedades de autenticación, implementando mecanismos que nos permitan verificar la autenticidad de la información, e integridad, verificando que esta sea correcta al momento que la Dirección General de Intereses Marítimos, Lacustre y Marina Mercante realice sus inspecciones.

#### **2.4.2 Conceptos Básicos de Criptografía**

En la criptografía existen dos conceptos básicos: el cifrado y descifrado de la información, uno no puede suceder sin el otro. Estos se realizan mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

La información original que debe protegerse se denomina texto en claro o texto en plano. El cifrado es el proceso de convertir el texto plano en un “caos lingüístico” ilegible, denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado se basa en la existencia de una clave, la cual es la información secreta que adapta el algoritmo de cifrado para cada uso distinto. El descifrado es el proceso inverso que recupera el texto plano a partir de criptograma y la clave. El protocolo criptográfico especifica los detalles de cómo se utilizan los algoritmos y las claves para conseguir el efecto deseado. El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios, es lo que constituyen en conjunto un criptosistema, que es con lo que el usuario final trabaja e interactúa. (Uriel,2010)

Para el presente Trabajo de Grado se aplicarán ambos conceptos, cifrado de información, aplicado en los certificados que son emitidos a las embarcaciones, y descifrado al momento de verificar la misma por parte de la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante en las inspecciones que realiza.

## 2.5 CRIPTOGRAFÍA ASIMÉTRICA

La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.

Se la conoce también como sistema de clave pública, y se basa en el uso de dos claves: una de ellas puede desencriptar lo que la otra ha encriptado. Estas claves son:

- Clave privada: es la que utiliza el propietario para encriptar los mensajes.
- Clave pública: es que se utiliza para desencriptar el mensaje.

Las claves privadas y públicas se generan siempre a la vez, de tal forma que si tuviéramos dos claves públicas diferentes nos encontraríamos con dos claves privadas igualmente diferentes.

Los algoritmos asimétricos están basados en funciones matemáticas, difíciles de resolver si no se conoce la clave privada. Las dos claves, pública y privada, están relacionadas matemáticamente, y éste es el motivo por el que habitualmente las claves no las elige los usuarios. La clave privada la debemos mantener en secreto, puesto que es la base de la seguridad futura. La clave pública, por el contrario, es ampliamente difundida por internet para que esté al alcance del mayor número de personas. (Queros, 2007)

Para el presente Trabajo de Grado las claves publicas generadas serán entregadas a los respectivos dueños de las embarcaciones, y la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante tendrá las claves privadas, la cual se utilizará en las inspecciones anuales que esta unidad realiza.

## **2.5.1 Ventajas**

La implementación de criptografía asimétrica trae consigo ventajas, debido al funcionamiento que esta tiene, entre las cuales podemos mencionar:

- Número de claves reducido, ya que cada individuo necesitará únicamente un par de claves.
- Computacionalmente es complicado encontrar la clave privada a partir de la llave pública.
- No es necesario transmitir la clave privada entre emisor y receptor.
- Permite autenticar a quien utilice la clave privada.

En el presente Trabajo de Grado, estas ventajas nos permitirán garantizar la integridad de la información, al momento de hacer seguimiento a las embarcaciones en las inspecciones anuales que se realizan por parte del personal asignado.

### **2.5.1.1 Método Wigginton**

“El método científico es un procedimiento para descubrir las condiciones en las que se presentan sucesos específicos, caracterizado generalmente por ser tentativo, verificable, de razonamiento riguroso y observación empírica.” (Tamayo, 2010)

Este es un método desarrollado por el Ingeniero Jim Wigginton entre los años 2007 hasta el año 2010, el cual pretende la elección de un algoritmo asimétrico dependiendo la necesidad prevista. El mismo colaboró con el desarrollo de distintos algoritmos de esta naturaleza incorporándolos en una librería compatible con el lenguaje PHP.

Este método consta de cuatro fases:

- A. Determinación del algoritmo a implementar: Se realiza un listado de algoritmos asimétricos los cuales pueden ser empleado, se toma en cuenta las características técnicas de cada uno de los mismos.
- B. Generar par de llaves: Debido a que se toman en cuenta algoritmos asimétricos se procede a realizar la generación de tanto la llave pública como la llave privada, describiendo el proceso por el cual las mismas son generadas.
- C. Identificación de información a encriptar: Se identifica cual ha de ser la información para encriptar, se realiza la identificación de esta y el impacto que podrían tener dentro del contexto actual.
- D. Generar código QR: Una vez terminado el proceso de encriptado de la información se procede a adjuntar la misma dentro de un código QR para después poder consultar esta.

Una vez concluidas las cuatro fases se tendrá una implementación de un algoritmo asimétrico dentro de un sistema web.

### **2.5.2 Algoritmo RSA**

RSA es el algoritmo más conocido y usado de los sistemas de clave pública, y también el más rápido de ellos. Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos.

RSA es una tecnología de cifrado de clave pública desarrollada por RSA Data Security. El cual basa su dificultad en la factorización números muy grandes. Según este principio, el algoritmo de cifrado RSA utiliza la factorización principal como la puerta trampa para el cifrado. Deducir una clave RSA, por lo tanto, requiere una gran cantidad de tiempo y poder de procesamiento. RSA es el método de cifrado estándar para datos importantes, especialmente datos que se transmiten a través de Internet.  
(Bagad, 2009)

RSA es un algoritmo de encriptación, utilizado para transmitir mensajes de forma segura a través de Internet. Se basa en el principio de que es fácil multiplicar números grandes, pero factorizar números grandes es muy difícil. Por ejemplo, es fácil comprobar que 31 y 37 se multiplican por 1147, pero tratar de encontrar los factores de 1147 es un proceso mucho más largo. Para el presente Trabajo de Grado se implementará el algoritmo RSA de modo que podamos generar tanto las claves públicas y privadas, que serán generados para los certificados de las embarcaciones. (Brillant, 2013 p.10)

### Desventajas

- La llave privada corre riesgo de ser perdida, inutilizando la llave pública
- El par de llaves es vulnerable si es que se realizan varios ataques si es que la implementación es pobre

### Ventajas

- Facilidad al momento de implementar debido a la compatibilidad con la mayoría de los dispositivos electrónicos.
- La encriptación tiene un tiempo mínimo a comparación del resto de los algoritmos asimétricos.
- Mayor soporte técnico en cuanto a documentación y mayor explicación, de modo que se tiene un mejor entendimiento de este.

#### **2.5.2.1 Funcionamiento del algoritmo**

A continuación, se explicará los pasos que sigue el algoritmo RSA para poder ser aplicado, desde el momento en que se generan las claves, hasta el proceso de verificación:

##### Generación de claves

- Se eligen dos números primos distintos p y q
- Se calcula  $n=p \cdot q$ .
- Con  $\varphi$  es la función  $\varphi$  de Euler calcula  $\varphi(n) = (p-1) \cdot (q-1)$ .
- Se escoge un entero positivo “e” menor que  $\varphi(n)-2$ , que sea coprimo con  $\varphi(n)$ .
- Se determina un d (mediante aritmética modular) que satisfaga la congruencia  $e \cdot d \equiv 1 \pmod{\varphi(n)}$ , es decir, que d sea el multiplicador modular inverso de e mod  $\varphi(n)$ .
- La clave pública es  $(n, e)$ , esto es, el módulo y el exponente de cifrado.
- La clave privada es  $(n, d)$ , esto es, el módulo y el exponente de descifrado, que debe mantenerse en secreto.

Cifrado de mensaje

- $C = [M(\text{mensaje})^e] \pmod{n}$

Descifrado de mensaje

- $M = [C^d] \pmod{n}$

### **2.5.2.2 Ejemplo**

A continuación, se demostrará un ejemplo básico del funcionamiento del algoritmo RSA. Para temas de demostración se tomarán números primos pequeños, con el valor de  $p=3$  y  $q=11$ , de modo que los cálculos a realizar no sean demasiado extensos y sean de fácil comprensión para el entendimiento y análisis. Finalmente se mostrará el proceso de desencriptación para comprobar el descifrado del mensaje como se observa en la Tabla 2.

**TABLA 2: EJEMPLO DE USO DE RSA**

Paso	Procedimiento	Descripción
1	$p=3; q=11$	Se escogen dos números primos
2	$n=3*11=33$	Se hace el cálculo de $n$ a través de la multiplicación de $p$ y $q$
3	$\varphi(n) = (p-1) * (q-1)$ $\varphi(33) = (3-1) * (10-1) = 20$	Se determina la función de Euler de $n$
4	$e=3$	Se escoge un valor coprimo a $\varphi(n)$
5	$d=7;$	Se determina mediante aritmética modular
6	clave pública $(n,e) = (33,3)$	Se generan los valores de la clave pública y se los transmite
7	clave privada $(n,e) = (33,7)$	Se genera los valores de la clave privada y se los almacena
8	mensaje =5	El mensaje que se desea transmitir
9	$C = (53) \text{ mod } 33 = 26$	Se procede a cifrar el mensaje, donde $c$ es el mensaje cifrado donde se hace uso de la clave publica
10	$M = 26^7 \text{ mod } 33 = 5$	Para poder de descifrar el mensaje original se hace uso de la clave privada, el cual como se puede observar coincide con el mensaje original.

**Fuente:** Elaboración propia

En la Tabla 2 se pudo observar un ejemplo del funcionamiento del algoritmo RSA, siguiendo todos los pasos que propone su teoría, además de su respectiva descripción.

### **2.5.3 Algoritmo DSA**

“El receptor de un mensaje puede utilizar el algoritmo de firma digital (DSA) para verificar que el mensaje no se haya alterado durante el tránsito y para determinar la identidad del remitente” (Instituto Nacional de Estándares y Tecnología, 1991).

DSA es uno de los muchos algoritmos que se utilizan para crear firmas digitales para la transmisión de datos. Se crea un par de números y se utiliza como firma digital. Permiten al receptor autenticar el origen del mensaje. La firma digital, creada mediante DSA, es privada en el punto de inicio de la transmisión de datos, mientras que termina en público. Esto significa que solo la persona que transmite los datos puede hacer la firma, que se agregará al mensaje, pero cualquiera puede autenticar la firma en el otro extremo.

### **2.5.4 Algoritmo DPH**

Primer algoritmo de clave pública, enunciado por W. Diffie y M. Hellman en 1976, que basa su seguridad en la dificultad de calcular logaritmos discretos en un campo finito. Se emplea para distribución de claves, pero no para cifrar y descifrar [CESID:1997].

El algoritmo de Diffie-Hellman permite acordar una clave secreta entre dos máquinas, a través de un canal inseguro y enviando únicamente dos mensajes. La clave secreta resultante no puede ser descubierta por un atacante, aunque éste obtenga los dos mensajes enviados por el protocolo. La principal aplicación de este protocolo es acordar una clave simétrica con la que posteriormente cifrar las comunicaciones entre dos máquinas.

Ventajas:

- Fácil de implementar.
- Dificultad de calcular los numeros discretos que se implementan.
- Permite el uso de curvas elípticas para mejorar la criptografía.

Desventajas:

- El procesamiento es muy pesado.
- Fácil de romper en términos de seguridad.
- Susceptible a ataques de “man in the middle”, por tanto si un tercer usuario se pone en medio de la conversación, también se le facilitaría las claves y por tanto, podría establecer comunicaciones con el emisor y el receptor suplantando las identidades.
- No proporciona autenticación.

## 2.6 METODOLOGÍA DE DESARROLLO

Una metodología de desarrollo de software brinda al equipo de trabajo un marco para construir aplicaciones de manera eficiente y rigurosa, garantizando un producto cercano al esperado. Si no se desarrolla a partir de una metodología, el resultado final será impredecible y no se podrá controlar el avance del proyecto.

“La metodología de desarrollo de software en ingeniería de software es un marco de trabajo usado para estructurar, planificar y controlar el proceso de desarrollo en sistemas de información” (Selectingdevelopmentapproach, 2019).

La metodología en el desarrollo de Software es un modo sistemático de realizar, gestionar y administrar un proyecto para de esta forma llevarlo a cabo con altas posibilidades de éxito. Esta clasificación nos indica como dividiremos un gran proyecto en módulos más pequeños llamados etapas, y las acciones que corresponden en cada una de ellas, nos ayuda a definir

entradas y salidas para cada una de las etapas y, sobre todo, normaliza el modo en que administraremos el proyecto. (Vargas, 2019)

Para el actual Trabajo de Grado se empleará una metodología de desarrollo de modo que se establezca un marco de trabajo, el cual nos permita planificar y gestionar el proyecto, controlando el proceso de desarrollo. El sistema se clasificará en módulos, de modo que se realicen las acciones correspondientes dependiendo de lo que se proponga desarrollar.

### **2.6.1 Técnicas de Recolección de Datos**

La recolección de Datos se refiere al uso de una gran diversidad de técnicas y herramientas que pueden ser utilizadas por el analista para desarrollar los sistemas de información, los cuales pueden ser la entrevistas, la encuesta, el cuestionario, la observación, el diagrama de flujo y el diccionario de datos. Todos estos instrumentos se aplicarán en un momento en particular, con la finalidad de buscar información que será útil a una investigación en común.

#### **2.6.1.1 Entrevistas**

La entrevista es una de las técnicas más comunes y es considerada como la relación directa entre el entrevistado y el objeto de estudio a través de individuos o grupos con el fin de obtener testimonios reales" (Hernandez,2009).

Una entrevista es un diálogo que se establece entre dos personas en el que una de ellas propone una serie de preguntas a la otra a partir de un guion previo. Se realiza con el fin de que el público pueda conocer la información de su persona, de su experiencia o conocimientos.

Sus ventajas son:

- Es adaptable y libre logrando un clima ameno que habilita la profundización sobre los temas de interés.
- Permite la repregunta si el entrevistado mencionó algún tema de interés.

Entre sus desventajas se tiene:

- Como los temas suelen expandirse, es más costosa de realizar por el tiempo empleado por parte del entrevistador.
- Se requiere una gran técnica e información en el tema a tratar para poder tener argumentos y opiniones que permitan profundizar y dialogar.

### **2.6.2 Metodología Ágil**

Existen marcadas diferencias entre una metodología ágil y una metodología tradicional, como se muestra en la Tabla 3.

**TABLA 3: COMPARACIÓN DE METODOLOGÍA**

Tradicional	Ágil
<ul style="list-style-type: none"> <li>• Orientados al proceso (funciona en cualquier equipo)</li> <li>• Modelo de desarrollo cascada</li> <li>• Se prioriza en base a la visión propia, no la del equipo</li> <li>• Es más caro</li> <li>• Se desarrollan cosas que no son necesarias</li> <li>• Documentación y detalle exhaustivo</li> <li>• Control descentralizado</li> </ul>	<ul style="list-style-type: none"> <li>• Orientado a las personas</li> <li>• Entregas incrementales e integración continua</li> <li>• Coste en base a valor para el cliente</li> <li>• Se prioriza en base a las necesidades del cliente</li> <li>• Costes ajustados</li> <li>• Simplicidad</li> <li>• Funcionalidad y utilidad</li> <li>• Autoorganización</li> </ul>

**Fuente:** Elaboración propia

Como se pudo observar en la Tabla 3 se puede observar las diferencias que existe entre las características que poseen las metodologías tradicionales y las metodologías agiles, las cuales serán empleadas en el presente Trabajo de Grado.

Las primeras metodologías agiles surgen de la búsqueda de mejorar procesos de desarrollo de software. Este tipo de metodología trabaja con tres valores fundamentales:

- Respuesta al cambio y capacidad de intervención: Promueve un comportamiento inmediato cuando se trata de corregir acciones, fallos o inconvenientes, incluso se trata sobre realizar mejoras. Su esencia es el cambio oportuno, la cual puede ser medida al final de cada etapa o fase. Colaboración directa con el cliente: Un contrato no puede evaluar la calidad de un producto; sí lo puede hacer la interacción directa con quienes son los principales beneficiarios de cada proceso.
- Preocupación por los integrantes de los equipos: El carácter de un producto es el resultado de una serie de acciones ejecutadas por equipos de trabajo.
- Mejores estrategias de acción: Toma de decisiones basadas en una retroalimentación constante entre los miembros que hacen parte del proyecto. La documentación es necesaria, pero no indispensable. De hecho, el acento debe ponerse en la elección de una buena herramienta (software) que satisfaga las necesidades del proyecto.

En base a las diferencias y valores revisados, se empleará la metodóloga ágil Design Sprint, debido a los beneficios que esta nos brinda: obtener comentarios de los usuarios antes de implementar el proyecto asegurando de esta manera la correcta definición del funcionamiento, permite la creación de un prototipo de la idea seleccionada y preparación para la prueba y por último ayuda a hacer un uso óptimo de los recursos: tiempo, personas y esfuerzos.

Tomando en cuenta las ventajas previamente mencionadas se hará uso de dicha metodología de manera que se pueda desarrollar el software en un menor tiempo, tomando en cuenta que se realizaran cambios, se tendrá una interacción directa con el cliente y se hará hincapié en el desarrollo de un software funcional e integral.

#### **2.6.2.1 RUP**

“El Proceso Unificado de Rational o RUP es un proceso de desarrollo de software desarrollado por la empresa Rational Software” (IBM,2003).

Es un proceso adaptable marco, destinado a ser adaptado por las organizaciones de desarrollo y equipos de proyectos de software que seleccionará a los elementos del proceso que son apropiados para sus necesidades. RUP es una implementación específica del proceso unificado.

Principales Características:

- Desarrollo iterativo.
- Forma disciplinada de asignar tareas y responsabilidades.
- Pretende implementar las mejores prácticas en Ingeniería de Software.
- Control de cambios.
- Modelado visual del software.

#### **2.6.2.2 Extreme Programming (XP)**

La programación extrema o Extreme Programming (XP) es una metodología de desarrollo de la ingeniería de software formulada por Kent Beck, autor del primer libro sobre la materia, *Extreme Programming Explained Embrace Change*, siendo el más destacado de los procesos ágiles de desarrollo de software se dice que “al igual que éstos, la programación extrema se diferencia de las metodologías tradicionales principalmente porque pone más énfasis en la adaptabilidad que en la previsibilidad; dentro la programación extrema” (Beck,1999).

Entre sus principales características se puede mencionar:

- Desarrollo iterativo e incremental: pequeñas mejoras, unas tras otras.
- Pruebas unitarias continuas,
- Programación en parejas
- Propiedad del código compartida
- Simplicidad en el código

#### **2.6.2.3 Metodología Design Sprint**

La metodología Design Sprint, tiene como objetivo según (Knapp, 2016), de “responder algunas de las preguntas críticas para el desarrollo de producto a través del diseño, creación de prototipos y pruebas de cliente utilizando el Design Thinking como estrategia para la reducción de riesgos”.

Los Design Sprint lo que intentan es concentrar una colección de buenas prácticas de Design Thinking, estrategia de negocios, innovación, análisis de comportamiento y otras, tratando de empaquetarlas en un proceso que cualquier equipo pudiera utilizar.

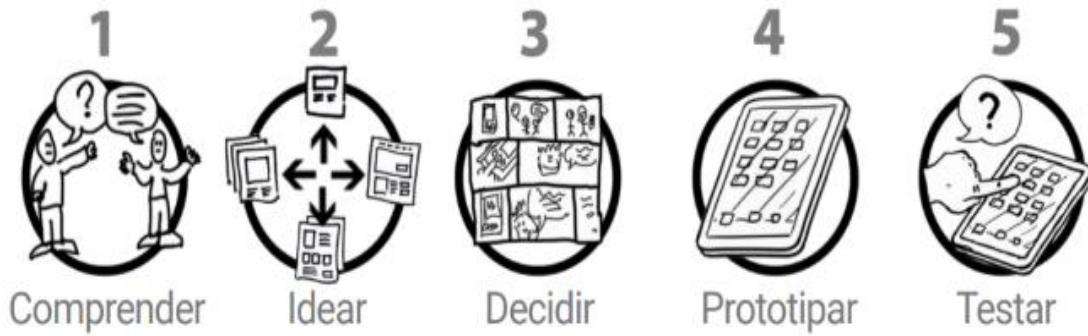
Se busca el trabajo con equipos multidisciplinarios (integrados generalmente por el dueño del producto y sus colaboradores en la construcción) se acote el ciclo de maduración de un producto a una semana para no tener que esperar al final de un costoso ciclo de desarrollo para entender si una solución es buena idea o no. En tal sentido, la idea es proporcionar una visión rápida del producto terminado teniendo en cuenta las necesidades de los clientes.

#### 2.6.2.4 Fases

La metodología Design Sprint según (Knapp, 2016), “cuenta con cinco fases según lo establecido, las cuales nos ayudaran a realizar el desarrollo de nuestro software”:

Esta metodología de desarrollo ágil se divide en cuatro fases, como se observa en la Figura 5.

**FIGURA 5: FASES DESIGN SPRINT**



**Fuente:** <https://theherocamp.com/product-lab/que-es-fases-sprint-design/>

En la Figura 5 se puede observar las fases de esta metodología, las mismas serán detalladas a continuación y posteriormente se detalla los entregables que se tiene en cada una de las fases.

- A. Entendimiento: En esta fase se explora el problema empresarial desde todos los ángulos posibles con el objetivo de establecer una base de conocimiento compartido. Se busca descubrir las oportunidades de negocio, el público, las competencias, las propuestas de valor y definir las métricas del éxito.
- B. Propuestas: Se comienzan a explorar, desarrollar e iterar sobre algunas formas creativas de resolver el problema independientemente de su viabilidad. Estas propuestas se trabajan individualmente (o en equipos pequeños) para plasmar

soluciones con el máximo detalle y profundidad a través de notas, mapas mentales o storyboards.

- C. Decidir: Se identifican las propuestas generadas en la fase anterior que tienen más oportunidad de lograr los objetivos propuestos. En tal sentido, tras criticar cada escenario se genera un plan dentro de un storyboard donde se intentará plasmar un plan paso a paso.
- D. Prototipado: Se diseñan y preparan prototipos que puedan probarse por personas que ajusten con los perfiles definidos en el storyboard definido en la fase anterior. En esta fase también se vela porque todo esté listo para la prueba del viernes confirmando el cronograma, revisando el prototipo y escribiendo un guion para las entrevistas.
- E. Prueba: Se realizan las validaciones pertinentes con el grupo de usuarios seleccionados como público objetivo para evaluar sus reacciones y posibles cambios. Estas pruebas hacen que todo el sprint valga la pena: al final del día se sabrá qué tan lejos se tiene que ir y qué hacer a continuación.

#### **2.6.2.5 Entregables**

Los entregables son productos que, en un cierto estado, se intercambian entre los clientes y los desarrolladores a lo largo de la ejecución del proyecto informático.

Según “Sprint”, libro escrito por Jake Knab, en el año 2016, creador de Design Sprint se puede tener los siguientes entregables, en la Tabla 4 se pueden observar los nombres y sus respectivas descripciones de estos en cada una de las fases que esta metodología propone.

**TABLA 4: DESCRIPCIÓN DE ENTREGABLES**

Fase	Entregable	Descripción
Entender	Entrevistas	Intercambio de ideas, opiniones mediante una conversación que se da entre una, dos o más personas donde un entrevistador es el designado para preguntar.
	Notas HMW	Notas adhesivas que contiene preguntas de cómo podríamos solucionar los distintos problemas que identificamos
	Mapa de ciclo de vida del cliente	Representación visual del recorrido que debe realizar un cliente para adquirir un producto o servicio, muestra las interacciones con la compañía, logrando visualizar cómo el cliente percibe su relación con la empresa, identificando metas, objetivos y actividades que realiza en su trayecto.
	Mapa de proyecto	Esquema gráfico, de tipo mapa mental que permite en forma muy rápida tener una mirada completa/global del proyecto
Propuestas	Boot up Notetaking	Diseño de bocetos que prepara al equipo para Crazy 8
	Crazy 8s	Ejercicio de dividir una hoja en ocho y generar ocho variantes de una idea del Boot up Notetaking
Decidir	Dot voting	Los participantes votan sobre sus opciones elegidas usando un número limitado de calcomanías o marcas con bolígrafos, siendo las calcomanías de puntos
	Heat map voting	Mapa que indica las características que son deseables de la elección realizada en el proceso anterior.
	Prototipos	Modelo que sirve como representación o simulación del producto final y que nos permite verificar el diseño y confirmar que cuenta con las características específicas planteadas
	Mock	Notación para prueba unitaria, como se observa en la Figura 6
Pruebas	Test de usabilidad	Técnica usada en el diseño de interacciones centrado en el usuario para evaluar un producto mediante pruebas con los usuarios mismos.

**Fuente:** Design, 2017, p. 20.

## FIGURA 6: PRUEBA UNITARIA

```
→ PayPalTesting git:(master) ✘ phpunit --testdox
PHPUnit 6.4.4 by Sebastian Bergmann and contributors.

s\Feature\PayPalController
[x] Get redirect link
[x] Mark payment approved and redirect
[x] Handle when payment fails

→ PayPalTesting git:(master) ✘ phpunit
PHPUnit 6.4.4 by Sebastian Bergmann and contributors.

...
3 / 3 (100%)

Time: 291 ms, Memory: 18.00MB

OK (3 tests, 9 assertions)
```

Fuente: PHP Unit Laravel

En la Figura 6 se observa el resultado de una prueba unitaria realizada con el framework Laravel, el cual analiza y realiza pruebas del código escrito en el mismo. Una vez finalizada la prueba esta muestra la cantidad errores que se hayan encontrado, esto dependiendo del número de archivos analizados, caso contrario el mensaje indica un 100% de efectividad.

En el actual Trabajo de Grado se utilizarán estos entregables, los cuales nos permitirá medir y verificar el desarrollo de la plataforma web. Al mismo tiempo estos nos ayudarán a comprobar el avance del trabajo en el proyecto para ser monitoreado.

## CAPÍTULO III

# MARCO PRÁCTICO



## **CAPÍTULO III**

### **MARCO PRÁCTICO**

El desarrollo del marco práctico del siguiente Trabajo de Grado se llevará a cabo como se muestra en la Tabla 5, basándose en la Metodología Design Sprint, asignando las etapas correspondientes a las actividades a realizar.

**TABLA 5: DESARROLLO DEL MARCO PRÁCTICO**

Temario	Objetivo secundario	Tareas	Fases	Entregables
3.1 Análisis de situación actual	Centralizar la información obtenida acerca de las embarcaciones registradas.	3.1.1 Contexto de la organización	Entrevistas	
		3.1.2 Identificación del personal		Organigrama de la unidad
		3.1.3 Consultas de información		Recopilación de documentos
		3.1.4 Análisis de procesos		Descripción de cada proceso
				Flujogramas
		3.1.5 Determinación de Requerimientos del Sistema		Diagrama de caso de uso de alto nivel
				Tabla de requerimientos
		3.1.6 Definición de módulos del Sistema		Notas HMW

Método Wigginton				
3.2 Implementación del algoritmo asimétrico	Implementación de algoritmo asimétrico para la emisión de certificados	3.2.1 Determinación de Algoritmo a Implementar	Elección de algoritmo	Tabla comparativa de algoritmos asimétricos
				Dot Voting
Temario	Objetivo secundario	Tareas	Fases	Entregables
3.2 Implementación del algoritmo asimétrico	Implementación de algoritmo asimétrico para la emisión de certificados	3.2.2 Generar par de llaves	Generación de llaves	Generación de números primos aleatoriamente
			Definir el mensaje a encriptar	Cálculo de parámetro “n”, función de “φ (n)”, “d” y “e”.
			Cargar la llave privada Cargar la llave publica Desencriptar	Obtención de llave privada y llave pública
		3.2.3 Identificación de información a encriptar	Encriptar el mensaje	Definición del proceso de gestión de llaves
				Revisión de reglamentos
				Flujogramas
		3.2.4 Generar código QR	Generar código QR	Identificación del tamaño del código
				Determinación de la calidad del código
				Determinación de contenido del código QR
				Generación del código QR

DESIGN SPRINT				
3.3 Desarrollo del sistema	Proporcionar al personal a cargo de las inspecciones información detallada de cada embarcación mediante una plataforma web	3.3.1 Sprint 1 Módulo de Gestión de Usuarios		
		3.3.1.1 Lista de requerimientos	Entendimiento • Saber quién es el usuario y cuáles son sus necesidades. • Conocer el contexto de la organización y del producto	Tabla de requerimientos del módulo  Diagrama entidad relación
Temario	Objetivo secundario	Tareas	Fases	Entregables
3.3 Desarrollo del sistema	Proporcionar al personal a cargo de las inspecciones información detallada de cada embarcación mediante una plataforma web	3.3.1.2 Especificación del proceso	Propuestas • Plantear ideas sin importar la calidad	Diagramas de caso de uso expandido  Diagrama de clases
		3.3.1.3 Diseño de procesos	Decidir • Tomar decisiones apoyándose en las conclusiones y la información recabada en las fases anteriores.	Modelo relacional de la base de datos  Diagrama de actividades
		3.3.1.4 Diseño de interfaces	Storyboard sprint 1	Storyboard sprint 1
		3.3.1.5 Diseño navegacional		Diagrama de componentes
		3.3.1.6 Construcción de interfaces		Pantallas
		3.3.1.7 Código		Codificación del modulo

Temario	Objetivo secundario	Tareas	Fases	Entregables
3.3 Desarrollo del sistema	Proporcionar al personal a cargo de las inspecciones información detallada de cada embarcación mediante una plataforma web	3.3.1.8 Prueba unitaria	Pruebas	Prueba Mock
<b>3.3.2 Sprint 2</b> <b>Módulo de Registro de Embarcaciones</b>				
		3.3.2.1 Lista de requerimientos	Entendimiento •Saber quién es el usuario y cuáles son sus necesidades. •Conocer el contexto de la organización y del producto	Tabla de requerimientos del módulo
		3.3.2.2 Especificación del proceso	Propuestas •Plantear ideas sin importar la calidad	Diagrama entidad relación Diagrama de clases Diagramas de caso de uso expandido
		3.3.2.3 Diseño de procesos	Decidir •Tomar decisiones apoyándose en las conclusiones y la información recabada en las fases anteriores.	Diagramas de caso de uso expandido Diagrama de clases Storyboard sprint 2
		3.3.2.4 Diseño de interfaces		
		3.3.2.5 Diseño navegacional	Prototipo •Definir el tipo de usuario que interactuará con cada módulo	Diagrama de componentes
		3.3.2.6 Construcción de interfaces	•Definir específicamente cual será la interacción de cada módulo del sistema	Pantallas
		3.3.2.7 Código		Codificación del modulo
		3.3.2.8 Prueba unitaria	Pruebas	Prueba Mock

Temario	Objetivo secundario	Tareas	Fases	Entregables
3.3 Desarrollo del sistema	Proporcionar al personal a cargo de las inspecciones información detallada de cada embarcación mediante una plataforma web	3.3.3 Sprint 3 Módulo de Inspección de Embarcaciones		
		3.3.3.1 Lista de requerimientos	Entendimiento •Saber quién es el usuario y cuáles son sus necesidades. •Conocer el contexto de la organización y del producto	Tabla de requerimientos del módulo  Diagrama entidad relación
		3.3.3.2 Especificación del proceso	Propuestas •Plantear ideas sin importar la calidad	Diagramas de caso de uso expandido  Diagrama de clases
		3.3.3.3 Diseño de procesos	Decidir •Tomar decisiones apoyándose en las conclusiones y la información recabada en las fases anteriores.	Modelo relacional de la base de datos  Diagrama de actividades  Storyboard sprint 3
		3.3.3.4 Diseño de interfaces		
		3.3.3.5 Diseño navegacional	Prototipo •Definir el tipo de usuario que interactuará con cada módulo	Diagrama de componentes
		3.3.3.6 Construcción de interfaces	•Definir específicamente cual será la interacción de cada módulo del sistema	Pantallas
		3.3.3.7 Código		Codificación del modulo
		3.3.3.8 Prueba unitaria	Pruebas	Prueba Mock

Temario	Objetivo secundario	Tareas	Fases	Entregables
3.3 Desarrollo del sistema	Proporcionar al personal a cargo de las inspecciones información detallada de cada embarcación mediante una plataforma web	3.3.4 Sprint 4 Módulo de Verificación de Documentos		
	3.3.4.1 Lista de requerimientos	Entendimiento • Saber quién es el usuario y cuáles son sus necesidades. • Conocer el contexto de la organización y del producto	Tabla de requerimientos del módulo	
	3.3.4.2 Especificación del proceso	Propuestas • Plantear ideas sin importar la calidad	Diagrama entidad relación	Diagramas de caso de uso expandido
	3.3.4.3 Diseño de procesos	Decidir • Tomar decisiones apoyándose en las conclusiones y la información recabada en las fases anteriores.	Diagrama de clases	Diagrama de actividades
	3.3.4.4 Diseño de interfaces	Prototipo • Definir el tipo de usuario que interactuará con cada módulo • Definir específicamente cual será la interacción de cada módulo del sistema	Storyboard sprint 4	Modelo relacional de base de datos
	3.3.4.5 Diseño navegacional			Diagrama de componentes
	3.3.4.6 Construcción de interfaces		Pantallas	
	3.3.4.7 Código		Codificación del modulo	
	3.3.4.8 Prueba unitaria	Pruebas	Prueba Mock	

Temario	Objetivo secundario	Tareas	Fases	Entregables
3.3 Desarrollo del sistema	Proporcionar al personal a cargo de las inspecciones información detallada de cada embarcación mediante una plataforma web	3.3.5 Sprint 5 Módulo de Reportes		
		3.3.5.1 Lista de requerimientos	Entendimiento •Saber quién es el usuario y cuáles son sus necesidades. Conocer el contexto de la organización y del producto	Tabla de requerimientos del módulo  Diagrama entidad relación
		3.3.5.2 Especificación del proceso	Propuestas •Plantear ideas sin importar la calidad	Diagramas de caso de uso expandido
		3.3.5.3 Diseño de procesos	Decidir •Tomar decisiones apoyándose en conclusiones e información recabada	Diagrama de actividades  Storyboard sprint 5
		3.3.5.4 Diseño de interfaces		
		3.3.5.5 Diseño navegacional	Prototipo •Definir el tipo de usuario que interactuará con cada módulo	Diagrama de componentes  Pantallas
		3.3.5.6 Construcción de interfaces	•Definir específicamente cual será la interacción de cada módulo del sistema	
		3.3.5.7 Código		Codificación del modulo
		3.3.5.8 Prueba unitaria	Pruebas	Prueba Mock
3.4 Pruebas del sistema		3.4.1 Prueba de integración	Test de usabilidad	
				Pruebas Mocha

Temario	Objetivo secundario	Tareas	Fases	Entregables
3.5 Implementación del sistema		3.5.1 Instalación del sistema	Manual de usuario del administrador Configuración de servidor	
		3.5.2 Revisión de funcionamiento	Reportes de funcionalidad del sistema a la Unidad de Marina Mercante	

**Fuente:** Elaboración propia

### 3.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

Se hará un análisis de la situación actual, tomando en cuenta el contexto de la organización, los procesos que se tienen, aquellas personas que están involucradas en los mismos y se recopilará la información para proceder al desarrollo del sistema.

#### 3.1.1 Contexto de la organización

La Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante es una unidad de las Fuerzas Armadas, creada con el objetivo de promover la seguridad y el desarrollo naviero, mercante, marítimo, fluvial y lacustre, acorde a los convenios internacionales vigentes.

La misma es dependiente del Viceministerio de Defensa a la cual envía informes del seguimiento y control que se realizan a las embarcaciones a nivel nacional, mediante los procesos de registro e inspección, procesos normados bajo “REGLAMENTO NACIONAL DE REGISTRO DE BUQUES, EMBARCACIONES Y ARTEFACTOS NAVALES” y “REGLAMENTO NACIONAL DE INSPECCIONES TÉCNICA DE BUQUES, EMBARCACIONES Y ARTEFACTOS NAVALES”, como se observa en el Anexo H.

Esta unidad actualmente no dispone de algún sistema el cual le facilite la realización de los distintos procesos, situación por la cual manejan toda la documentación de

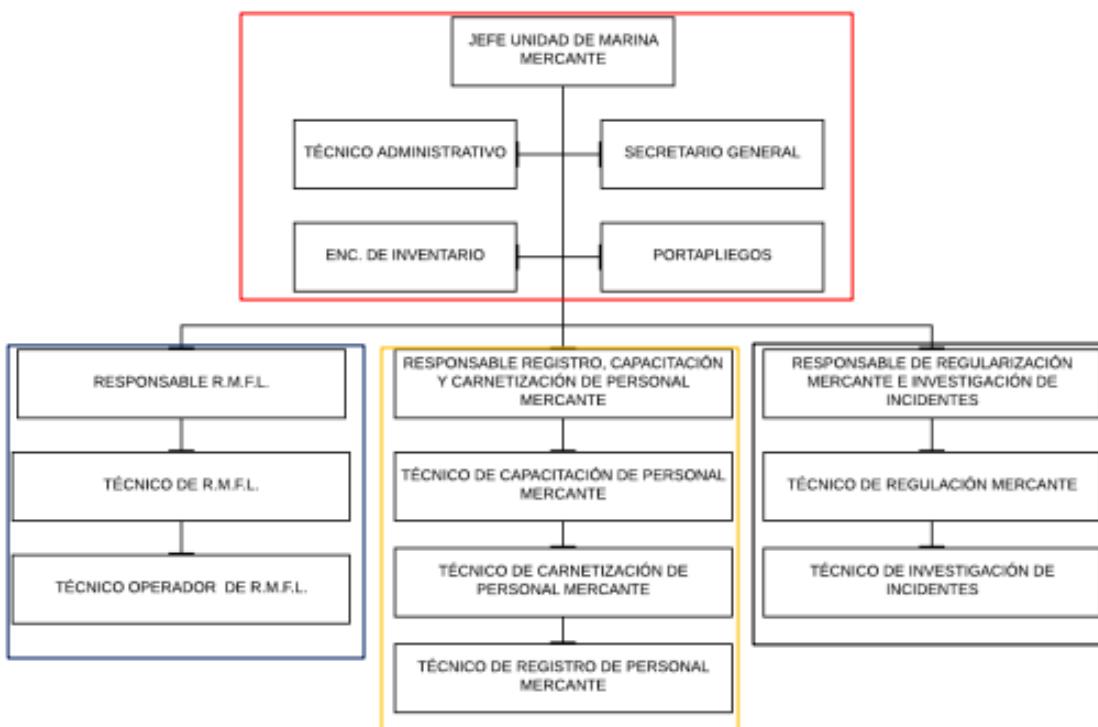
manera física e incluso usan algunas herramientas ofimáticas para poder almacenar datos relevantes de las distintas embarcaciones.

Teniendo como requerimientos, la centralización de información de todas las embarcaciones, registrar usuarios los cuales puedan, y por último la generación automática de certificados de registro y de seguridad de la navegación.

### 3.1.2 Identificación del personal

El personal que trabaja en esta unidad está a cargo del jefe de la Unidad de Marina Mercante, teniendo debajo el Técnico administrativo, Secretario general, Portapliegos y Encargado de Inventario y como tercer nivel se tiene una mayor variedad de técnicos los cuales tiene funciones más de soporte. Dicha organización se puede observar en la Figura 7.

**FIGURA 7: ORGANIGRAMA DEL PERSONAL DE DGIMFLMM**



Fuente: DGIMFLMM

En la Figura 7, se puede observar la jerarquía de la organización, se muestra el puesto que cada uno ocupa y las dependencias que existen, las tareas que cada uno de estos realiza se detalla en el Anexo I. Para aquellas personas que están remarcadas con el color rojo son las que tendrán acceso a la parte de reportes, las remarcadas con color azul, serán las encargadas de realizar las inspecciones y registros a las embarcaciones y por último, las de color amarillo estarán encargadas de la gestión de usuarios.

### **3.1.3 Consulta de información**

Este proceso hace referencia a la consulta de información acerca de las embarcaciones, por parte de los dueños de estas y de Unidades de las Fuerzas Armadas. Un punto importante para mencionar es que la información se encuentra centralizada solamente en la Unidad de Marina Mercante.

Actualmente este cuenta con grandes deficiencias, esto debido a que la mayor parte de la información está almacenada en medios físicos (carpetas, folders) en la Dirección General de Intereses Marítimos, Fluviales, Lacustres y Marina Mercante. Para fines de agilizar el proceso de consultas, el trabajo se realiza con herramientas ofimáticas (Excel), las cuales tienen registrados solamente algunos datos de las distintas embarcaciones, e incluso se tiene diferentes versiones.

Debido a estas razones, las Unidades de las Fuerzas Armadas no pueden realizar consultas de datos en cualquier momento, sino deben de mandar un requerimiento de los mismos a la Unidad donde se encuentran almacenados. Este proceso tiene una duración aproximada de dos días:

- Primer día: se analiza la solicitud, si esta es aprobada se procede a realizar la búsqueda de la carpeta correspondiente a la embarcación.
- Segundo día: se hace entrega de todos los datos encontrados.

El presente Trabajo de Grado plantea centralizar la información que se tiene de gestiones pasadas y almacenar la información técnica de las embarcaciones en una base de datos, posterior a eso se irá completando los certificados y fotografías correspondientes a cada una. Para este proceso se recolectó todos los datos de los medios ofimáticos, posterior a eso se parametrizaron los mismos, esto con el objetivo de realizar un cargado masivo de aquellas embarcaciones de las cuales se tenía plenitud de información.

### **3.1.4 Análisis de procesos**

Se pudieron identificar dos procesos fundamentales, los cuales son: el registro de embarcaciones y las inspecciones anuales a nivel nacional.

#### **3.1.4.1 Registro de embarcaciones**

El proceso de registro de embarcaciones surge a partir de la necesidad de tener un control de la cantidad de las mismas que navegan en los distintos escenarios acuáticos a nivel nacional, centralizar la información de las mismas para que se puedan hacer consultas en cualquier momento y de implementación de normas de seguridad digitales que respalden la información obtenida.

El mismo comienza cuando se presenta una solicitud para registrar la misma al Ministerio de Defensa. Actualmente existen cuatro tipos de registro, como se observa en el Anexo J, teniendo cada uno diferentes requisitos, los cuales son descriptos a continuación:

Registro provisional: Es la inscripción de un buque, embarcación y artefacto naval en el ámbito Marítimo y la Hidrovia Paraguay - Paraná, registrado en la Unidad de Marina Mercante, por un periodo de un año, hasta que el armador y/o propietario cumpla con los siguientes requisitos:

- a) Solicitud de cotización en base a las características técnicas del buque, embarcación o artefacto naval.
- b) Solicitud de Registro, dirigida a la Autoridad Marítima.
- c) Adjuntar los siguientes requisitos que debe cumplir el interesado:
  - Fotocopia de compra y venta (Bill of sale). Notariado y legalizado en el Consulado Boliviano.
  - Para los buques, embarcaciones o artefactos navales nuevos, título de propiedad y certificado del Constructor.
  - Fotocopia de cese de bandera anterior o documento que certifique que está en trámite. notariado y legalizado en el Consulado Boliviano.
  - Fotocopias de los certificados estatutarios y de registro de la bandera anterior. Notariado y legalizado en el Consulado Boliviano.

Registro permanente: Es la inscripción de un buque, embarcación y artefacto naval en el ámbito marítimo y la Hidrovia Paraguay - Paraná, registrado en la Unidad de Marina Mercante, por un periodo de cinco años, el mismo que puede ser renovado por un nuevo periodo, una vez cumplido con los siguientes requisitos:

- a) Solicitud de cotización en base a las características técnicas del buque, embarcación o artefacto naval.
- b) Solicitud de Registro dirigida a la Autoridad Marítima.
- c) Adjuntar los siguientes requisitos que debe cumplir el interesado:
  - Documento original de compra y venta (Bill of sale). Notariado y Legalizado en el Consulado Boliviano.
  - Certificado original del Cese de Bandera anterior. Notariado y legalizado en el Consulado Boliviano.
  - Certificados Estatutarios y de Registro de la bandera anterior. Notariado y legalizado en el Consulado Boliviano.
  - Certificado libre de hipoteca y gravamen

Registro especial. - Es una modalidad de inscripción de un buque, embarcación y artefacto naval en el ámbito marítimo y la Hidrovía Paraguay - Paraná, registrado en la Unidad de Marina Mercante, por un periodo máximo de tres meses, no autorizado para actividades comerciales, pudiendo ser empleado para realizar un viaje de entrega, de prueba o para desguace.

- a) Solicitud de cotización en base a las características técnicas del buque, embarcación o artefacto naval.
- b) Solicitud de Registro, dirigida a la Autoridad Marítima.
- c) Adjuntar los siguientes requisitos que debe cumplir el interesado:
  - Fotocopia legalizada de compra y venta (Bill of sale).
  - Buques, embarcaciones o artefactos navales nuevos, fotocopia legalizada del título de propiedad y certificado del constructor.
  - Fotocopia de Cese de Bandera anterior o documento que certifique que está en trámite. Notariado y legalizado en el Consulado Boliviano.
  - Fotocopias de los Certificados Estatutarios y de Registro de la bandera anterior.
  - Fotocopia legalizada del Poder Notariado. (Representante legal con domicilio en Bolivia).

Registro Dual. - Es una modalidad de registro de un buque, Embarcación y artefacto naval en la Unidad de Marina Mercante, que ya está registrada en otro país, por el periodo que dure el contrato de fletamiento. Se puede dar dos casos:

Cuando Bolivia es segunda bandera, y solicitan un registro dual en nuestro país, se inscribirá al buque, embarcación o artefacto naval por el tiempo que dure el un contrato de fletamiento, si es que cumple con los siguientes requerimientos:

- a) Solicitud de cotización en base a las características técnicas del buque, embarcación o artefacto naval.
- b) Solicitud de Registro, dirigida a la Autoridad Marítima.
- c) Adjuntar los siguientes requisitos que debe cumplir el interesado.

- Fotocopia del Contrato de Fletamiento. Notariado y legalizado en el Consulado Boliviano.
- Fotocopia u Original de Cese de Bandera anterior o documento que certifique que está en trámite. Notariado y legalizado en el Consulado Boliviano.
- Original de Poder de abogado (Representante legal con domicilio en Bolivia).
- Fotocopias de los Certificados Estatutarios y de Registro de la bandera anterior. Notariado y Legalizado en el Consulado Boliviano.

Cuando Bolivia es primera bandera, y solicitan un registro dual para otro país, se entregará un certificado o permiso para el registro, durante el tiempo que dure el contrato de fletamiento, si es que cumple con los siguientes requerimientos:

- a) Solicitud de cotización en base a las características técnicas del buque, embarcación o artefacto naval.
- b) Solicitud de Registro, dirigida a la Autoridad Marítima.
- c) Adjuntar los siguientes requisitos que debe cumplir el interesado:
  - Carta de aceptación para buque registrado en Bolivia, con contrato de fletamiento.
  - Original del contrato de fletamiento. Notariado y legalizado en el Consulado Boliviano.
  - Original de Cese de Bandera anterior o documento que certifique que está en trámite. Notariado y legalizado en el Consulado Boliviano.
  - Original de Poder de abogado (Representante legal con domicilio en Bolivia).
  - Fotocopias de los Certificados Estatutarios y de Registro de la bandera anterior. Notariado y legalizado en el Consulado Boliviano.

### **3.1.4.2 Inspección de embarcaciones**

El proceso inspección surge de la necesidad de dar seguimiento a todas las embarcaciones que navegan en los distintos escenarios acuáticos a nivel nacional y automatizar la generación de listas de inspección que se tienen.

La Dirección General de Intereses Marítimos, Fluviales, Lacustres y Marina Mercante, establecerá las condiciones y requisitos a que se sujetarán los propietarios o armadores de buques, embarcaciones y artefactos navales, establecidos en “Reglamento nacional para la construcción de embarcaciones y artefactos navales”, designando a la Unidad de Marina Mercante como la encargada de su cumplimiento, como se observa en el Anexo K.

Las reglas de inspección se efectuarán de acuerdo con el tonelaje, la naturaleza, la finalidad de los servicios y la navegación a efectuarse, donde se establecerán las exigencias técnicas y administrativas a que tienen que ajustarse en la construcción, modificación o reparación de buques o artefactos navales, como se observa en el Anexo L cumpliendo con las exigencias recomendadas por la Organización Marítima Internacional (OMI), el Acuerdo de la Hidrovia Paraguay-Paraná y el presente reglamento. A continuación, se detallan los dos tipos de inspecciones existentes.

**Inspección ordinaria.** - Es la que se realiza en forma anual por parte de la Unidad de Marina Mercante, referida a la verificación de las condiciones de seguridad del casco, máquina, superestructura y radio comunicaciones, conforme a cronograma de actividades del Plan Operativo Anual.

**Inspección extraordinaria.** - Son las realizadas fuera de los plazos y/o lugares determinados por la Unidad de Marina Mercante, con cargo al armador o propietario del buque, embarcación o artefacto naval, debiendo cumplir con lo siguiente:

- Solicitud escrita dirigida al Jefe de la Unidad de Marina Mercante, especificando los motivos del requerimiento de Inspección.
- Cumplir con el pago de pasajes y viáticos del personal técnico.
- La inspección técnica se realizará en el área de operación de la embarcación

Una vez terminada la inspección se llena un formulario, el cual refleje la presentación de los requerimientos previamente establecidos, obteniendo un porcentaje de cumplimiento. Si es que el resultado se encuentra entre 90%-100%, la embarcación puede realizar sus actividades con normalidad ya que su funcionamiento es óptimo. En el caso de que se obtenga un 70%-89%, la misma puede navegar, pero no cuenta con algunos documentos, los cuales se deben regular en el plazo de una semana. Finalmente, si este es menor al 70%, esta no podrá realizar ningún movimiento, ya que es susceptible a fallos, poniendo así en riesgo la seguridad de la tripulación, como se observa en la Tabla 6.

**TABLA 6: COMPARACIÓN INSPECCIONES DE EMBARCACIONES**

Porcentaje	Entrada	Proceso	Salida
>70%	Documentos de revisión	Elaboración de informe correspondiente y registro de resultado	Funcional
70%-89%		Anotación de observaciones correspondiente y registro de resultado	Funcional
90%-100%		Registro de resultado	Funcional

**Fuente:** Elaboración propia

### 3.1.5 Determinación de Requerimientos del Sistema

Para realizar la determinación de requerimientos se tuvo reuniones con el personal de la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, en el cual se analizaron las necesidades que esta tiene, obteniendo como resultado una tabla de requerimientos, como se observa en la Tabla 7.

**TABLA 7: TABLA DE REQUERIMIENTOS**

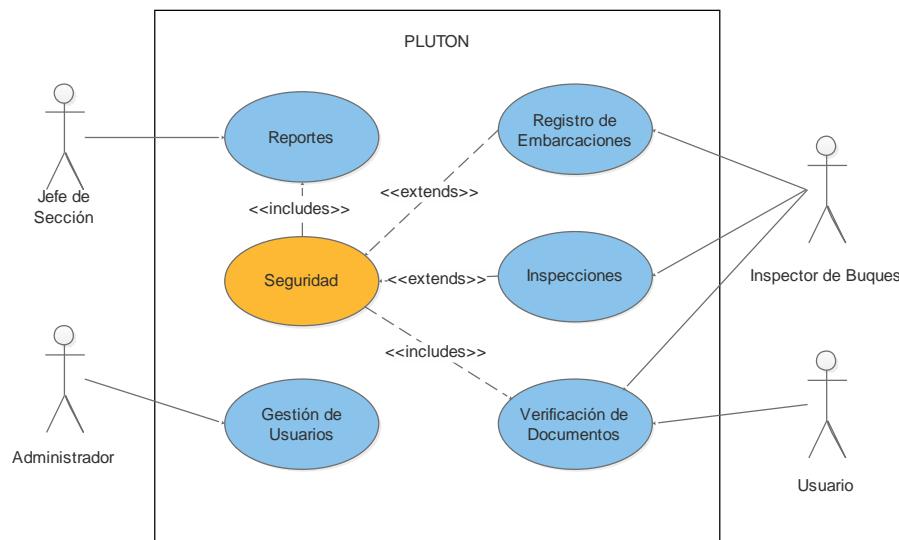
Nº	Requerimiento	Descripción	Tipo	Prioridad
1	Control de acceso de usuarios del sistema	Método de seguridad previo al ingreso al sistema	Funcional	Alta
2	Registro de los datos de una embarcación nueva	Registro de los datos de una nueva embarcación a la base de datos	Funcional	Media
3	Crear una tabla en la base de datos para resguardar los datos de las embarcaciones	Donde se alojarán todos los datos las embarcaciones	Funcional	Media
4	Modificación de datos para el inicio de sesión (usuario y contraseña)	Actualizar el nombre de usuario y contraseña para acceder al sistema	Funcional	Baja
5	Crear interfaces en PHP y HTML, con el framework Laravel	Tener una interfaz intuitiva para facilitar todas las operaciones y que sea responsive	No funcional	Alta
6	Registro de datos de inspección de embarcación	Registro de los datos de una embarcación inspeccionada	Funcional	Alta
7	Consulta de información acerca de las embarcaciones	Consultas de datos de una embarcación, certificados y detalles de las inspecciones previas realizadas	Funcional	Alta
8	Asignación de roles de usuarios	Determinar el rol que cumplirá un determinado usuario en el sistema	Funcional	Alta
9	Generación de certificados	Generación de certificados digitales de registro e inspección de las embarcaciones	Funcional	Alta

**Fuente:** Elaboración propia

Como se puede observar en la Tabla 7, se observan los requerimientos identificados y clasificados con sus respectivas prioridades, esto después de tener reuniones con el distinto personal de la Unidad.

Una vez identificados los requerimientos se determinó los actores que estarán presentes en el sistema, y las actividades que cada uno realizará, como se observa en la Figura 8.

**FIGURA 8: DIAGRAMA DE CASO DE USO DE ALTO NIVEL**



**Fuente:** Elaboración propia

Como se observa la Figura 8, se describe brevemente los procesos que cada actor realizará dentro del sistema.

### 3.1.6 Definición de módulos del sistema

A partir de la información recopilada y los requerimientos identificados por la Unidad se pudo definir los siguientes módulos para el sistema:

- Gestión de usuarios: Módulo que controle aquellas personas que puedan ingresar al sistema, dependiendo del rol se modificará, dar de alta y baja a los demás usuarios.
- Registro de embarcaciones: En este módulo se podrá realizar el registro de una embarcación nueva, llenando todos los campos que correspondan dependiendo de la embarcación.

- Reportes: Este módulo facilitará la emisión de reportes de embarcaciones registradas e inspeccionadas, los cuales son emitidos hacia el Viceministerio de Defensa.
- Seguridad: Administra la parte criptográfica, este módulo es el cual nos permite generar el par de llaves (llave pública y llave privada), las cuales se almacenarán en la base de datos, y a partir de los parámetros que se le dase genera el código QR.
- Inspecciones: Este módulo generará distintos tipos de formularios, esto según el tipo de embarcación a la cual se realice la inspección, para posterior a eso mostrar su cotización, información obtenida a partir de la lista de precios, la cual estará almacenada en la base de datos, dependiendo del rol se podrá cambiar las ponderaciones establecidas dentro de los requerimientos que incluyen los distintos formularios, como se observa en la Figura 9.

**FIGURA 9: PONDERACIONES DE CHECKLIST**

POSEE OTROS AMBIENTES	20%	Medida Adoptad	SI	NO	
COCINA	3%				
BAÑO	9%				
CAMAROTES	5%				
COMEDOR	1%				
ALMACÉN	1%				
DEPÓSITOS	1%				

Fuente: DGIMFLMM

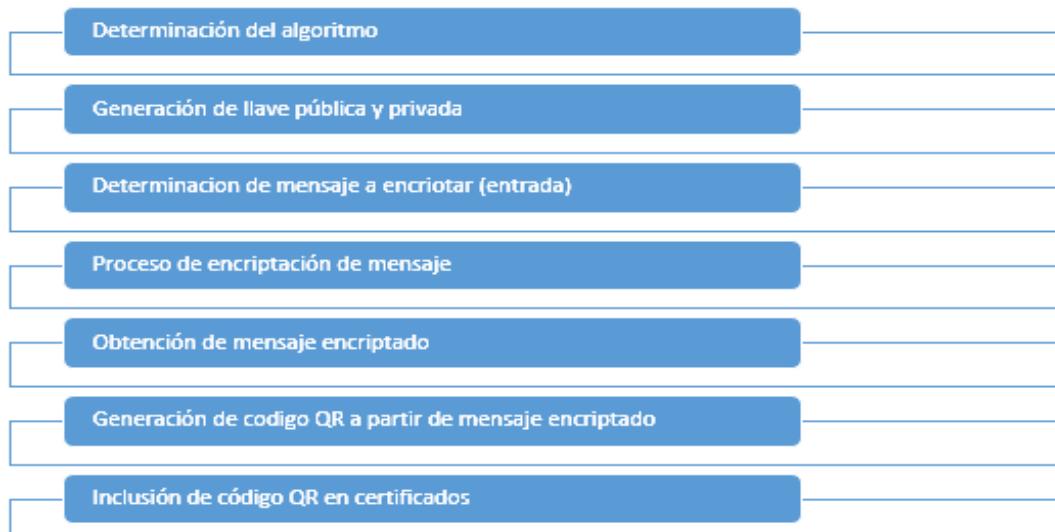
- Verificación de documentos

### 3.2 IMPLEMENTACIÓN DEL ALGORITMO ASIMÉTRICO

El algoritmo para usarse será RSA, debido a que este algoritmo es el que necesita de mínimos recursos para poder realizar la generación del par de llaves. El mismo una vez ejecutado, generará tanto llaves públicas como llaves privadas que serán almacenadas en la base de datos, estas estarán asociadas al número de registro

de las embarcaciones para futuras consultas. Al momento de imprimir los certificados, en los mismos se incluirá un código QR, el cual contendrá la información de la llave pública, como se observa en la Figura 10.

### **FIGURA 10: IMPLEMENTACIÓN DE ALGORITMO ASIMÉTRICO**



**Fuente:** Elaboración propia

#### **3.2.1 Determinación del Algoritmo a Implementar**

El algoritmo RSA nos proporciona las siguientes características:

- Integridad de la información: Salvaguarda la precisión y completitud de la información y sus métodos de proceso.
- No repudio: Autentificación que con un alto aseguramiento pueda ser reafirmado como genuino.

Se determinó el uso del algoritmo RSA, debido a que este presenta notorias ventajas ante los otros, cuenta con un mayor nivel de seguridad y el tiempo que emplea para procesar la información es menor.

Como se observa en la Tabla 8, se realizará una comparación de los distintos algoritmos asimétricos que se tienen, de modo que se pueda determinar el mejor para que pueda ser aplicado en el sistema.

**TABLA 8: COMPARACIÓN DE ALGORITMOS ASIMÉTRICOS**

Algoritmo	Longitud de clave	Fuerza de seguridad	Creación de llaves (tiempo)	Verificación de llaves (tiempo)
RSA	1024 bits	80 bits	4.85 s	1.91 ms
	2048 bits	112 bits	24.06 s	8.33 ms
	4096 bits	128 bits	189.07 s	30.91 ms
DSA	512 bits	-	1.01 s	7.86 ms
	1024 bits	80 bits	1.34 s	10.36 ms
DPH	1024 bits	-	1s	1.10ms

**Fuente:** Elaboración propia

Una vez realizada la capacitación a todo el personal de la Unidad de Marina Mercante, acerca de los tres algoritmos asimétricos analizados se usará el Dot Voting, como se ve en la Tabla 9, de modo que se pueda determinar cuál algoritmo se ha de implementar, esta votación se realizará tomando en cuenta a todo el personal dentro de la Unidad de Marina Mercante.

**TABLA 9: DOT VOTING DE ALGORITMO VS PERSONAL**

Personal	DHP	DSA	RSA
Jefe de la unidad de marina mercante	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Secretario General	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Portapliegos	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Responsable R.M.F.L.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Responsable registro, capacitación y carnétización de personal mercante	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Total	1	1	3

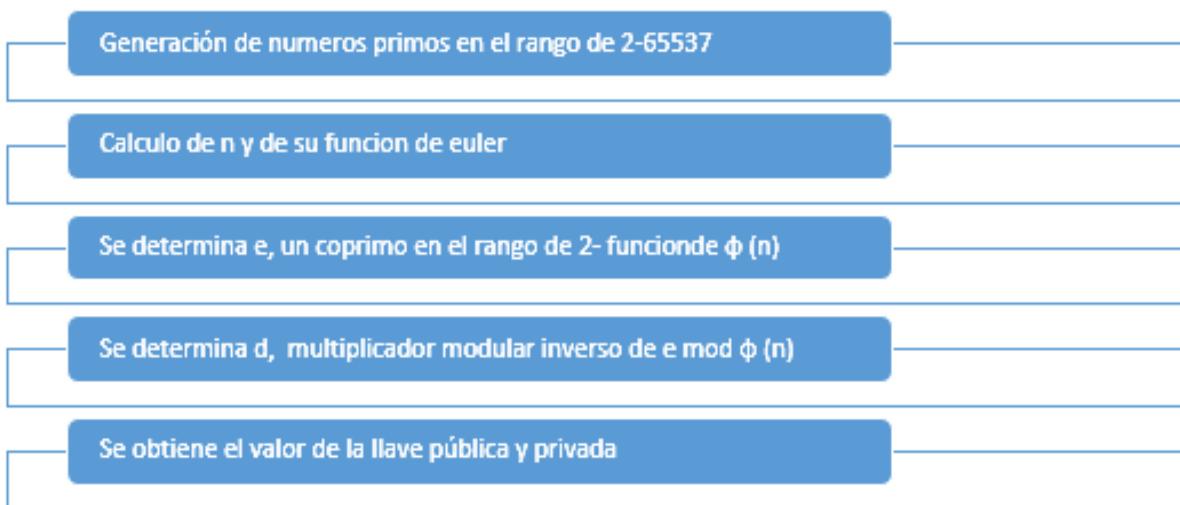
**Fuente:** Elaboración propia

En la Figura 9, se puede observar la tabla de resultados del proceso de Dot Voting realizado en el caso de estudio.

### 3.2.2 Generación de llaves

Para poder generar las llaves primaria y secundaria se usa la ayuda de la librería Phpseclib, la cual es una librería compatible con versiones de PHP 4 en adelante. La misma nos ayudara a generar distintos pares de claves públicas y privado a partir del proceso explicado en Marco Teórico, Criptografía Asimétrica, Algoritmo RSA, como se observa en la Figura 11.

**FIGURA 11: GENERACIÓN DE PARES DE LLAVES**



**Fuente:** Elaboración propia

El proceso de generación de llaves primeramente generara dos números aleatorios en el rango de 2-65537. Posterior a eso se realizan el cálculo de todas las operaciones matemáticas descritas para finalmente poder generar las claves públicas y privadas, los cuales serán devueltas encriptadas en "base64", como se observa en la Figura 12. Cada vez generado un nuevo certificado el valor de llaves cambiara, esto debido a que se usa una función de generación de números aleatorias.

**FIGURA 12: LLAVE ENcriptada EN BASE64**

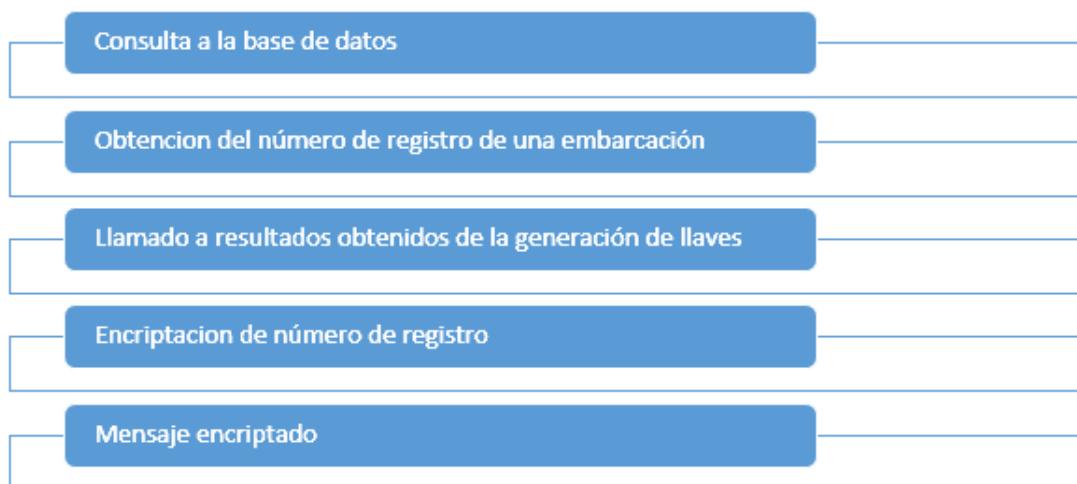
```
return "-----BEGIN OPENSSH PRIVATE KEY-----\r\n".
chunk_split(base64_encode($key), 70) .
"-----END OPENSSH PRIVATE KEY-----";
```

Fuente: Phpseclib

### 3.2.3 Determinación de Información a Encriptar

La información por encriptar será el número de registro de la embarcación. La cual será obtenida mediante una consulta a la base de datos para su posterior encriptación, como se observa en la Figura 13.

**FIGURA 13: OBTENCIÓN DE MENSAJE A ENcriptar**



Fuente: Elaboración propia

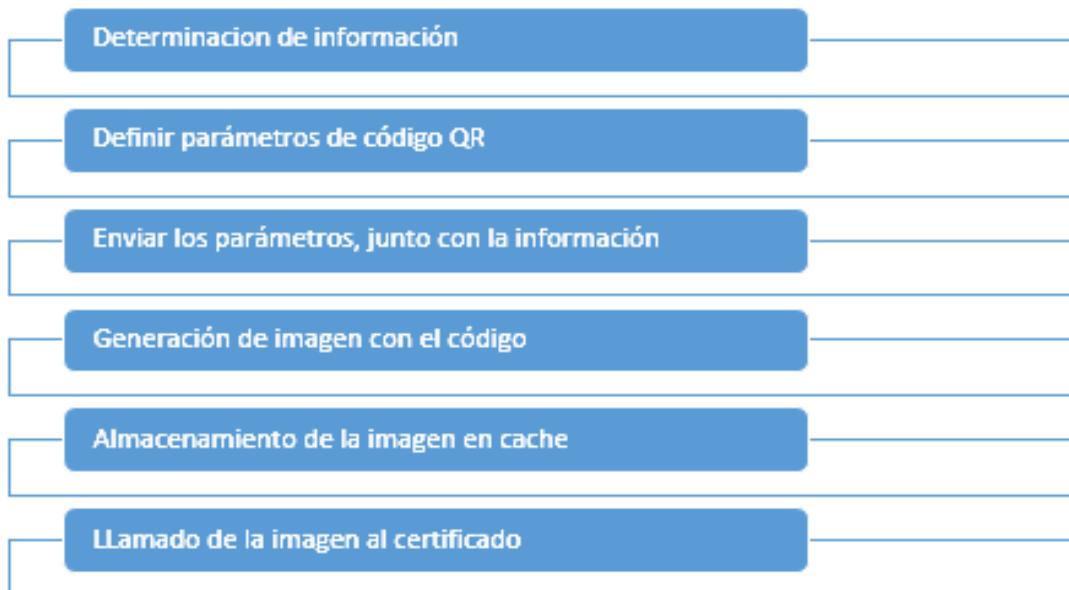
En la Figura 13 se observa el proceso para la obtención del mensaje encriptado. Una vez se tenga la información del número de registro de la embarcación, se procederá a realizar su encriptación con los valores previamente obtenido en el proceso de generación de llaves, obteniendo como resultado el mensaje encriptado.

El resultado encriptado será almacenado en la base de datos, juntamente con los datos de la persona que generó el certificado. Este proceso se lo realizará de tal manera, de poder identificar el tipo del mismo, y en caso de cualquier suceso inoportuno identificar al responsable de la emisión. La misma podrá estar sujeta a consultas debido a que será almacenada en la base de datos, como se observa en el Anexo M.

### 3.2.4 Generación de código QR

Los códigos QR serán añadidos a los diferentes certificados, como medida de registro de la llave publica, precautelando las medidas de seguridad. El proceso que se tendrá para la generación del código QR se muestra en la Figura 14.

**FIGURA 14: PROCESO DE GENERACIÓN DE CÓDIGO QR**



**Fuente:** Elaboración propia

Para la generación de códigos QR, se hará el uso de la librería Qr\_codes. La generación de estos contendrá la llave pública encriptada, al escanear el mismo se mostrará una versión digital de dicho certificado, de modo que se pueda comparar

la información plasmada en los certificados físicos. Este código será añadido en la cabecera de los mismo, como se observa en la Figura 15.

**FIGURA 15: CÓDIGO QR AÑADIDO A CERTIFICADO**



**Fuente:** Elaboración propia

Como se observa en la Figura 15, se tendrá impreso el código QR en las cabeceras de los distintos certificados que se emite. Para poder generar estos se les debe pasar parámetros y la información que se mostrará una vez escaneado al mismo.

Los códigos serán generados para poder cumplir con la función de, establecer un canal directo para la consulta a la información de la base de datos, con el fin de visualizar los registros almacenados sobre los códigos, pudiendo ser leídos por cualquier lector de códigos QR.

### **3.3 DESARROLLO DEL SISTEMA**

Para el desarrollo del sistema en general se determinaron cuatro iteraciones, en la que cada una tendrá distintos entregables.

### 3.3.1 Sprint 1 Módulo de Gestión de Usuarios

Para el primer módulo del sistema se realizó la gestión de usuarios, los cuales tendrán distintas tareas dentro del sistema.

#### 3.3.1.1 Lista de requerimientos Sprint 1

Para el desarrollo del presente módulo se realizó la lista de requerimientos por parte del caso de estudio, el cual nos brinda especificaciones las cuales deben ser incorporadas, como se observa en la Tabla 10.

**TABLA 10: LISTA DE REQUERIMIENTOS GESTIÓN DE USUARIOS**

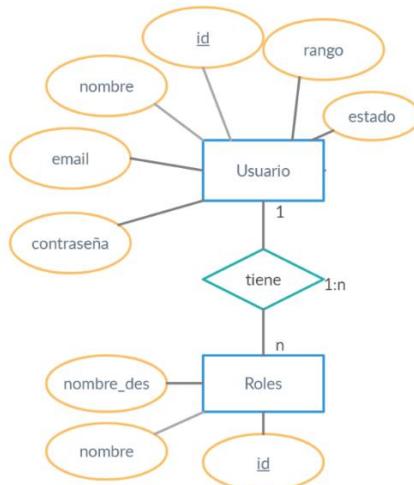
Nº	Requerimiento	Descripción	Tipo	Prioridad
1	Registro de nuevos usuarios por parte del administrador	Capacidad del administrador de registrar a un usuario nuevo en el sistema, para que este pueda desarrollar las actividades previstas	Funcional	Alta
2	Modificación de datos usuarios por parte del administrador	Capacidad del administrador de modificar los datos de un usuario	Funcional	Media
3	Dar de baja a usuarios, por parte del administrador	Capacidad del administrador para deshabilitar el ingreso a un usuario al sistema	Funcional	Media
4	Modificaciones de contraseña, por parte del usuario	Capacidad del usuario para poder modificar el dato de su contraseña, por cuestiones de seguridad	Funcional	Baja
5	Roles de usuarios	Dividir las responsabilidades de cada uno de los usuarios	No funcional	Alta
6	Accesos de usuarios	Determinar los accesos de los usuarios a los módulos del sistema	No funcional	Alta

**Fuente:** Elaboración propia en colaboración de Unidad de Marina mercante

En la Tabla 10 se puede observar los requerimientos solicitados por la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, para gestionar los diferentes usuarios que se prevé tener.

Para el presente módulo se determinó la información que debe almacenar, por lo cual se dio inicio a realizar el modelo entidad-relación para el presente sistema, como se observa en Figura 16.

**FIGURA 16: DIAGRAMA E-R SPRINT 1**



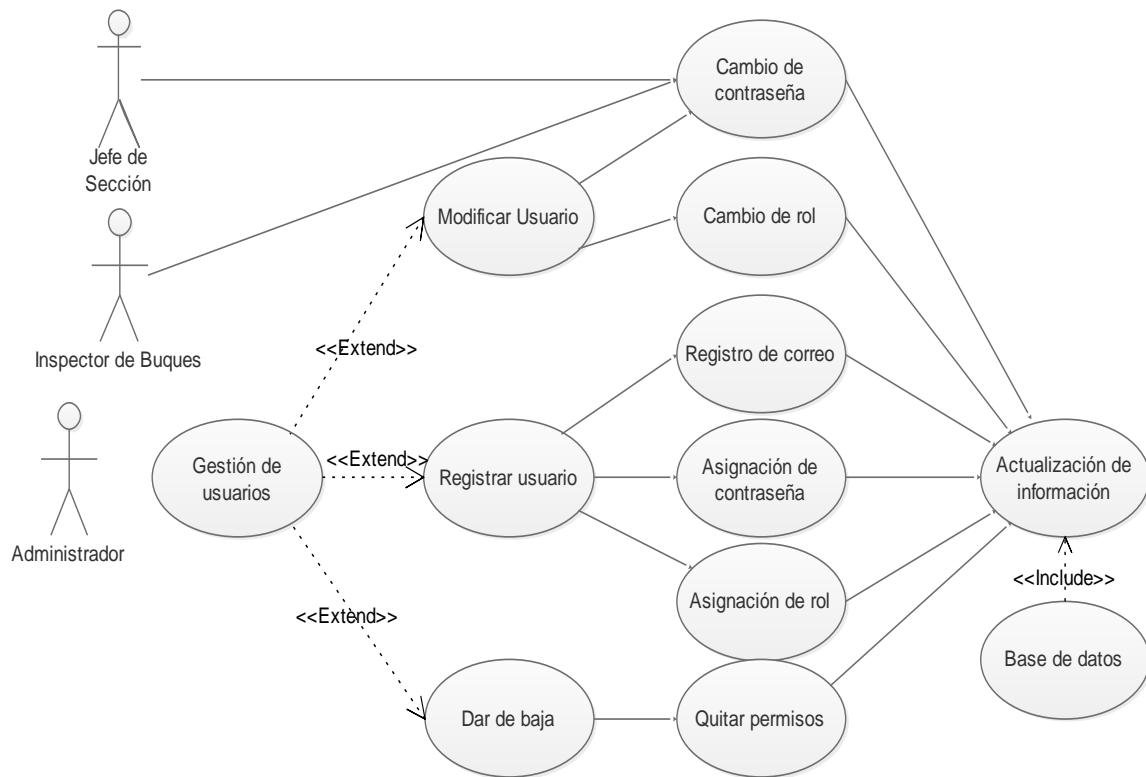
**Fuente:** Elaboración propia

En la Figura 16, se observa la entidad “Usuario”, la cual presenta sus diferentes atributados, además se puede evidencia que el identificador de esta es el atributo “id”.

### 3.3.1.2 Especificación de Procesos Sprint 1

En el módulo de Gestión de Usuarios se tendrá a un administrador, el mismo estará a cargo de realizar los procesos de altas, bajas y modificaciones de los usuarios que hagan uso del sistema, como se ve en la Figura 17.

**FIGURA 17: DIAGRAMA DE CASO DE USO (GESTIÓN DE USUARIOS)**

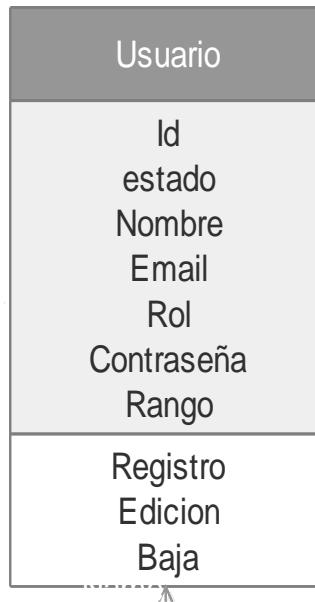


**Fuente:** Elaboración propia

Como se observa en la Figura 17, se ve cómo el usuario con el rol administrador realiza los distintos procesos para gestionar usuarios, para posterior guardarlos en la base de datos. De otra manera los actores con los roles de “Jefe de Sección” e “Inspector de Buques” pueden acceder a la opción de cambio de contraseña para el próximo inicio de sesión.

Una vez determinados los actores presentes dentro de este módulo y teniendo en cuenta las acciones que estos realizan, se realizó el diagrama de clases de la entidad “Usuarios”, como se observa en la Figura 18.

**FIGURA 18: DIAGRAMA DE CLASES SPRINT 1**



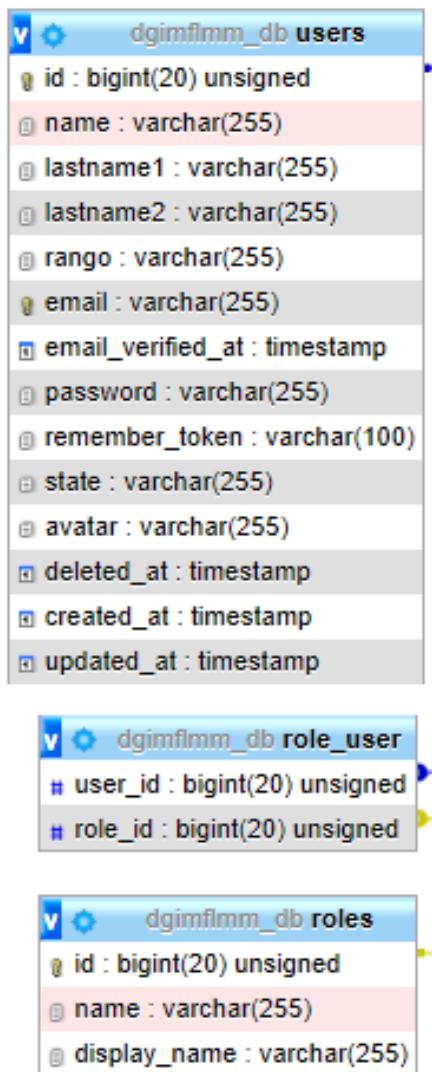
**Fuente:** Elaboración propia

Como se observa en la Figura 18 se tiene a la entidad “Usuario”, con los distintos atributos previamente mencionados, además se identificaron las acciones que estos podrán realizar dentro del sistema

### 3.3.1.3 Diseño de Procesos Sprint 1

Una vez que ya definido la entidad y actores presente en este módulo se procedió a crear esta tabla dentro del gestor de base de datos. Se creo la tabla de usuarios con sus respectivos atributos, teniendo como llave primaria el atributo “id”, la cual se relaciona con la tabla “Roles” y se usa la tabla pivot “Role-User” para establecer la relación entre las mismas, como se observa en la Figura 19.

**FIGURA 19: DIAGRAMA RELACIONAL SPRINT 1**

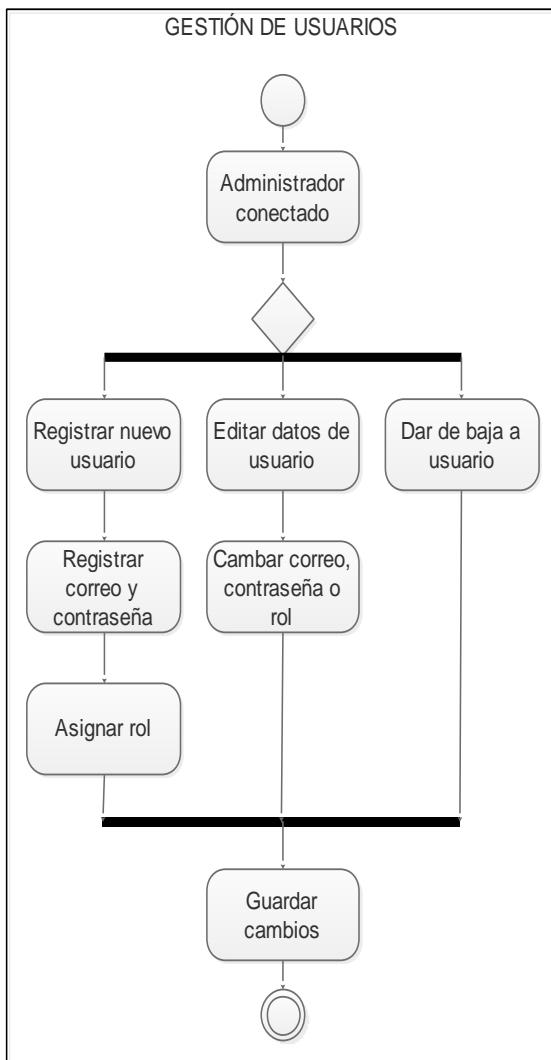


**Fuente:** Elaboración propia

Como se observa en la Figura 19, se procedió a crear la tabla de usuarios dentro del gestor de base de datos, de manera que se pueda proceder a registro a los mismo que podrán ingresar al sistema.

El proceso antes descrito se encuentra explicado de manera simplificada, en un diagrama de actividades, como se observa en la Figura 20.

**FIGURA 20: DIAGRAMA DE ACTIVIDADES (SPRINT 1)**



**Fuente:** Elaboración propia

Como se observa en la Figura 20, se elaboró el diagrama de actividades del módulo “Gestión de Usuarios”.

#### 3.3.1.4 Diseño de Interfaces Sprint 1

Posterior a determinar las tareas que realiza el administrador, se realizó el diseño de las pantallas las que nos mostrará el sistema, como se ve en la Figura 21.

**FIGURA 21: BOCETO DE INICIO DE SESIÓN**



**Fuente:** Elaboración propia

Como se observa en la Figura 21, se planteó el diseño de la pantalla de Inicio de Sesión, esta será la primera página que se desplegará.

Posterior a eso se realizó el diseño de la interfaz para poder registrar usuarios nuevos y asignarles un rol respectivamente, como se observa en la Figura 22.

**FIGURA 22: BOCETO DE REGISTRO DE USUARIO**

A wireframe diagram of a user registration form titled "REGISTRO DE USUARIO". It contains six input fields: "NOMBRE", "CORREO", "ESTADO" (with a dropdown arrow icon), "CONTRASEÑA", "CONFIRMAR", and "ROL" (with four small square checkboxes). A blue rectangular button is located at the bottom right. The form is set against a light gray background with dark gray vertical side bars on the left and right.

**Fuente:** Elaboración propia

En la figura 22, se muestra el boceto de la pantalla, la cual se mostrará al administrador cuando realice el registro de un usuario nuevo.

El diseño de la interfaz para modificar información de usuario, con la capacidad de cambiar la contraseña, el correo y el rol, como se observa en la Figura 23.

**FIGURA 23: BOCETO DE MODIFICACIÓN DE USUARIO**



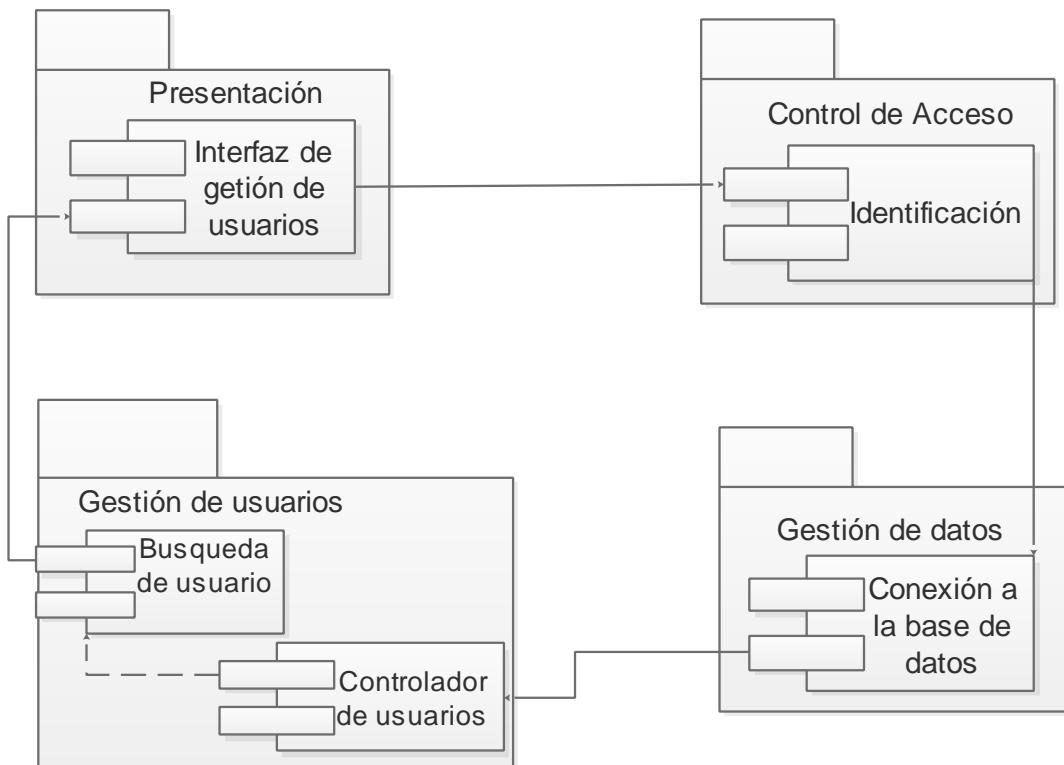
**Fuente:** Elaboración propia

En la figura 23, se muestra el boceto de la pantalla, la cual se mostrará al administrador cuando realice la modificación a los datos de un usuario.

### 3.3.1.5 Diseño de Navegacional Sprint 1

El módulo de “Gestión de Usuarios” estará compuesto por cuatro componentes, como se observa en la Figura 24.

**FIGURA 24: DIAGRAMA DE COMPONENTES (GESTIÓN DE USUARIOS)**



**Fuente:** Elaboración propia

En la Figura 24, se muestra la organización de los componentes de software de este.

### 3.3.1.6 Construcción de Interfaces Sprint 1

Una vez realizado el diseño de las interfaces, se codificaron las mismas en el framework Laravel. La primera pantalla que se codificó fue la de “Inicio de Sesión”, como se observa en la Figura 25.

**FIGURA 25: PANTALLA INICIO DE SESIÓN**

La imagen muestra una pantalla de inicio de sesión con el título "MarinaMercante" en la parte superior. El formulario se titula "Ingrese sus credenciales". Contiene dos campos principales: "Correo Electrónico" y "Contraseña", ambos con iconos de correo electrónico y candado respectivamente. Hay un checkbox para "Recuérdame" y un botón azul "Iniciar". Abajo del formulario, hay un enlace "Olvide mi contraseña".

**Fuente:** Elaboración propia

En la Figura 25 se observa el resultado de la codificación e implementación de la pantalla por la cual los usuarios acceden al sistema.

Para el registro de nuevos usuarios, y poder asignarles un rol respectivamente, se codificó la pantalla de registro, como se observa en Figura 26.

**FIGURA 26: PANTALLA DE REGISTRO DE USUARIO**

La imagen muestra una pantalla para "Registrar Usuario". La sección "Foto de Perfil" incluye un placeholder de perfil y un botón "Examinar...". Los campos obligatorios son "Nombre" (Nombre...), "Apellido Paterno" (Apellido Paterno...) y "Apellido Materno" (Apellido Materno...). Los campos adicionales incluyen "Estado" (selección activo), "Rango" (selección Alférez), "Correo Electrónico" (luisricardorivasgivenc@gmail.com), "Roles" (checkboxes para Administrador y Inspector de Buques, ambos desmarcados), "Contraseña" (campo con asteriscos) y "Confirmar Contraseña" (campo vacío). Un botón azul "Guardar" se encuentra en la parte inferior.

**Fuente:** Elaboración propia

Como se observa en la Figura 26, se codificó e implementó la pantalla, la cual permite registrar nuevos usuarios y asignar roles dentro del sistema.

De la misma manera se codifica la pantalla para modificar usuarios, en los cuales el usuario puede cambiar el nombre y correo electrónico de los mismos, como se observa en la Figura 27.

**FIGURA 27: PANTALLA DE EDICIÓN DE USUARIOS**

The screenshot shows a user interface for editing a user profile. The title is "Editar Usuario". There is a placeholder for a profile picture with the text "Examinar..." and "No se ha seleccionado ningún archivo.". Below it, there are input fields for "Nombre" (Luis), "Apellido Paterno" (Rivas), and "Apellido Materno" (Givencer). To the right, there are dropdown menus for "Estado" (activo) and "Rango" (Alférez). There is also a text input for "Correo Electrónico" (luisricardorivasgivencer@gmail.com). At the bottom, there is a section for "Roles" with checkboxes for "Administrador" and "Inspector de Buques", both of which are checked. A blue "Guardar" button is at the very bottom.

**Fuente:** Elaboración propia

Como se observa en la Figura 27, se codificó e implementó la pantalla la cual permite registrar nuevos usuarios y asignar roles dentro del sistema.

### 3.3.1.7 Código Sprint 1

Para que este módulo funcione correctamente se realizó la siguiente codificación, la cual se ejecuta desde la carpeta de los controladores, como se observa en la Figura 28.

**FIGURA 28: CÓDIGO PARA GESTIÓN DE USUARIOS**

```

class UsersController extends Controller
{
    function __construct()
    {
        $this->middleware('auth');
        $this->middleware(['roles:admin', ['except'=>['edit', 'updates']]]);
    }

    public function index()
    {
        return view('users.index', [
            'users'=>User::all()
        ]);
    }

    public function create()
    {
        return redirect()->route('users.create');
    }

    public function store(Request $request)
    {
        User::create([
            'name' => request('name'),
            'email' => request('email'),
            'state' => request('activo'),
            'password' => request('pass'),
        ]);
    }
}

return redirect()->route('users.index');
}

public function show($id)
{
    $user = User::findOrFail($id);
    return view('users.show', compact('user'));
}

public function edit($id)
{
    $user = User::findOrFail($id);
    $this->authorize($user);
    return view('users.edit', compact('user'));
}

public function update(UpdateUserRequest $request, $id)
{
    $user = User::findOrFail($id);
    $this->authorize($user);
    $user->update($request->all());
    return redirect()->route('usuarios.index');
}

public function destroy($id)
{
    $user = User::findOrFail($id);
    $this->authorize($user);
    $user->delete();
    return redirect()->route('usuarios.index');
}

```

**Fuente:** Elaboración propia

Como se observa en la Figura 28 se tiene el código desarrollado, el cual es responsable del funcionamiento del módulo correspondiente.

### 3.3.1.8 Prueba Unitaria Sprint 1

Una vez concluida la codificación se procedió a realizar las pruebas "Mock", siendo estas pruebas unitarias, las cuales nos indican si todo se realiza de la manera correcta, como se observa en la Figura 29.

**FIGURA 29: PRUEBA UNITARIA MOCK (GESTIÓN DE USUARIOS)**

```
PASS Tests\Unit\UserControllerTest
✓ index
✓ show
✓ create
✓ edit
✓ destroy

Tests: 6 passed
Time: 0.06s
```

**Fuente:** Elaboración propia

Como se observa en la Figura 29, se realizaron y pasaron satisfactoriamente las pruebas unitarias, las cuales evaluaron los distintos métodos usados al codificar el módulo “Gestión de Usuarios”.

### 3.3.2 Sprint 2 Módulo de Registro de Embarcaciones

Para el segundo módulo del sistema se realizó el desarrollo, de modo que se registren nuevas embarcaciones

#### 3.3.2.1 Lista de Requerimientos Sprint 2

Para el desarrollo del presente modulo se realiza la lista de requerimientos por parte del caso de estudio, el cual nos brinda las especificaciones las cuales deben ser incorporadas, como se observa en la Tabla 11.

**TABLA 11: REQUERIMIENTOS MÓDULO DE INSPECCIONES**

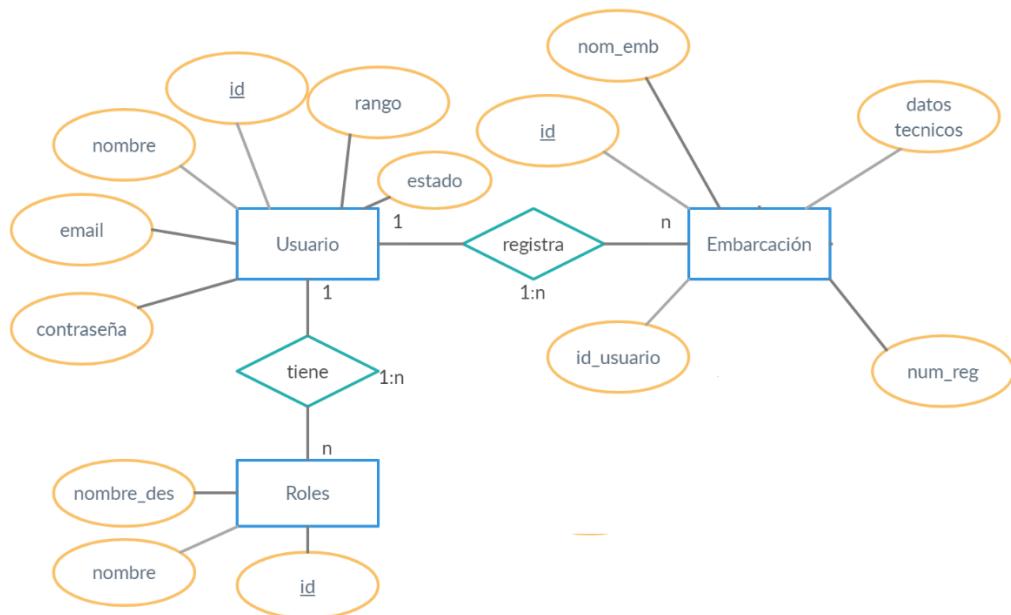
Número	Requerimiento	Descripción	Tipo	Prioridad
1	Generar número de registro de manera automática al momento	Capacidad del sistema, de generar un número de registro de manera automática al momento de registrar una embarcación, tomando en cuenta el formato que se usa actualmente	Funcional	Alta
2	Identificar la cuenca a la cual está registrada la embarcación	Asociar el nombre de la cuenca a la cual pertenece la embarcación	Funcional	Media
3	Control previo registro	Mostrar los requisitos previos para el registro de una embarcación, si es que los cumple proceder con el registro	Funcional	Baja
4	Formulario de registro	Generar un formulario de registro para las embarcaciones nuevas, donde se llenen todos los datos correspondientes	No funcional	Alta
5	Guardar información	Una vez registrada una embarcación, registrar toda la información en la base de datos	Funcional	Alta

**Fuente:** Elaboración propia

En la Tabla 11 se puede observar los requerimientos solicitados por la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, para realizar el registro de embarcaciones

Para el presente módulo se determinó la información que debe almacenar, por lo cual se dio inicio a realizar el modelo entidad-relación para el presente sistema, como se observa en Figura 30.

**FIGURA 30: DIAGRAMA E-R SPRINT 2**



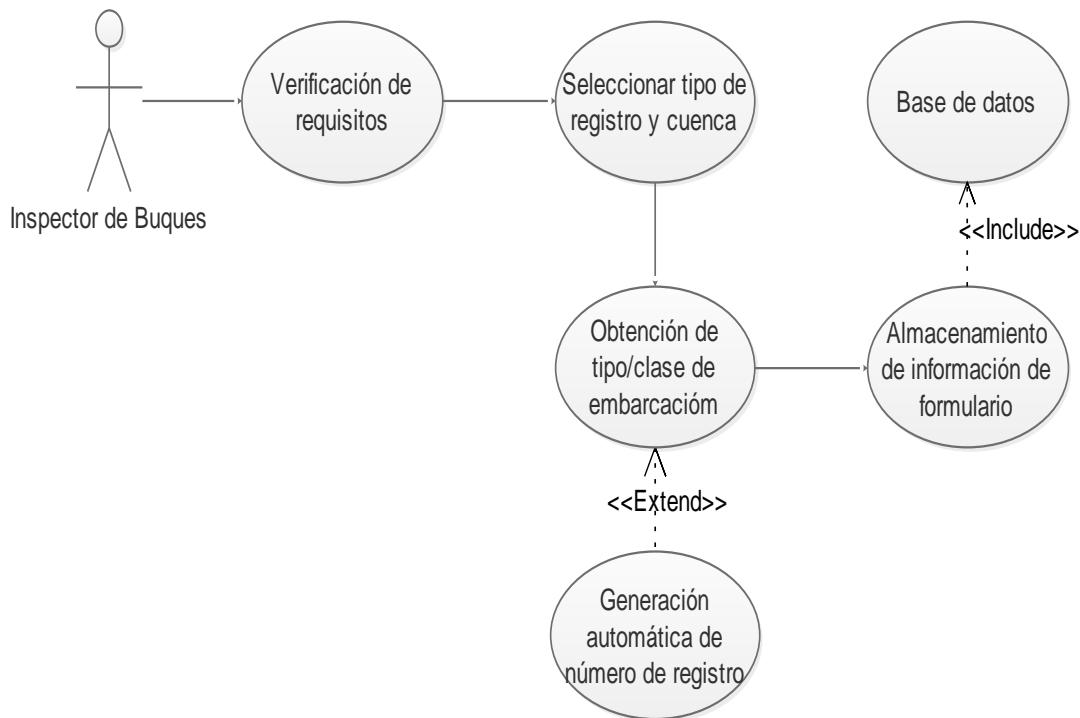
**Fuente:** Elaboración propia

En la Figura 30, se observa la entidad “Embarcación”, la cual presenta sus diferentes atributados, además se puede evidencia que el identificador de esta es el atributo “id”.

### 3.3.2.2 Especificación del Proceso Sprint 2

En el módulo de “Registro” se tendrá a un “Inspector de Buques”, definido por el caso de estudio, el mismo estará a cargo de realizar los registros correspondientes, como se ve en la Figura 31.

**FIGURA 31: DIAGRAMA DE CASO DE USO (REGISTRO)**

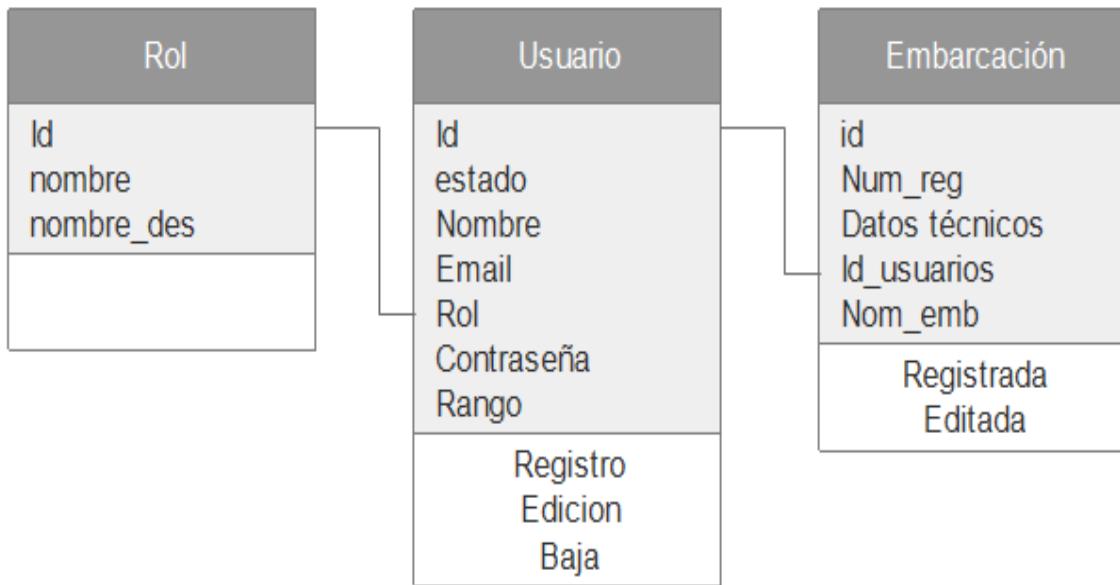


**Fuente:** Elaboración propia

Como se observa en la Figura 31, se ve cómo el usuario con el rol “Inspector de Buques” realiza los distintos procesos para registrar una embarcación, para posterior guardar la información en la base de datos

Una vez determinados los actores presentes dentro de este módulo y teniendo en cuenta las acciones que estos realizan, se realizó el diagrama de clases de la entidad “Embarcaciones”, como se observa en la Figura 32.

**FIGURA 32: DIAGRAMA DE CLASES SPRINT 2**



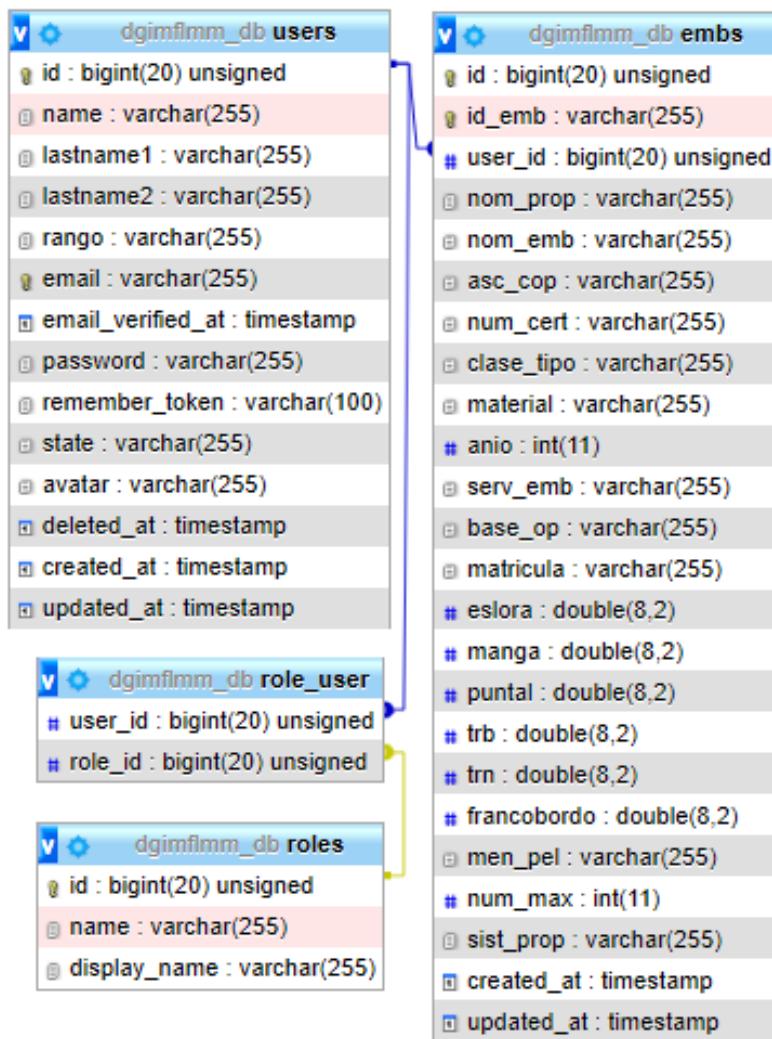
**Fuente:** Elaboración propia

Como se observa en la Figura 32 se tiene a la entidad “Usuario”, con los distintos atributos previamente mencionados, además se identificaron las acciones que estos podrán realizar dentro del sistema.

### 3.3.2.3 Diseño de Procesos Sprint 2

Una vez que ya definido la entidad y actores presente en este módulo se procedió a crear esta tabla dentro del gestor de base de datos. Esta se encuentra relacionada con la tabla usuarios de manera que se tenga el id de usuario que registra una de estas, este campo será identificado de manera automática una vez un “Inspector de Buques” ingrese con sus credenciales al sistema y proceda a realizar este proceso, como se observa en la Figura 33.

**FIGURA 33: DIAGRAMA RELACIONAL SPRINT 2**

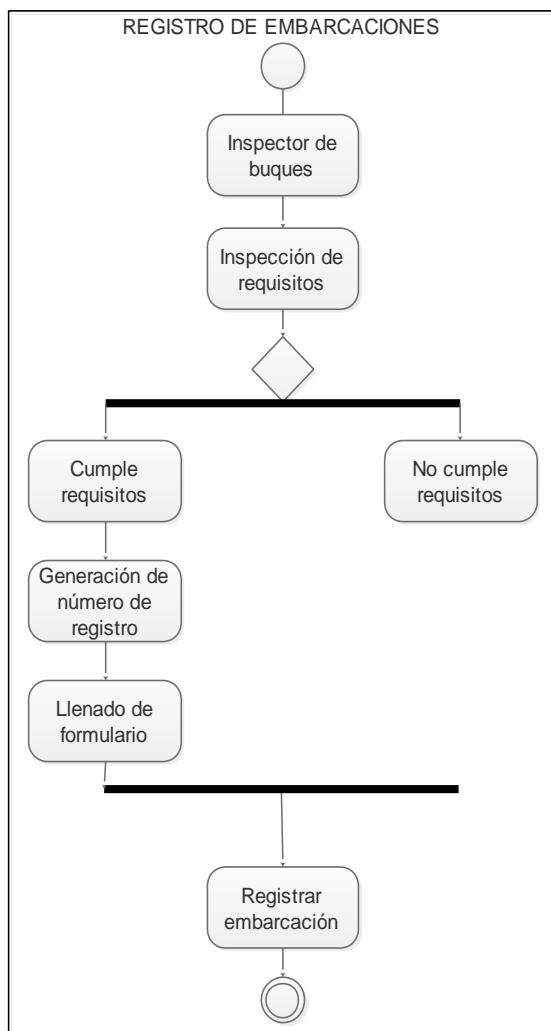


Fuente: Elaboración propia

Como se observa en la Figura 33, se procedió a crear la tabla de usuarios dentro del gestor de base de datos, de manera que se pueda proceder a registro a los mismo que podrán ingresar al sistema.

El proceso antes descrito se encuentra explicado de manera simplificada, en un diagrama de actividades, como se observa en la Figura 34.

**FIGURA 34: DIAGRAMA DE ACTIVIDADES (SPRINT 2)**



**Fuente:** Elaboración propia

Como se observa en la Figura 34, se muestra el proceso que se realiza al momento de registrar una embarcación.

#### 3.3.2.4 Diseño de Interfaces Sprint 2

Una vez identificadas las acciones que se realizaran, se procedió al diseño de pantallas para el correspondiente módulo, como se observa en la Figura 35.

**FIGURA 35: BOCETO DE REQUISITOS**



Este boceto de requisitos muestra una interfaz de usuario para la verificación de requisitos. El título es "Marina Mercante". Abajo de él, hay dos cuadros desplegables que contienen listas de requisitos. A la derecha de cada cuadro desplegable, hay tres botones: "Requerimiento", "Cumple" y "No cumple". Los botones "Cumple" y "No cumple" tienen un efecto de radio.

**Fuente:** Elaboración propia

Como se observa en la Figura 35, se plantea el diseño de registro y verificación, si se cumplen los requerimientos para posterior registro.

Una vez concluido con la verificación de registro se pasó al diseño de la pantalla de registro de embarcación, como se observa en la Figura 36.

**FIGURA 36: BOCETO DE REGISTRO**



Este boceto de registro muestra una interfaz de usuario para el ingreso de datos. El título es "Registro". Hay un cuadro de texto para "Nº DE REGISTRO" y tres cuadros desplegables para otros datos. Los cuadros desplegables tienen un efecto de radio.

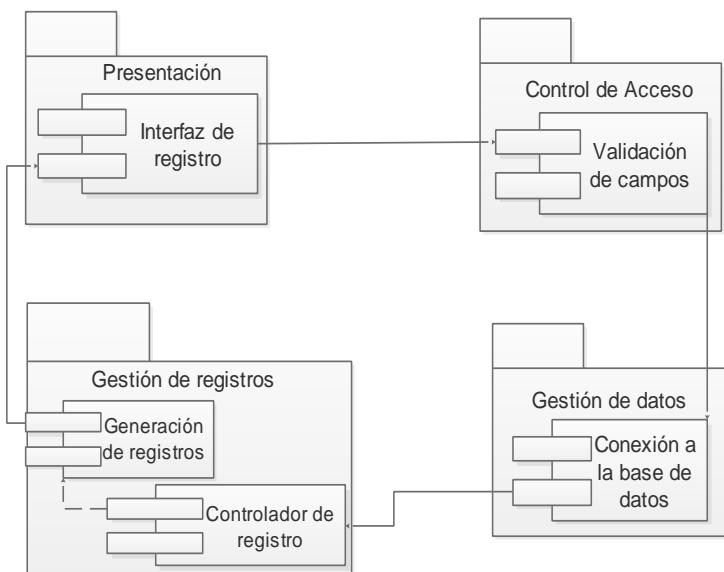
**Fuente:** Elaboración propia

Como se observa en la Figura 36, se planteó el diseño de formulario de registro de embarcación, con la asignación de número de registro automático.

### 3.3.2.5 Diseño Navegacional Sprint 2

El módulo de "Registro de Embarcaciones" estará compuesto por cuatro componentes, como se observa en Figura 37.

**FIGURA 37: DIAGRAMA DE COMPONENTES (REGISTRO)**



**Fuente:** Elaboración propia

En la Figura 37, se muestra la organización de los componentes de software del módulo " Registro de Embarcaciones "

### 3.3.2.6 Construcción de Interfaces Sprint 2

Una vez realizado el diseño de las interfaces, se codificaron las mismas en el framework Laravel. Para poder realizar el registro, como se observa en la Figura 38.

**FIGURA 38: PANTALLA DE REQUISITOS DE REGISTRO**

The screenshot shows a web-based application titled 'Unidad de Marina Mercante'. The main title 'Requisitos' is displayed prominently. On the left, there are dropdown menus for 'Cuenta:' (set to 'PLATA') and 'Tipo de Registro:' (set to 'PROVISIONAL'). Below these are three checkboxes: 'Solicitud de Cotización', 'Solicitud de Registro dirigida a la Autoridad Marítima', and 'Documentos Adjuntos Completos'. To the right is a table with columns 'Requisito' and 'Si' (Yes) or 'No'. The first row has 'Solicitud de Cotización' checked under 'Si'. The second row has 'Solicitud de Registro dirigida a la Autoridad Marítima' checked under 'Si'. The third row has 'Documentos Adjuntos Completos' checked under 'Si'. A blue 'Registrar' button is located at the bottom.

**Fuente:** Elaboración propia

Como se observa en la Figura 38, se tiene el formulario previo al registro al registro de una embarcación.

Posterior a la verificación de requisitos, se redireccionará al formulario de registro de embarcación, como se observa en la Figura 39.

**FIGURA 39: PANTALLA DE REGISTRO DE EMBARCACIÓN**

The screenshot shows a 'Registrar Embarcación' (Register Vessel) form. It includes fields for: 'Nº de Registro' (P-20083), 'Nombre de Propietario' (empty), 'Nombre de Embarcación' (empty), 'Asociación Cooperativa' (empty), 'Número de Certificado' (empty), 'Clase/Tipo' (selected as 'BARCAZA CERRADA'), 'Servicio' (empty), 'Base Operativa' (empty), 'Matrícula' (empty), 'Eslora' (empty), 'Manga' (empty), 'Puntal' (empty), 'TRB' (empty), 'TRN' (empty), 'Francobordo' (empty), 'Sistema de Propulsión' (empty), 'Mcía. Pel.' (selected as 'SI'), 'Max. Pax.' (empty), 'Material' (selected as 'MADERA'), and 'Año Cons.' (empty). A blue 'Guardar' (Save) button is at the bottom.

**Fuente:** Elaboración propia

Como se observa en la Figura 39 el formulario para registrar una embarcación, con el número de registro asignado.

### 3.3.2.7 Código Sprint 2

Para que este módulo funcione correctamente se realizó la siguiente codificación, la cual se ejecuta desde la carpeta de los controladores, como se observa en la Figura 40.

**FIGURA 40: CÓDIGO PARA REGISTRO DE EMBARCACIÓN**

```
Class EmbsController extends Controller

    public function index()
    {
        return view('embs.index',[

            'embs'=>Emb::all()
        ]);
    }

    public function create()
    {
        $anio = (Carbon::now()->year)%100;
        $co=Emb::orderBy('id', 'desc')
            ->take(1)
            ->get();
        $co=$co->pluck('id')->implode(', ')+1;
        $mes = (Carbon::now()->month);
        if ($mes<10) $mes='0'.$mes;
        $reg='A-'.$anio.'.'.$mes.'.'.$co;

        return view('embs.create',compact('reg'));
    }

    public function store(SaveEmbRequest $request)
    {
        $emb=Emb::create( $request->all());
        return redirect()->route('embs.index')->with('success', 'Embarcación Registrada');
    }

    public function show($id)
    {
        $emb = Emb::findOrFail($id);
        return view('embs.show',compact('emb'));
    }

    public function edit($id)
    {
        $emb = Emb::findOrFail($id);
        return view('embs.edit',compact('emb'));
    }

    public function update(SaveEmbRequest $request, $id)
    {
        $emb = Emb::findOrFail($id);
        $emb->update($request->all());
        return redirect()->route('embs.index');
    }

    public function destroy($id)
    {
        //
    }

    public function preview(Request $request)
    {
        return view('embs.preview');
    }
}
```

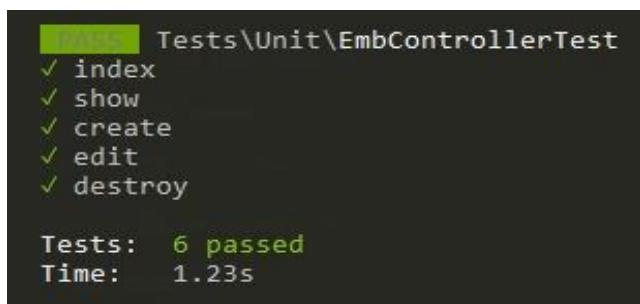
**Fuente:** Elaboración propia

Como se observa en la Figura 40, se codificaron los distintos métodos para poder realizar el registro de embarcaciones en base a los requisitos previamente mencionados en la Tabla 11 del presente documento.

### 3.3.2.8 Prueba Unitaria Sprint 2

Una vez concluida la codificación se procedió a realizar las pruebas "Mock", para el controlador de embarcaciones, como se observa en la Figura 41.

**FIGURA 41: PRUEBA UNITARIA MOCK (REGISTRO DE EMBARCACIÓN)**



```
Tests\Unit\EmbControllerTest
✓ index
✓ show
✓ create
✓ edit
✓ destroy

Tests:  6 passed
Time:   1.23s
```

**Fuente:** Elaboración propia

Como se observa en la Figura 41, todas las pruebas del módulo de "Registro de Embarcaciones" se efectuaron de manera exitosa.

### 3.3.3 Sprint 3 Módulo de Inspección de Embarcaciones

Para el segundo módulo del sistema se realizó el desarrollo el módulo que permitirá realizar las inspecciones a las embarcaciones registradas.

#### 3.3.3.1 Lista de Requerimientos Sprint 3

Para el desarrollo de presente módulo, se realizó una lista requerimientos por parte del caso de estudio correspondiente, el cual nos brinda las especificaciones, funcionales y no funcionales las cuales deben ser incorporadas, como se observa en la Tabla 12.

**TABLA 12: REQUERIMIENTOS MODULO DE INSPECCIONES**

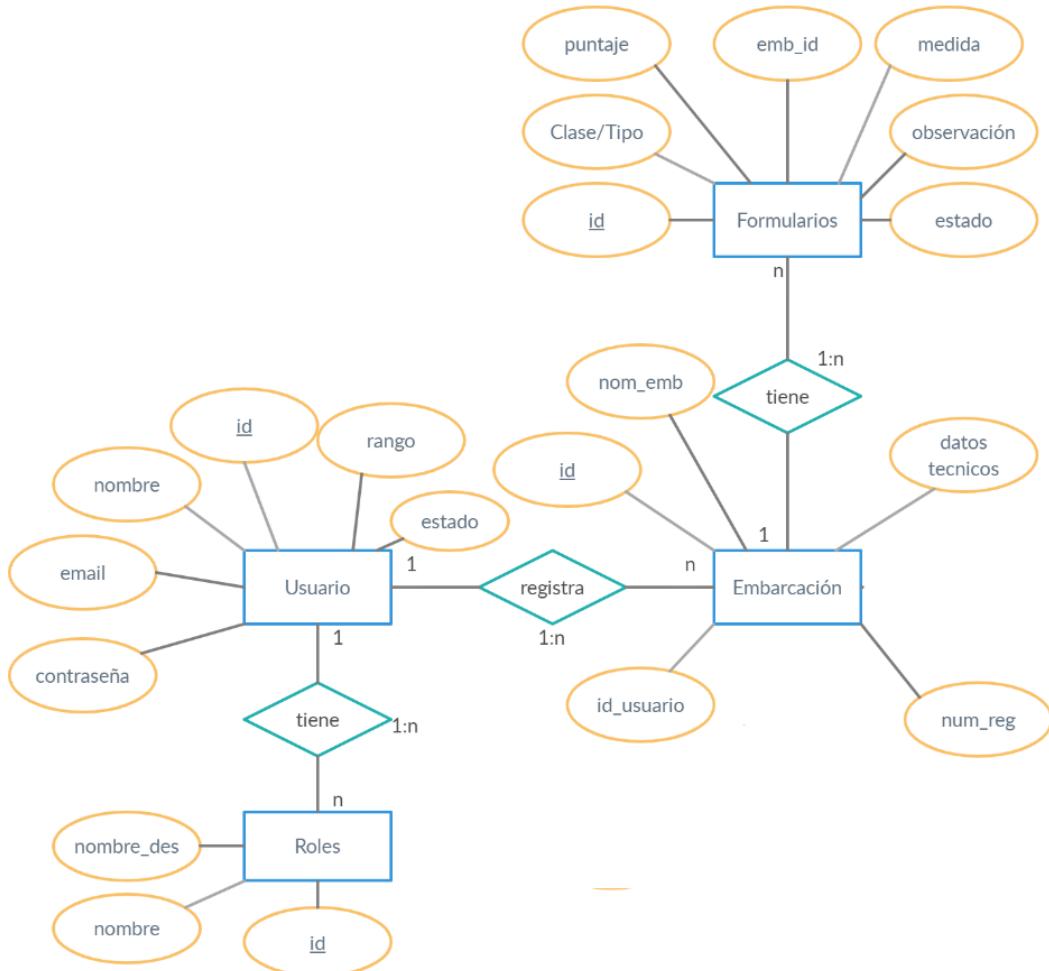
Número	Requerimiento	Descripción	Tipo	Prioridad
1	Generar formularios de manera automática	Generar formularios de acuerdo con el tipo /clase para poder inspeccionar	Funcional	Alta
2	Validación de campos obligatorios en el formulario	Capacidad del sistema de controlar los campos obligatorios	Funcional	Media
3	Mostrar el progreso del llenado, del formulario de inspección	Mostrar porcentaje de llenado de acuerdo con el llenado del formulario	No funcional	Baja
4	Generación de certificado(os)	Generación automática de certificados, si es que aprueba la inspección correspondiente	Funcional	Baja

**Fuente:** Elaboración propia

En la Tabla 12 se puede observar los requerimientos solicitados por la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, para realizar las inspecciones a las distintas embarcaciones.

Para el presente módulo se determinó la información que debe almacenar, por lo cual se dio inicio a realizar el modelo entidad-relación para el presente sistema, como se observa en Figura 42.

**FIGURA 42: DIAGRAMA E-R SPRINT 3**



**Fuente:** Elaboración propia

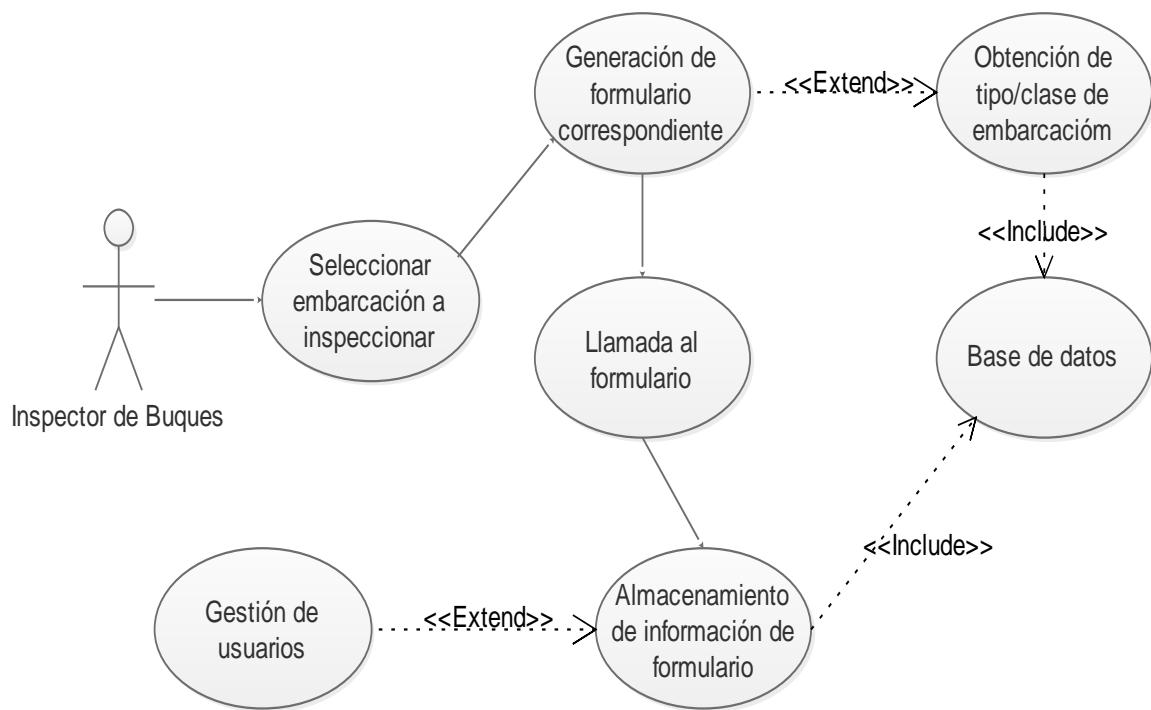
En la Figura 42, se observa la entidad “Embarcación”, la cual presenta sus diferentes atributados, además se puede evidencia que el identificador de esta es el atributo “id”.

### 3.3.3.2 Especificación del Proceso Sprint 3

En el módulo de inspecciones se tendrá un “Inspector de Buques” definido por el caso de estudio, el mismo estará a cargo de realizar las inspecciones

correspondientes, y dependiendo el resultado emitir el certificado correspondiente. cómo se observa en la Figura 43.

**FIGURA 43: DIAGRAMA DE CASO DE USO (INSPECCIÓN)**

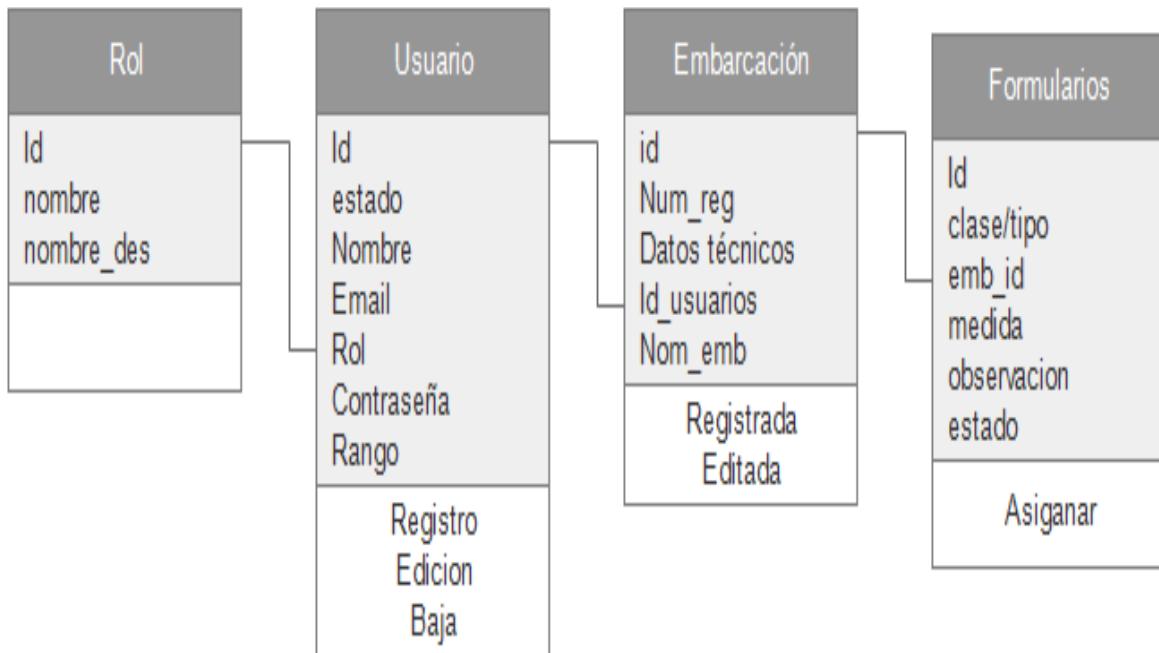


**Fuente:** Elaboración propia

Como se observa en la Figura 43, se ve cómo el usuario con el rol “Inspector de Buques”, realiza los distintos procesos de inspección de embarcaciones, para posterior guardarlos en la base de datos.

Una vez determinados los actores presentes dentro de este módulo y teniendo en cuenta las acciones que estos realizan, se realizó el diagrama de clases de la entidad “Embarcaciones”, como se observa en la Figura 44.

**FIGURA 44: DIAGRAMA DE CLASES SPRINT 3**



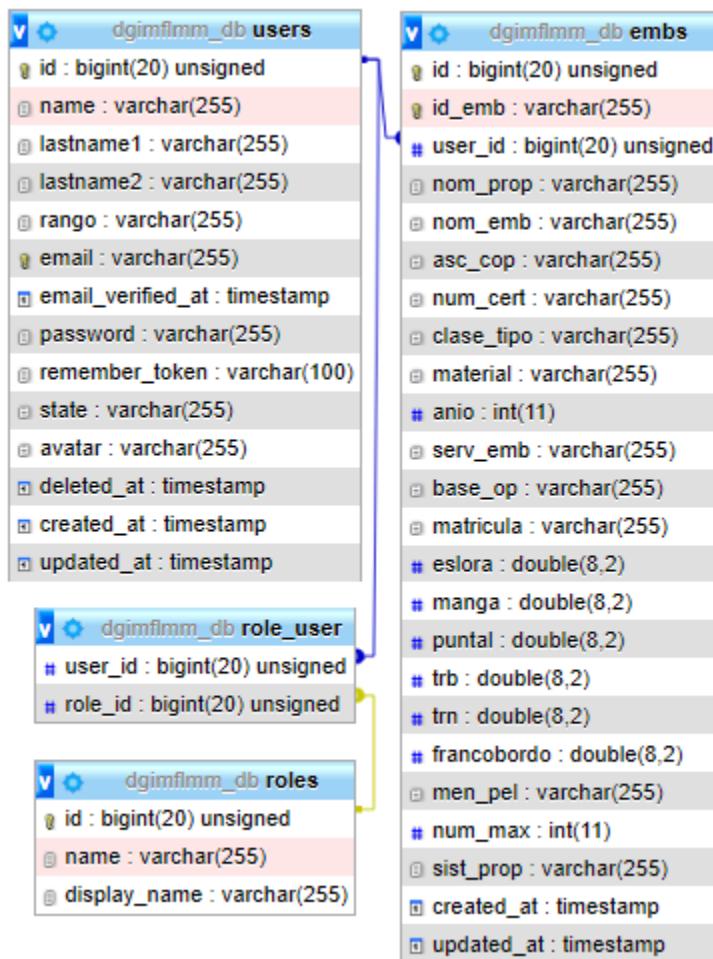
**Fuente:** Elaboración propia

Como se observa en la Figura 44 se tiene a la entidad “Inspección de Embarcación”, con los distintos atributos previamente mencionados, además se identificaron las acciones que estos podrán realizar dentro del sistema. Además, se puede observar que este presenta una relación con la tabla de embarcaciones, obteniendo de ahí su información.

### 3.3.3.3 Diseño de Procesos Sprint 3

Una vez que ya definido la entidad y actores presente en este módulo se procedió a crear esta tabla dentro del gestor de base de datos, como se observa en la Figura 45.

**FIGURA 45: DIAGRAMA RELACIONAL SPRINT 3**

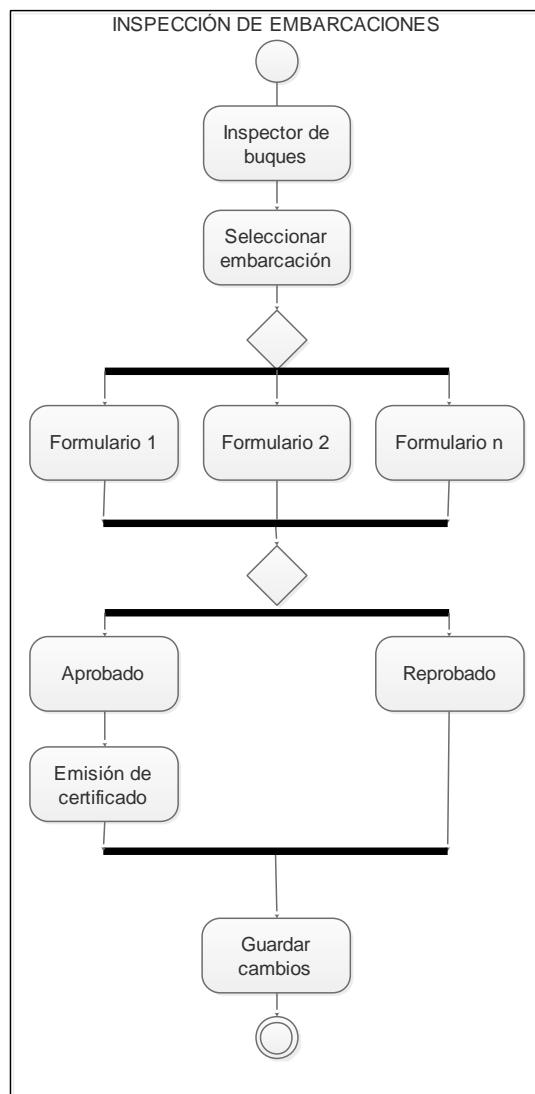


**Fuente:** Elaboración propia

Como se observa en la Figura 45, se procedió a crear la tabla de usuarios dentro del gestor de base de datos, de manera que se pueda proceder a registro a los mismo que podrán ingresar al sistema.

El proceso por el cual se realiza la inspección a una determinada embarcación se encuentra descrita de una manera más simplificada y concisa, realizada en un diagrama de actividades, como se observa en Figura 46.

**FIGURA 46: DIAGRAMA DE ACTIVIDADES (SPRINT 3)**



**Fuente:** Elaboración propia

Como se observa en la figura 46, se muestra el proceso que se realiza al momento de inspeccionar una embarcación.

#### 3.3.3.4 Diseño de Interfaces Sprint 3

Una vez identificadas las acciones que se realizarán, se procedió al diseño de pantallas para el correspondiente módulo como se observa en la Figura 47.

**FIGURA 47: BOCETO DE REALIZAR INSPECCIÓN**



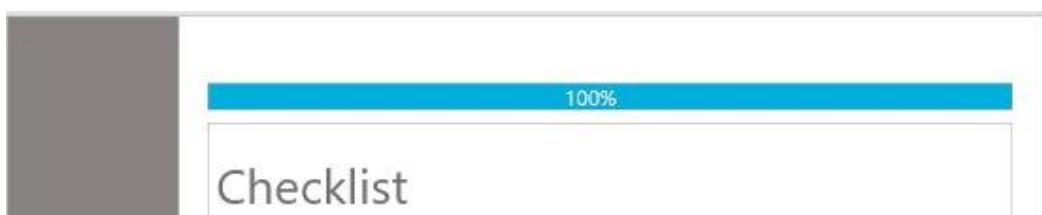
Embarcaciones			
Id	Nombre	Clase/Tipo	Acción
#	nombre	clase/tipo	inspección certificado
#	nombre	clase/tipo	inspección certificado
#	nombre	clase/tipo	inspección certificado

**Fuente:** Elaboración propia

Como se observa en la Figura 47, se plantea el diseño donde se escoge una embarcación para poder hacer la inspección.

Una vez seleccionada la embarcación, se redirigirá al formulario correspondiente, el cual a medida que se vaya llenando los datos mostrará una barra de progreso, como se observa en la Figura 48.

**FIGURA 48: BOCETO DE BARRA DE PROGRESO**



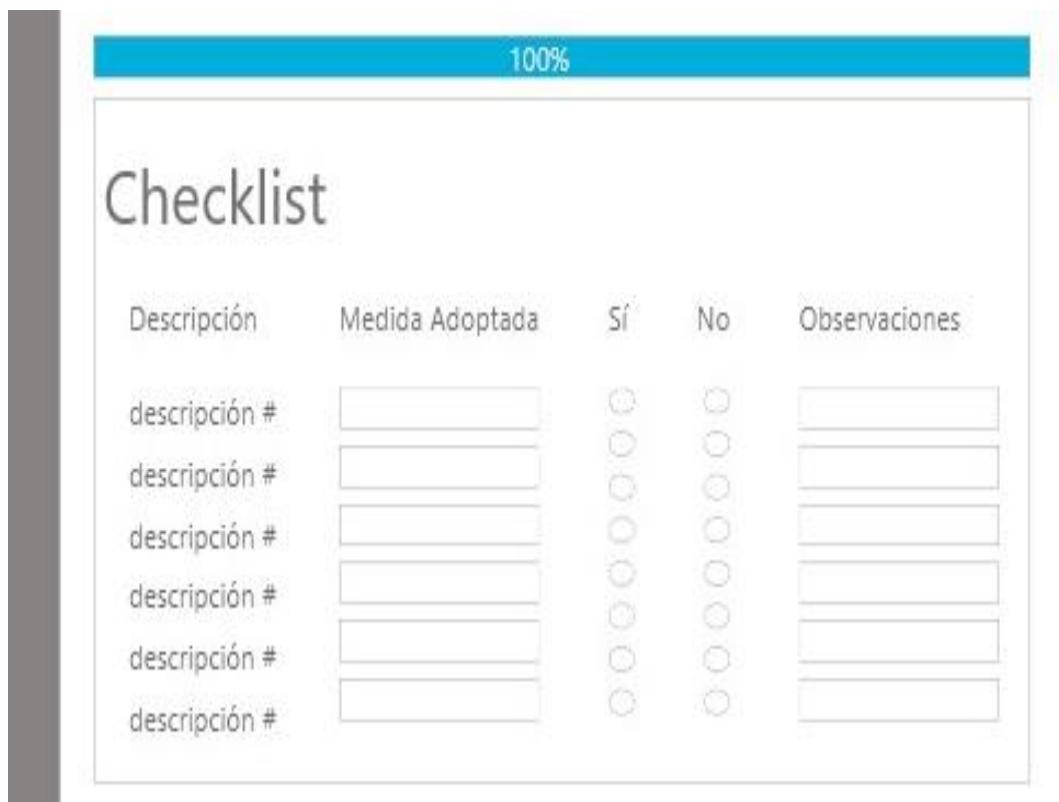
**Fuente:** Elaboración propia

Como se observa en la Figura 48, el formulario irá mostrando el porcentaje de su avance a medida que se vaya completando cada aspecto a ser considerado.

Para cada formulario se tendrán distintas descripciones o aspectos a ser considerados, además se podrá llenar los campos de “medida adoptada” y “observaciones” de manera opcional, esto siguiendo el modelo actual de formularios

que la Dirección General de Intereses Marítimos, Fluviales, Lacustres y Marina Mercante implementa, como se observa en la Figura 49.

**FIGURA 49: BOCETO DE FORMULARIO DE INSPECCIÓN**



100%

Checklist

Descripción	Medida Adoptada	Sí	No	Observaciones
descripción #	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
descripción #	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
descripción #	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
descripción #	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
descripción #	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
descripción #	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>

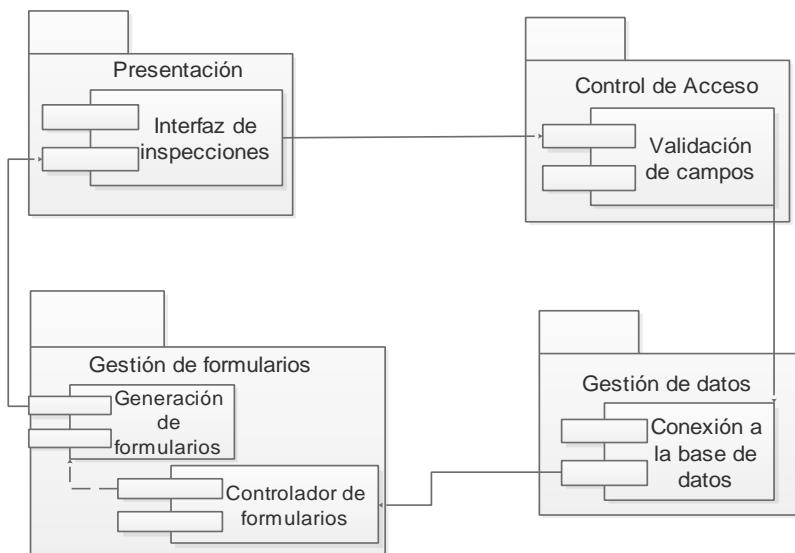
**Fuente:** Elaboración propia

Como se observa en la Figura 49, el formulario irá mostrando el porcentaje de su avance a medida que se vaya completando cada aspecto a ser considerado.

### 3.3.3.5 Diseño Navegacional Sprint 3

El módulo de “Inspecciones” estará compuesto por cuatro componentes, como se observa en Figura 50.

**FIGURA 50: DIAGRAMA DE COMPONENTES (INSPECCIONES)**



**Fuente:** Elaboración propia

En la Figura 50, se muestra la organización de los componentes de software del módulo "Inspecciones".

### 3.3.3.6 Construcción de Interfaces Sprint 3

Una vez realizado el diseño de las interfaces, se codificaron las mismas en el framework Laravel. Para poder realizar inspección se debe ingresar a través del primer ícono, como se observa en la Figura 51.

**FIGURA 51: PANTALLA PARA ACCEDER A INSPECCIÓN**

La captura de pantalla muestra una lista de embarcaciones registradas:

Número de registro	Nombre de embarcación	Clase/Tipo	Acción
a1919	Rivas	DRAGA	Inspección
A-20072	Jose	DRAGA	Inspección

**Fuente:** Elaboración propia

Como se observa en la Figura 51, se codificó e implementa la pantalla por la cual se accederá a los distintos formularios.

Una vez ingresado al ícono, el mismo generará el formulario correspondiente al tipo de embarcación, como se observa en la Figura 52.

**FIGURA 52: PANTALLA DE FORMULARIO DE INSPECCIÓN**

La captura de pantalla muestra la interfaz de usuario de la aplicación PLUTON. En la parte superior izquierda, hay un menú lateral oscuro con opciones como 'Administrador', 'Usuarios', 'Embarcaciones', 'Inspecciones' (destacada en azul), 'Solicitudes', 'Verificar Documento', 'Reportes', 'Manuales' y 'Cerrar Sesión'. En la parte superior central, se muestra el encabezado 'UNIDAD DE MARINA MERCANTE' y 'Checklist'. A la derecha, hay enlaces a 'Home' y 'Página de Inicio'. El checklist es una tabla que muestra la documentación y elementos varios que deben ser revisados. Los encabezados de la tabla son: 'DOCUMENTACIÓN Y ELEMENTOS VARIOS', 'MEDIDA ADOPTADA', 'SÍ' y 'NO'. La sección 'OBSERVACIONES' es un cuadro vacío para anotar comentarios. Los ítems de la lista son:

DOCUMENTACIÓN Y ELEMENTOS VARIOS	MEDIDA ADOPTADA	SÍ	NO	OBSERVACIONES
CERTIFICADO DE REGISTRO ORIGINAL (EO)	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
CERTIFICADO DE SEGURIDAD DE LA NAVEGACIÓN ORIGINAL VIGENTE. (EO)	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
CERTIFICADO DE FRANCOBORDO ORIGINAL VIGENTE. (ER)	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
CERTIFICADO DE MATRÍCULA ORIGINAL VIGENTE. (EO)	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
EL PATRÓN TIENE CARNET DE TRIPULANTE VIGENTE. (EO)	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>

En la parte inferior de la lista, hay un botón 'Siguiente'.

**Fuente:** Elaboración propia

Como se observa en la Figura 52, se muestra el progreso del formulario, además de tener los parámetros al momento de realizar la inspección.

### 3.3.3.7 Código Sprint 3

Para que este módulo funcione correctamente se realizó la siguiente codificación, la cual se ejecuta desde la carpeta de los controladores, como se observa en la Figura 53.

**FIGURA 53: CÓDIGO PARA INSPECCIONES**

```

class UsersController extends Controller
{
    function __construct()
    {
        $this->middleware('auth');
        $this->middleware('roles:admin',['except'=>['edit','updates']]);
    }

    public function index()
    {
        return view('users.index',[ 'users'=>User::all()]);
    }

    public function create()
    {
        return redirect()->route('users.create');
    }

    public function store(Request $request)
    {
        User::create([
            'name' => request('name'),
            'email' => request('email'),
            'state' => request('activo'),
            'password' => request('pass'),
        ]);
    }
}

return redirect()->route('users.index');

}

public function show($id)
{
    $user = User::findOrFail($id);
    return view('users.show',compact('user'));
}

public function edit($id)
{
    $user = User::findOrFail($id);
    $this->authorize($user);
    return view('users.edit',compact('user'));
}

public function update(UpdateUserRequest $request, $id)
{
    $user = User::findOrFail($id);
    $this->authorize($user);
    $user->update($request->all());
    return redirect()->route('usuarios.index');
}

public function destroy($id)
{
    $user = User::findOrFail($id);
    $this->authorize($user);
    $user->delete();
    return redirect()->route('usuarios.index');
}

```

**Fuente:** Elaboración propia

Como se observa en la Figura 53, se codificaron los distintos métodos para poder realizar el control de inspecciones de acuerdo con los requisitos previamente mencionados en la Tabla 12 del presente documento.

### 3.3.3.8 Prueba Unitaria Sprint 3

Una vez concluida la codificación se procedió a realizar las pruebas "Mock", para el controlador de formularios, como se observa en la Figura 54.

**FIGURA 54: PRUEBA UNITARIA MOCK (GESTIÓN DE USUARIOS)**

```
Tests\Unit\ChecklistControllerTest
✓ index
✓ show
✓ create
✓ edit
✓ destroy

Tests: 6 passed
Time: 0.06s
```

**Fuente:** Elaboración propia

Como se observa en la Figura 54, todas las pruebas del módulo de “Inspecciones” se efectuaron de manera exitosa.

### **3.3.4 Sprint 4 Módulo Verificación de Documentos**

El cuarto modulo del sistema se realizará con el fin de verificar la información de los documentos emitidos por el caso de estudio.

#### **3.3.4.1 Lista de Requerimientos Sprint 4**

Para el desarrollo del presente modulo se realiza la lista de requerimientos por parte del caso de estudio, el cual nos brinda las especificaciones las cuales deben ser incorporadas, como se observa en la Tabla 13.

**TABLA 13: REQUERIMIENTOS MÓDULO DE SEGURIDAD**

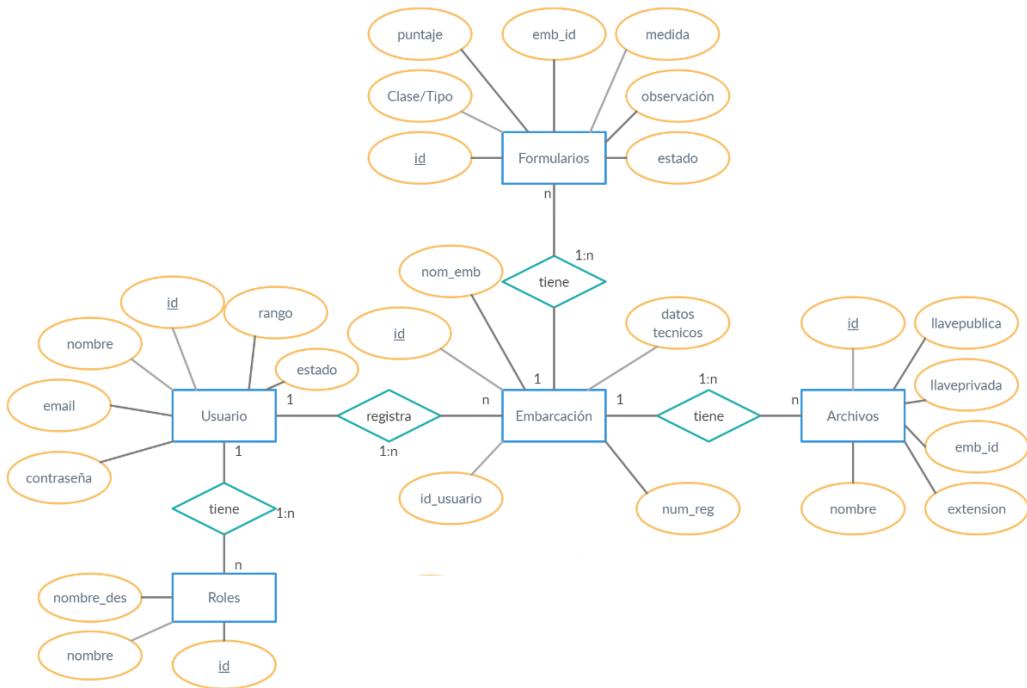
Número	Requerimiento	Descripción	Tipo	Prioridad
1	Generación de par de llaves	Capacidad del sistema de generar llave pública y llave privada	Funcional	Alta
2	Guardar el par de llaves	Guardar el par de llaves generado, y asociarlo a un documento.	Funcional	Alta
3	Código QR leíble	Capacidad de que el código QR sea leíble por cualquier aplicación	No funcional	Media
4	Búsqueda de documento por código	Poder encontrar el documento a partir del escaneo del código QR en el certificado	Funcional	Baja
5	Mostrar enlace para visualizar el archivo	Una vez leído el código QR mostrar un enlace, el cual redireccione al certificado virtual	No funcional	Baja

**Fuente:** Elaboración propia

En la Tabla 13 se puede observar los requerimientos solicitados por la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, para verificar los distintos documentos.

Para el presente módulo se determinó la información que debe almacenar, por lo cual se dio inicio a realizar el modelo entidad-relación para el presente sistema, como se observa en Figura 55.

**FIGURA 55: DIAGRAMA E-R SPRINT 4**



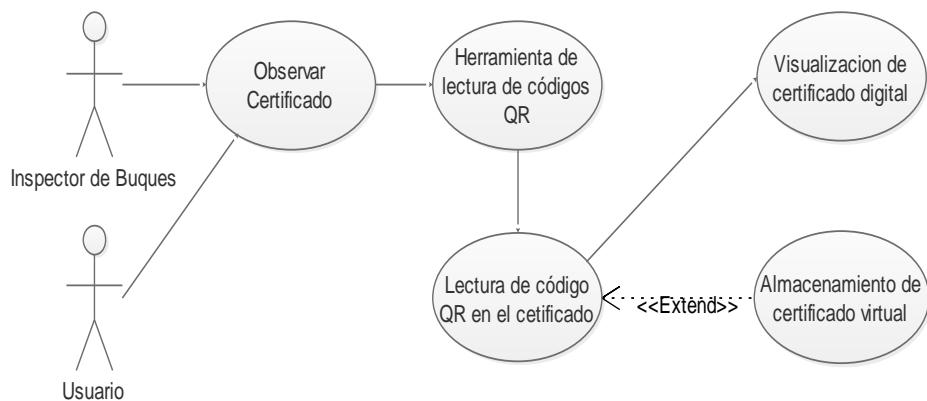
**Fuente:** Elaboración propia

En la Figura 55, se observa la entidad “Verificación de Documentos”, la cual presenta sus diferentes atributados, además se puede evidenciar que el identificador de esta es el atributo “id”.

### 3.3.4.2 Especificación del Proceso Sprint 4

En el módulo de “Verificación de Documentos”, el Inspector de Buques y un Usuario pueden obtener la información acerca de su certificado emitido por el caso de estudio, como se observa en la Figura 56.

**FIGURA 56: DIAGRAMA DE CASO DE USO (VERIFICACIÓN)**

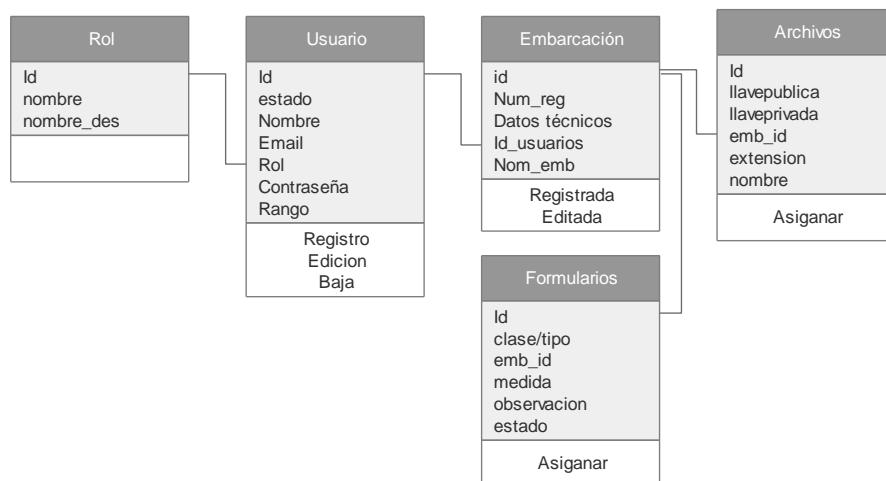


**Fuente:** Elaboración propia

Como se observa en la Figura 56, se ve cómo los actores “Usuario” e “Inspector de Buques” realizan la verificación de la información acerca de un certificado.

Una vez determinados los actores presentes dentro de este módulo y teniendo en cuenta las acciones que estos realizan, se realizó el diagrama de clases de la entidad “Embarcaciones”, como se observa en la Figura 57.

**FIGURA 57: DIAGRAMA DE CLASES SPRINT 4**



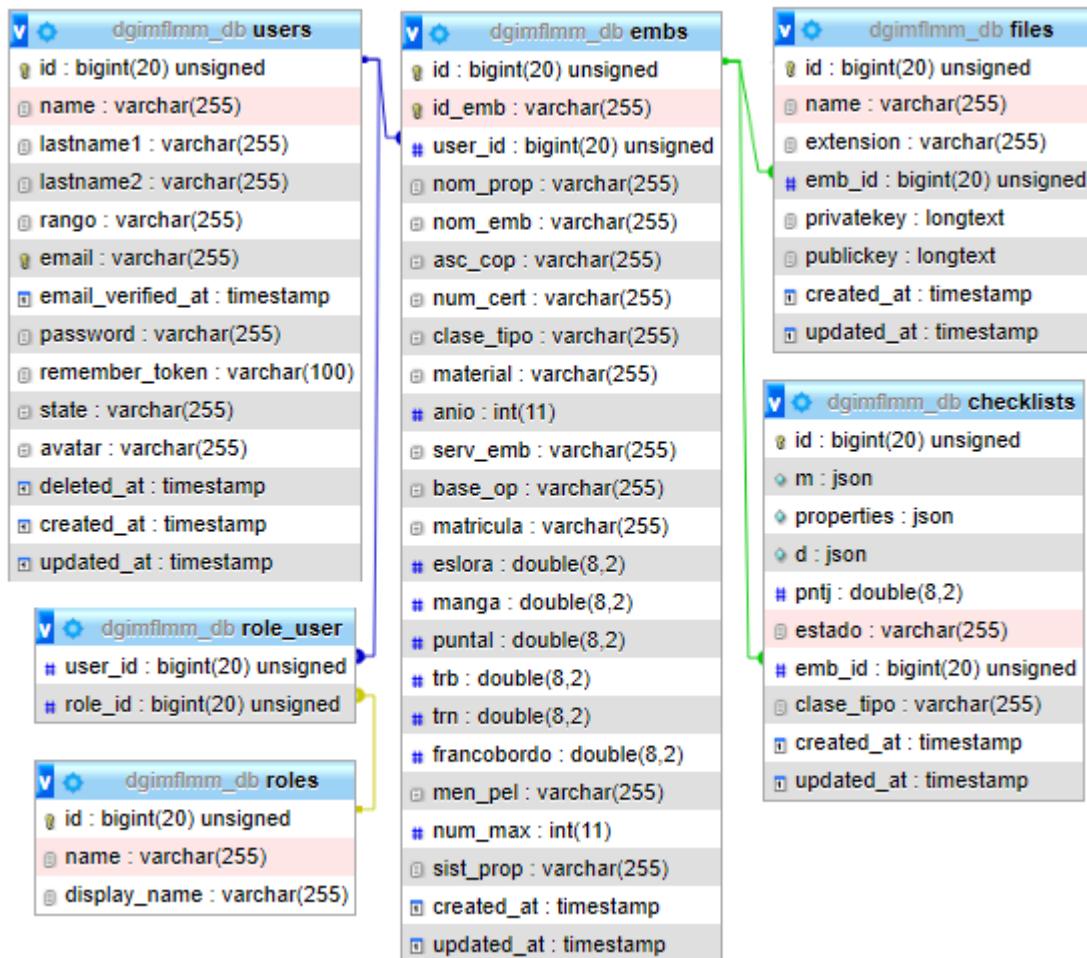
**Fuente:** Elaboración propia

Como se observa en la Figura 57 se tiene a la entidad “Inspección de Embarcación”, con los distintos atributos previamente mencionados, además se identificaron las acciones que estos podrán realizar dentro del sistema.

### 3.3.4.3 Diseño de Procesos Sprint 4

Una vez que ya definido la entidad y actores presente en este módulo se procedió a crear esta tabla dentro del gestor de base de datos, como se observa en la Figura 58.

**FIGURA 58: DIAGRAMA RELACIONAL SPRINT 4**

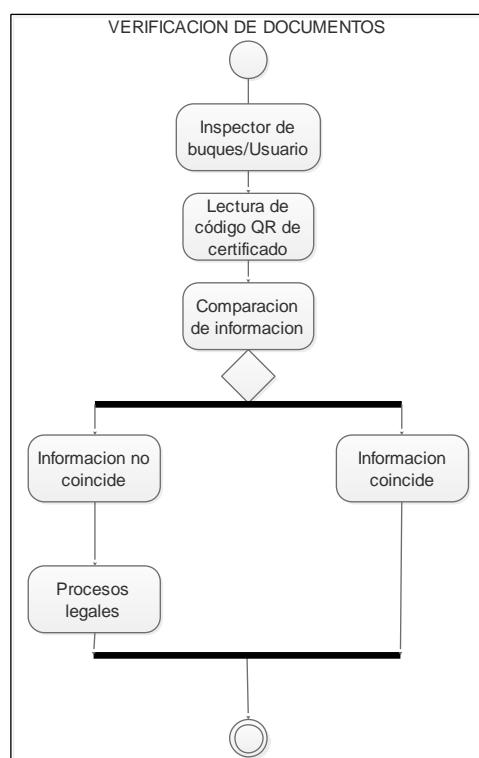


Fuente: Elaboración propia

Como se observa en la Figura 58, se procedió a crear la tabla de usuarios dentro del gestor de base de datos, de manera que se pueda proceder a registro a los mismo que podrán ingresar al sistema.

Se puede observar los pasos que se siguen para poder realizar la verificación de información de un certificado emitido por la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, como se observa en la Figura 59.

**FIGURA 59: DIAGRAMA DE ACTIVIDADES (SPRINT 4)**



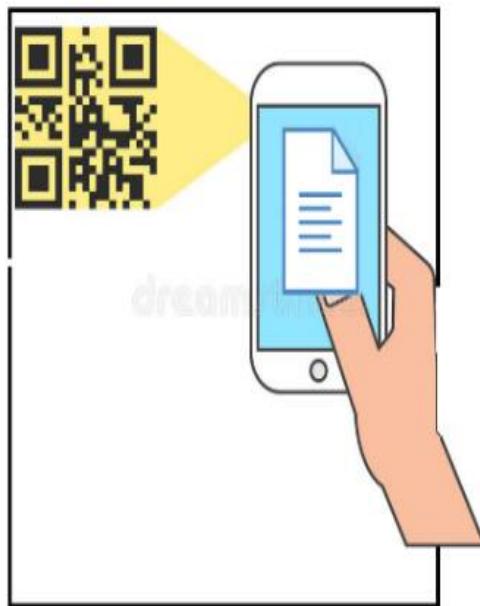
**Fuente:** Elaboración propia

Como se observa en la Figura 59, se muestra el proceso que se realiza al momento de revisión de documentos.

### 3.3.4.4 Diseño de Interfaces Sprint 4

Una vez identificadas las acciones que se realizaran, se procedió al diseño de pantallas para el correspondiente módulo, como se observa en la Figura 60.

**FIGURA 60: BOCETO DE VERIFICACIÓN DE DOCUMENTO**



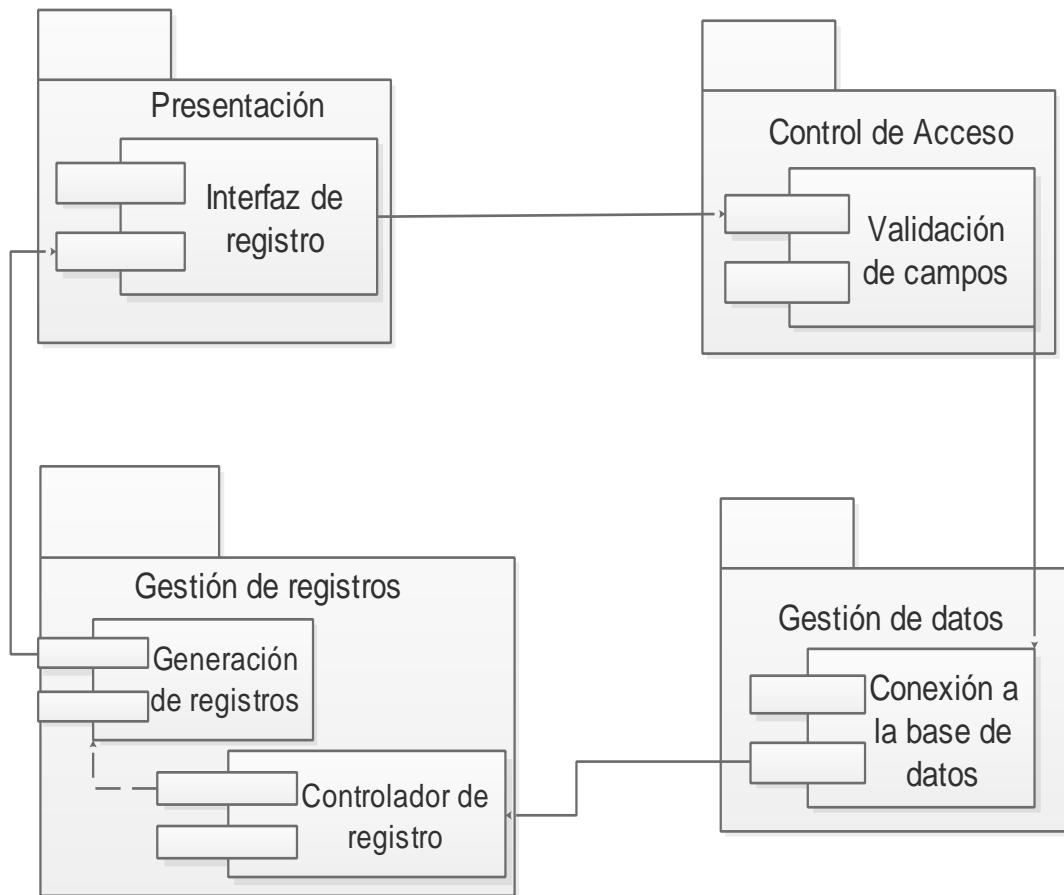
**Fuente:** Elaboración propia

Como se observa en la Figura 60, se planteó el funcionamiento de la verificación de documentos a partir de un código QR.

### 3.3.4.5 Diseño Navegacional Sprint 4

El módulo de "Verificación de Documentos." estará compuesto por cuatro componentes, como se observa en Figura 61.

**FIGURA 61: DIAGRAMA DE COMPONENTES (VERIFICACIÓN)**



**Fuente:** Elaboración propia

En la Figura 61, se muestra la organización de los componentes de software del módulo “Verificación de Documentos.”

#### 3.3.4.6 Construcción de Interfaces Sprint 4

Una vez realizado el diseño de las interfaces, se codificaron las mismas en el framework Laravel. Para poder realizar el registro, como se observa en la Figura 62.

**FIGURA 62: PANTALLA DE VERIFICACIÓN DE DOCUMENTO**

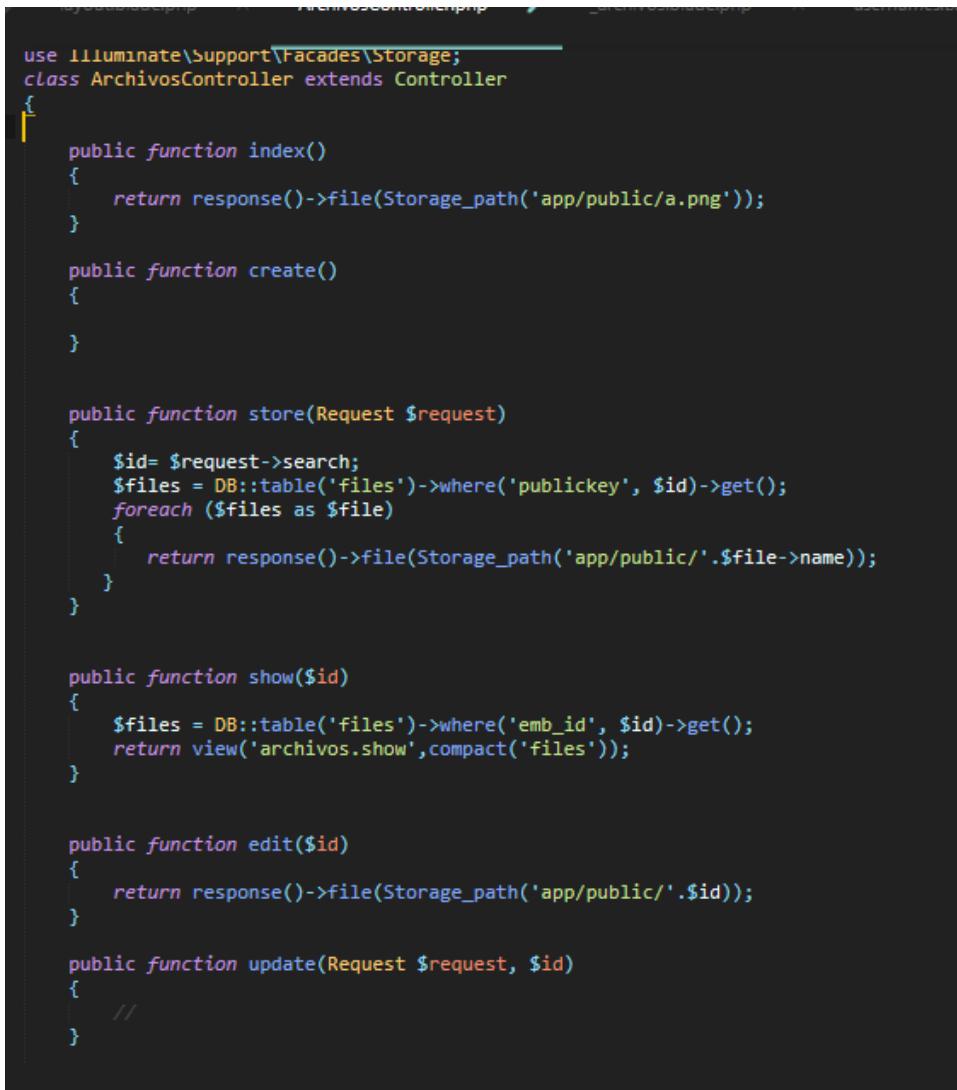
**Fuente:** Elaboración propia

Como se observa en la Figura 62, se tiene el formulario previo al registro al registro de una embarcación.

### 3.3.4.7 Código Sprint 4

Para que este módulo funcione correctamente se realizó la siguiente codificación, la cual se ejecuta desde la carpeta de los controladores, como se observa en la Figura 63.

**FIGURA 63: CÓDIGO PARA VERIFICACIÓN DE DOCUMENTOS**



```
use Illuminate\Support\Facades\Storage;
class ArchivosController extends Controller
{
    public function index()
    {
        return response()->file(Storage_path('app/public/a.png'));
    }

    public function create()
    {

    }

    public function store(Request $request)
    {
        $id= $request->search;
        $files = DB::table('files')->where('publickey', $id)->get();
        foreach ($files as $file)
        {
            return response()->file(Storage_path('app/public/'.$file->name));
        }
    }

    public function show($id)
    {
        $files = DB::table('files')->where('emb_id', $id)->get();
        return view('archivos.show',compact('files'));
    }

    public function edit($id)
    {
        return response()->file(Storage_path('app/public/'.$id));
    }

    public function update(Request $request, $id)
    {
        //
    }
}
```

**Fuente:** Elaboración propia

#### 3.3.4.8 Prueba Unitaria Sprint 4

Una vez concluida la codificación se procedió a realizar las pruebas "Mock", para el controlador de verificación de documentos, como se observa en la Figura 64.

**FIGURA 64: PRUEBA UNITARIA MOCK (VERIFICACIÓN)**

```
PASS  Tests\Unit\ArchivosControllerTest
✓ index
✓ show
✓ create
✓ edit
✓ destroy

Tests:  6 passed
Time:   1.11s
```

**Fuente:** Elaboración propia

Como se observa en la Figura 64, todas las pruebas del módulo de "Verificación de Documentos" se efectuaron de manera exitosa.

### 3.3.5 Sprint 5 Módulo de Reportes

El ultimo modulo del sistema hace referencia a los reportes de diferentes parámetros especificados por el caso de estudio.

#### 3.3.5.1 Lista de Requerimientos Sprint 5

Para el desarrollo del presente modulo se realiza la lista de requerimientos por parte del caso de estudio, el cual nos brinda las especificaciones las cuales deben ser incorporadas, como se observa en la Tabla 14.

**TABLA 14: REQUERIMIENTOS MÓDULO DE REPORTES**

Número	Requerimiento	Descripción	Tipo	Prioridad
1	Generar reportes en formato PDF	Capacidad del sistema, de generar los reportes especificados en formato PDF	Funcional	Media
2	Generar reportes de embarcaciones	Generar reportes de todas las embarcaciones registradas, incluyendo la persona responsable de tal hecho	Funcional	Alta
3	Generar reportes de usuarios	Generar un reporte, el cual muestre los usuarios activos e inactivos del sistema	Funcional	Alta
4	Inclusión de cabecera en el reporte	Incluir en la cabecera del reporte el nombre de la unidad, el país y una imagen de las FF.AA.	No funcional	Baja
5	Insertar marca de agua	Insertar una marca de agua en los reportes a ser emitidos	No funcional	Baja

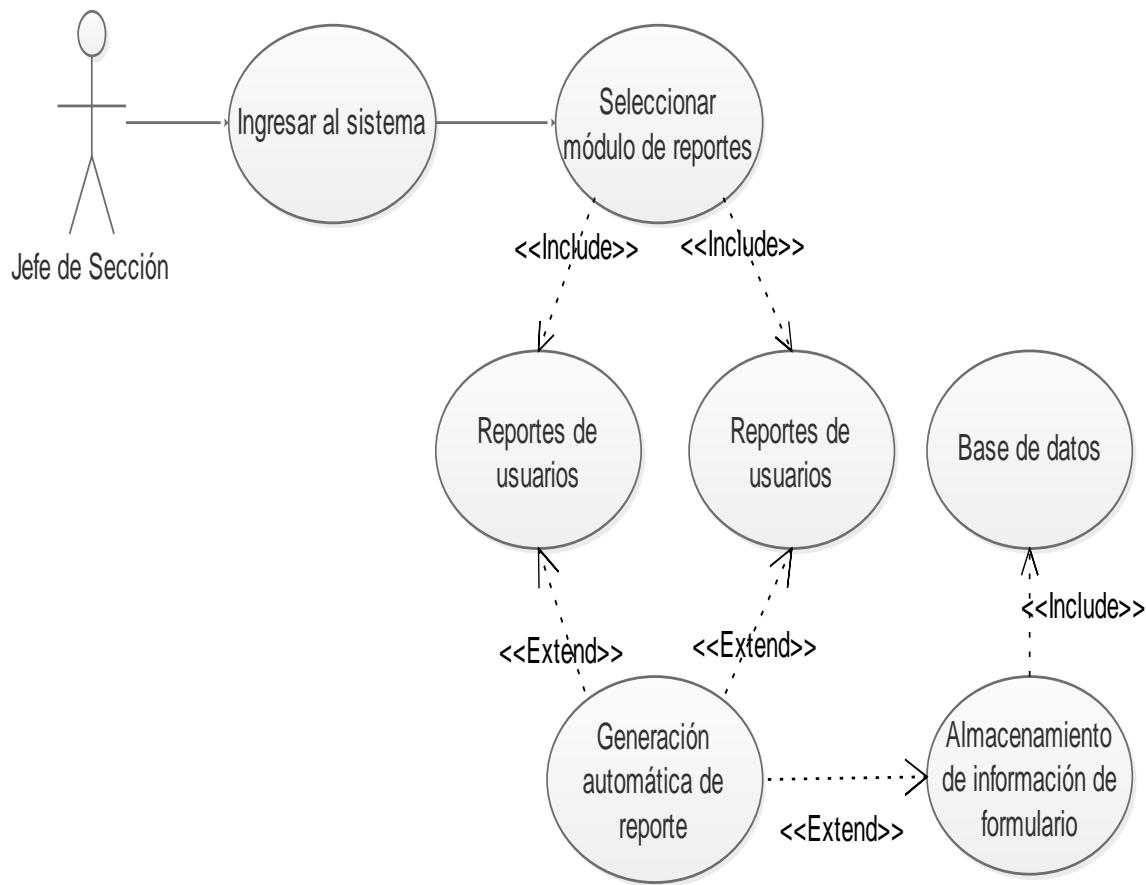
**Fuente:** Elaboración propia

En la Tabla 14 se puede observar los requerimientos solicitados por la Dirección General de Intereses Marítimos, Fluviales Lacustre y Marina Mercante, para los reportes que el sistema emita.

### 3.3.5.2 Especificación del Proceso Sprint 5

En el módulo de “Reportes”, el Jefe de Sección, elaborara los dos distintos reportes, de modo que, de conocimiento a instancias superiores, como se observa en la Figura 65.

**FIGURA 65: DIAGRAMA DE CASO DE USO (REPORTES)**



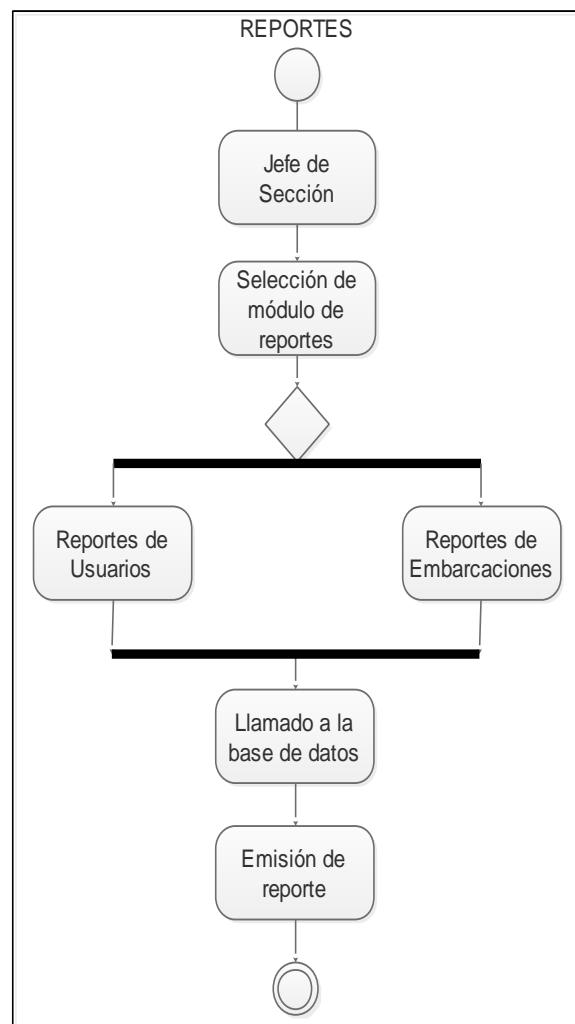
**Fuente:** Elaboración propia

Como se observa en la Figura 65, se ve cómo el usuario con el rol “Jefe de Sección” realiza los distintos procesos para emitir los reportes.

### 3.3.5.3 Diseño de Procesos Sprint 5

El proceso antes descrito se encuentra explicado de manera simplificada, como se observa en la Figura 66.

**FIGURA 66: DIAGRAMA DE ACTIVIDADES (SPRINT 5)**



**Fuente:** Elaboración propia

Como se observa en la Figura 66, se muestra el proceso que se realiza al momento de generar reportes.

#### 3.3.5.4 Diseño de Interfaces Sprint 5

Una vez identificadas las acciones que se realizaran, se procedió al diseño de pantallas para el correspondiente módulo, como se observa en la Figura 67.

## FIGURA 67: BOCETO DE REPORTE

Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante Unidad de Marca Mercante La Paz-Bolivia			
<h3>Reportes de Embarcaciones</h3>			
<b>Nombre:</b> Luis			
<b>Fecha:</b> 2020-10-29 22:42:02			
<b>Lista de Embarcaciones</b>			
Número de Registro	Nombre de Embarcación	Encargado del Registro	Fecha de Registro
P-12970001	PTO. QUIJARRO	Luis	1995-03-27 00:00:00
P-11980002	ULISES II	Luis	1989-01-22 00:00:00
P-11980003	ULISES I	Luis	1989-01-03 00:00:00
P-11980004	ULISES	Luis	1997-05-24 00:00:00
P-11980005	FRANCIS ENA I	Luis	1988-06-25 00:00:00
P-11980006	FRANCIS ENA II	Luis	1997-10-11 00:00:00
P-11980007	NANI KARINA	Luis	1992-03-27 00:00:00
P-11980008	PERU	Luis	1995-07-16 00:00:00

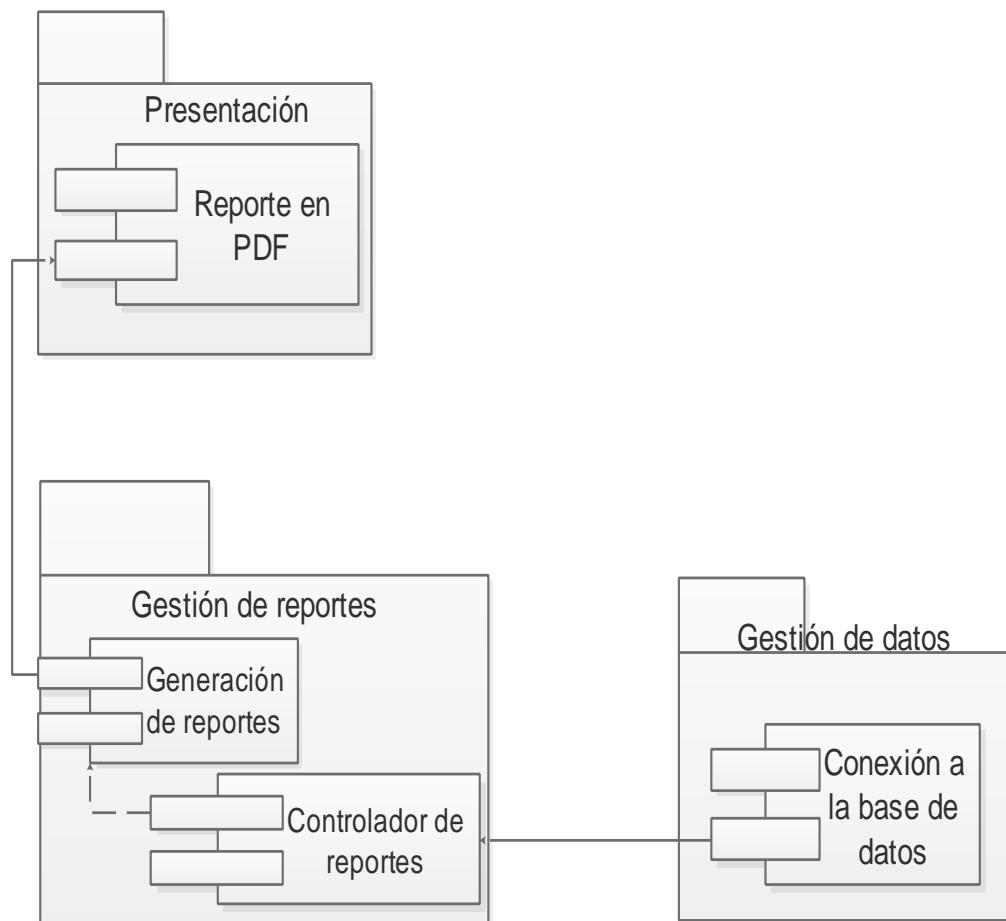
**Fuente:** Elaboración propia

Como se observa en la Figura 67, se plantea el diseño de reporte.

### 3.3.5.5 Diseño Navegacional Sprint 5

El módulo de "Reportes" estará compuesto por cuatro componentes, como se observa en Figura 68.

**FIGURA 68: DIAGRAMA DE COMPONENTES (REPORTES)**



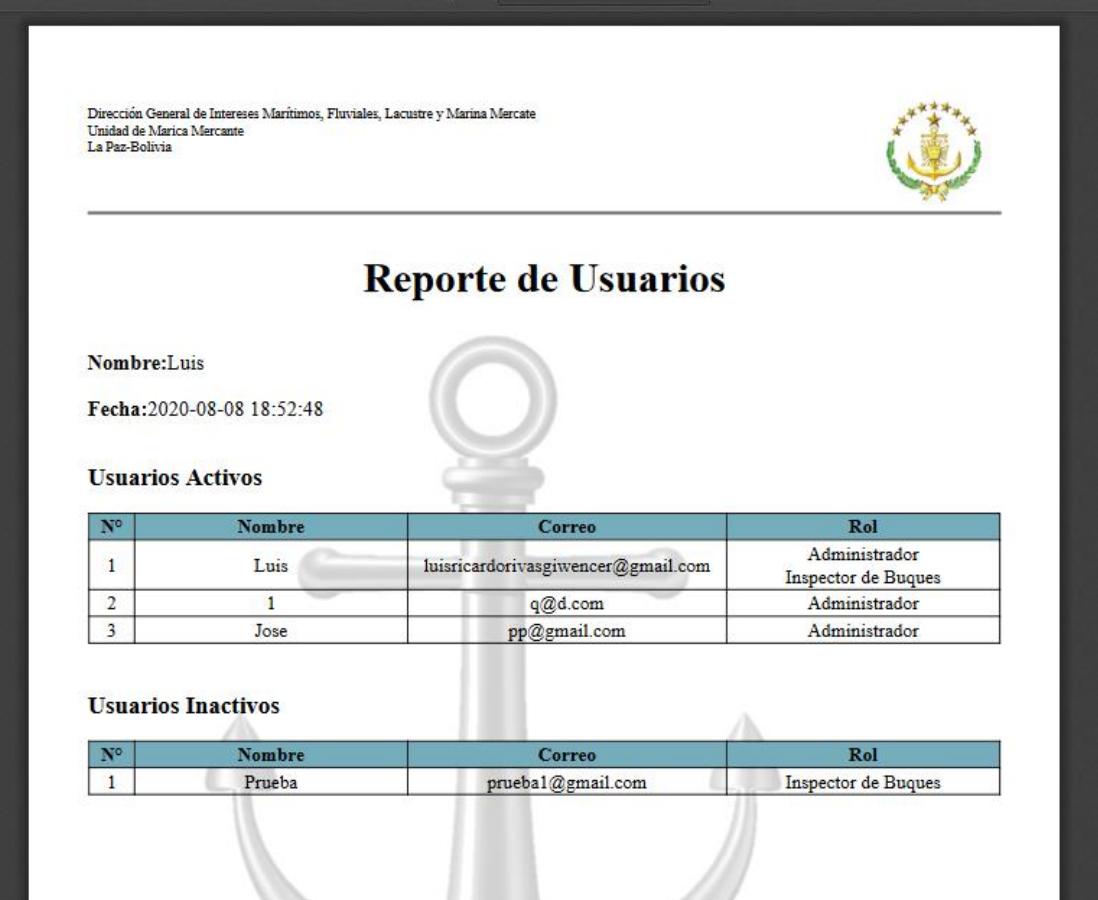
**Fuente:** Elaboración propia

En la Figura 68, se muestra la organización de los componentes de software del módulo "Reportes"

#### 3.3.5.6 Construcción de Interfaces Sprint 5

Una vez realizado el diseño del reporte, se codificaron los mismos en el framework Laravel para emitir reportes, como se observa en la Figura 69.

**FIGURA 69: REPORTE**



Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante  
Unidad de Marca Mercante  
La Paz-Bolivia

**Reporte de Usuarios**

**Nombre:** Luis  
**Fecha:** 2020-08-08 18:52:48

**Usuarios Activos**

Nº	Nombre	Correo	Rol
1	Luis	luisricardorivasgwencer@gmail.com	Administrador Inspector de Buques
2	1	q@d.com	Administrador
3	Jose	pp@gmail.com	Administrador

**Usuarios Inactivos**

Nº	Nombre	Correo	Rol
1	Prueba	prueba1@gmail.com	Inspector de Buques

**Fuente:** Elaboración propia

Como se observa en la Figura 69 el formulario para registrar una embarcación, con el número de registro asignado.

### 3.3.5.7 Código Sprint 5

Para que este módulo funcione correctamente se realizó la siguiente codificación, la cual se ejecuta desde la carpeta de los controladores, como se observa en la Figura 70.

## FIGURA 70: CÓDIGO PARA REPORTE

```
class ReportController extends Controller
{
    public function index()
    {
        $fecha=Carbon::now();
        $pdf=PDF::loadView('reports.index',[

            'users'=>User::all(),
            ],compact('fecha'));
        return $pdf->stream();
    }

    public function create()
    {
        $fecha=Carbon::now();
        $users=User::all();
        $pdf=PDF::loadView('reports.show',[

            'embs'=>Emb::all(),
            ],
            compact('fecha','users'));
        return $pdf->stream();
    }

    public function show($id)
    {
        $pdf=PDF::loadView('reports.index',[

            'embs'=>Emb::all(),
            ],compact('fecha')));
        return $pdf->stream();
    }

    public function edit($id)
    {
        //
    }

    public function update(Request $request, $id)
    {
        //
    }

    public function destroy($id)
    {
        //
    }
}
```

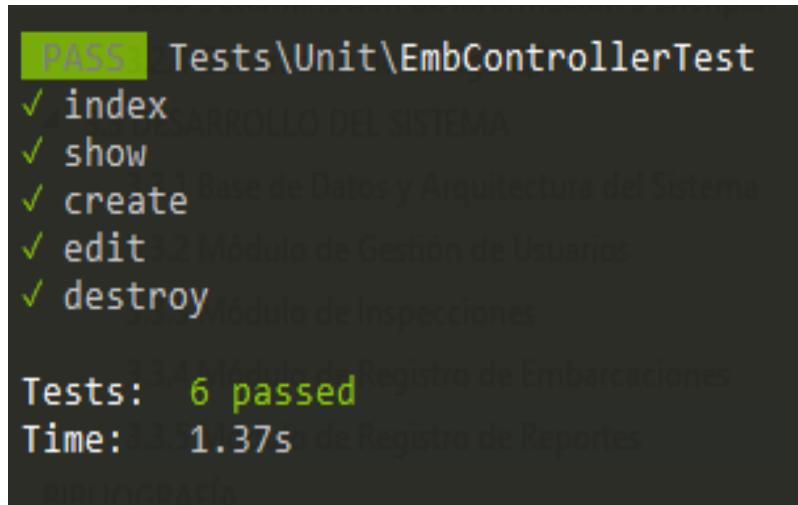
Fuente: Elaboración propia

Como se observa en la Figura 70, se codificaron los distintos métodos para poder realizar el registro de embarcaciones en base a los requisitos previamente mencionados en la Tabla 14 del presente documento.

### 3.3.5.8 Prueba Unitaria Sprint 5

Una vez concluida la codificación se procedió a realizar las pruebas "Mock", para el controlador de embarcaciones, como se observa en la Figura 71.

**FIGURA 71: PRUEBAS UNITARIAS MOCK (REPORTES)**



```
PASS  Tests\Unit\EmbControllerTest
✓ index
✓ show
✓ create
✓ edit
✓ destroy

Tests:  6 passed
Time:  1.37s
```

**Fuente:** Elaboración propia

Como se observa en la Figura 71, todas las pruebas del módulo de "Reportes" se efectuaron de manera exitosa.

### **3.4 PRUEBAS DEL SISTEMA**

Tras concluir con el desarrollo de los módulos del sistema, y los respectivos sprints, se empezó a realizar pruebas de funcionamiento.

#### **3.4.1 Pruebas de Integración**

A manera de comprobar que la integración de módulos se realizó de manera correcta se realizaron dos pruebas, las pruebas de usabilidad y las pruebas Mock. Estas nos garantizarán que el sistema funcione correctamente.

El primer tipo de pruebas realizadas son las pruebas de usabilidad, las cuales son realizadas con ayuda del framework Laravel, de modo que las mismas simulan el funcionamiento del sistema, como se observa en la Figura 72.

**FIGURA 72: EXAMEN DE USABILIDAD**

```
=> ...ntegration\Console\CreateIndexCommandTest ✓
=> ...ntegration\Console\DeleteIndexCommandTest ✓
=> ...gration\Console\IndexDocumentsCommandTest ✓ ✓ ✓
=> Tests\Integration\DocumentTest           ✓ ✓ ✓ ✓ ✓
=> ...gration\Hydrators\ArrayObjectHydratorTest ✓ ✓ ✓ ✓ ✓
=> Tests\Integration\IndexSettingsTest      ✓ ✓
=> Tests\Integration\IndexTest              ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
=> Tests\Integration\IndexableObserverTest  ✓ ✓ ✓ ✓ ✓
=> Tests\Integration\Indexing\IndexQueryTest ✓ ✓ ✓ ✓ ✓ ✓ ✓
10/10 [=====] 100%✓ ✓
=> Tests\Integration\Indexing\LoggerTest     ✓ ✓
=> ...positories\Elasticsearch\FindByFieldTest •
=> Tests\Integration\ServiceProviderTest      ✓ ✓ ✓ ✓ ✓ ✓ ✓

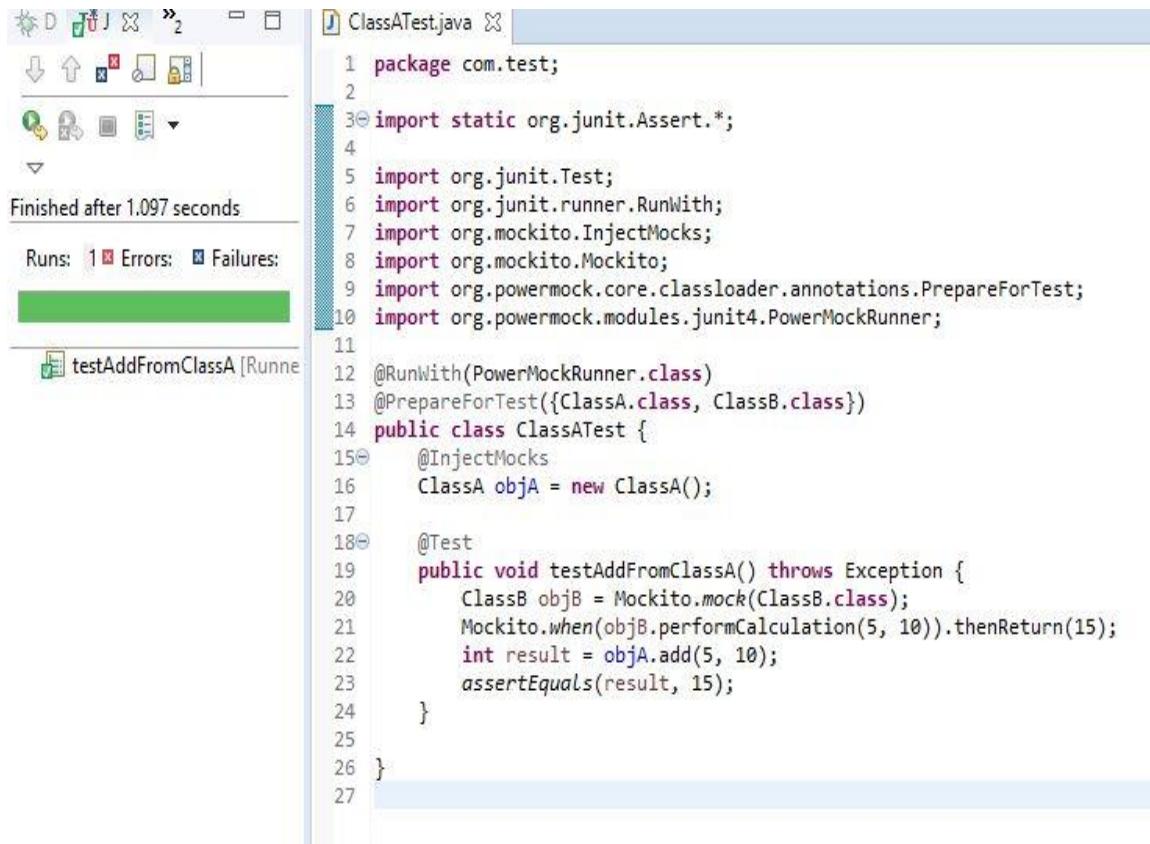
Time: 7.73 seconds, Memory: 28.00MB
```

**Fuente:** Elaboración propia

Como se observa en la Figura 72, se tiene el resultado de las pruebas de usabilidad proporcionadas por el framework de desarrollo.

Por último, se realizó las pruebas Mock del sistema, las cuales simulan la creación de objetos y prueban todos los módulos del sistema, como se observa en la Figura 73.

**FIGURA 73: PRUEBAS MOCK DEL SISTEMA**



```
1 package com.test;
2
3 import static org.junit.Assert.*;
4
5 import org.junit.Test;
6 import org.junit.runner.RunWith;
7 import org.mockito.InjectMocks;
8 import org.mockito.Mockito;
9 import org.powermock.core.classloader.annotations.PrepareForTest;
10 import org.powermock.modules.junit4.PowerMockRunner;
11
12 @RunWith(PowerMockRunner.class)
13 @PrepareForTest({ClassA.class, ClassB.class})
14 public class ClassATest {
15     @InjectMocks
16     ClassA objA = new ClassA();
17
18     @Test
19     public void testAddFromClassA() throws Exception {
20         ClassB objB = Mockito.mock(ClassB.class);
21         Mockito.when(objB.performCalculation(5, 10)).thenReturn(15);
22         int result = objA.add(5, 10);
23         assertEquals(result, 15);
24     }
25
26 }
27
```

**Fuente:** Elaboración propia

### 3.5 IMPLEMENTACIÓN DEL SISTEMA

Una vez concluido el desarrollo del sistema se procederá a su implementación de modo que todos los usuarios respectivos tengan acceso y realicen las acciones que le corresponden.

Para la implementación del sistema se escogió el servidor del Heroku frente al de Amazon Web Service, esto debido a las ventajas que ofrece, como se observar en la Tabla 15.

**TABLA 15: COMPARACIÓN HEROKU VS AWS**

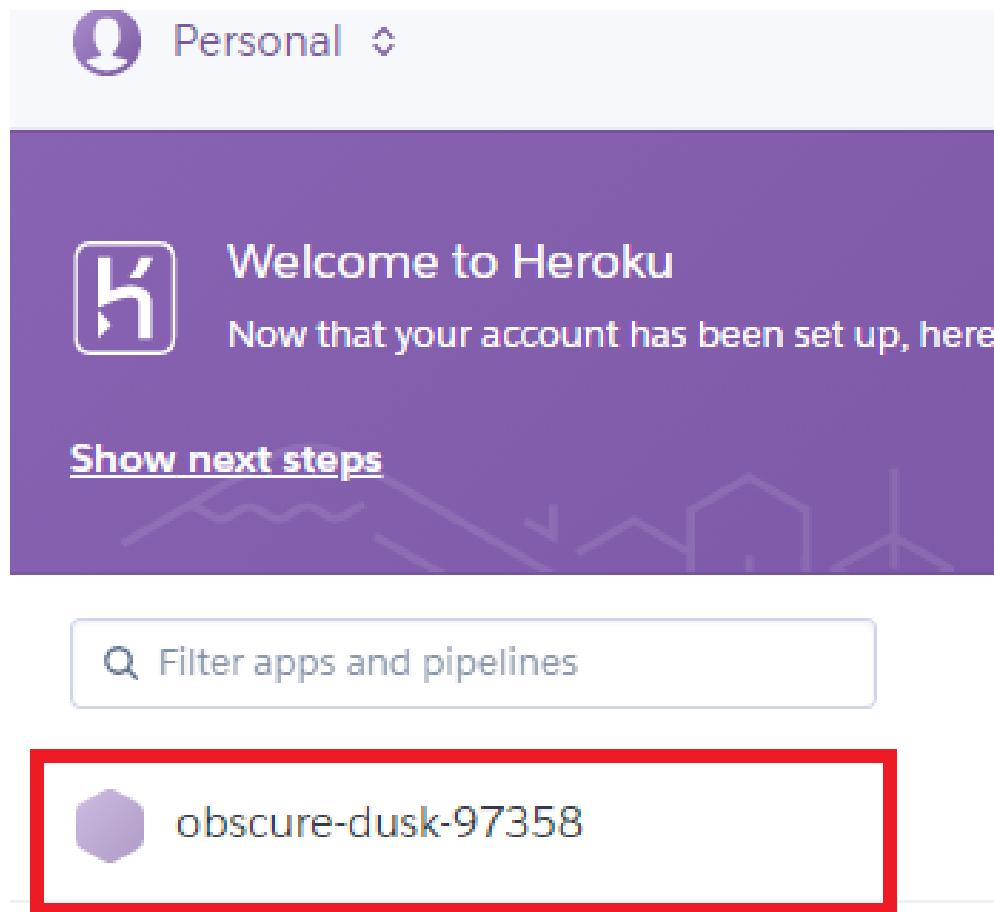
Factor	Heroku	AWS
Propietario	Salesforce.com	Amazon.com
Almacenado en	Centro de datos de Amazon	Servidores propios
Tipo de servicio	PaaS	IaaS PaaS
Lenguajes	Node.js, Java, Ruby, PHP, Phyton, Go, Scala, Clojure	Ruby, .NET, Node.js, Docker, PHP, Linux, Windows
Áreas de operación	Internacional	Internacional
Ingeniero en desarrollo necesitado	Sin necesidad	Necesario
Escalado automático	Si	Si
Despliegue rápido	Si	No
Conformidad con estándares de despliegue	Si	Si
Costo(básico)/adicional	Gratis/ 35\$ por complemento	1 año gratis/ 15\$ por mes
Servicios soportados	Todos	Todos

**Fuente:** Recopilación de fuentes virtuales

### 3.5.1 Instalación del sistema

Una vez concluido el sistema procedió a realizar la implementación dentro un servidor de prueba (simulación), llamado Heroku. Para desplegar el presente proyecto primeramente se creó un proyecto, como se observa en la Figura 74.

**FIGURA 74: CREACIÓN DE PROYECTO HEROKU**



**Fuente:** [www.Heroku.com](http://www.Heroku.com)

Como se observa en la Figura 74 se creó un proyecto dentro de Heroku, el cual crea el mismo con un nombre aleatorio.

Posterior a la creación del proyecto se procedió a subir los archivos dentro del mismo, los cuales se encuentran en un ordenador local, para tal acción se hizo el uso de Heroku CLI, el cual es el uso de línea de comando para cargar los archivos, como se observa en la figura 75.

**FIGURA 75: SUBIDA DE ARCHIVOS A HEROKU**

```
remote:      Discovered Package: laravel/tinker    REDIS_PORT=6379
remote:      Discovered Package: laravel/ui
remote:      Discovered Package: nesbot/carbon      MAIL_MAILER=smtp
remote:      Discovered Package: realrashid/sweetalert2 MAIL_HOST=smtp.mailtrap.io
remote:      Discovered Package: simplesoftwareio/simple-qrcode MAIL_PORT=2525
remote:      Package manifest generated successfully. MAIL_USERNAME=null
remote:      -----> Preparing runtime environment...
remote:      -----> Checking for additional extensions to install MAIL_PASSWORD=null
remote:      -----> Discovering process types MAIL_FROM_ADDRESS=null
remote:      Procfile declares types -> web MAIL_FROM_NAME="${APP_NAME}"
remote:      AWS_ACCESS_KEY_ID=
remote:      AWS_SECRET_ACCESS_KEY=
remote:      AWS_DEFAULT_REGION=us-east-1 AWS_BUCKET=
remote:      AWS_BUCKET=
remote:      Done: 28M
remote:      -----> Launching...
remote:      Released v4
remote:      https://obscure-dusk-97358.herokuapp.com/ deployed to Heroku
remote:      PUSHED APP TO
remote:      PUSHER_APP_KEY=
remote:      PUSHER_APP_SECRET=
remote:      PUSHER_APP_CLUSTER=mt1
remote: bootstrap
remote: Verifying deploy... done.
To https://git.heroku.com/obscure-dusk-97358.git
 * [new branch]      master => master
MTM PUSHED APP KEY=PKGRJNHRP-4U
```

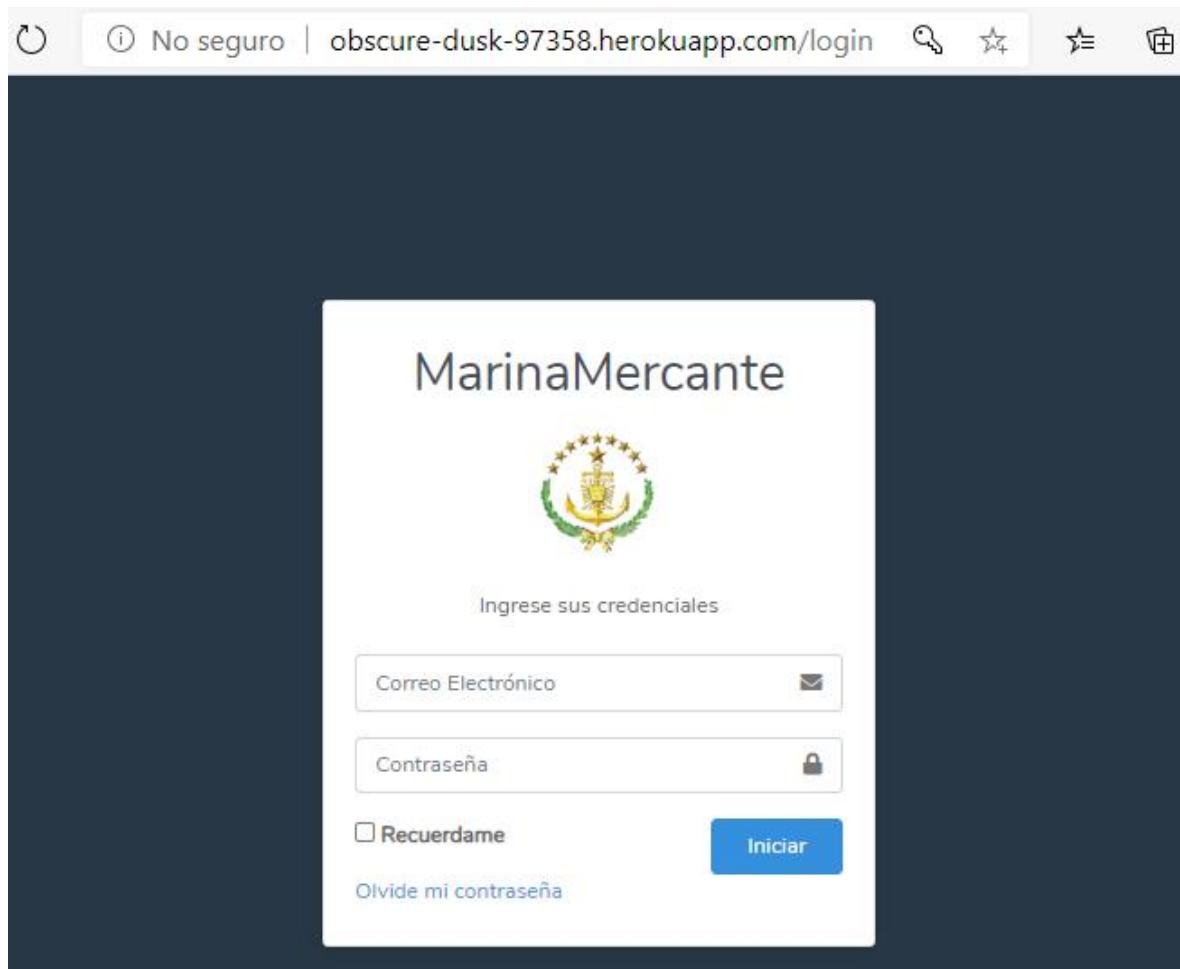
**Fuente:** Elaboración propia

En la Figura 75 se observa que los archivos de actual Trabajo de Grado fueron subidos de manera correcta al proyecto el cual fue creado.

### 3.5.2 Revisión de funcionamiento

Una vez subidos los archivos se procedió a ingresar a la dirección la cual nos dio el proyecto creado, en el cual se puede observar que el sistema se encuentra en el servidor de Heroku, como se observa en la Figura 76.

**FIGURA 76: SISTEMA SUBIDO A LA PLATAFORMA HEROKU**



**Fuente:** www.Heroku.com

## CAPÍTULO IV

# ANÁLISIS COSTO BENEFICIO



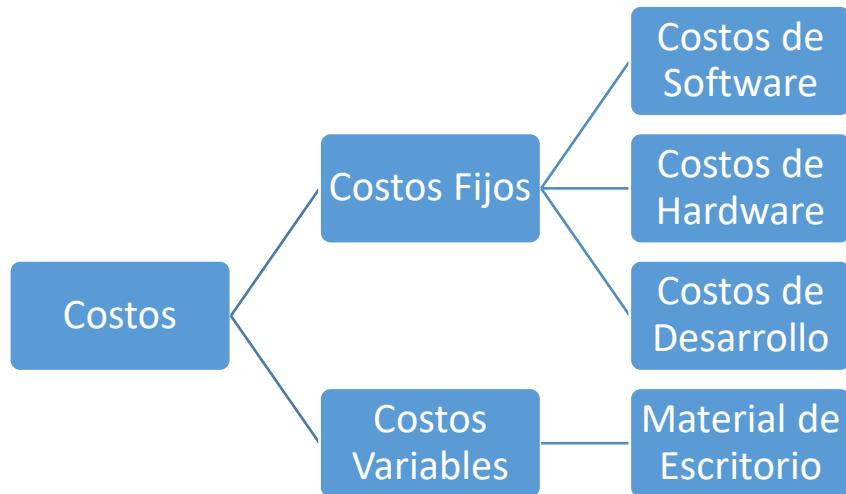
## CAPÍTULO IV

### ANÁLISIS COSTO BENEFICIO

#### 4.1 DETERMINACIÓN DE COSTOS

En este punto se detallan los costos involucrados en el desarrollo del sistema propuesto en el presente Trabajo de Grado, como se observa en la Figura 76.

**FIGURA 77: ESQUEMA DE COSTO-BENEFICIOS**



**Fuente:** Elaboración propia

En la Figura 76 se puede observar el tipo de costos determinados durante el desarrollo del sistema.

#### **4.1.1 Costos Fijos**

A continuación, se detallarán los costos fijos en los que se incurrieron en el sistema. Para el desarrollo de este se considera a estos costos como aquellos que se mantienen constantes durante el desarrollo del Trabajo de Grado.

##### **4.1.1.1 Costos de Software**

A continuación, en la Tabla 16 se detalla los costos de software en los cuales incurrirán los clientes para poder hacer uso del sistema y sus funcionalidades.

**TABLA 16: TABLA DE COSTOS DE SOFTWARE (CLIENTES)**

**(Expresado en bolivianos)**

Nombre	Descripción	Costo
Navegador	Navegador web por el cual se puede acceder al sistema, el mismo es compatible con: Chrome, Opera, Firafox y el navegador Edge	0
Lector de código QR	Aplicación para poder leer códigos QR, disponible tanto para dispositivos Android, como para dispositivos los IOS	0
<b>Total Bolivianos</b>		<b>0</b>

**Fuente:** Elaboración propia

Como se observa en la Tabla 16 los clientes no incurren en ningún gasto, debido a que dichos softwares se pueden descargar de manera gratuita de internet.

A continuación, en la Tabla 17 se detalla los costos en los cuales incurrirán los servidores para poder hacer uso del sistema y sus funcionalidades.

**TABLA 17: TABLA DE COSTOS DE SOFTWARE (SERVIDOR)**

Nombre	Descripción	Costo
Laragon	Entorno de desarrollo virtual, el cual tiene la capacidad de realizar hosts virtuales	0
PHP7.4	Lenguaje de código abierto en su séptima versión	0
HTML	Lenguaje de marcado para elaboración de páginas web	0
JavaScript	Lenguaje de programación	0
PHPMyAdmin	Gestor de Base de Datos	0
Laravel	Framework para el desarrollo de aplicaciones	0
Ubuntu 20.04.1	Sistema operativo donde se encontrará el sistema y la base de datos	0
<b>Total Bolivianos</b>		<b>0</b>

**Fuente:** Elaboración propia

Como se observa en la Tabla 17 los servidores no incurren en ningún gasto, debido a que dichos softwares son de código abierto, de manera que cualquier persona los puede adquirir.

#### 4.1.1.2 Costos de Hardware

A continuación, en la Tabla 18 se detalla los costos de hardware en los cuales incurrirán los clientes para poder hacer uso del sistema y sus funcionalidades.

**TABLA 18: TABLA DE COSTOS DE HARDWARE (CLIENTE)**

**(Expresado en bolivianos)**

Nombre	Descripción técnica	Descripción de uso	Cantidad	Costo Unitario	Costo Total
Tabletas	Tabletas marca Samsung modelo Tab a	Las tablets serán utilizadas para que los inspectores puedan realizar las actividades de seguimiento y control	5	1497	7.485
<b>Total Bolivianos</b>					<b>7.485</b>

**Fuente:** Elaboración propia

Como se observa en la Tabla 18 los clientes para poder realizar el uso del sistema, en cuanto al hardware, tiene un costo de Bs 7.485.- (Siete mil cuatrocientos ochenta y cinco bolivianos 00/100).

A continuación, en la Tabla 19 se detalla los costos en los cuales incurrirán los servidores, tomando en cuenta la parte del hardware, para poder hacer uso del sistema y sus funcionalidades.

**TABLA 19: TABLA DE COSTOS DE HARDWARE (SERVIDOR)**

Nombre	Descripción técnica	Descripción de uso	Cantidad	Costo Unitario	Costo Total
Estación de trabajo	Ordenador personal, procesador core i5 de quinta generación, tarjeta de video de 4gb de Ram, memoria HHDD 500gb	La estación de trabajo será utilizada para poder configurar el servidor y cargar la información precisa al registro	1	5350	5.350
<b>Total Bolivianos</b>					<b>5.350</b>

**Fuente:** Elaboración propia

Como se observa en la Tabla 19 el costo del hardware para los servidores es de Bs. 5.350.- (Cinco mil trescientos cincuenta bolivianos 00/100).

#### 4.1.1.3 Costos de Desarrollo

Para realizar el cálculo del costo para el desarrollo del software del presente Trabajo de Grado se utilizó el modelo COCOMO II, utilizando y explicando las fórmulas correspondientes.

Para el cálculo del esfuerzo en personas se utiliza la siguiente Ecuación 1:

## **ECUACIÓN 1: CÁLCULO DEL ESFUERZO**

$$E = A * (KLCD)^B$$

**Fuente:** COCOMO II

Donde:

- E: esfuerzo aplicado en persona/mes.
- KLD: líneas de código expresada en miles.
- A/B: constante del modelo COCOMO

Para el cálculo del tiempo necesario para el desarrollo del proyecto, se utiliza la Ecuación 2.

## **ECUACIÓN 2: CÁLCULO DEL TIEMPO**

$$T = C * E^D$$

**Fuente:** COMO II

Donde:

- T: tiempo de desarrollo en meses.
- C, D: constante del modelo COCOMO.
- E: esfuerzo aplicado.

También se debe realizar el cálculo de persona necesarias para el desarrollo del sistema, como se observa en la Ecuación 3.

## **ECUACIÓN 3: CÁLCULO DE CANTIDAD DE PERSONAS**

$$P = \frac{E}{T}$$

**Fuente:** COMO II

Donde:

- P: cantidad de personas.
- T: tiempo de desarrollo en meses.
- E: esfuerzo aplicado.

Para el desarrollo del sistema se toma en cuenta el salario mínimo nacional establecido en el año 2020 el cual es de Bs 2.122.- (Dos mil ciento veintidós bolivianos 00/100), el cual fue establecido mediante el Decreto Supremo 3888 del 1 de mayo del 2019.

#### **ECUACIÓN 4: CÁLCULO DE COSTO DE DESARROLLO DE SOFTWARE**

$$CT = SPT$$

**Fuente:** COMO II

Donde:

- P: cantidad de personas.
- T: tiempo de desarrollo en meses.
- S: esfuerzo aplicado.

Para proceder a realizar los cálculos en la Tabla 18, se detallan las líneas de código escritas y funcionales, para poder determinar el esfuerzo empleado.

**TABLA 20: LÍNEAS DE CÓDIGO DESARROLLADAS**

Lenguaje de programación	# de líneas de código
PHP	4424
HTML	2267
JavaScript	325
Laravel Blade	530
<b>Total</b>	<b>7546</b>

**Fuente:** Elaboración propia

Como se observa en la Tabla 18 se tiene las líneas de código según el lenguaje de programación desarrollado.

Una vez se tiene la cantidad de líneas de código se debe determinar el tipo de proyecto, los cuales se clasifican de la siguiente manera:

- Orgánicos: proyectos considerados sencillos, menores de 50 KDLC (miles de líneas de código) en los cuales se tiene experiencia de proyectos similares y se encuentran en entornos estables.
- Semi acoplados: proyectos intermedios en complejidad y tamaño (menores de 300 KDLC) donde la experiencia en este tipo de proyectos es variable, y las cuales restricciones intermedias.
- Empotrados: proyectos bastante complejos, en los que apenas se tiene información.

Se determina que el proyecto es pertenece a la clasificación de proyecto orgánico debido a la cantidad de líneas de código identificadas.

Una vez determinado el tipo de proyecto se debe identificar el valor de las constantes, las cuales están descritas en la Tabla 19.

**TABLA 21: COEFICIENTES DE DESARROLLO**

TIPO	A	B	C	D
Orgánico	2.4	1.05	2.5	0.38
Semi orgánico	3	1.12	2.25	0.35
Empotrado	3.6	1.2	2.5	0.32

**Fuente:** COCOMO II

Como se observa en la Tabla 19, se hará uso los valores de las constantes establecidas para un tipo de proyecto orgánico.

Una vez determinados los valores, se procederá a calcular el valor del esfuerzo aplicado en el presente Trabajo de Grado.

$$E = A * (KLCD)^B$$

$$E = 2.4 * (7.546)^{1.05}$$

$$E = 20,0361 \text{ personas/mes}$$

Una vez realizado el cálculo del esfuerzo se tomará este valor para calcular el tiempo de desarrollo necesario.

$$T = C * E^D$$

$$T = 2,5 * 20,0361^{0.38}$$

$$T = 7,8096 \text{ meses} = 8 \text{ meses}$$

Se determinó que el tiempo para el desarrollo del software es de 8 meses, este tiempo único para la programación o desarrollo del software para la entrega de prototipos iniciales.

Una vez obtenido el tiempo de desarrollo se procederá a calcular la cantidad de personas requeridas para el presente Trabajo de Grado.

$$P = \frac{E}{T}$$

$$P = \frac{20,0361}{7,8096}$$

$$P = 2,5656 = 3 \text{ personas}$$

Con los valores calculados del esfuerzo y el tiempo para el desarrollo del proyecto se determinó que la cantidad de personas es de 3.

Por último, con los resultados obtenidos se procedió el costo total del desarrollo del software.

$$CT = S * P * T$$

$$CT = 2.122 * 2,5656 * 7,8096$$

$$CT = Bs\ 42.517,0493.-$$

De acuerdo con el cálculo del costo realizado, el precio del producto de software o del desarrollo, en base al cálculo de la cantidad de líneas de código es igual a Bs. 42.517 (cuarenta y dos mil quinientos diecisiete bolivianos, con centavos 50/100).

#### **4.1.2 Costos Variables**

Los costos variables serán tomados en cuenta como aquellos en los que se fueron incurridos y que no están directamente relacionados con el desarrollo del proyecto, en la Tabla 22 se detallan de manera más específica.

**TABLA 22: COSTOS VARIABLES**

**(Expresado en bolivianos)**

Nombre	Descripción	Costo
Paquete de hojas bond	Paquete de hojas bond tamaño carta	30
Tinta	Costo de tinta para impresiones	60
Anillado	Anillados en ejemplares del trabajo entregado	50
Fotocopias	Fotocopias entregadas del presente trabajo	50
Servidor base de datos. "db.r5.24xlarge"	Servidor el cual alojara la base de datos del sistema, la cotización realizada se puede observar en el Anexo N	906,6
Servidor de aplicación	Servidor el cual contendrá la parte funcional, y las distintas vistas del sistema, las características de la cotización y especificaciones se encuentran en el Anexo O	2.881,8
Internet	Servicio de internet, plan de 4Gb, brindada por la empresa Tigo	0
<b>Total Bolivianos</b>		<b>3.978,4</b>

**Fuente:** Elaboración propia

Como se observa en la Tabla 22, se incurrió en un total de Bs 3.978,4.- (tres mil novecientos setenta y ocho bolivianos, con 40/100 centavos) al momento de considerar los costos variables.

Ese considera que el costo del servicio de internet con un valor de Bs 0, debido a que este costo ya se considera dentro del Plan Operativo Anual de la institución.

#### **4.1.3 Costo Total**

A continuación, se realiza el cálculo de los costos totales incurridos en el proyecto, tomando en cuenta los costos fijos y los costos variables los cuales fueron incurridos en el proyecto, como se observa en la Tabla 23.

**TABLA 23: COSTOS TOTALES DE DESARROLLO DEL PROYECTO**

**(Expresado en bolivianos)**

Tipo de Costo	Descripción	Monto (Bs)
Costos Fijos	Costo de desarrollo de software	54.476.-
	Costos de software de servidor	0
	Costos de software de cliente	0
	Costos de hardware de servidor	0
	Costos de hardware de cliente	12.835.-
<b>Total, costos fijos</b>		<b>67.311.-</b>
Costos Variables	Material de Escritorio, servidor e internet	3.978,4.-
<b>Total, costos variables</b>		<b>3.978,4.-</b>

**Fuente:** Elaboración propia

Una vez determinados los diferentes costos que representa en el presente Trabajo de Grado, se pueden sumar de las siguientes formas para obtener el costo total o costo general de la titulación, estos costos se pueden calcular utilizando la siguiente fórmula y luego reemplazar el valor calculado previamente.

$$CT = CF + CV$$

$$CT = Bs\ 67.311\ + Bs\ 3.978,4s$$

$$CT = Bs\ 71.289,4 -$$

Por lo tanto, el costo total del presente Trabajo de Grado es de Bs. 71.289,4.- (setenta y un mil doscientos ochenta y nueve bolivianos, con centavos 40/100).

## 4.2 DETERMINACIÓN DE BENEFICIOS

Para la estimación de beneficios se tendrán en cuenta dos tipos de este: beneficios cualitativos y beneficios cuantitativos.

### 4.2.1 Beneficios Cualitativos

El objetivo del presente Trabajo de Grado trae consigo los siguientes beneficios cualitativos a la Dirección General de Intereses Marítimo, Fluviales, Lacustre Marina Mércate:

- Centralización de información de las embarcaciones a una base de datos, las cuales previamente se encontraban en medios físico y ofimáticos, la misma se encontraba descentralizada.
- Automatización de registro de embarcaciones, el cual previamente se realizaba de manera manual. En esta situación el inspector de embarcaciones llevaba consigo todos los formularios correspondientes, además de la solicitud de registro derivada por el Ministerio de Defensa. Con el presente Trabajo de Grado todos los campos a llenar se desplegarán de manera virtual en las tabletas que se usarán para este proceso.
- Automatización del proceso de inspección de embarcaciones, el cual se realizaba de manera manual, en el cual el inspector llevaba distintos formularios que correspondían a las mismas dependiendo la clase. Con el sistema se genera un

formulario de manera automática el cual según la presentación de requerimientos se generará una ponderación de manera automática.

- Generación automática de reportes de todas las embarcaciones y usuarios registrados, además poder mostrar las embarcaciones tanto registradas como inspeccionadas en un rango de fechas.
- Implementación de seguridad en los certificados emitidos, de manera que se minimice el riesgo de duplicidad de certificados emitidos por la Unidad de Marina Mercante.
- Verificación de la autenticidad de los certificados de registro y seguridad de la navegación en los documentos emitidos por el caso de estudio a partir de la lectura del código QR que este trae

#### **4.2.2 Beneficios Cuantitativos**

En el presente Trabajo de Grado los beneficios cuantitativos surgen a partir de los beneficios cualitativos, entre los que se pudo cuantificar los siguientes aspectos.

- Ahorros en las comisiones, las cuales son destinadas al registro, control y seguimiento de las embarcaciones.
- Uso eficiente del recurso papel: Reducción en las cantidades de compra de papel de alto relieve en el cual se imprime los certificados, esto debido a que previamente existían errores al insertar los datos de manera manual.
- Uso eficiente del recurso papel: Reducción en la compra de tinta para sellos al tener una mejora en la entrega e impresión de certificados que emita la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante.

Estos beneficios se pueden ver expresados cuantitativamente en la Tabla 24.

**TABLA 24: BENEFICIOS CUANTITATIVOS****(Expresado en bolivianos)**

Recurso	Descripción	Total estimado (Bs)
Papel para impresión de certificados	Ahorro en la cantidad de papel especial para la emisión de los diversos certificados emitidos	2.000
Tinta para la impresión de certificados	Debido a que se realizó una mejora en la entrega de certificados no será necesario la reimpresión constante debido a errores que se presenten al momento de imprimir y entregar los mismos	600
Dinero destinado a las comisiones de registro, control y seguimiento de embarcaciones	Debido a que el control, seguimiento y registro de embarcaciones toma un menor tiempo, el dinero destinado a las comisiones se reducirá debido a que estos procesos se realizaran de una manera más rápida	12.000
<b>Total Bolivianos</b>		<b>14.600</b>

**Fuente:** Elaboración propia

Como se observa en la Tabla 24 se tiene que el proyecto brindará un beneficio económico de Bs 14.600.- (catorce mil seiscientos bolivianos).

#### 4.3 RELACIÓN COSTO BENEFICIO

Para realizar la relación costo beneficio se tomará en cuenta el concepto de VAN (Valor Actual Neto) y TIR (Tasa Interna de Retorno) donde:

A. VAN: Cantidad de dinero invertida en un proyecto para determinar si realmente este puede dar beneficios a la empresa, se calcula mediante la siguiente formula:

$$VAN = Inv. + \sum_{t=1}^n \frac{F_t}{(1+k)^t}$$

Donde:

- Inv: inversión en el periodo cero.
- n: horizonte de la evaluación.
- Ft: flujo neto en el periodo t.
- k: tasa de descuento de la inversión

B. TIR: Cantidad de dinero invertida en un proyecto para determinar si realmente este puede dar beneficios a la empresa, se calcula mediante la siguiente formula:

$$TIR = Inv. + \sum_{T=0}^n \frac{F_n}{(1+i)^n}$$

Donde:

- Inv: inversión en el periodo cero.
- n: vida útil del proyecto.
- Fn: flujo de efectivo anual.
- k: tasa de descuento de la inversión

C. B/C: Cantidad de dinero invertida en un proyecto para determinar si realmente este puede dar beneficios a la empresa, se calcula mediante la siguiente formula:

$$B/C = \frac{B}{C}$$

Donde:

- B: Es el beneficio.
- C: Costo total.

Para poder determinar adecuadamente estos valores se realizará el flujo de caja del proyecto tomando en cuenta los costos y beneficios previstos. La tasa de interés del depósito a plazo fijo es del 5%.

La cantidad de años del flujo de caja es 5 años acorde al ciclo de vida del software, se muestra en la Tabla 25 el flujo de caja de la inversión.

**TABLA 25: FLUJO DE CAJA**

**(Expresado en bolivianos)**

Año	2020	2021	2022	2023	2024	2025
C.V.		3.978,4	3.978,4	3.978,4	3.978,4	3.978,4
Inv	42.517,05					
B		14.600	14.600	14.600	14.600	14.600
Flujo de Caja	-42.517,05	10.621,6	10.621,6	10.621,6	10.621,6	10.621,6

**Fuente:** Elaboración propia

Como se observa en la Tabla 25 se observa el Flujo de Caja el cual nos ayudara a determinar los parámetros previamente descritos, tomando en cuenta 5 años para el ciclo de vida para el software. Los valores que se usan para realizar los cálculos fueron los de los costos variables y precio de desarrollo de software como gasto incurrido y como ganancia el beneficio calculado.

$$VAN= Bs 3.468,92$$

$$TIR=8\%$$

$$B/C=0,081$$

Se observa que una vez calculada el valor del TIR y el VAN en el plazo de 5 años se tiene que la inversión es viable ya que los resultados obtenidos muestran un valor

del VAN > 0 cuyo valor es Bs 3.468,92.- (tres mil cuatrocientos sesenta y ocho bolivianos, con centavos 92/100) que significa que en el plazo de cinco años el proyecto tendrá dicho valor después de su implementación,

El TIR calculado es de 8% (ocho por ciento), este porcentaje resultante significa que se podrá cubrir la tasa de rentabilidad igual a 5%, lo cual nos indica que el proyecto es rentable.

## CAPÍTULO V

# CONCLUSIONES Y RECOMENDACIONES



## **CAPÍTULO V**

### **CONCLUSIONES Y RECOMENDACIONES**

#### **5.1 CONCLUSIONES**

A continuación, se describe las conclusiones a las que se llegó, luego de haber concluido el trabajo.

- Los problemas identificados dentro de la Unidad de Marina Mercante para el control y seguimiento de embarcaciones, permitió establecer los objetivos para la automatización del proceso de emisión de certificados con la aplicación de seguridad en los procesos de registro e inspección de estas.
- El análisis de algoritmos asimétricos llevó por consiguiente la selección del algoritmo RSA debido al nivel de seguridad que brinda, la compatibilidad con las tecnologías actuales y la optimización de tiempos en la encriptación y desencriptación de datos.
- La aplicación de la metodología Design Sprint en el desarrollo del sistema se realizó debido a que permite la fácil identificación de requerimientos a partir de sus entregables personalizados “Entrevistas y Notas HMW”.
- La aplicación de criptografía asimétrica en los certificados que emite la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, para el seguimiento y control durante las inspecciones a través del sistema web permitió verificar la autenticidad de información de los certificados que presentan los dueños de las embarcaciones a través de la lectura de códigos QR que estos poseen.
- La migración de información de alrededor de 1500 embarcaciones, que se encontraban desde el año 1980 hasta el año 2018 en medios ofimáticos y físicos, a una base de datos relacional, permitió realizar consultas de forma eficaz y eficiente

demostrando la funcionalidad del sistema permitiendo realizar consultas con información real.

- La aplicación del algoritmo RSA genera un par de llaves, de modo que se asigna la llave pública a los certificados de las embarcaciones para que el personal de la Unidad de Marina Mercante pueda comprobar la veracidad de la información.

## 5.2 RECOMENDACIONES

A continuación, se describe las recomendaciones a las que se llegó, luego de haber concluido el trabajo.

- Se recomienda realizar procesos de capacitación al personal que se incorpore a la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, de manera que tengan conocimiento para el uso adecuado del sistema, apoyados también en los manuales de usuarios.
- Se recomienda adquirir un plan de internet plan de velocidad de 40Mbps debido a la cobertura y velocidad que ofrece.
- Para una mayor fluidez en el procesamiento de información por parte de los inspectores al momento de realizar el registro e inspección de embarcaciones se contar con equipos con las condiciones de hardware adecuadas, con 6Gb de RAM y 128Gb de almacenamiento
- Realizar copias de respaldo de las bases de datos, semestralmente de modo de resguardar la información debido a que las inspecciones se realizan de manera anual, teniendo así un respaldo continuo de la información.
- Crear un correo institucional para poder administrar las distintas cuentas de usuarios que serán creadas

# BIBLIOGRAFÍA



## BIBLIOGRAFÍA

- [Aguilar, 2016] “IMPLEMENTACIÓN DE UN MODELO SIMPLIFICADO DE FIRMA DIGITAL BASADO EN LA TECNOLOGÍA PKI Y LA INVOCACIÓN POR PROTOCOLOS CASO DE ESTUDIO: MUNICIPALIDAD DE MIRAFLORES”, Ing. Gino Brehan Aguilar Alcarráz, Universidad Mayor de San Andrés, 2016
- [Blanchard, 1995] “INGENIERÍA DE SISTEMAS” Benjamin Blanchard, 1995, página 19
- [Gonzales, 2004] “SEGURIDAD EN REDES Y CRIPTOGRAFÍA”, Ing. Dante Iván González Sánchez, Instituto Tecnológico y de Estudios Superiores de Monterrey (México), 2004
- [Hall, 1962] “METHODOLOGY FOR SYSTEMS ENGINEERING”, Arthur D. Hall, Estados Unidos, 1962
- [Kerlinger,1981]. “INVESTIGACIÓN DEL COMPORTAMIENTO”, Fred N. Kerlinger,1981
- [Larousse, 2009] DICCIONARIO LAROUSSE, edición 2009
- [Leon, 2005] “ENCRYPTACION RSA DE ARCHIVOS DE TEXTO”. Magister Katia Regina Leon Lomparte, Pontificia Universidad Católica de Perú, 2005

- [Mirabal, 2010] “SEGURIDAD EN TRANSACCIONES EN LINEA CON TARJETA DE DEBITO MEDIANTE METODOS DE ENCRYPTACION HIBRIDA”, Licenciado Arturo Ricardo Mirabal Alvarado, Universidad Mayor de San Andrés,2010
- [Sampieri, 2012] “METODOLOGÍA DE LA INVESTIGACIÓN”, Roberto Sampieri. McGra-Hill Quinta ed., 2010
- [Sena, 2009] “DIAGRAMAS UML”, Senna, 2009, p.5
- [SILBERSCHATZ, 1987] SILBERSCHATZ, H. F. Horth – Sudarshan.FUNDAMENTOS DE BASES DE DATOS (4°Edición). McGraw-Hill, 2002
- [Sobrevila, 2008] “INGENIERÍA GENERAL”, Marcelo Antonio Sobrevilla, Buenos Aires – Argentina, 2008
- [Tamayo, 2010] “LA INVESTIGACIÓN, EL PROCESO DE LA INVESTIGACIÓN CIENTÍFICA”, Mario Tamayo, 2010

# GLOSARIO



**TERMINO:****CONCEPTO:**

Algoritmo	Conjunto ordenado de operaciones sistemáticas que permite hacer un cálculo y hallar la solución de un tipo de problemas.
Autentico:	Que está autorizado o legalizado y tiene valor oficial
Calado	Profundidad que alcanza en el agua la parte sumergida de una embarcación.
Cifrar	Escribir un mensaje en clave mediante un sistema de signos formado por números, letras, símbolos, etc.
Confidencial:	Cualidad de confidencial. Propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas
Coadyuvar	Contribuir o ayudar a la consecución de una cosa.
Criptoanálisis	Parte de la criptología que se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad sin el conocimiento de información secreta.
Criptografía	Ámbito de la criptología que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

**TERMINO:****CONCEPTO:**

Criptología	Disciplina que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas.
Disponibilidad:	Condición de estar disponible alguien o algo.
Embarcación:	Construcción capaz de flotar, de ser dirigida por el hombre y propulsada por el viento u otro procedimiento, designa especialmente las de poco tonelaje
Eslora	Longitud de una embarcación desde la proa a la popa.
Estegoanálisis	Disciplina dedicada al estudio de la detección de mensajes ocultos usando esteganografía. Dichos mensajes pueden estar ocultos en diferentes tipos de medio, como pueden ser por ejemplo las imágenes digitales, los archivos de vídeo, los archivos de audio o incluso un simple texto plano.
Francobordo	Distancia vertical desde la cubierta principal de una embarcación hasta la línea de carga que indica el calado máximo autorizado.
Hash:	Algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.
Integridad:	Que está completo o tiene todas sus partes.

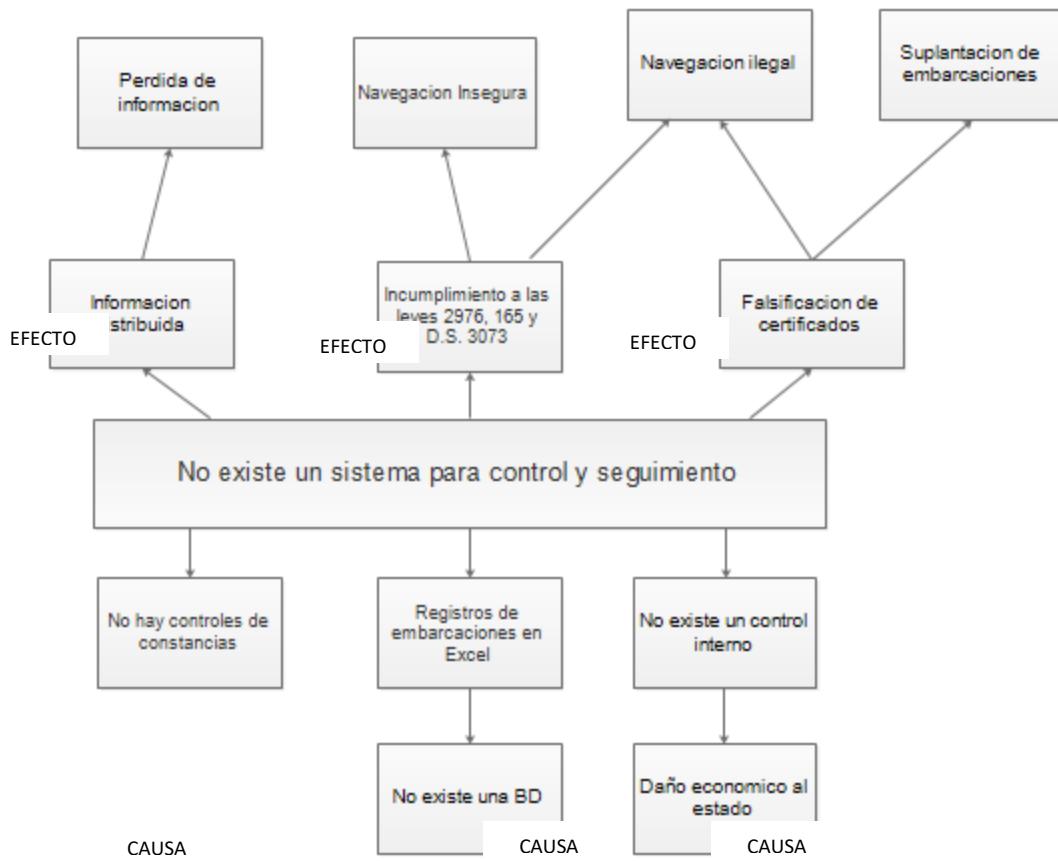
**TERMINO:****CONCEPTO:**

Manga:	Objeto de tela ligera en forma de cono alargado que, situado en lo alto de un mástil, sirve para señalar la dirección y la intensidad del viento.
Ofimática	Conjunto de métodos, aplicaciones y herramientas informáticas que se usan en labores de oficina con el fin de perfeccionar, optimizar, mejorar el trabajo y operaciones relacionados.
Protocolo	Conjunto de reglas de formalidad que rigen los actos y ceremonias diplomáticos y oficiales.
Puntal:	Madero o barra de material fuerte y resistente que se fija en posición inclinada en algún lugar para sujetar una pared, una estructura o un edificio que puede caerse.
Relieve:	Configuración de una superficie con distintos niveles o partes que sobresalen más o menos. Parte que sobresale en una superficie plana.
Unidireccional:	Que tiene una sola dirección. Que va en una sola dirección.
Virtual:	Que tiene existencia aparente y no real

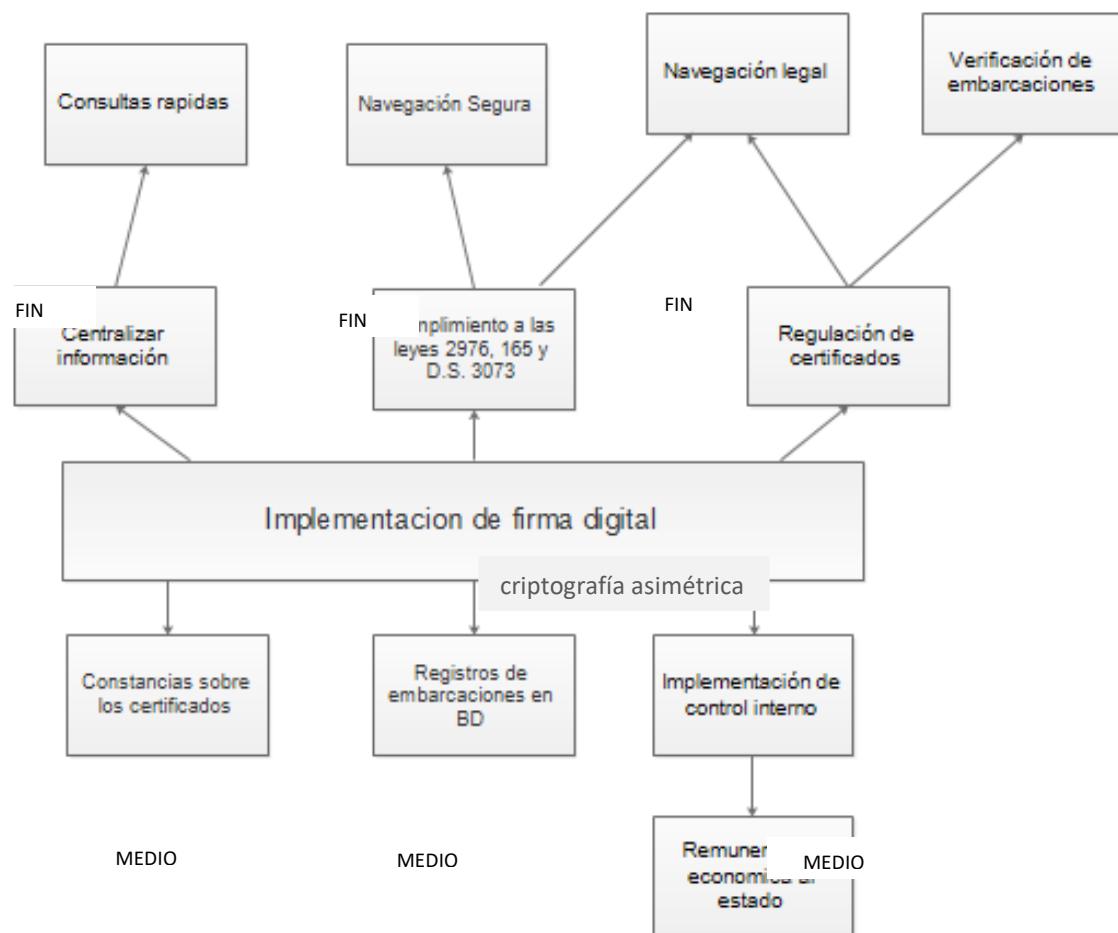
## ANEXOS



## ANEXO A: ÁRBOL DE PROBLEMAS



## ANEXO B: ÁRBOL DE OBJETIVOS



## ANEXO C:

### FORMULARIO DE INSPECCIÓN

*Leyendo Nuevo* ✓

FORM . SF - 002

**Ministerio de Defensa Nacional - DGIMFLMM.**  
Marina Mercante Nacional

**FORMULARIO DE INSPECCION PARA BUQUES, EMBARCACIONES O ARTEFACTOS NAVALES  
MENORES A 10 TRB**

1. PROPIETARIO/ARMADOR: *José Luis Aravena Chávez*

2. CAPITAN/PATRON: *Capt. P. R. L. Aravena*

3. NOMBRE EMBARCACIÓN: *Capitán P. R. L. Aravena*

4. TIPO DE EMBARCACIÓN: *Barco Pesca*

5. AÑO Y LUGAR DE CONSTR: *2016, Isla San Juan*

6. MATERIAL DE CONSTR: *Madera*

7. SERVICIO DE LA EMBARCACIÓN: *Pesca*

8. DOMICILIO DEL PROPIETARIO: *Ahuayangue, Chile*

18. CASCO

QUILLA	R/E
CUADERNAS	R/E
OBRAS VIVAS	R/E
OBRAS MUERTAS	R/E
PINTURA	R/E
CUBIERTA PRINCIPAL	N/T
CALAFATEADO	N/T
BANCADAS	N/T
ENJARETADO	R/E
UNIÓN DICHAPAS	N/T
ESPESOR DE CHAPAS	N/T

19. SISTEMA DE PROPULSIÓN

FUERA DE BORDA	V
TANQUE COMBUSTIBLE	V
MOTOR DE CENTRO	X
MOTOR DE COLA	X
BATERIA	X
CABLEADO ELECTRICO	X
MARCA PARSON	V
POTENCIA 15 HP	V
NUMERO	511010583

20. SISTEMA DE GOBIERNO

RUEDA CABILLAS	
SISTEMA DE CABLEADO	
PALA DE GOBIERNO	

21. COMUNICACIONES

EQUIPO COMUNICACIONES	
HANDIE	
MEGAFONO / OTROS	
VENGALAS	

22. EQUIPOS DE CONTINGENCIA

CHALECO SALVAVIDAS	N/T
GUNDOLAS	N/T
ESTINGUIDORES	N/T
CAJA DE HERRAMIENTAS	N/T
REMOS	V
CINGA	V
DEFENSAS	N/T
BITAS/CORNAMUSAS	N/T
CABLES/CABOS	N/T

23. LUCES DE NAVEGACION

LUZ DE TOPE	
LUCES DE COSTADO	

24. COMPARTIMENTOS

SALA DE PASAJEROS	N/T
BASUREROS	N/T

25. PRIMEROS AUXILIOS

BOTIQUIN	N/T
LINTERNA	N/T

26. DOCUMENTOS

CERTIFICADO DE REGISTRO	
CERTIFICADO DE SEG. NAV.	
CERTIFICADO DE FRANCOB.	
CERTIFICADO DE DOT. MIN.	
ROL DE TRIPULACION	
CARNET DE TRIP. PERS. EMB.	
LIBRO DE MÁQUINAS	
LIBRO DE DESC. DE BASURA	

**INFORME DE INSPECCION**

ITEM	DEFICIENCIA	TIEMPO PARA SOLUCIONAR EL PROBLEMA
18	Rebe sangre por agujero de tubo	
22	No completo chaleco salvavidas	
	Extinguidor	
25	Rebe caja de herramientas	
	Rebe compresor de botigas	

(B) BUENO; (RE) REGULAR ESTADO, (FS) FUERA DE SERVICIO, (NT) NO TIENE; (NC) NO CORRESPONDE.

Lugar y fecha: *Carroll* 07/10/2019

*[Signatures]*

CAPITAN O PROPIETARIO

INSPECTOR TECNICO

JEFE DE COMISION

**ANEXO D:**  
**FOTO DE EMBARCACIÓN**



**ANEXO E:**  
**CERTIFICADO DE SEGURIDAD**

Nº 012199

  
**ESTADO PLURINACIONAL DE BOLIVIA**  
 MINISTERIO DE DEFENSA  
*Ministerio de Defensa*  
**DIRECCIÓN GENERAL DE INTERESES MARÍTIMOS,  
 FLUVIALES, LACUSTRES Y DE MARINA MERCANTE**

Nº REGISTRO	L - 10195487
-------------	--------------

**CERTIFICADO DE SEGURIDAD DE LA NAVEGACIÓN**

EXPEDIDO EN CUMPLIMIENTO AL D.S. Nº 3073  
 REGLAMENTO TECNICO A LA LEY Nº 165 GENERAL DE TRANSPORTE EN LA  
 MODALIDAD DE TRANSPORTE ACUATICO, TITULO TERCERO, CAPITULO SEGUNDO ART. 21

PROPIETARIO (S): **JOSE LUIS AMARU CHOQUE**  
 ANTERIOR PROPIETARIO: **SUPERIO FLORES NINA**  
 FECHA DE INSPECCIÓN: **07 DE OCTUBRE DE 2019**  
 LUGAR DE INSPECCIÓN: **COACOLLO**  
 BASE DE OPERACIONES: **COACOLLO**

NOMBRE DE LA EMBARCACIÓN			MATRICULA	INDICATIVO DE LLAMADA	
BUFALO			EN TRAMITE	- -	
SERVICIOS DE LA EMBARCACIÓN			TIPO	AÑO DE CONSTRUCCIÓN	
PESCA			BOTE AMOTOR	2016	
ESLORA	MANGA	PUNTAL	ARQUEO BRUTO	ARQUEO NETO	FRANCOBORDO
6,05 MTS.	1,55 MTS.	0,50 MTS.	1,08 UNIDAD DE REGISTRO	1,00 UNIDAD DE REGISTRO	mm.
TIPO Y MARCA DE MOTOR			NUMERO DE MOTOR	POTENCIA PROPULSIVA TOTAL	POTENCIA ELÉCTRICA NOMINAL TOTAL
FUERA DE BORDA			1	15	CONTINUA: 12.V.
PARSUR			L-511010583	HP	ALTERNA: - -
MATERIAL DEL CASCO			PESO Y ALTURA DE CUBERTADA	MERCANCÍAS PELIGROSAS	NÚMERO MÁXIMO DE PASAJEROS
MADERA			- -	NO	4

SE CERTIFICA:

QUE LA EMBARCACIÓN, HA SIDO OBJETO DE INSPECCIONES DE CONFORMIDAD CON LO PRESCRITO EN EL REGLAMENTO DE INSPECCIONES PARA EMBARCACIONES MERCANTES Y QUE Dicha INSPECCION, HA PUESTO DE MANIFIESTO QUE EL ESTADO DE CASCO, LA ESTRUCTURA, MAQUINAS Y EL EQUIPO ES SATISFACTORIO Y QUE LA EMBARCACION CUMPLE CON LAS PRESCRIPCIONES PERTINENTES EN LAS REGLAMENTACIONES VIGENTES.

EL PRESENTE CERTIFICADO ES VALIDO POR: CINCO AÑOS, A PARTIR DEL: 07/10/2019  
 DEBIENDO SOMETERSE A LAS INSPECCIONES ANUALES OBLIGATORIAS EN LAS FECHAS ESTABLECIDAS POR LA AUTORIDAD COMPETENTE.

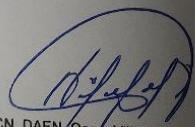
COACOLLO, 07 DE OCTUBRE DE 2019



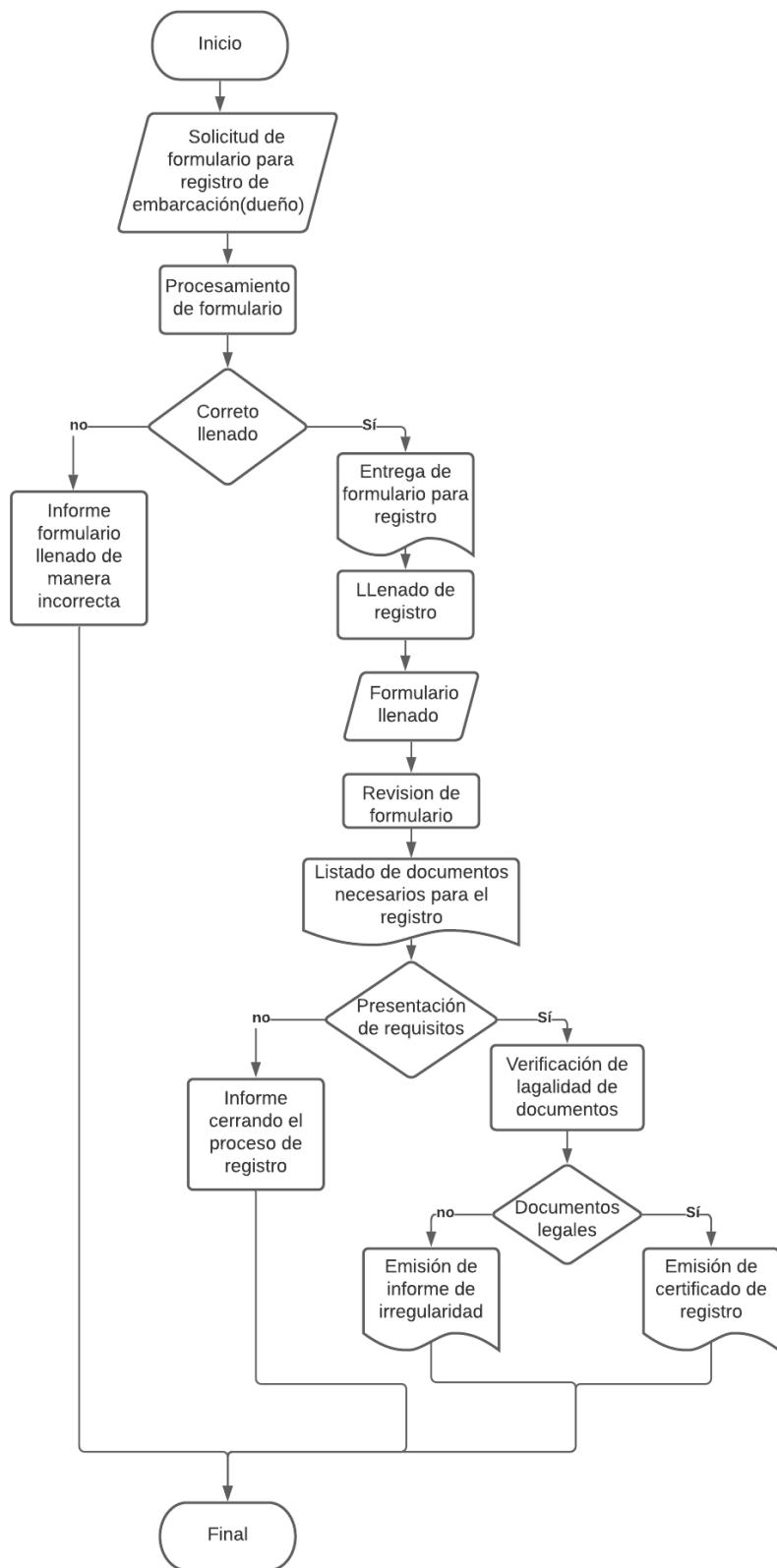
CN/DAEN. Oscar Villafurte Sejas  
 JEFE DE LA UNIDAD DE MARINA MERCANTE  
 MINISTERIO DE DEFENSA

CN/DAEN. Juan Rosas Morales  
 DIRECTOR GENERAL DE INTERESES MARÍTIMOS  
 FLUVIALES, LACUSTRES Y MARINA MERCANTE ai.  
 MINISTERIO DE DEFENSA

**ANEXO F:**  
**REGISTRO DE EMBARCACIONES**

ESTADO PLURINACIONAL DE BOLIVIA MINISTERIO DE DEFENSA DIRECCION GENERAL DE INTERESES MARITIMOS FLUVIALES, LACUSTRES Y DE MARINA MERCANTE	Nº 012198												
 <b>CERTIFICADO DE REGISTRO</b> <b>EXPEDIDO DE CONFORMIDAD AL RECONOCIMIENTO</b> <b>EFFECTUADA POR LA DIRECCIÓN DE MARINA MERCANTE NACIONAL</b>													
<b>PROPIETARIO (S): JOSE LUIS AMARU CHOQUE</b> <b>ANTERIOR PROPIETARIO: SUPERIO FLORES NINA</b> <b>FECHA DE INSPECCIÓN: 07 DE OCTUBRE DE 2019</b> <b>LUGAR DE INSPECCIÓN: COACOLLO</b> <b>BASE DE OPERACIONES: COACOLLO</b>													
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="3">NOMBRE DE LA EMBARCACIÓN</th> <th>MATRICULA</th> <th colspan="2">INDICATIVO DE LLAMADA</th> </tr> </thead> <tbody> <tr> <td colspan="3">BUFALO</td> <td>EN TRAMITE</td> <td colspan="2">--</td> </tr> </tbody> </table>		NOMBRE DE LA EMBARCACIÓN			MATRICULA	INDICATIVO DE LLAMADA		BUFALO			EN TRAMITE	--	
NOMBRE DE LA EMBARCACIÓN			MATRICULA	INDICATIVO DE LLAMADA									
BUFALO			EN TRAMITE	--									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">SERVICIOS DE LA EMBARCACIÓN</th> <th>TIPO</th> <th colspan="2">AÑO DE CONSTRUCCIÓN</th> </tr> </thead> <tbody> <tr> <td colspan="2">PESCA</td> <td>BOTE AMOTOR</td> <td colspan="2">2016</td> </tr> </tbody> </table>		SERVICIOS DE LA EMBARCACIÓN		TIPO	AÑO DE CONSTRUCCIÓN		PESCA		BOTE AMOTOR	2016			
SERVICIOS DE LA EMBARCACIÓN		TIPO	AÑO DE CONSTRUCCIÓN										
PESCA		BOTE AMOTOR	2016										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>ESLORA</th> <th>MANGA</th> <th>PUNTAL</th> <th>ARQUEO BRUTO</th> <th>ARQUEO NETO</th> <th>FRANCOBORDO</th> </tr> </thead> <tbody> <tr> <td>6,05 MTS.</td> <td>1,55 MTS.</td> <td>0,50 MTS.</td> <td>1,08 UNIDAD DE REGISTRO</td> <td>1,00 UNIDAD DE REGISTRO</td> <td>-- mm.</td> </tr> </tbody> </table>		ESLORA	MANGA	PUNTAL	ARQUEO BRUTO	ARQUEO NETO	FRANCOBORDO	6,05 MTS.	1,55 MTS.	0,50 MTS.	1,08 UNIDAD DE REGISTRO	1,00 UNIDAD DE REGISTRO	-- mm.
ESLORA	MANGA	PUNTAL	ARQUEO BRUTO	ARQUEO NETO	FRANCOBORDO								
6,05 MTS.	1,55 MTS.	0,50 MTS.	1,08 UNIDAD DE REGISTRO	1,00 UNIDAD DE REGISTRO	-- mm.								
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>TIPO Y MARCA DE MOTOR</th> <th>NUMERO DE MOTOR</th> <th>POTENCIA PROPULSIVA TOTAL</th> <th>POTENCIA ELÉCTRICA NOMINAL TOTAL</th> </tr> </thead> <tbody> <tr> <td>FUERA DE BORDA PARSUN</td> <td>1 L-511010583</td> <td>15 HP</td> <td>CONTINUA: 12.V. ALTERNA: --</td> </tr> </tbody> </table>		TIPO Y MARCA DE MOTOR	NUMERO DE MOTOR	POTENCIA PROPULSIVA TOTAL	POTENCIA ELÉCTRICA NOMINAL TOTAL	FUERA DE BORDA PARSUN	1 L-511010583	15 HP	CONTINUA: 12.V. ALTERNA: --				
TIPO Y MARCA DE MOTOR	NUMERO DE MOTOR	POTENCIA PROPULSIVA TOTAL	POTENCIA ELÉCTRICA NOMINAL TOTAL										
FUERA DE BORDA PARSUN	1 L-511010583	15 HP	CONTINUA: 12.V. ALTERNA: --										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>MATERIAL DEL CASCO</th> <th>PESO Y ALTURA DE CUBERTADA</th> <th>MERCANCIAS PELIGROSAS</th> <th>NÚMERO MÁXIMO DE PASAJEROS</th> </tr> </thead> <tbody> <tr> <td>MADERA</td> <td>--</td> <td>NO</td> <td>4</td> </tr> </tbody> </table>		MATERIAL DEL CASCO	PESO Y ALTURA DE CUBERTADA	MERCANCIAS PELIGROSAS	NÚMERO MÁXIMO DE PASAJEROS	MADERA	--	NO	4				
MATERIAL DEL CASCO	PESO Y ALTURA DE CUBERTADA	MERCANCIAS PELIGROSAS	NÚMERO MÁXIMO DE PASAJEROS										
MADERA	--	NO	4										
<p><b>SE CERTIFICA:</b>          QUE LA EMBARCACIÓN, A LA FECHA DE REGISTRO CUMPLE CON LAS EXIGENCIAS DEL D.S. 12684          "LEY DE NAVEGACION MARÍTIMA, FLUVIAL Y LACUSTRE" CAPÍTULO II, REGISTRO DE          EMBARCACIONES Y CON LAS PRESCRIPCIONES PERTINENTES DE LA R.M. 0736 QUE APRUEBA EL          REGLAMENTO DE REGISTRO DE BUQUES, EMBARCACIONES Y ARTEFACTOS NAVALES.</p>													
<small>COACOLLO, 07 DE OCTUBRE DE 2019</small>													
 CN. DAEN Oscar Villafuerte Sejas DE LA UNIDAD DE MARINA MERCANTE MINISTERIO DE DEFENSA			 CN. DAEN. Juan Rosas Morales DIRECTOR GENERAL DE INTERESES MARÍTIMOS FLUVIALES, LACUSTRES Y MARINA MERCANTE al. MINISTERIO DE DEFENSA										

**ANEXO G:**  
**PROCESO DE EMISIÓN DE CERTIFICADO DE REGISTRO**



**ANEXO H:**  
**REGLAMENTO NACIONAL DE REGISTROS DE BUQUES,**  
**EMBARCACIONES Y ARTEFACTOS NAVALES**

**CAPITULO III**

**NORMAS PARA LA CONSTRUCCIÓN DE EMBARCACIONES**

El espesor del fondo y del costado del enchapado del casco, en toda su extensión no será menor del expresado.

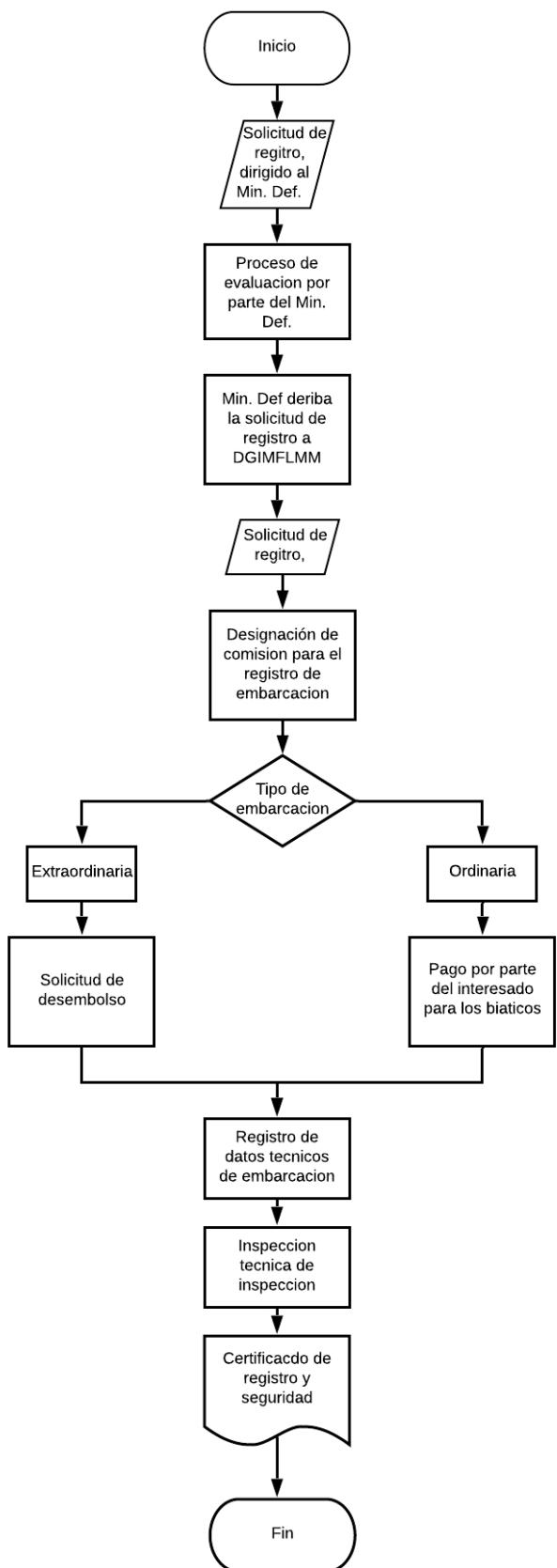
ESLORA (metros)	CON BAOS TRANSVERSALES (milímetros)	CON BAOS LONGITUDINALES (milímetros)
23.0	5.0	4.5
30.5	5.5	4.5
38.0	6.0	5.0
45.0	6.5	5.5
53.5	7.0	6.0
61.0	7.5	6.5
68.5	8.0	7.0
76.0	8.5	7.5
84.0	9.0	8.0
91.5	9.5	8.5

**ANEXO I:**  
**TAREAS DEL PERSONAL DE UNIDAD DE MARINA MERCANTE**

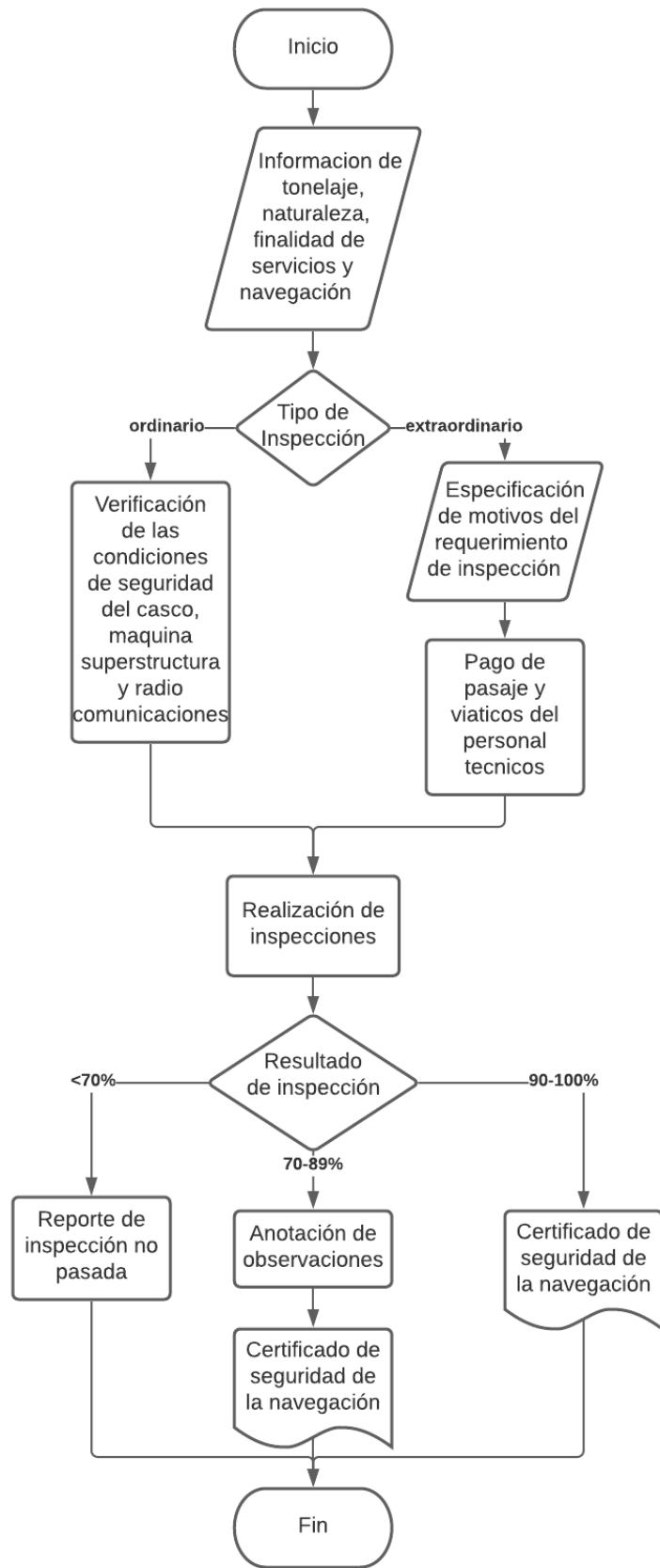
Cargo	Tarea
Jefe de la Unidad de Marina Mercante	Promover y fomentar el desarrollo de la Marina Mercante, las actividades Naviero Mercantes, la Industria Naval, la navegación y actividades conexas a nivel nacional e internacional, proponer estrategias para mejorar e incentivar la navegación mercante, turística y deportiva.
Técnico administrativo	Asistir a la Unidad de Marina Mercante, con relación al seguimiento de la documentación, operativizando procedimientos administrativos.
Secretario General	Brindar asistencia a la Unidad de Marina Mercante, con relación a la elaboración de documentación, recepción y despacho de correspondencia, seguimiento y archivo de documentación y atención al público interno y externo.
Encargado de inventario	Brindar asistencia a la Unidad de Marina Mercante, con relación al material de activos fijos y biblioteca
Portapliegos	Desarrollar mecanismos de orden administrativo en la ejecución de los roles y tareas asignadas, manteniendo el flujo de comunicación con todas las áreas de manera oportuna y correcta, actualizando el archivo y operativizando procesos y procedimientos administrativos
Responsable de regulación mercante e investigación de incidentes	Proponer, elaborar, recomendar la normativa necesaria, para la actualización de los reglamentos de la Marina Mercante y regular los procedimientos de incidentes ocurridos en el ámbito acuático y la navegación Marítima Fluvial y Lacustre.
Técnico de regulación mercante	Coadyuvará en la elaboración de la normativa necesaria, para la actualización de los reglamentos de la Marina Mercante y colaborará con la investigación de incidentes en la navegación Marítima Fluvial y Lacustre.
Técnico investigación de incidentes	Coadyuvar en la investigación de incidentes sobre hechos acaecidos en el ámbito acuático y la navegación Marítima Fluvial y Lacustre.

Responsable del registro marítimo, fluvial y lacustre	Ejecutar el registro, inspección y reconocimiento a los buques, embarcaciones y artefactos navales, de navegación nacional, así como a las líneas navieras, agencias navieras, astilleros e industrias afines a la actividad Naviero–Mercante, en los ámbitos Marítimo, Fluvial y Lacustre, velando por el cumplimiento de la Normativa en actual vigencia, los Convenios y Acuerdos internacionales suscritos y/o ratificados por Bolivia.
Técnico de registro marítimo fluvial y lacustre	Coadyuvar con el registro, inspección y control a los buques, embarcaciones y artefactos navales, de navegación nacional e internacional, así como a las líneas navieras, agencias navieras, astilleros e industrias afines a la actividad Naviero–Mercante, en los ámbitos Marítimo, Fluvial y Lacustre, velando por el cumplimiento de la Normativa en actual vigencia, los Convenios y Acuerdos internacionales suscritos y/o ratificados por Bolivia.
Técnico operador de registro marítimo fluvial y lacustre	Elaborar y alimentar la base de datos para el registro Marítimo Fluvial y Lacustre de buques, embarcaciones y artefactos navales, de navegación nacional e internacional, así como a las líneas navieras, agencias navieras, astilleros e industrias afines a la actividad Naviero–Mercante.
Responsable de registro, carnetización Y capacitación del personal mercante	Planificar, actualizar y ejecutar los cursos de capacitación para el personal destinado en la Unidad, inspectores, investigadores y otros, en el ámbito Fluvial y Lacustre, en el marco de la normativa y reglamentación vigente.
Técnico de capacitación del personal mercante	Colaborar en la planificación, mejoramiento y ejecución de los cursos de capacitación y actualización para inspectores e investigadores Fluviales y Lacustres en el marco de la normativa y reglamentación vigente.
Técnico de carnetización de personal mercante	Registro, carnetización, titulación, certificación y habilitación del personal mercante tanto a nivel nacional como internacional.
Técnico de registro de personal mercante	Coadyuvar en el registro, carnetización, titulación, certificación y habilitación del personal mercante tanto a nivel nacional como internacional.

**ANEXO J:**  
**PROCESO DE REGISTRO DE EMBARCACIÓN**



**ANEXO K:**  
**PROCESO DE INSPECCIÓN DE EMBARCACIÓN**



## ANEXO L:

### EJECUCIÓN DE LA INSPECCIÓN TÉCNICA

**Artículo 23° (Items de Inspección).** La Inspección técnica de una embarcación en aguas interiores, comprende los siguientes ítems:

**a) CASCO Y SUPERESTRUCTURA.**

- Medición de las dimensiones principales eslora, manga y puntal.
- Determinación de las condiciones de la estanqueidad del casco.
- Medición y determinación de las condiciones del material de la superestructura.
- Verificación del estado del pintado de la embarcación.
- Medición de los espesores de las chapas de cascos metálicos, admitiéndose un desgaste máximo del 30% del espesor original. En el caso de embarcaciones de madera verificar el buen estado de las mismas.
- Verificar que la embarcación tenga inscrito en los lugares correspondientes el nombre y matrícula.
- Verificar el marcado y pintado de la Marca de Francobordo.

**b) MÁQUINAS**

- Prueba del funcionamiento de la máquina principal y máquinas auxiliares.
- Verificación de limpieza de sentina.
- Verificación del panel de instrumentos.
- Verificación y prueba del sistema de gobierno.
- Verificación de la caja repuestos y herramientas.
- Verificación las condiciones de estanqueidad del sistema de alimentación de combustible.

**c) ELECTRICIDAD.**

- Prueba del sistema eléctrico.
- Prueba del arranque de la máquina propulsora

- Prueba del funcionamiento del generador auxiliar.
- Verificación del sistema de luces, navegación, luz de tope, estela, reflectores y sirena.
- Verificación del tablero de alimentación de energía eléctrica.
- Verificación de la carga de las baterías de acumuladores.
- Verificación del sistema de toma de tierra.

**d) COMUNICACIONES.**

- Prueba del sistema de comunicaciones, recepción/transmisión.
- Verificación de las antenas.

**e) EQUIPOS.**

- Verificación la cantidad necesaria y la fecha de carga de los extinguidores contra incendios.
- Verificación del número y estado de los chalecos y aros salvavidas.
- Verificación de las balsas salvavidas (si corresponde).
- Verificación de los botes salvavidas (si corresponde).
- Verificación del funcionamiento de las bombas del achique.
- Verificación de las anclas, cadenas y cabos de amarre.
- Verificación del botiquín de primeros auxilios.
- Verificación de las cartas e instrumentos de navegación.

**f) DOCUMENTACIÓN.**

- Verificación de la siguiente documentación:
- Certificado de Seguridad de la Navegación.
- Documentación que acredite el derecho propietario
- Certificado de matrícula.
- Certificado de arqueo. (si corresponde)
- Certificado de franco bordo. (si corresponde)
- Rol de tripulación con sus respectivas Libretas de embarco.

- Libro de bitácora y de máquinas.
- Plan de contingencias. (si corresponde)

### **g) PREVENCIÓN DE LA CONTAMINACIÓN DEL MEDIO ACUÁTICO.**

- Verificación de la cantidad suficiente de basureros a bordo.
- Plan de contingencia por derrame de hidrocarburos. (si corresponde)
- Libro de descargo de basura y aguas servidas o negras en tierra, refrendados por la Capitanía de Puerto.
- Libro de descargas de sentina (aceites, combustibles) en tierra refrendados por la capitanía de Puerto.

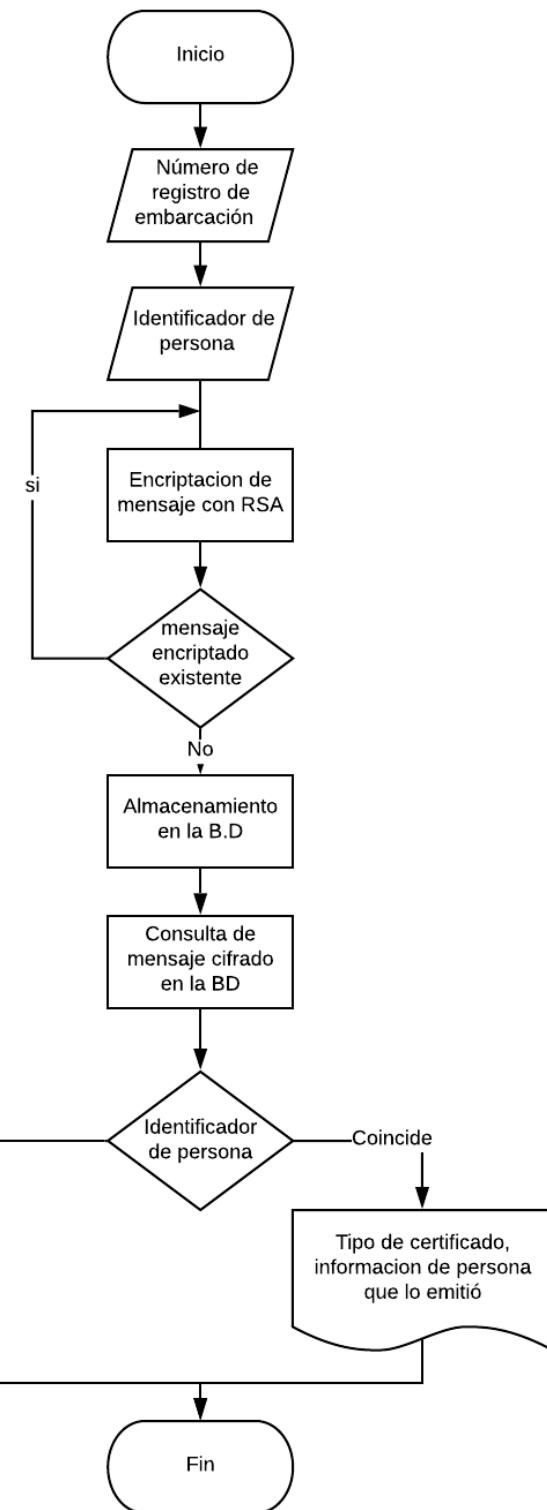
**Articulo 24º (Ámbito marítimo)** En el ámbito marítimo las reglas para realizar las inspecciones técnicas se regirán de acuerdo al convenio para la Seguridad de la Vida Humana en el Mar (SOLAS) de la Organización Marítima Internacional.

**Articulo 25º (Ámbito de la Hidrovía)** en el ámbito de la Hidrovía Paraguay- Paraná las directrices para realizar las inspecciones técnicas se regirán conforme al Reglamento de Reconocimientos, Inspecciones y Certificados de Seguridad para las Embarcaciones.

**Artículo 26° (Prohibición).** Queda prohibido arrojar lastre, escombros, basura, derrame de derivados de petróleo, aguas producidas por el lavado de minerales, materiales nocivos que ocasionen daños o perjuicios en aguas de jurisdicción nacional, tales como en puertos, ríos y lagos.

■ .

**ANEXO M:**  
**DETERMINACIÓN DE MENSAJES A ENCRYPTAR**



**ANEXO N:**  
**COTIZACIÓN DE SERVIDORES PARA BASES DE DATOS**

Instancias optimizadas para memoria – Generación actual	Precio por hora
db.r6g.large	0,215 USD
db.r6g.xlarge	0,43 USD
db.r6g.2xlarge	0,859 USD
db.r6g.4xlarge	1,718 USD
db.r6g.8xlarge	3,437 USD
db.r6g.12xlarge	5,155 USD
db.r6g.16xlarge	6,874 USD
db.r5.large	0,24 USD
db.r5.xlarge	0,48 USD
db.r5.2xlarge	0,96 USD
db.r5.4xlarge	1,92 USD
db.r5.8xlarge	3,84 USD
db.r5.12xlarge	5,76 USD
db.r5.16xlarge	7,68 USD
db.r5.24xlarge	11,52 USD

## ANEXO O: COTIZACIÓN DE SERVIDOR PARA APLICACIÓN

Supongamos que su aplicación móvil recibe una media de 100 conexiones nuevas por segundo y cada una dura 3 minutos. Un cliente envía una media de 4 solicitudes por segundo por conexión y se procesan 1000 bytes por conexión. Usted ha configurado 20 reglas en el balanceador de carga para direccionar las solicitudes de su cliente. Calculamos los costes mensuales del balanceador de carga de aplicaciones utilizando el precio de la región EE.UU. Este del modo siguiente:

- Conexiones nuevas (por segundo): cada LCU ofrece 25 conexiones por segundo. Dado que nuestra aplicación móvil usa 100 conexiones nuevas por segundo, esto equivale a 4 LCU (100 conexiones por segundo/25 conexiones por segundo).
- Conexiones activas (por minuto): cada LCU ofrece hasta 3 000 conexiones activas por minuto. Dado que su aplicación móvil recibe 100 conexiones por segundo y cada una dura 3 minutos, esto equivale a un máximo de 18 000 conexiones activas por minuto o 6 LCU (18 000 conexiones activas por minuto/3 000 conexiones activas por minuto).
- Bytes procesados (GB por hora): cada LCU ofrece 1 GB por hora. Dado que nuestra aplicación móvil transfiere una media de 1000 bytes de datos por conexión, esto equivale a 0,36 GB por hora o 0,36 LCU (0,36 GB/1 GB).
- Evaluaciones de regla (por segundo): cada LCU ofrece 1 000 evaluaciones de regla por segundo. Dado que su aplicación recibe 4 solicitudes/seg por conexión, esto equivale a 400 solicitudes/seg en todas las conexiones. Con 20 reglas configuradas en un máximo de 4 000 evaluaciones de regla por segundo (20 reglas configuradas – 10 reglas gratis)\* 400 o 4 LCU (4 000 evaluaciones de regla por segundo/1 000 evaluaciones de regla por segundo).

Al utilizar estos valores, la tarifa por hora se calcula teniendo en cuenta la LCU máxima consumida en las cuatro dimensiones. En este ejemplo, las conexiones activas (6 LCU) son mayores que las conexiones nuevas (4 LCU), el ancho de banda (0,36 LCU) y las evaluaciones de regla (4 LCU). Esto da como resultado un cargo total de 0,048 USD **por hora** (6 LCU \* 0,008 USD) o 34,56 USD **por mes** (0,048 USD \* 24 horas \* 30 días).

**ANEXO P:**  
**CARTA DE ACEPTACIÓN DE CASO DE ESTUDIO**

La Paz 20 de marzo de 2020

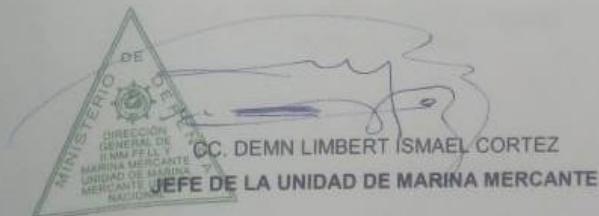
Señor:

My. DIM. Yusef Aparicio Romay  
**JEFE DE CARRERA - INGENIERÍA DE SISTEMAS**  
**ESCUELA MILITAR DE INGENIERÍA**  
Presente. –

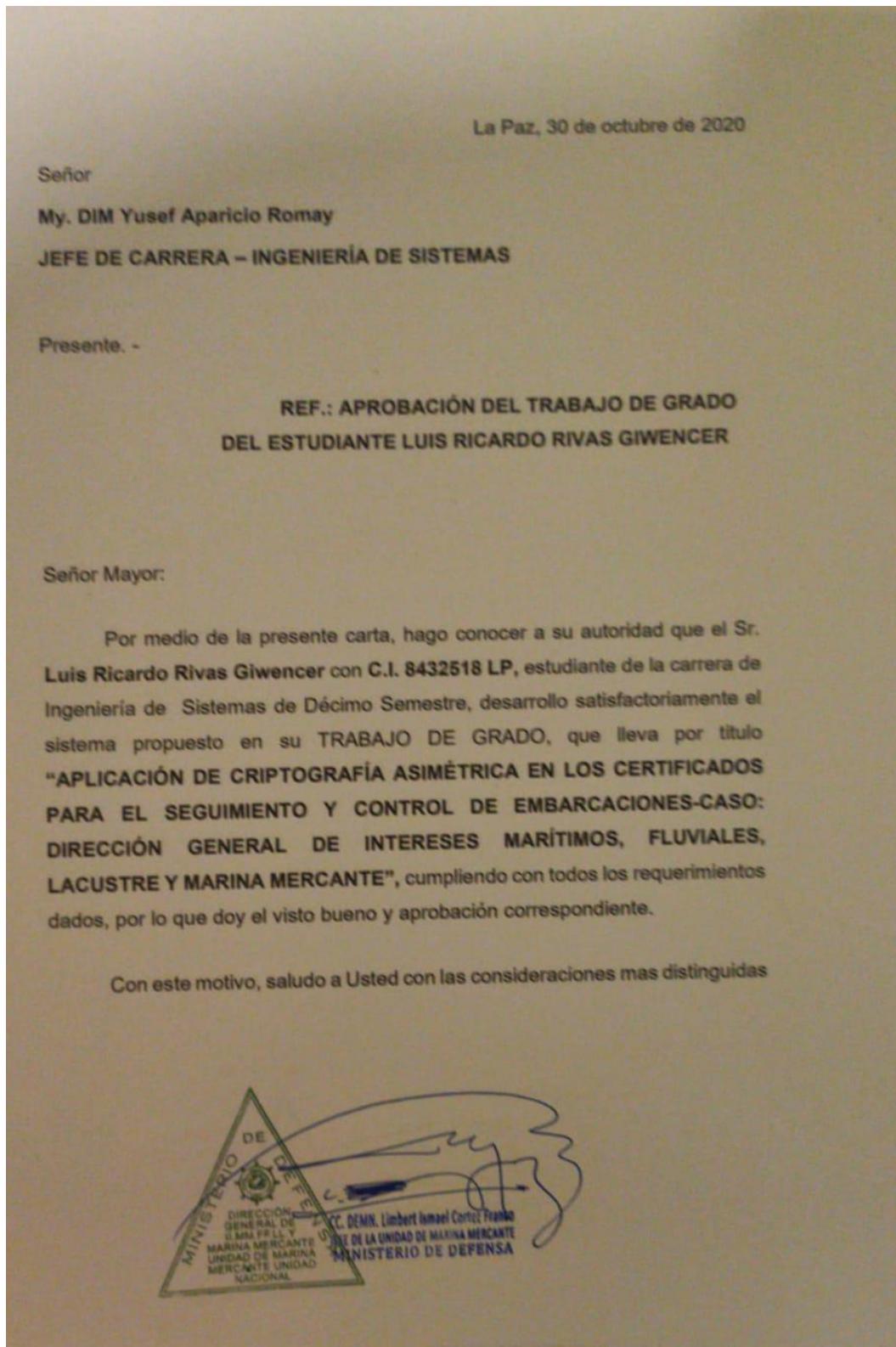
Señor Mayor:

Por intermedio de la presente, manifiesto que se brindara la ayuda necesaria a el estudiante, LUIS RICARDO RIVAS GIWENCER, en su trabajo de grado que lleva por título: "APLICACIÓN DE CRIPTOGRAFIA ASIMÉTRICA EN LOS CERTIFICADOS DE REGISTRO PARA EL CONTROL Y SEGUIMIENTO DE EMBARCACIONES - CASO: DIRECCIÓN GENERAL DE INTERESES MARITIMOS, FLUVIALES, LACUSTRE Y MARINA MERCANTE", brindándole la información que él precise y para que logre implementar el trabajo de manera óptima.

Con este motivo saludo a usted con las consideraciones distinguidas.



**ANEXO Q:**  
**CARTA DE CONFORMIDAD DE CASO DE ESTUDIO**





ESCUELA MILITAR DE INGENIERÍA  
“Mcal Antonio Jose de Sucre”

## FICHA DE INVESTIGACIÓN

### 1.- Título del proyecto

### APLICACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA EN LOS CERTIFICADOS PARA EL SEGUIMIENTO Y CONTROL DE EMBARCACIONES

---

### 2.- Objetivo

Aplicar criptografía asimétrica en los certificados que emite la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, para realizar el seguimiento y control durante las inspecciones, verificando la autenticidad de la información en los mismos.

---

### 3.- Tipo de proyecto

Investigación Aplicada

Investigación Básica

Otro(especificar)

### 4.- Área de investigación

Inteligencia Artificial, Agente Inteligente, Tecnología de Radiofrecuencia

### 5.- Línea de investigación

Seguridad

### 6.- Carrera

Ingeniería de Sistemas

### 7.- Unidad Académica

Unidad Académica La Paz

### 8.- Periodo Académico

1°                    2°

### 9.- Gestión

II-2020

### 10.-Nombre del estudiante

Luis Ricardo Rivas Giwencer

### 11.- Nombre del Tutor

Lic. Cynthia Rodriguez Canaviri