

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: Trabajo de Grado
presentado como requisito parcial
para optar al Título de Licenciatura
en Ingeniería de Sistemas

TUTOR: LIC. CYNTHIA RODRIGUEZ CANAVIRI

LA PAZ, 2020

ÍNDICE

CAPÍTULO I GENERALIDADES

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

CAPÍTULO II MARCO TEÓRICO

2.1	INGENIERÍA DE SISTEMAS.....	12
2.1.1	Ingeniería.....	13
2.1.2	Sistema.....	14
2.2	INGENIERÍA DE SOFTWARE.....	14
2.2.1	Metodología Ágil.....	15
2.2.2	Modelos de Desarrollo de Software.....	16
2.3	SEGURIDAD DE SISTEMAS	18
2.3.1	Pilares de la seguridad de la información	19
2.4	CRIPTOGRAFÍA.....	20
2.4.1	Objetivos de la Criptografía	21

2.4.2	Conceptos Básicos de Criptografía	22
2.5	CRIPTOGRAFÍA ASIMÉTRICA.....	23
2.5.1	Ventajas.....	24
2.5.2	Algoritmo RSA	25
2.6	METODOLOGÍA DE DESARROLLO.....	28
2.6.1	Metodología Design Sprint	29
2.6.2	Lenguaje de Modelado Unificado (UML)	32
CAPÍTULO II MARCO PRÁCTICO		
3.1	ANÁLISIS DE LA SITUACIÓN ACTUAL.....	40
3.1.1	Contexto de la organización	41
3.1.2	Identificación del personal	41
3.1.3	Consulta de información	42
3.1.4	Análisis de procesos.....	43
3.1.4.1	Registro de embarcaciones	43
3.1.4.2	Inspección de embarcaciones	47
3.1.5	Determinación de Requerimientos del Sistema	48
3.1.6	Definición de módulos del sistema	50
3.2	IMPLEMENTACIÓN DEL ALGORITMO ASIMÉTRICO	52
3.2.1	Determinación del algoritmo a implementar	52
3.2.2	Generación de llaves	54
3.2.3	Determinación de Información a Encriptar.....	55
3.2.4	Generación de código QR	56
3.3	DESARROLLO DEL SISTEMA.....	57
3.3.1	Sprint 0 Base de Datos y Arquitectura del Sistema	57
3.3.1.1	Desarrollo de la Base de Datos	58
3.3.1.2	Arquitectura del sistema	64
3.3.2	Sprint 1 Módulo de Gestión de Usuarios	66
3.3.2.1	Lista de Requerimientos	66
3.3.2.2	Especificación del Proceso	67
3.3.2.3	Diseño de Procesos.....	67
3.3.2.4	Diseño de Interfaces.....	68
3.3.2.5	Diseño Navegacional.....	70
3.3.2.6	Construcción de Interfaces	71

3.3.2.7 Código	72
3.3.2.8 Prueba Unitaria.....	73
3.3.3 Sprint 2 Módulo de Inspecciones.....	74
3.3.3.1 Lista de Requerimientos	74
3.3.3.2 Especificación del Proceso.....	75
3.3.3.3 Diseño de Procesos.....	75
3.3.3.4 Diseño de Interfaces.....	76
3.3.3.5 Diseño Navegacional.....	78
3.3.3.6 Construcción de Interfaces	79
3.3.3.7 Código	80
3.3.3.8 Prueba Unitaria.....	81
3.3.4 Sprint 3 Módulo de Registro de Embarcaciones.....	81
3.3.4.1 Lista de Requerimientos	81
3.3.4.2 Especificación del Proceso.....	83
3.3.4.3 Diseño de Procesos.....	83
3.3.4.4 Diseño de Interfaces.....	84
3.3.4.5 Diseño Navegacional.....	86
3.3.4.6 Construcción de Interfaces	86
3.3.4.7 Código	87
3.3.4.8 Prueba Unitaria.....	88
3.3.5 Sprint 4 Módulo Verificación de Documentos	89
3.3.5.1 Lista de Requerimientos	89
3.3.5.2 Especificación del Proceso.....	90
3.3.5.3 Diseño de Procesos.....	90
3.3.5.4 Diseño de Interfaces.....	91
3.3.5.5 Diseño Navegacional.....	92
3.3.5.6 Construcción de Interfaces	93
3.3.5.7 Código	93
3.3.5.8 Prueba Unitaria.....	94
3.3.6 Sprint 5 Módulo de Registro de Reportes.....	95
3.3.6.1 Lista de Requerimientos	95
3.3.6.2 Especificación del Proceso.....	96
3.3.6.3 Diseño de Procesos.....	96

3.3.6.4	Diseño de Interfaces.....	97
3.4	PRUEBAS DEL SISTEMA.....	101
3.4.1	Pruebas de Integración.....	101
3.5	IMPLEMENTACIÓN DEL SISTEMA.....	102
3.5.1	Instalación del sistema	102
3.5.2	Revisión de funcionamiento.....	103
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	19
FIGURA 5: PRUEBA UNITARIA	32
FIGURA 6: ORGANIGRAMA DEL PERSONAL DE DGIMFLMM.....	42
FIGURA 7: DIAGRAMA DE CASO DE USO DE ALTO NIVEL	50
FIGURA 8: PONDERACIONES DE CHECKLIST	51
FIGURA 9: IMPLEMENTACIÓN DE ALGORITMO ASIMÉTRICO	52
FIGURA 10: GENERACIÓN DE PARES DE LLAVES	54
FIGURA 11: LLAVE ENCRIPTADA EN BASE64	55
FIGURA 12: OBTENCIÓN DE MENSAJE A ENCRIPTAR.....	55
FIGURA 13: PROCESO DE GENERACIÓN DE CÓDIGO QR	56
FIGURA 14: CÓDIGO QR AÑADIDO A CERTIFICADO	57
FIGURA 15: MODELO ENTIDAD-RELACIÓN	58
FIGURA 16: DIAGRAMA DE CLASES.....	59
FIGURA 17: TABLA DE EMBARCACIONES	60
FIGURA 18: TABLA DE MOVIMIENTOS ECONÓMICOS	60
FIGURA 19: TABLA DE ARCHIVOS.....	61
FIGURA 20: TABLA DE REINICIO DE CONTRASEÑAS	61
FIGURA 21: TABLA DE ASIGNACIÓN DE ROLES	62
FIGURA 22: TABLA DE RELACIÓN USUARIO-ROL	62
FIGURA 23: TABLA DE USUARIOS.....	63
FIGURA 24: MODELO RELACIONAL DE BASE DE DATOS	64
FIGURA 25: DIAGRAMA DE CLASES.....	65
FIGURA 26: DIAGRAMA DE DESPLIEGUE	65
FIGURA 27: DIAGRAMA DE CASO DE USO (GESTIÓN DE USUARIOS)	67
FIGURA 28: DIAGRAMA DE ACTIVIDADES (GESTIÓN DE USUARIOS)	68
FIGURA 29: BOCETO DE INICIO DE SESIÓN	69
FIGURA 30: BOCETO DE REGISTRO DE USUARIO	69
FIGURA 31: BOCETO DE MODIFICACIÓN DE USUARIO	70

FIGURA 32: DIAGRAMA DE COMPONENTES (GESTIÓN DE USUARIOS).....	70
FIGURA 33: PANTALLA INICIO DE SESIÓN	71
FIGURA 34: PANTALLA DE REGISTRO DE USUARIO.....	71
FIGURA 35: PANTALLA DE EDICIÓN DE USUARIOS	72
FIGURA 36: CÓDIGO PARA GESTIÓN DE USUARIOS.....	73
FIGURA 37: PRUEBA UNITARIA MOCK (GESTIÓN DE USUARIOS).....	73
FIGURA 38:DIAGRAMA DE CASO DE USO (INSPECCIÓN DE EMBARCACIÓN). 75	
FIGURA 39: DIAGRAMA DE ACTIVIDADES (INSPECCIÓN DE EMBARCACIÓN). 76	
FIGURA 40: BOCETO DE REALIZAR INSPECCIÓN	77
FIGURA 41: BOCETO DE BARRA DE PROGRESO.....	77
FIGURA 42: BOCETO DE FORMULARIO DE INSPECCIÓN.....	78
FIGURA 43: DIAGRAMA DE COMPONENTES (INSPECCIONES)	78
FIGURA 44: PANTALLA PARA ACCEDER A INSPECCIÓN.....	79
FIGURA 45: PANTALLA DE FORMULARIO DE INSPECCIÓN.....	79
FIGURA 46: CÓDIGO PARA INSPECCIONES.....	80
FIGURA 47: PRUEBA UNITARIA MOCK (GESTIÓN DE USUARIOS).....	81
FIGURA 48: DIAGRAMA DE CASO DE USO (REGISTRO DE EMBARCACIÓN) ...	83
FIGURA 49: DIAGRAMA DE ACTIVIDADES (REGISTRO DE EMBARCACIÓN)	84
FIGURA 50: BOCETO DE REQUISITOS.....	85
FIGURA 51: BOCETO DE REGISTRO	85
FIGURA 52: DIAGRAMA DE COMPONENTES (REGISTRO).....	86
FIGURA 53: PANTALLA DE REQUISITOS DE REGISTRO	87
FIGURA 54: PANTALLA DE REGISTRO DE EMBARCACIÓN	87
FIGURA 55: CÓDIGO PARA REGISTRO DE EMBARCACIÓN	88
FIGURA 56: PRUEBA UNITARIA MOCK (REGISTRO DE EMBARCACIÓN)	88
FIGURA 57: DIAGRAMA DE CASO DE USO (VERIFICACIÓN DE DOCUMENTOS)	90
FIGURA 58: DIAGRAMA DE ACTIVIDADES (VERIFICACIÓN DE DOCUMENTOS)	91
FIGURA 59:BOCETO DE VERIFICACIÓN DE DOCUMENTO	92
FIGURA 60: DIAGRAMA DE COMPONENTES (VERIFICACIÓN DE DOCUMENTOS)	92
FIGURA 61: PANTALLA DE VERIFICACIÓN DE DOCUMENTO.....	93

FIGURA 62: CÓDIGO PARA VERIFICACIÓN DE DOCUMENTOS	94
FIGURA 63: PRUEBA UNITARIA MOCK (VERIFICACIÓN DE DOCUMENTOS)	94
FIGURA 64: DIAGRAMA DE CASO DE USO (REPORTES)	96
FIGURA 65: DIAGRAMA DE ACTIVIDADES (REPORTES)	97
FIGURA 66: BOCETO DE REPORTE	98
FIGURA 67: DIAGRAMA DE COMPONENTES (REPORTES)	98
FIGURA 68: REPORTE	99
FIGURA 69: CÓDIGO PARA REPORTE	100
FIGURA 70: PRUEBAS UNITARIAS MOCK (REPORTES)	100
FIGURA 71: EXÁMEN DE USABILIDAD	101
FIGURA 72: PRUEBAS MOCK DEL SISTEMA	102

ÍNDICE DE TABLAS

TABLA 1: COMPARACIÓN DE METODOLOGÍA	15
TABLA 2: EJEMPLO DE USO DE RSA	27
TABLA 3: DESCRIPCIÓN DE ENTREGABLES.....	31
TABLA 4: DIAGRAMAS UML.....	34
TABLA 5: DESARROLLO DEL MARCO PRÁCTICO	36
TABLA 6: COMPARACIÓN INSPECCIONES DE EMBARCACIONES.....	48
TABLA 7: TABLA DE REQUERIMIENTOS	49
TABLA 8: COMPARACIÓN DE ALGORITMOS ASIMÉTRICOS.....	53
TABLA 9: DOT VOTING DE ALGORITMO VS PERSONAL	53
TABLA 10: REQUERIMIENTOS (GESTIÓN DE USUARIOS)	66
TABLA 11: REQUERIMIENTOS MODULO DE INSPECCIONES.....	74
TABLA 12: REQUERIMIENTOS MÓDULO DE INSPECCIONES.....	82
TABLA 13: REQUERIMIENTOS MÓDULO DE SEGURIDAD.....	89
TABLA 14: REQUERIMIENTOS MÓDULO DE REPORTES	95

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: REGLAMENTO NACIONAL PARA LA CONSTRUCCIÓN
- ANEXO M: DETERMINACIÓN DE MENSAJES A ENCRIPITAR

CAPÍTULO I GENERALIDADES



RESUMEN

En este capítulo se desarrollan los puntos principales del presente proyecto, empezando por una introducción al área de estudio, los antecedentes, el planteamiento del problema, los objetivos propuestos y de esta manera concluir con la justificación y los alcances para tener una base general del desarrollo del Trabajo de Grado propuesto.

1.1 INTRODUCCIÓN

La criptología es la disciplina que se encarga del estudio de la escritura secreta, esta 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 defina a la criptografía como el estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y 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, y posee las siguientes propiedades: confidencialidad, integridad, vinculación y autenticación.

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 descifrar 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 lograra 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 unidades más pequeñas

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.

Misión

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.

Visión

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.

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 HÍBRIDA**”, 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 híbrida 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 híbrida 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. 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 este proceso 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 seis meses (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, se entregará los mismos a los dueños, a los cuales se les proporcionará una clave pública generada a partir del número de motor de la embarcación que corresponde, la Dirección General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante tendrá un respaldo digital de estos en una plataforma web (ver nexa G).

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 asignado 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

CONCLUSIÓN

Este capítulo concluye con la justificación y los alcances que están ligados a este Trabajo de Grado, se determinaron tres objetivos específicos a cumplir y cómo se pretende dar el correcto cumplimiento a los mismos.

CAPÍTULO II

MARCO TEÓRICO



RESUMEN

En el presente capítulo se establecen las bases teóricas para el desarrollo del Trabajo de Grado, incluye Ingeniería de Sistemas, Ingeniería de Software, Seguridad de Sistemas, Criptografía, Criptografía Asimétrica y Metodología de Desarrollo.

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 asegurarla 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 Metodología Ágil

Existen marcadas diferencias entre una metodología ágil y una metodología tradicional, como se muestra en la Tabla 1.

TABLA 1: COMPARACIÓN DE METODOLOGÍA

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

Fuente: Elaboración propia

Como se pudo observar en la Tabla 1 se puede observar las diferencias que existe entre las características que poseen las metodologías tradicionales y las metodologías ágiles, las cuales serán empleadas en el presente Trabajo de Grado.

Las primeras metodologías ágiles 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 usará una metodóloga ágil 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.

2.2.2 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.

2.2.2.1 Modelo en espiral

Es un modelo de proceso de software evolutivo que conjuga la naturaleza iterativa de construcción de prototipos con los aspectos controlados y sistemáticos del modelo lineal secuencial. Proporciona el potencial para el desarrollo rápido de versiones incrementales del software y las mejoras a menudo tienen lugar en pasos muy pequeños como se puede observar en la Figura 3.

FIGURA 3: MODELO EN ESPIRAL



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

En la Figura 3, 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.

2.3 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 4. 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://rosarioherediaprojectodesoftware.wordpress.com/2017/09/10/espinal-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. Analizando la norma ISO/IEC 27002, 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 descifrar 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 descifrar 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 asociadas 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 necesitara 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.

2.5.2 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).

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.

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 $n=p*q$
- Con ϕ es la función ϕ de Euler calcula $\phi(n)=(p-1)*(q-1)$
- Se escoge un entero positivo “e” menor que $\phi(n)-2$, que sea coprimo con $\phi(n)$
- Se determina un d (mediante aritmética modular) que satisfaga la congruencia $e * d = 1 \pmod{\phi(n)}$, es decir, que d sea el multiplicador modular inverso de $e \pmod{\phi(n)}$
- 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, 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	$\varphi(n)=(p-1)*(q-1)$ $\varphi(33) = (3-1)*(11-1) = 20$	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	$C = (5^3) \bmod 33 = 26$	Se procede a cifrar el mensaje, donde c es el mensaje cifrado donde se hace uso de la clave publica
10	$M = 26^7 \bmod 33 = 5$	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.

2.6 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 Metodología Design Sprint

Metodología desarrollada por Jake Knapp con el objetivo 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.

2.6.1.1 Fases

La metodología Design Sprint cuenta con 5 fases según lo establecido, las cuales nos ayudaran a realizar el desarrollo de nuestro software:

- 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.

2.6.1.2 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 Knapp, en el año 2016, creador de Design Sprint se puede tener los siguientes entregables, en la Tabla 3 se pueden observar los nombres y sus respectivas descripciones de los mismos en cada una de las fases que esta metodología propone.

TABLA 3: 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 las más comunes. Este enfoque de votación adhesiva es una forma de votación acumulativa
	Heat map voting	Mapa que indica las características que son deseables de la elección realizada en el proceso anterior.
Prototipar	Storyboards,	Representaciones visuales de una interacción con el producto software
	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 5
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 5: PRUEBA UNITARIA

```
→ PayPalTesting git:(master) X 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) X 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 5 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.

2.6.2 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.

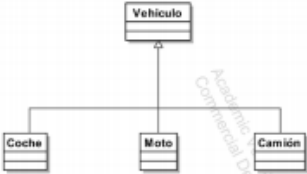

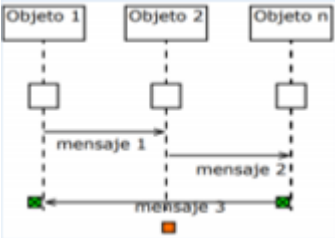
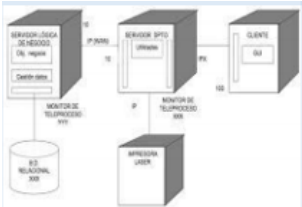
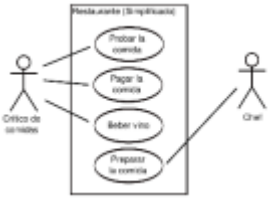
2.6.2.1 Diagramas UML

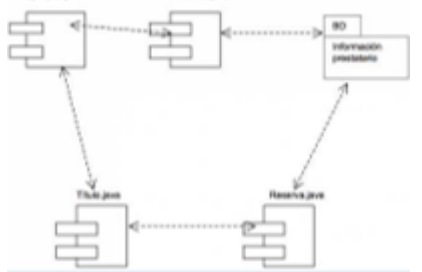
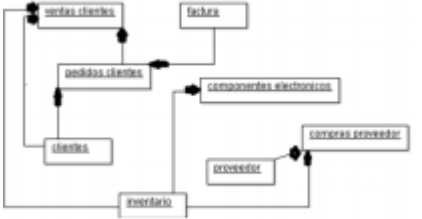
Para la representación de diferentes procesos, actores y actividades se utilizan distintos diagramas que posee UML, cada diagrama tiene un propósito específico, como se puede apreciar en la Tabla 4.

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 4: DIAGRAMAS UML

Diagrama	Descripción	Prioridad
<p>Diagrama de clases</p> 	<p>Muestra una colección de elementos de modelado declarativo (estáticos), tales como clases, tipos y sus contenidos y relaciones</p>	Alta
<p>Diagrama de actividades</p> 	<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
<p>Diagrama de secuencias</p> 	<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>Diagrama de despliegue físico</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>	Media
<p>Diagrama de casos de uso</p> 	<p>Un diagrama que muestra las relaciones entre los actores y el sujeto (sistema), y los casos de uso</p>	Media

<p>Diagrama de componentes</p> 	<p>Representan los componentes que conforman una aplicación, sistema o empresa. Los componentes, sus relaciones, iteraciones y sus interfaces publicas</p>	<p>Media</p>
<p>Diagrama de objetos</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.

CONCLUSIÓN

En este capítulo se determinó el tipo de criptografía y normas ISO a usar, se concluyó que la metodología de desarrollo de software a utilizar en el presente Trabajo de Grado será la metodología Sprint Design, además del uso de notación UML para el mejor entendimiento del todo el proceso de desarrollo del sistema.

CAPÍTULO III

MARCO PRÁCTICO



RESUMEN

En el presente capítulo se comienza con el desarrollo del sistema planteado en el Trabajo de Grado, incluye análisis de la situación actual, implementación del algoritmo asimétrico, desarrollo del sistema, pruebas del sistema e implementación.

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	Etapas	Tareas	Entregables
3.1 Análisis de situación actual	Entendimiento <ul style="list-style-type: none"> Saber quién es el usuario y cuáles son sus necesidades. Conocer el contexto de la organización y del producto 	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 Analizar los procesos	Descripción de cada proceso Flujogramas
	Propuestas <ul style="list-style-type: none"> Plantear ideas sin importar la calidad 	3.1.5 Determinación de requerimientos del sistema	Diagrama de caso de uso de alto nivel
			Tabla de requerimientos
	Decidir <ul style="list-style-type: none"> Tomar decisiones apoyándose en las conclusiones y la información recabada en las fases anteriores. 	3.1.6 Definir los módulos del Sistema	Notas HMW

3.2 Implementación del algoritmo asimétrico	<p>Método Wigginton</p> <ul style="list-style-type: none"> • Generación de llaves • Definir el mensaje a encriptar • Cargar la llave privada • Encriptar el mensaje • Generar código QR • Cargar la llave publica • Desencriptar el mensaje <p>Prototipo</p> <ul style="list-style-type: none"> • Definir el tipo de usuario que interactuará con cada módulo • Definir específicamente cual será la interacción de cada módulo del sistema 	3.2.1 Determinación del algoritmo a implementar	Tabla comparativa de algoritmos asimétricos
		3.2.2 Generar par de llaves	Dot Voting
			Generación de números primos aleatoriamente
			Cálculo de parámetro “n”, función de “ ϕ (n)”, “d” y “e”.
			Obtención de llave privada y llave pública
		3.2.3 Identificación de información a encriptar	Definición del proceso de gestión de llaves
			Revisión de reglamentos
		3.2.4 Generar código QR	Flujogramas
			Identificación del tamaño del código
			Determinación de la calidad del código
			Determinación de contenido del código QR
3.3 Desarrollo del sistema	<p>Sprints</p> <ul style="list-style-type: none"> • Análisis • Diseño • Desarrollo • Pruebas 	3.3.1 Sprint 0 Base de datos y Arquitectura del Sistema	
		3.3.1.1 Construcción de la Base de Datos	Diagrama entidad relación
			Diagrama de clases
			Diccionario de base de datos
			Modelo relacional de la base de datos
		3.3.1.2 Arquitectura del sistema	Diagrama de despliegue

		3.3.2 Sprint 1 Módulo de Gestión de Usuarios	
		3.3.2.1 Lista de requerimientos	Tabla de requerimientos del módulo
		3.3.2.2 Especificación del proceso	Diagrama de casos de uso expandido
		3.3.2.3 Diseño de procesos	Diagrama de actividades
		3.3.2.4 Diseño de interfaces	Storyboard sprint 1
		3.3.2.5 Diseño navegacional	Diagramas de componentes
		3.3.2.6 Construcción de interfaces	Pantalla
		3.3.2.7 Código	Codificación del Módulo
		3.3.2.8 Prueba unitaria	Mock
		3.3.3 Sprint 2 Módulo de Inspecciones	
		3.3.3.1 Lista de requerimientos	Tabla de requerimientos del módulo
		3.3.3.2 Especificación del proceso	Diagrama de casos de uso expandido
		3.3.3.3 Diseño de procesos	Diagrama de actividades
		3.3.3.4 Diseño de interfaces	Storyboard sprint 2
		3.3.3.5 Diseño navegacional	Diagramas de componentes
		3.3.3.6 Construcción de interfaces	Pantalla
		3.3.3.7 Código	Codificación del Módulo

		3.3.3.8 Prueba unitaria	Mock
		3.3.4 Sprint 3 Módulo de Registro de Embarcaciones	
		3.3.4.1 Lista de requerimientos	Tabla de requerimientos del módulo
		3.3.4.2 Especificación del proceso	Diagrama de casos de uso expandido
		3.3.4.3 Diseño de procesos	Diagrama de actividades
		3.3.4.4 Diseño de interfaces	Storyboard sprint 3
		3.3.4.5 Diseño navegacional	Diagramas de componentes
		3.3.4.6 Construcción de interfaces	Pantalla
		3.3.4.7 Código	Codificación del Módulo
		3.3.4.8 Prueba unitaria	Mock
		3.3.5 Sprint 4 Módulo de Seguridad	
		Lista de requerimientos	Tabla de requerimientos del módulo
		Especificación del proceso	Diagrama de casos de uso expandido
		Diseño de procesos	Diagrama de actividades
		Diseño de interfaces	Storyboard sprint 4
		Diseño navegacional	Diagramas de componentes
		Construcción de interfaces	Pantalla
		Código	Codificación del Módulo
		Prueba unitaria	Mock

		3.3.6 Sprint 5 Módulo de Registro de Embarcaciones	
		Lista de requerimientos	Tabla de requerimientos del módulo
		Especificación del proceso	Diagrama de casos de uso expandido
		Diseño de procesos	Diagrama de actividades
		Diseño de interfaces	Storyboard sprint 5
		Diseño navegacional	Diagramas de componentes
		Construcción de interfaces	Pantalla
		Código	Codificación del Módulo
3.4 Pruebas del sistema	Pruebas <ul style="list-style-type: none"> • Prototipos • Entrevistas • Probar el prototipo con usuarios reales. 	Prueba de integración	Test de usabilidad
			Pruebas Mocha
3.5 Implementación del sistema	Entrega <ul style="list-style-type: none"> • Dejar total libertad de uso. • Aprender del uso dado por el usuario. 	3.5.1 Instalación del sistema	Manual de usuario del administrador
			Configuración de servidor
		3.5.2 Revisión de funcionamiento	Configuración de equipos Reportes de funcionalidad del sistema

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 recopilara 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.

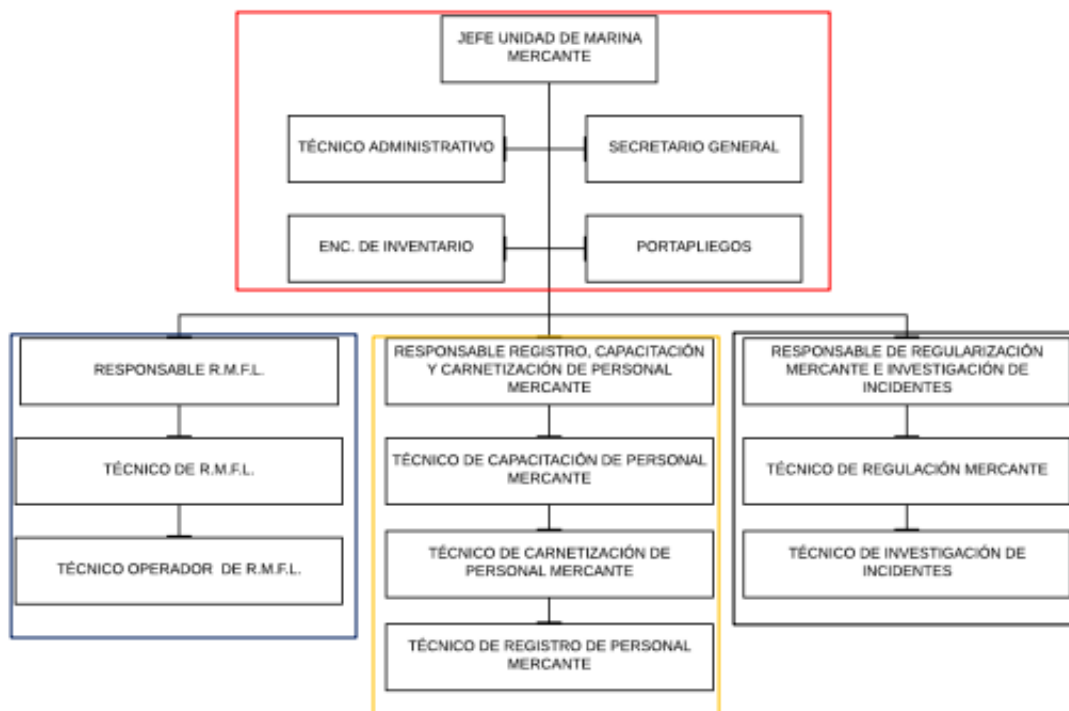
Esta unidad actualmente no cuenta con ningún sistema el cual le facilite la realización de los distintos procesos, situación por la cual manejan toda la documentación de manera física e incluso usan algunas herramientas ofimáticas para poder almacenar datos relevantes de las distintas embarcaciones.

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 tienen funciones más de soporte. Dicha organización se puede observar en la Figura 6.

FIGURA 6: ORGANIGRAMA DEL PERSONAL DE DGIMFLMM



Fuente: DGIMFLMM

En la Figura 6, 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 ira completando los certificado y fotografías correspondientes a cada una.

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 pueden 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 Hidrobia 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 Hidrobia 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 fletamento. 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 fletamento, 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 Fletamento. 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 fletamento, 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 fletamento.
 - Original del contrato de fletamento. 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 Hidrobia 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

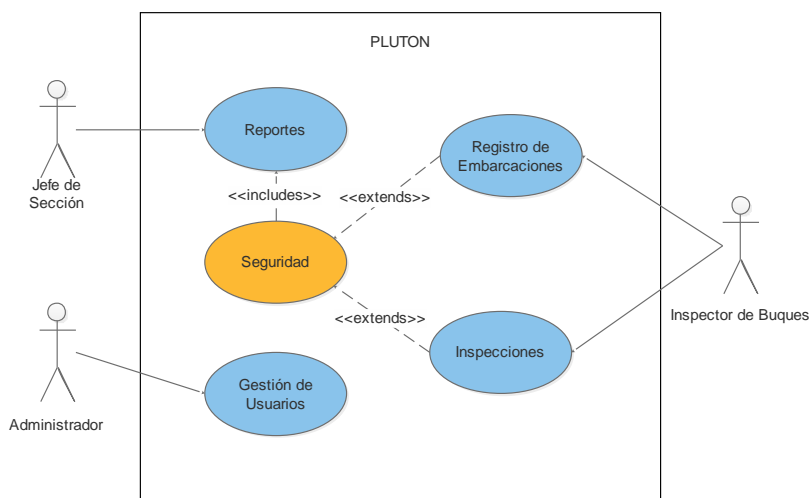
Número	Requerimiento	Descripción	Tipo	Prioridad
1	Control de acceso de usuarios del sistema	Método de seguridad previo al ingreso al sistema	Funcional	Alta
2	Registro de los datos de una embarcación nueva	Registro de los datos de una nueva embarcación a la base de datos	Funcional	Media
3	Crear una tabla 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 responsiva	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 realizara, como se observa en la Figura 8.

FIGURA 7: 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 realizara 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: Modulo que controle aquellas personas que puedan ingresar al sistema, dependiendo del rol se modificara, 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 da se 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 8.

FIGURA 8: PONDERACIONES DE CHECKLIST

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

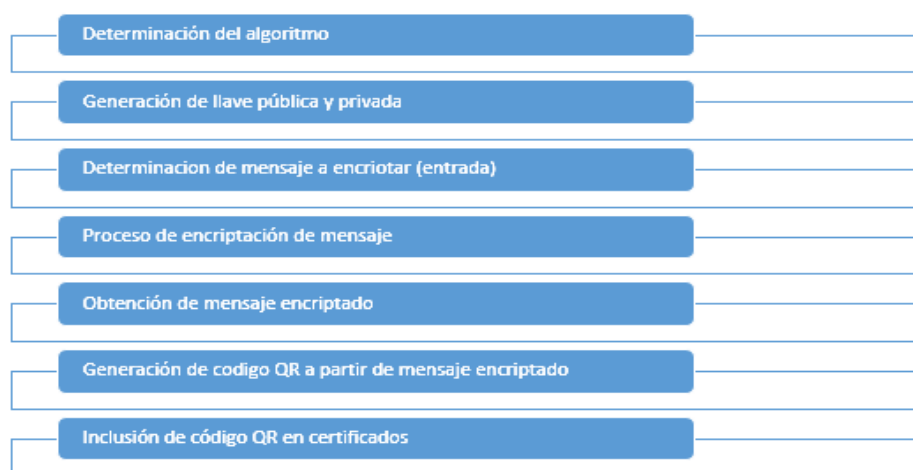
Fuente: DGIMFLMM

- Consultas: Módulo que nos permitirá consultar toda la información que se tenga registrada de una embarcación, se podrán ver los certificados con las que esta cuenta, información acerca de su tripulación e imágenes de la misma.

3.2 IMPLEMENTACIÓN DEL ALGORITMO ASIMÉTRICO

El algoritmo para usarse será RSA, debido a que este algoritmo es el que necesito 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 9.

FIGURA 9: 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: Autenticación que con un alto aseguramiento pueda ser reafirmado como genuino.

Se determino es 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 realizara 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 carnetización de personal mercante	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Res. regulación mercante e investigación de incidentes	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Total	1	1	4

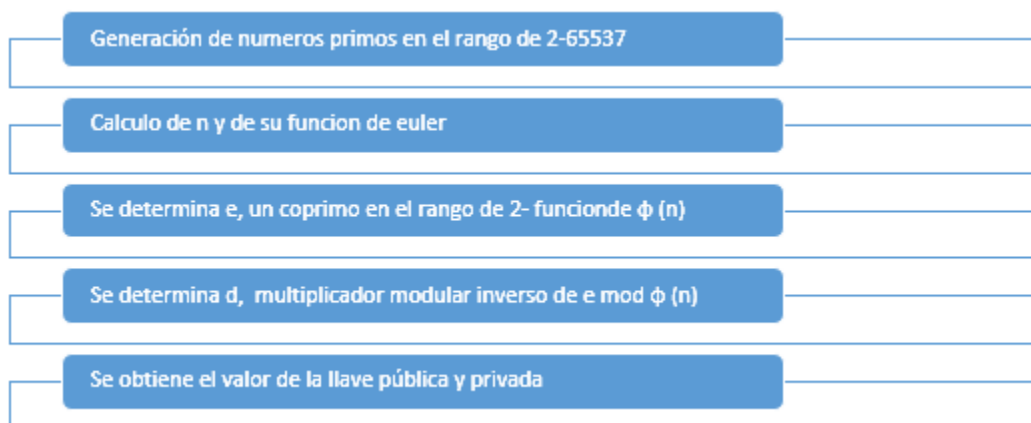
Fuente: Elaboración propia

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 10.

FIGURA 10: 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 11. 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 11: LLAVE ENCRYPTADA EN BASE64

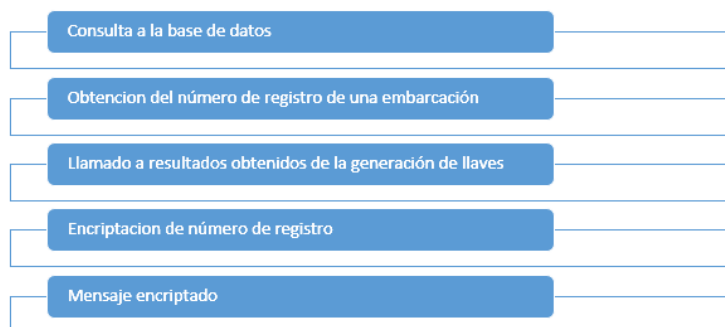
```
return "-----BEGIN OPENSSH PRIVATE KEY-----\r\n" .  
    chunk_split(base64_encode($key), 70) .  
    "-----END OPENSSH PRIVATE KEY-----";
```

Fuente: Phpseclib

3.2.3 Determinación de Información a Encriptar

La información a 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 12.

FIGURA 12: OBTENCIÓN DE MENSAJE A ENCRYPTAR



Fuente: Elaboración propia

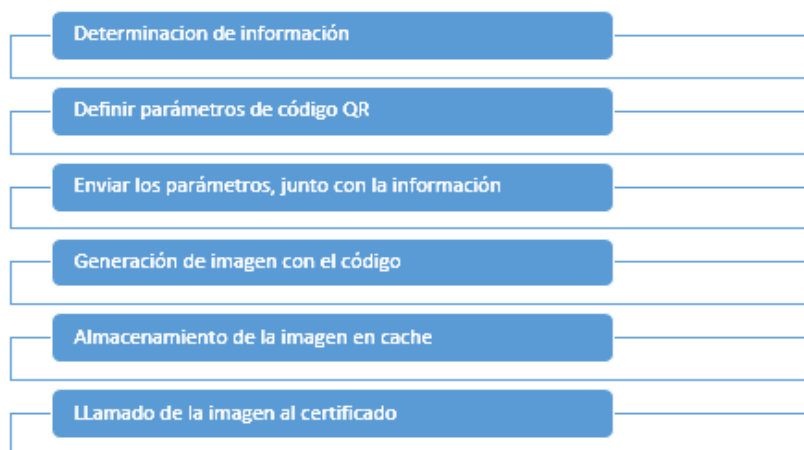
En la Figura 12 se observa el proceso para la obtención del mensaje encriptado. Una vez se tenga la información del número de registro de la embarcación, se procederá a realizar su encriptación con los valores previamente obtenido en el proceso de generación de llaves, obteniendo como resultado el mensaje 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 13.

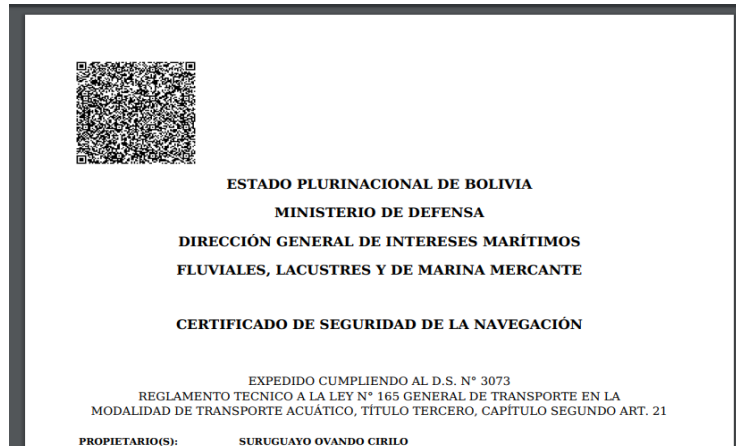
FIGURA 13: PROCESO DE GENERACIÓN DE CÓDIGO QR



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 14.

FIGURA 14: CÓDIGO QR AÑADIDO A CERTIFICADO



Fuente: Elaboración propia

Como se observa en la Figura 14, 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 0 Base de Datos y Arquitectura del Sistema

La primera fase del desarrollo del sistema, en la cual se trabajará la parte lógica del sistema.

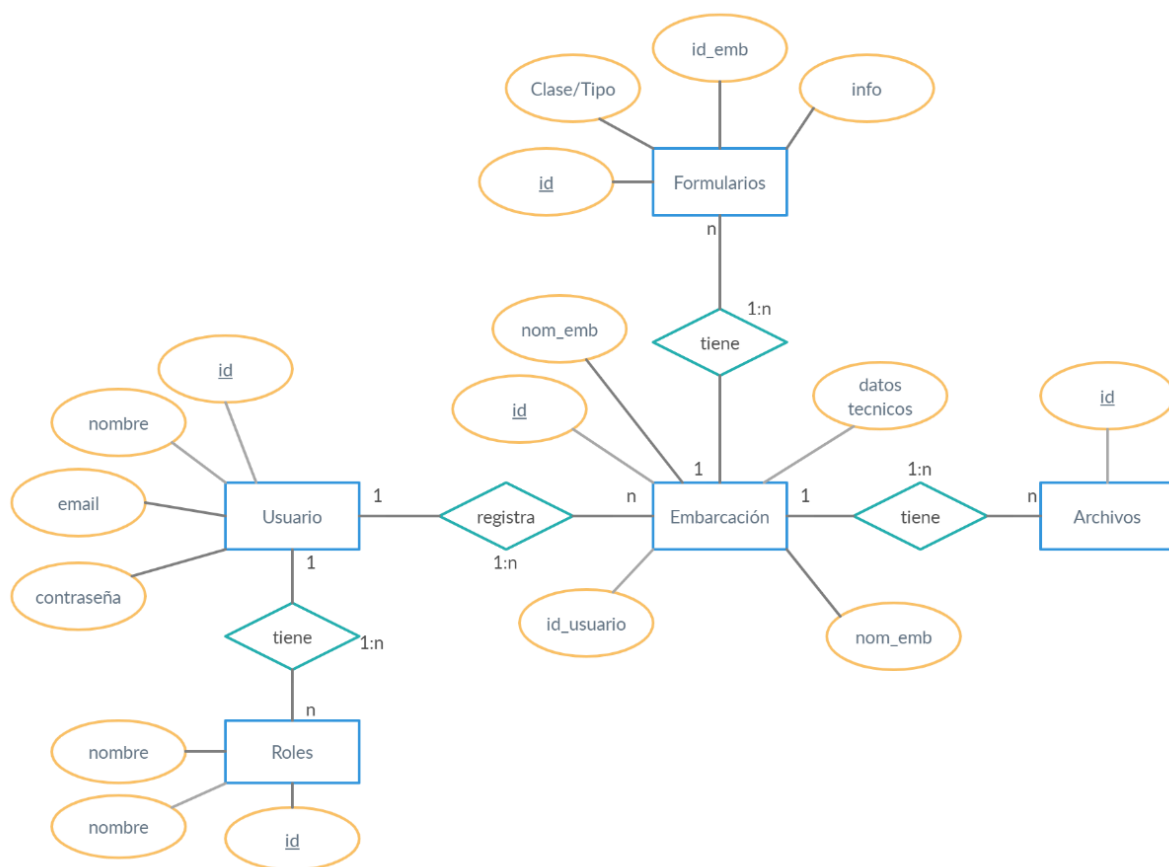
3.3.1.1 Desarrollo de la Base de Datos

Se realizará el desarrollo de la base de datos, de modo que se almacene toda la información futura acerca de las embarcaciones registrados y usuarios que tengan acceso al sistema, por lo cual este punto se dividirá en dos partes: diseño de la base de datos y construcción de esta.

- Diseño de la Base de Datos

Para el diseño de la base de datos se realizó un diagrama entidad – relación, en el cual se muestran las entidades presentes en la base de datos con sus respectivos atributos y las relaciones que tienen, como se observa en la Figura 15.

FIGURA 15: MODELO ENTIDAD-RELACIÓN

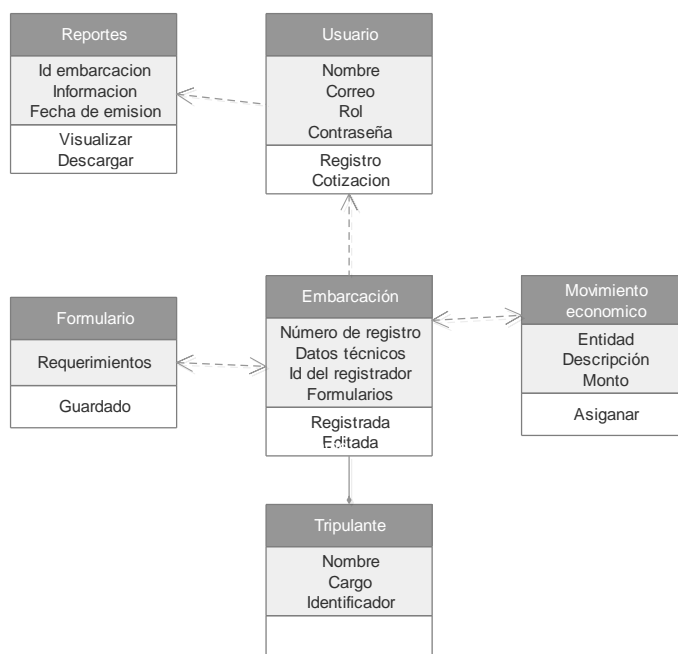


Fuente: Elaboración propia

Como se observa en la Figura 15 se tiene el modelo el cual nos muestra los objetos y atributos presentes en la base de datos.

A modo de visualizar las relaciones entre las distintas clases que involucran el sistema planteado se elaboró el diagrama de clases de la base de datos, como se observa en la Figura 16.

FIGURA 16: DIAGRAMA DE CLASES



Fuente: Elaboración propia

- Construcción de la Base de Datos

La construcción de la base de datos tiene como objetivo mejorar el almacenamiento y procesamiento de información, ayudando en la futura toma de decisiones.

Para los formularios se elaboró la tabla “embs”, la cual contendrá la información de las embarcaciones registradas, como se observa en la Figura 17.

FIGURA 17: TABLA DE EMBARCACIONES

embs

Columna	Tipo	Nulo	Predeterminado	Comentarios
id (Primaria)	bigint(20)	No		
id_emb	varchar(255)	No		
user_id	bigint(20)	No		
nom_prop	varchar(255)	No		
nom_emb	varchar(255)	No		
asc_cop	varchar(255)	No		
num_cert	varchar(255)	No		
clase_tipo	varchar(255)	No		
serv_emb	varchar(255)	No		
base_op	varchar(255)	No		
matricula	varchar(255)	No		
eslora	double(8,2)	No		
manga	double(8,2)	No		
puntal	double(8,2)	No		
trb	double(8,2)	No		
trn	double(8,2)	No		
sist_prop	varchar(255)	No		
created_at	timestamp	Sí	NULL	
updated_at	timestamp	Sí	NULL	

Fuente: Elaboración propia

Como se observa en la Figura 17, se elaboró la tabla de la base de datos la cual almacenara la información correspondiente a las embarcaciones registradas.

Para los formularios se elaboró la tabla “banks” la cual contendrá la información de los movimientos económicos realizados por la Dirección General de Intereses Marítimos Fluviales, Lacustre y Marina Mercante, como se observa en la Figura 19.

FIGURA 18: TABLA DE MOVIMIENTOS ECONÓMICOS

banks

Columna	Tipo	Nulo	Predeterminado	Comentarios
id (Primaria)	bigint(20)	No		
descripcion	varchar(255)	No		
monto	double(8,2)	No		
emb_id	bigint(20)	No		
created_at	timestamp	Sí	NULL	
updated_at	timestamp	Sí	NULL	

Fuente: Elaboración propia

Corno se observa en la Figura 19, se tiene el registro de los distintos movimientos económicos, juntamente a su descripción realizados por el caso de estudio respectivo.

Para los archivos se elaboró la tabla “files” la cual contendrá la información de los archivos subidos, ya sea acerca de embarcaciones o por parte de los usuarios, como se observa en la Figura 20.

FIGURA 19: TABLA DE ARCHIVOS

files

Columna	Tipo	Nulo	Predeterminado	Comentarios
id (<i>Primaria</i>)	bigint(20)	No		
name	varchar(255)	No		
size	varchar(255)	No		
emb_id	bigint(20)	No		
created_at	timestamp	Sí	<i>NULL</i>	
updated_at	timestamp	Sí	<i>NULL</i>	

Fuente: Elaboración propia

Como se observa en la Figura 20, se tiene el registro de los distintos archivos que se suban al sistema, a modo de tener un respaldo a posterior.

Se elaboró la tabla “password_resets”, la cual da a reestablecer las contraseñas por parte de los usuarios como se observa en la Figura 21.

FIGURA 20: TABLA DE REINICIO DE CONTRASEÑAS

password_resets

Columna	Tipo	Nulo	Predeterminado	Comentarios
email	varchar(255)	No		
token	varchar(255)	No		
created_at	timestamp	Sí	<i>NULL</i>	

Fuente: Elaboración propia

Como se observa en la Figura 21, se tiene el registro de formateo de contraseñas el cual envía un formulario al correo electrónico del usuario.

Se elaboró la tabla “roles” en la cual se establecen los roles con los que se identificará a los usuarios una vez ingresado al sistema, como se observa en la Figura 22.

FIGURA 21: TABLA DE ASIGNACIÓN DE ROLES

roles

Columna	Tipo	Nulo	Predeterminado	Comentarios
id (Primaria)	bigint(20)	No		
name	varchar(255)	No		
display_name	varchar(255)	No		

Fuente: Elaboración propia

Como se observa en la Figura 22, se tiene el registro de roles que pueden ser asignados a los usuarios.

Se elaboró la tabla "role_user". la cual ayuda establece la relación entre el rol que se le es asignado a un determinado usuario, como se observa en la Figura 23.

FIGURA 22: TABLA DE RELACIÓN USUARIO-ROL

role_user

Columna	Tipo	Nulo	Predeterminado	Comentarios
user_id	bigint(20)	No		
role_id	bigint(20)	No		

Fuente: Elaboración propia

Como se observa en la Figura 23, se tiene el registro de roles que pueden ser asignados a los distintos usuarios.

Para el registro de los usuarios se elaboró la tabla "users", la cual almacenará la información de los usuarios registrados juntamente a los datos de correos y contraseñas encriptadas, como se observa en la Figura 24.

FIGURA 23: TABLA DE USUARIOS

users

Columna	Tipo	Nulo	Predeterminado	Comentarios
id (<i>Primaria</i>)	bigint(20)	No		
name	varchar(255)	No		
email	varchar(255)	No		
email_verified_at	timestamp	Sí	<i>NULL</i>	
password	varchar(255)	No		
remember_token	varchar(100)	Sí	<i>NULL</i>	
state	varchar(255)	No	activo	
deleted_at	timestamp	Sí	<i>NULL</i>	
created_at	timestamp	Sí	<i>NULL</i>	
updated_at	timestamp	Sí	<i>NULL</i>	

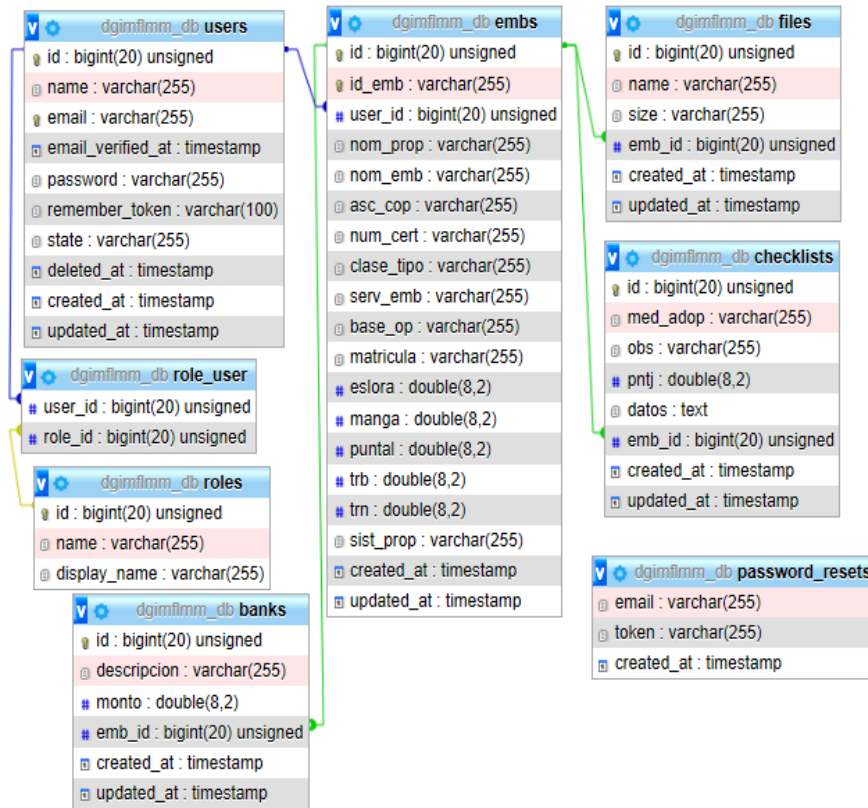
Fuente: Elaboración propia

Como se observa en la Figura 24, se tiene el registro de los usuarios que pueden ingresar al sistema.

El diseño lógico de la base datos, es la conversión del diseño conceptual (modelo entidad-relación), diseñado anteriormente.

Se realizó el modelo relacional, el cual es un modelo de datos funcional, se obtuvo a partir del gestor de base de datos PhpMyadmin, el cual se basa en relaciones y atributos, como se observa en la Figura 25.

FIGURA 24: MODELO RELACIONAL DE BASE DE DATOS



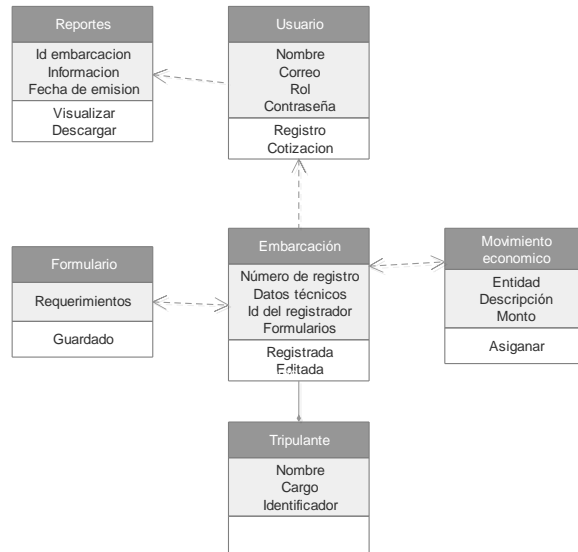
Fuente: Elaboración propia

Como se observa en la Figura 25 se ven las tablas existentes dentro la base de datos, los atributos y las relaciones que estas tienen entre sí, de modo que la misma cuente con información consistente.

3.3.1.2 Arquitectura del sistema

A modo de visualizar las relaciones entre las distintas clases que involucran el sistema planteado se elaboró el diagrama de clases de la base de datos, como se observa en la Figura 26.

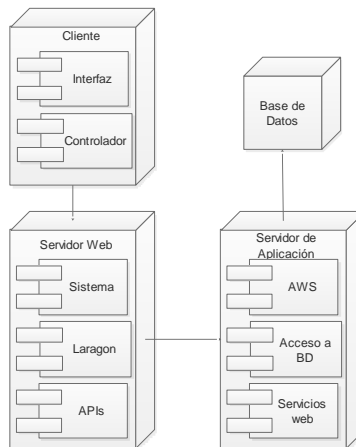
FIGURA 25: DIAGRAMA DE CLASES



Fuente: Elaboración propia

A continuación se muestra la representación de la arquitectura 3 capas que se aplicara al presente Trabajo de Grado, como se observa en la Figura 26.

FIGURA 26: DIAGRAMA DE DESPLIEGUE



Fuente: Elaboración propia

En la Figura 27 se puede observar los nodos y componentes por los cuales está compuesto el sistema, y cómo se realizará el intercambio de información.

3.3.2 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.

3.3.2.1 Lista de Requerimientos

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: REQUERIMIENTOS (GESTIÓN DE USUARIOS)

Número	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

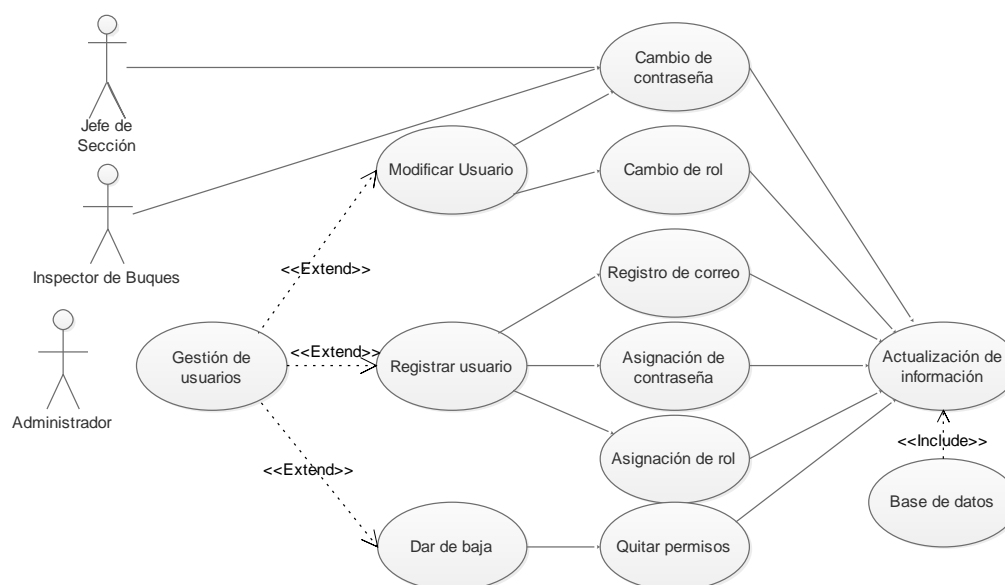
Fuente: Elaboración propia

En 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.

3.3.2.2 Especificación del Proceso

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 28.

FIGURA 27: DIAGRAMA DE CASO DE USO (GESTIÓN DE USUARIOS)



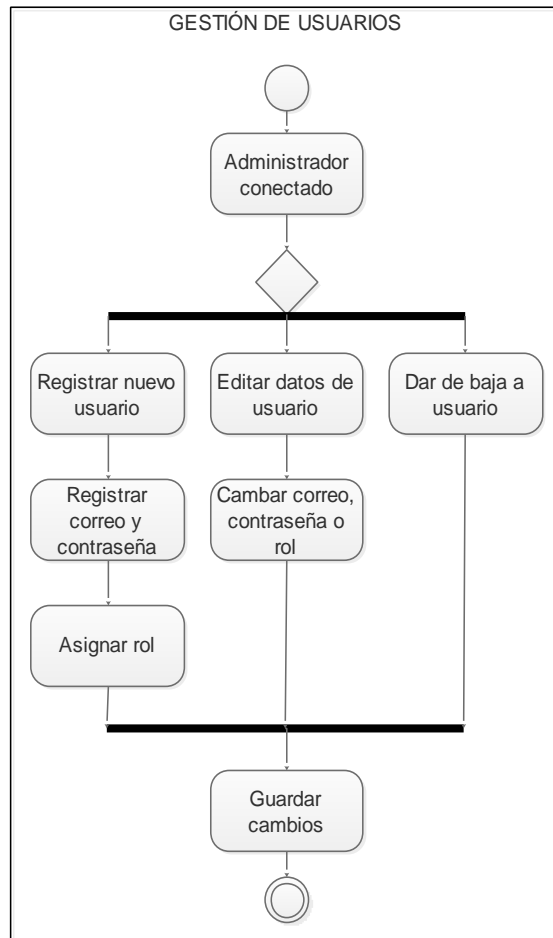
Fuente: Elaboración propia

Como se observa en la Figura 28, se ve cómo el usuario con el rol administrador realiza los distintos procesos para gestionar usuarios, para posterior guardarlos en la base de datos.

3.3.2.3 Diseño de Procesos

El proceso antes descrito se encuentra explicado de manera simplificada, en un diagrama de actividades, como se observa en la Figura 29.

FIGURA 28: DIAGRAMA DE ACTIVIDADES (GESTIÓN DE USUARIOS)



Fuente: Elaboración propia

Como se observa en la Figura 29, se elaboró el diagrama de actividades del módulo “Gestión de Usuarios”.

3.3.2.4 Diseño de Interfaces

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 30.

FIGURA 29: BOCETO DE INICIO DE SESIÓN



The wireframe shows a login interface with a title 'MARINA MERCANTE' at the top. Below the title are two rectangular input fields, one for the username and one for the password. At the bottom right of the form is a blue button labeled 'Ingresar'.

Fuente: Elaboración propia

Como se observa en la Figura 30, 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 31.

FIGURA 30: BOCETO DE REGISTRO DE USUARIO



The wireframe displays a registration form titled 'REGISTRO DE USUARIO'. It contains several input fields: 'NOMBRE', 'CORREO', 'ESTADO' (which has a dropdown arrow), 'CONTRASEÑA', and 'CONFIRMAR'. Below these is a 'ROL' section with four checkboxes. A blue button is positioned at the bottom right of the form.

Fuente: Elaboración propia

En la figura 31, 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 32.

FIGURA 31: BOCETO DE MODIFICACIÓN DE USUARIO



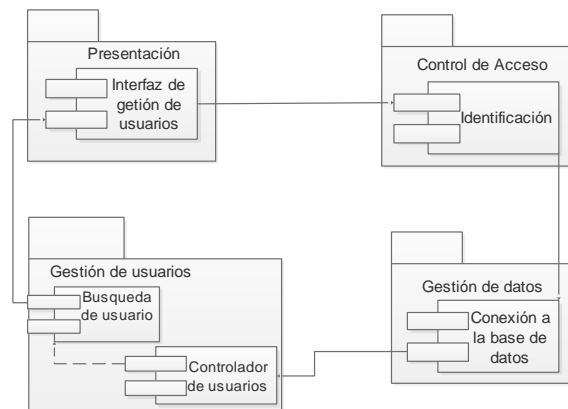
Fuente: Elaboración propia

En la figura 32, se muestra el boceto de la pantalla, la cual se mostrará al administrador cuando realice la modificación a los datos de un usuario.

3.3.2.5 Diseño Navegacional

El módulo de “Gestión de Usuarios” estará compuesto por cuatro componentes, como se observa en la Figura 33.

FIGURA 32: DIAGRAMA DE COMPONENTES (GESTIÓN DE USUARIOS)



Fuente: Elaboración propia

En la Figura 33, se muestra la organización de los componentes de software de este.

3.3.2.6 Construcción de Interfaces

Una vez realizado el diseño de las interfaces, se codificaron las mismas en el framework Laravel. La primera pantalla que se codifico fue la de “Inicio de Sesión”, como se observa en la Figura 34.

FIGURA 33: PANTALLA INICIO DE SESIÓN

The image shows a login interface for 'MarinaMercante'. At the top, the title 'MarinaMercante' is displayed. Below it, a box contains the instruction 'Ingrese sus credenciales'. There are two input fields: 'Correo Electrónico' with an envelope icon and 'Contraseña' with a lock icon. Below the password field is a checkbox labeled 'Recuerdame' and a blue button labeled 'Iniciar'. A link 'Olvide mi contraseña' is located below the 'Recuerdame' checkbox.

Fuente: Elaboración propia

En la Figura 34 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 codifico la pantalla de registro, como se observa en Figura 35.

FIGURA 34: PANTALLA DE REGISTRO DE USUARIO

The image shows a user registration form titled 'Registrar Usuario'. It features a 'Foto de Perfil' section with a circular placeholder and a button 'Examinar...' with a note 'No se ha seleccionado ningún archivo.'. Below this are input fields for 'Nombre:', 'Apellido Paterno:', and 'Apellido Materno:'. To the right, there are dropdown menus for 'Estado:' (set to 'activo') and 'Rango:' (set to 'Alférez'. Below these are a text field for 'Correo Electrónico:' containing 'luiscardinvasgiveness@gmail.com' and a 'Roles' section with checkboxes for 'Administrador' and 'Inspector de Buzones'. There are also fields for 'Contraseña:' (masked with asterisks) and 'Confirmar Contraseña:'. A blue 'Guardar' button is at the bottom.

Fuente: Elaboración propia

Como se observa en la Figura 35, se codificó e implemento 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 36.

FIGURA 35: PANTALLA DE EDICIÓN DE USUARIOS

Fuente: Elaboración propia

Como se observa en la Figura 36, se codificó implemento la pantalla la cual permite registrar nuevos usuarios y asignar roles dentro del sistema.

3.3.2.7 Código

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 37.

FIGURA 36: 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 37, se codificaron los distintos métodos para poder realizar la gestión de usuarios de acuerdo con los requisitos previamente mencionados en la Tabla 10 del presente documento.

3.3.2.8 Prueba Unitaria

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 38.

FIGURA 37: PRUEBA UNITARIA MOCK (GESTIÓN DE USUARIOS)

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

Tests: 6 passed
Time: 0.06s
```

Fuente: Elaboración propia

Como se observe en la Figura 38, se realizaron y pasaron satisfactoriamente las pruebas unitarias, las cuales evaluaron los distintos métodos usados al codificar el módulo “Gestión de Usuarios”.

3.3.3 Sprint 2 Módulo de Inspecciones

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

3.3.3.1 Lista de Requerimientos

Para el desarrollo de presente módulo, se realizó una lista de 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 11.

TABLA 11: 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

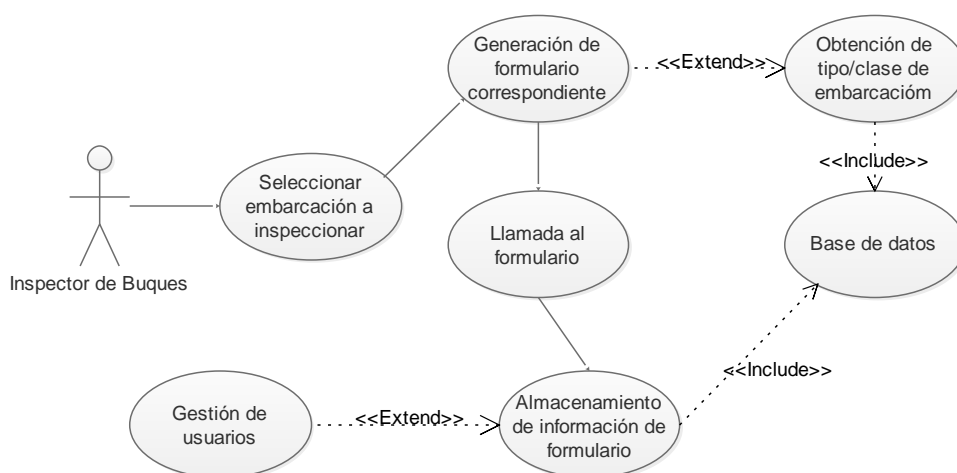
Fuente: Elaboración propia

En la Tabla 11 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.

3.3.3.2 Especificación del Proceso

En el módulo de inspecciones se tendrá un “Inspector de Buques” definido por el caso de estudio, el mismo estará a cargo de realiza las inspecciones correspondientes, y dependiendo el resultado emitir el certificado correspondiente. cómo se observa en la Figura 39.

FIGURA 38: DIAGRAMA DE CASO DE USO (INSPECCIÓN DE EMBARCACIÓN)



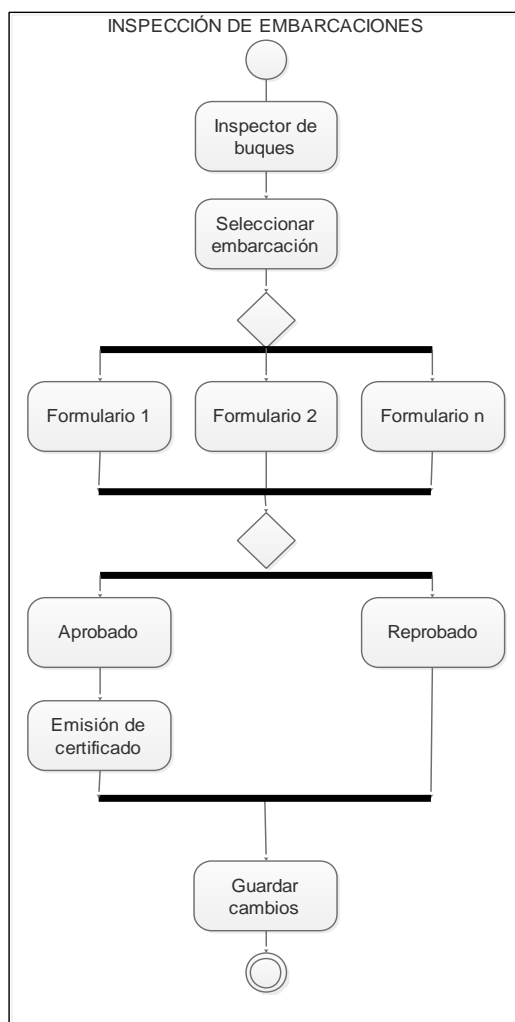
Fuente: Elaboración propia

Como se observa en la Figura 39, 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.

3.3.3.3 Diseño de Procesos

El proceso por el cual se realiza la inspección a una determinada embarcación se encuentro descrita de una manera más simplificada y concisa, realizada en un diagrama de actividades, como se observa en Figura 40.

FIGURA 39: DIAGRAMA DE ACTIVIDADES (INSPECCIÓN DE EMBARCACIÓN)



Fuente: Elaboración propia

Como se observa en la figura 40, se muestra el proceso que se realiza al momento de inspeccionar una embarcación.

3.3.3.4 Diseño de Interfaces

Una vez identificadas las acciones que se realizarán, se procedió al diseño de pantallas para el correspondiente módulo como se observa en la Figura 41.

FIGURA 40: BOCETO DE REALIZAR INSPECCIÓN

The mockup shows a sidebar on the left and a main content area. The main content area has a header 'Embarcaciones' and a table below it. The table has four columns: 'Id', 'Nombre', 'Clase/Tipo', and 'Acción'. There are three rows of data, each with a '#' in the 'Id' column, 'nombre' in the 'Nombre' column, 'clase/tipo' in the 'Clase/Tipo' column, and 'inspección certificado' in the 'Acción' column.

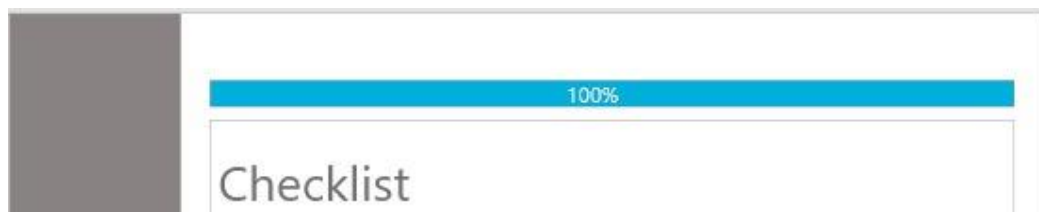
Id	Nombre	Clase/Tipo	Acción
#	nombre	clase/tipo	inspección certificado
#	nombre	clase/tipo	inspección certificado
#	nombre	clase/tipo	inspección certificado

Fuente: Elaboración propia

Como se observa en la Figura 41, 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 42.

FIGURA 41: BOCETO DE BARRA DE PROGRESO



Fuente: Elaboración propia

Como se observa en la Figura 42, el formulario ira 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 43.

FIGURA 42: BOCETO DE FORMULARIO DE INSPECCIÓN

The sketch shows a form titled "Checklist" with the following structure:

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"/>

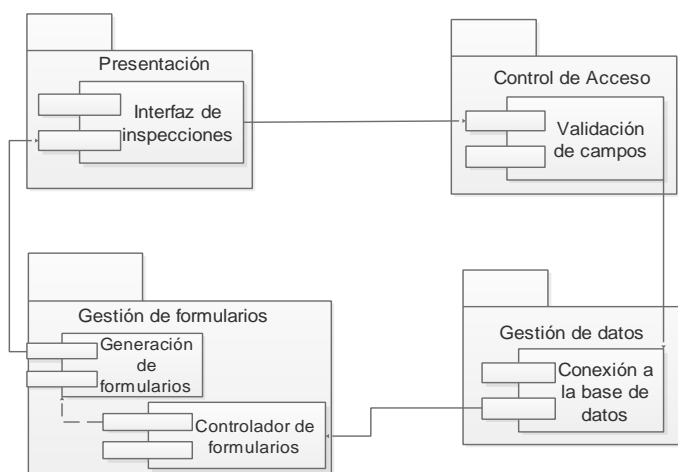
Fuente: Elaboración propia

Como se observa en la Figura 43, el formulario ira mostrando el porcentaje de su avance a medida que se vaya completando cada aspecto a ser considerado.

3.3.3.5 Diseño Navegacional

El módulo de “Inspecciones” estará compuesto por cuatro componentes, como se observa en Figura 44.

FIGURA 43: DIAGRAMA DE COMPONENTES (INSPECCIONES)



Fuente: Elaboración propia

En la Figura 44, se muestra la organización de los componentes de software del módulo "Inspecciones".

3.3.3.6 Construcción de Interfaces

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 icono, como se observa en la Figura 45.

FIGURA 44: PANTALLA PARA ACCEDER A INSPECCIÓN



Número de registro	Nombre de embarcación	Clase/Tipo	Acción
1919	Rivas	DRAGA	Inspección
A-20072	Jose	DRAGA	Inspección

Fuente: Elaboración propia

Como se observa en la Figura 45, se codificó e implementa la pantalla por la cual se accederá a los distintos formularios.

Una vez ingresado al icono, el mismo generará el formulario correspondiente al tipo de embarcación, como se observa en la Figura 46.

FIGURA 45: PANTALLA DE FORMULARIO DE INSPECCIÓN



Descripción	Medida Adoptada	Sí	No	Descripción
Requerimiento 1	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Requerimiento 2	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>

[Siguiente](#)

Fuente: Elaboración propia

Como se observa en la Figura 46, se muestra el progreso del formulario, además de tener los parámetros al momento de realizar la inspección.

3.3.3.7 Código

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 47.

FIGURA 46: 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');
    }
}
```

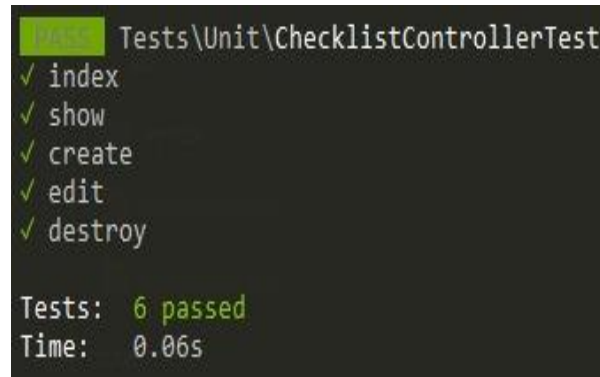
Fuente: Elaboración propia

Como se observa en la Figura 47, se codificaron los distintos métodos para poder realizar el control de inspecciones de acuerdo con los requisitos previamente mencionados en la Tabla 11 del presente documento.

3.3.3.8 Prueba Unitaria

Una vez concluida la codificación se procedió a realizar las pruebas "Mock", para el controlador de formularios, como se observa en la Figura 48.

FIGURA 47: 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 47, todas las pruebas del módulo de "Inspecciones" se efectuaron de manera exitosa.

3.3.4 Sprint 3 Módulo de Registro de Embarcaciones

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

3.3.4.1 Lista de Requerimientos

Para el desarrollo del presente módulo 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 12.

TABLA 12: 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

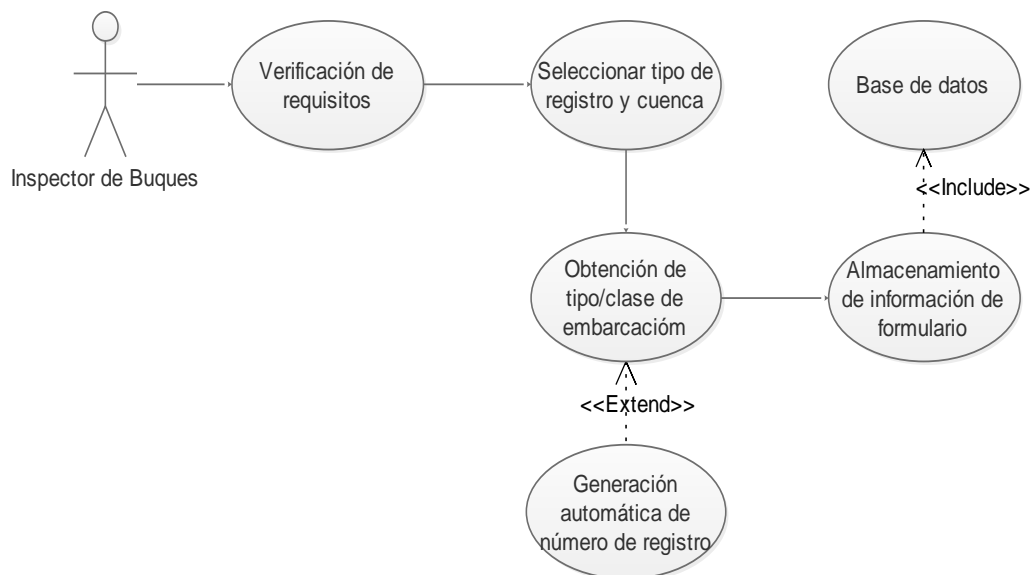
Fuente: Elaboración propia

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

3.3.4.2 Especificación del Proceso

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 49.

FIGURA 48: DIAGRAMA DE CASO DE USO (REGISTRO DE EMBARCACIÓN)



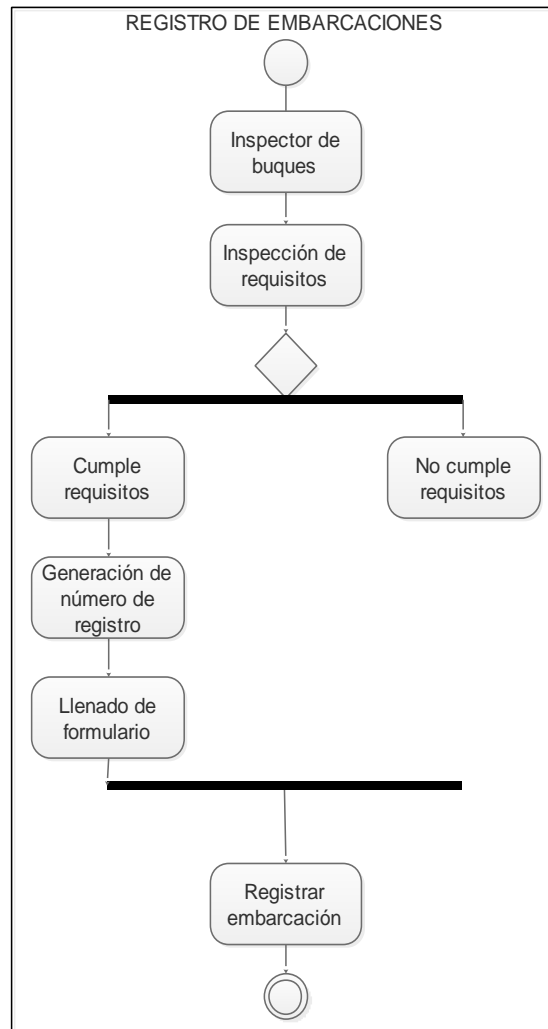
Fuente: Elaboración propia

Como se observa en la Figura 48, 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

3.3.4.3 Diseño de Procesos

El proceso antes descrito se encuentra explicado de manera simplificada, como se observa en la Figura 49.

FIGURA 49: DIAGRAMA DE ACTIVIDADES (REGISTRO DE EMBARCACIÓN)



Fuente: Elaboración propia

Como se observa en la Figura 49, se muestra el proceso que se realiza al momento de registrar una embarcación.

3.3.4.4 Diseño de Interfaces

Una vez identificadas las acciones que se realizarán, se procedió al diseño de pantallas para el correspondiente módulo, como se observa en la Figura 50.

FIGURA 50: BOCETO DE REQUISITOS

Marina Mercante

Requerimiento Cumple No cumple

requerimiento	<input type="radio"/>	<input type="radio"/>
requerimiento	<input type="radio"/>	<input type="radio"/>
requerimiento	<input type="radio"/>	<input type="radio"/>

Fuente: Elaboración propia

Como se observa en la Figura 50, 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 51.

FIGURA 51: BOCETO DE REGISTRO

Registro

N° DE REGISTRO

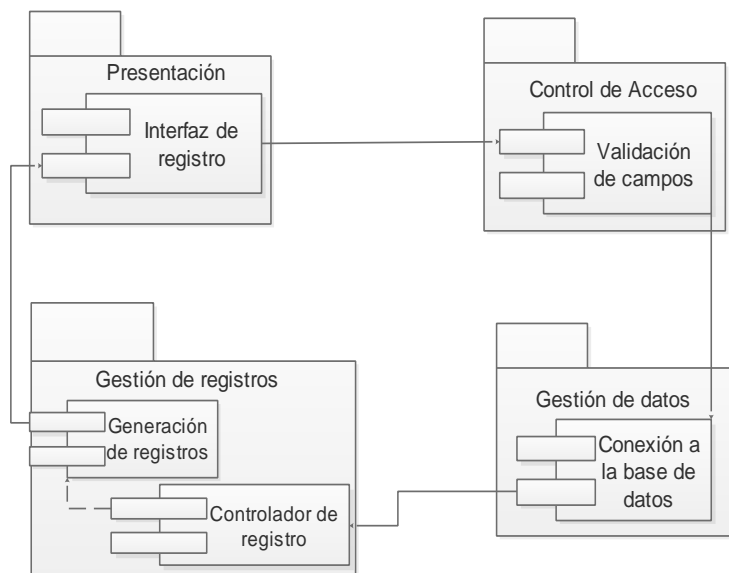
Fuente: Elaboración propia

Como se observa en la Figura 51, se planteó el diseño de formulario de registro de embarcación, con la asignación de número de registro automático.

3.3.4.5 Diseño Navegacional

El módulo de "Registro de Embarcaciones" estará compuesto por cuatro componentes, como se observa en Figura 52.

FIGURA 52: DIAGRAMA DE COMPONENTES (REGISTRO)



Fuente: Elaboración propia

En la Figura 52, se muestra la organización de los componentes de software del módulo " Registro de Embarcaciones "

3.3.4.6 Construcción de Interfaces

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 53.

FIGURA 53: PANTALLA DE REQUISITOS DE REGISTRO

Requisito	Sí	No
Solicitud de Certificación	<input checked="" type="radio"/>	<input type="radio"/>
Solicitud de Registro obligada a la Autoridad Marítima	<input checked="" type="radio"/>	<input type="radio"/>
Documentos Adjuntos Completos	<input checked="" type="radio"/>	<input type="radio"/>

Fuente: Elaboración propia

Como se observa en la Figura 53, 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 54.

FIGURA 54: PANTALLA DE REGISTRO DE EMBARCACIÓN

N° de Registro:		Nombre de Propietario:		Nombre de Embarcación:	
P-20083					
Asociación Cooperativa:		Número de Certificado:			
Clase/Tipo:		Servicio:		Base Operativa:	
BARCAZA CERRADA					
Matrícula:					
Eslora:	Manga:	Puntal:	TRB:	TRR:	Francobordo:
Sistema de Propulsión:	Mód. Pel.:	Max. Pax.:	Material:	Año Cons.:	
	SI		MADERA		

Fuente: Elaboración propia

Como se observa en la Figura 54 el formulario para registrar una embarcación, con el número de registro asignado.

3.3.4.7 Código

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 36.

FIGURA 55: 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 55, se codificaron los distintos métodos para poder realizar el registro de embarcaciones en base a los requisitos previamente mencionados en la Tabla 12 del presente documento.

3.3.4.8 Prueba Unitaria

Una vez concluida la codificación se procedió a realizar las pruebas "Mock", para el controlador de embarcaciones, como se observa en la Figura 56.

FIGURA 56: 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 56, todas las pruebas del módulo de "Registro de Embarcaciones" se efectuaron de manera exitosa.

3.3.5 Sprint 4 Módulo Verificación de Documentos

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

3.3.5.1 Lista de Requerimientos

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

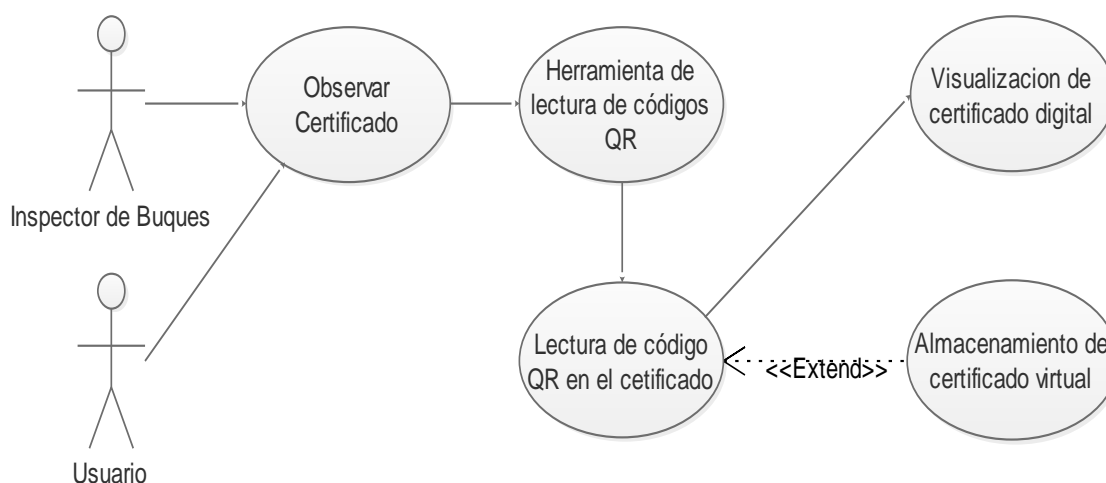
Número	Requerimiento	Descripción	Tipo	Prioridad
1	Generación de par de llaves	Capacidad del sistema de generar llave pública y llave privada	Funcional	Alta
2	Guardar el par de llaves	Guardar el par de llaves generado, y asociarlo a un documento.	Funcional	Alta
3	Código QR leíble	Capacidad de que el código 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

3.3.5.2 Especificación del Proceso

En el módulo de “Verificación de Documentos”, el Inspector de Vuques y un Usuario pueden obtener la información acerca de su certificado emitido por el caso de estudio, como se observa en la Figura 57.

FIGURA 57: DIAGRAMA DE CASO DE USO (VERIFICACIÓN DE DOCUMENTOS)



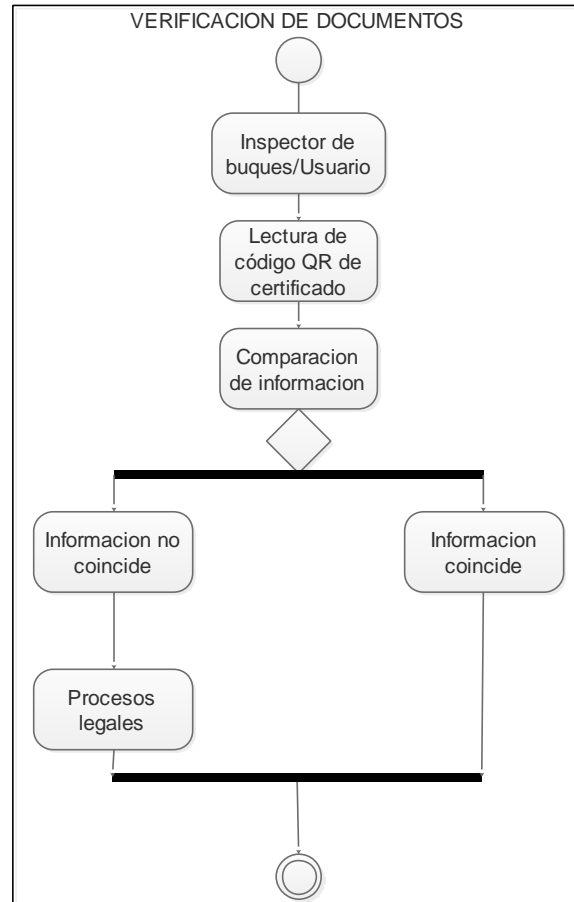
Fuente: Elaboración propia

Como se observa en la Figura 57, se ve cómo los actores “Usuario” e “Inspector de Buques” realiza la verificación de la información acerca de un certificado.

3.3.5.3 Diseño de Procesos

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 58.

FIGURA 58: DIAGRAMA DE ACTIVIDADES (VERIFICACIÓN DE DOCUMENTOS)



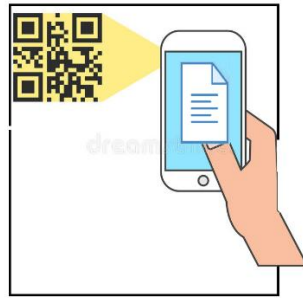
Fuente: Elaboración propia

Como se observa en la Figura 58, se muestra el proceso que se realiza al momento de revisión de documentos.

3.3.5.4 Diseño de Interfaces

Una vez identificadas las acciones que se realizaran, se procedió al diseño de pantallas para el correspondiente módulo, como se observa en la Figura 59.

FIGURA 59:BOCETO DE VERIFICACIÓN DE DOCUMENTO



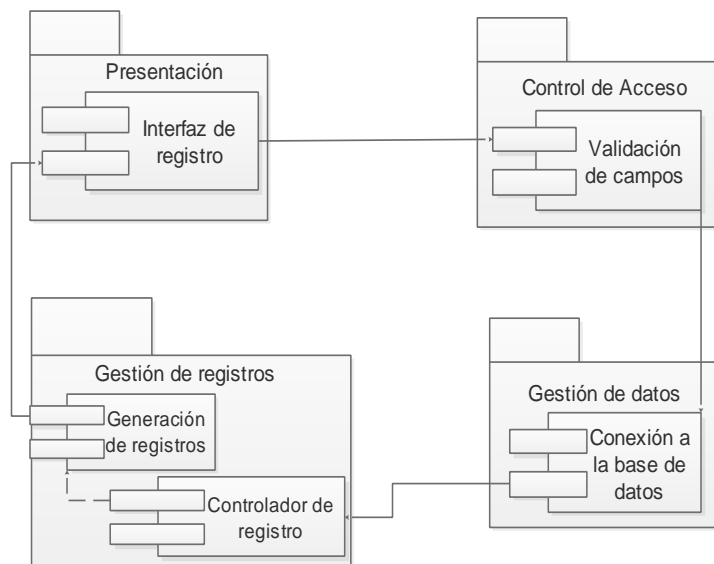
Fuente: Elaboración propia

Como se observa en la Figura 59, se planteó el funcionamiento de la verificación de documentos a partir de un código QR.

3.3.5.5 Diseño Navegacional

El módulo de "Verificación de Documentos." estará compuesto por cuatro componentes, como se observa en Figura 60.

FIGURA 60: DIAGRAMA DE COMPONENTES (VERIFICACIÓN DE DOCUMENTOS)



Fuente: Elaboración propia

En la Figura 60, se muestra la organización de los componentes de software del módulo “Verificación de Documentos.”

3.3.5.6 Construcción de Interfaces

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 61.

FIGURA 61: PANTALLA DE VERIFICACIÓN DE DOCUMENTO

The screenshot displays a web interface for document verification. On the left, a QR code is shown next to the text: "ESTADO PLURINACIONAL DE BOLIVIA, MINISTERIO DE DEFENSA, DIRECCIÓN GENERAL DE INTERESES MARÍTIMOS, FLUVIALES, LACUSTRE Y MARINA MERCANTE". Below this is a "CERTIFICADO DE SEGURIDAD DE LA NAVEGACIÓN" form. The form includes fields for "PROPIETARIO(S)", "ANTERIOR PROPIETARIO", "FECHA DE INSPECCIÓN", "LUGAR DE INSPECCIÓN", and "BASE DE OPERACIONES". It also features a table with columns for "NOMBRE DE LA EMBARCACIÓN", "MATRÍCULA", "INDICATIVO DE LLAMADA", "TIPO", and "AÑO DE CONSTRUCCIÓN". The table contains data for a vessel named "BARCAZA CERRADA" with a length of 123, a width of 0, and a gross weight of 0. The form is signed by "asd" and dated "P-2008624".

On the right, the same form is shown in a "VISTA DESDE LECTURA DE CÓDIGO QR" (QR code reading view). This view includes a "edit" button and a "VISTA DESDE LECTURA DE CÓDIGO QR" label. The form content is identical to the left view, but it includes a "VISTA DESDE LECTURA DE CÓDIGO QR" label and a "VISTA DESDE LECTURA DE CÓDIGO QR" button. The form is signed by "asd" and dated "P-2008624".

Fuente: Elaboración propia

Como se observa en la Figura 61, se tiene el formulario previo al registro al registro de una embarcación.

3.3.5.7 Código

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 62.

FIGURA 62: 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

3.3.5.8 Prueba Unitaria

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 63.

FIGURA 63: PRUEBA UNITARIA MOCK (VERIFICACIÓN DE DOCUMENTOS)

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

Tests: 6 passed
Time: 1.11s
```

Fuente: Elaboración propia

Como se observa en la Figura 63, todas las pruebas del módulo de "Verificación de Documentos" se efectuaron de manera exitosa.

3.3.6 Sprint 5 Módulo de Registro de Reportes

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

3.3.6.1 Lista de Requerimientos

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

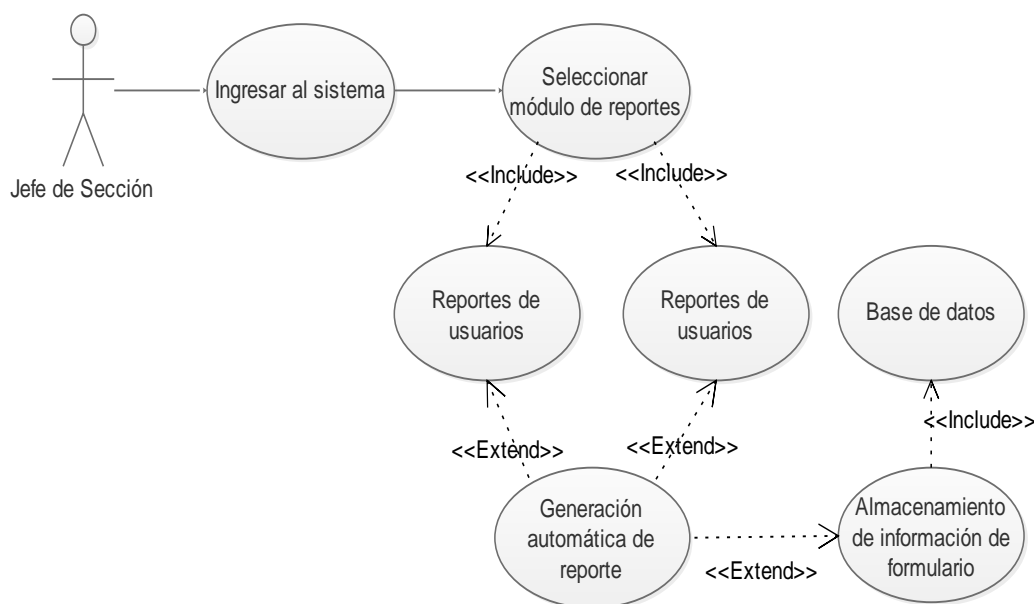
Fuente: Elaboración propia

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.

3.3.6.2 Especificación del Proceso

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 64.

FIGURA 64: DIAGRAMA DE CASO DE USO (REPORTES)



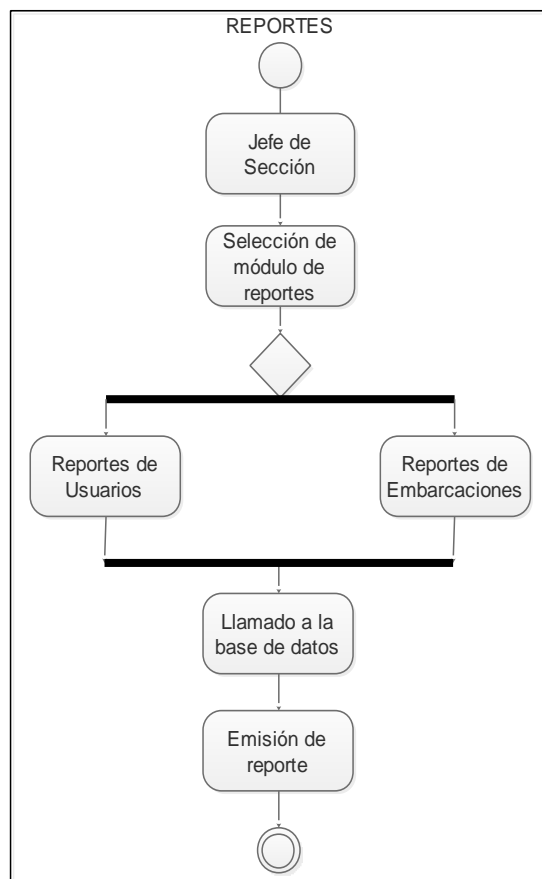
Fuente: Elaboración propia

Como se observa en la Figura 64, se ve cómo el usuario con el rol “Jefe de Sección” realiza los distintos procesos para emitir los reportes.

3.3.6.3 Diseño de Procesos

El proceso antes descrito se encuentra explicado de manera simplificada, como se observa en la Figura 65.

FIGURA 65: DIAGRAMA DE ACTIVIDADES (REPORTES)



Fuente: Elaboración propia

Como se observa en la Figura 65, se muestra el proceso que se realiza al momento de generar reportes.

3.3.6.4 Diseño de Interfaces

Una vez identificadas las acciones que se realizaran, se procedió al diseño de pantallas para el correspondiente módulo, como se observa en la Figura 66.

FIGURA 66: BOCETO DE REPORTE

Lista de Embarcaciones			
Nombre:Luis			
Usuarios Activos			
Número de Registro	Nombre de Embarcación	Encargado del Registro	Fecha de Registro
A195	RIVAS	Luis	
A-20082	R	Luis	2020-08-03 02:43:46

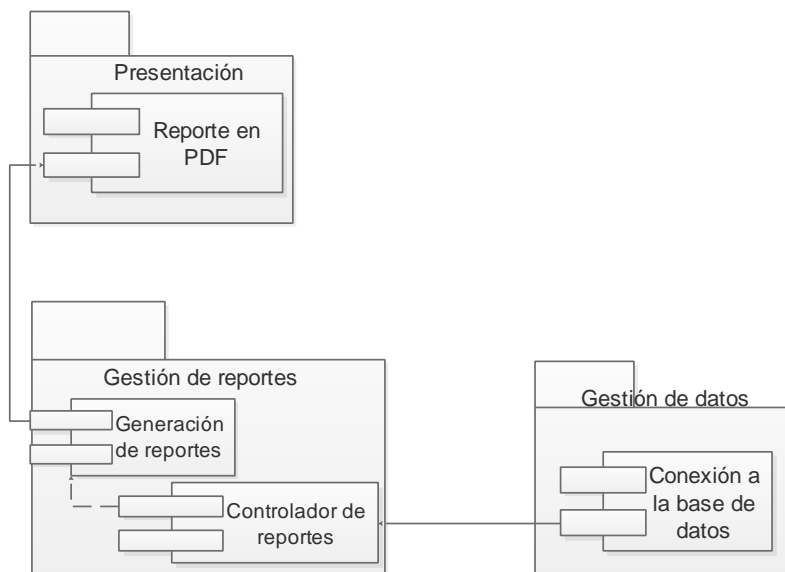
Fuente: Elaboración propia

Como se observa en la Figura 66, se plantea el diseño de reporte.

3.3.6.5 Diseño Navegacional

El módulo de "Reportes" estará compuesto por cuatro componentes, como se observa en Figura 67.

FIGURA 67: DIAGRAMA DE COMPONENTES (REPORTES)



Fuente: Elaboración propia

En la Figura 67, se muestra la organización de los componentes de software del módulo " Reportes "

3.3.6.6 Construcción de Interfaces

Una vez realizado el diseño del reporte, se codificaron los mismos en el framework Laravel para emitir reportes, como se observa en la Figura 68.

FIGURA 68: 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	luisricardorivasgiwencer@gmail.com	Administrador
2	1	q@d.com	Inspector de Buques
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 68 el formulario para registrar una embarcación, con el número de registro asignado.

3.3.6.7 Código

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 69.

FIGURA 69: 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 69, 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.

3.3.6.8 Prueba Unitaria

Una vez concluida la codificación se procedió a realizar las pruebas "Mock", para el controlador de embarcaciones, como se observa en la Figura 70.

FIGURA 70: 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 70, 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 71.

FIGURA 71: EXÁMEN 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 ✓✓
==> ...epositories\Elasticsearch\FindByFieldTest ●
==> Tests\Integration\ServiceProviderTest ✓✓✓✓✓✓✓✓

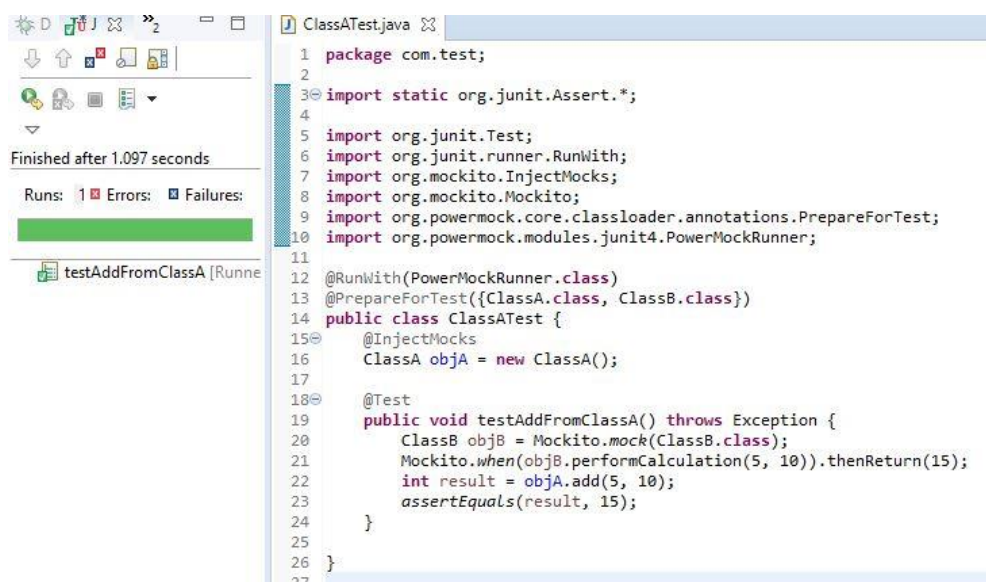
Time: 7.73 seconds, Memory: 28.00MB
```

Fuente: Elaboración propia

Como se observa en la Figura 71, 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 72.

FIGURA 72: 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
```

Finished after 1.097 seconds

Runs: 1 Errors: 0 Failures: 0

testAddFromClassA [Runne

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

3.5.1 Instalación del sistema

Para la instalación del sistema se usará los servicios de “Amazon Web Service”, el cual es un proveedor de servidores virtuales privados. Se contratarán dos máquinas

virtuales, una dedicada para la parte que almacene el sistema y otra para que se pueda almacenar la base de datos.

En la primera máquina virtual se instalará la parte funcional del sistema el cual tenga las diferentes interfases y archivos de modo que pueda funcionar de manera correcta. En la segunda máquina virtual se realizará la instalación de la base de datos, donde se almacenará la información de todos los registros correspondientes.

Una vez subido el sistema se realizará la configuración y enlace de la base de datos, de modo que exista una comunicación adecuada.

3.5.2 Revisión de funcionamiento

Una vez implementado el sistema se revisará el funcionamiento de este, si todos los módulos funcionan de la manera que se espera. Por lo siguiente se realizaron los reportes de conformidad, los cuales demuestran que el caso de estudio se encuentra conforme.

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
- [Larousse, 2009] DICCIONARIO LAROUSSE, edición 2009
- [Leon, 2005] "ENCRIPCIÓN 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 DÉBITO MEDIANTE MÉTODOS DE ENCRIPCIÓN HÍBRIDA", 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

[Sobrevila, 2008]

“INGENIERÍA GENERAL”, Marcelo Antonio Sobrevilla, Buenos Aires – Argentina, 2008

GLOSARIO

Autentico:	Que está autorizado o legalizado y tiene valor oficial
Calado	Profundidad que alcanza en el agua la parte sumergida de una embarcación.
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.
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.
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.
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.

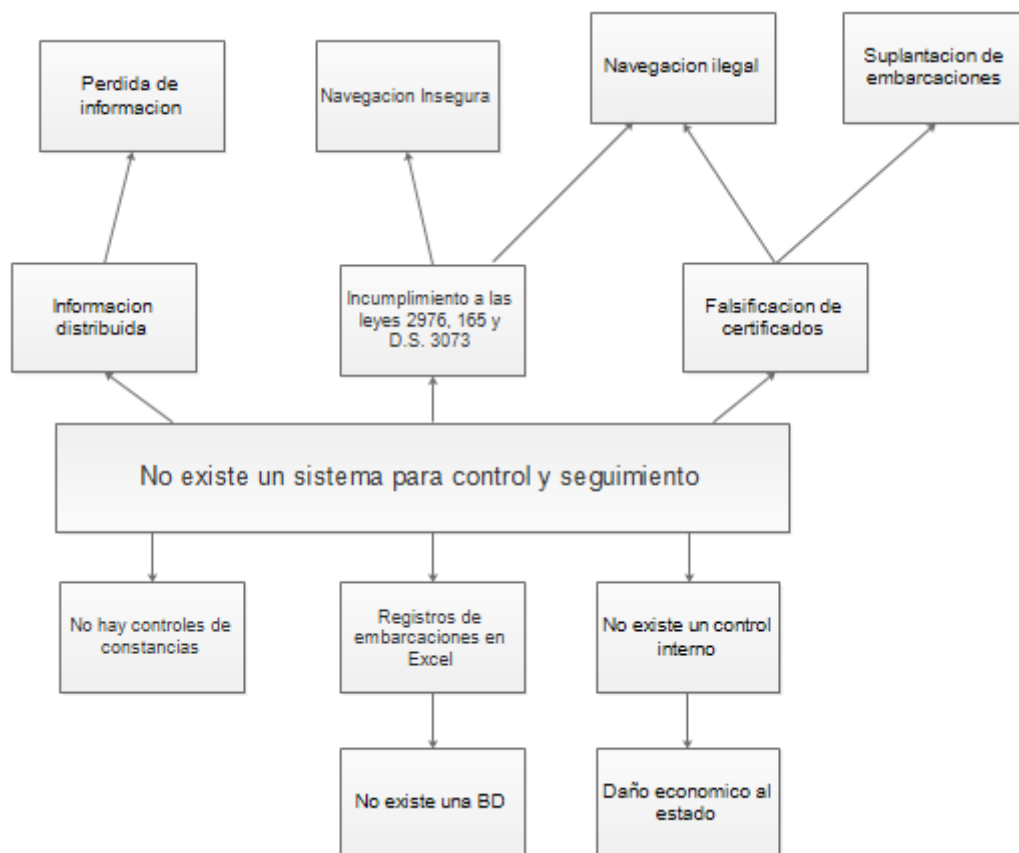
Puntal:	Madero o barra de material fuerte y resistente que se fija en posición inclinada en algún lugar para sujetar una pared, una estructura o un edificio que puede caerse.
Relieve:	Configuración de una superficie con distintos niveles o partes que sobresalen más o menos. Parte que sobresale en una superficie plana.
Unidireccional:	Que tiene una sola dirección. Que va en una sola dirección.
Virtual:	Que tiene existencia aparente y no real

ANEXOS



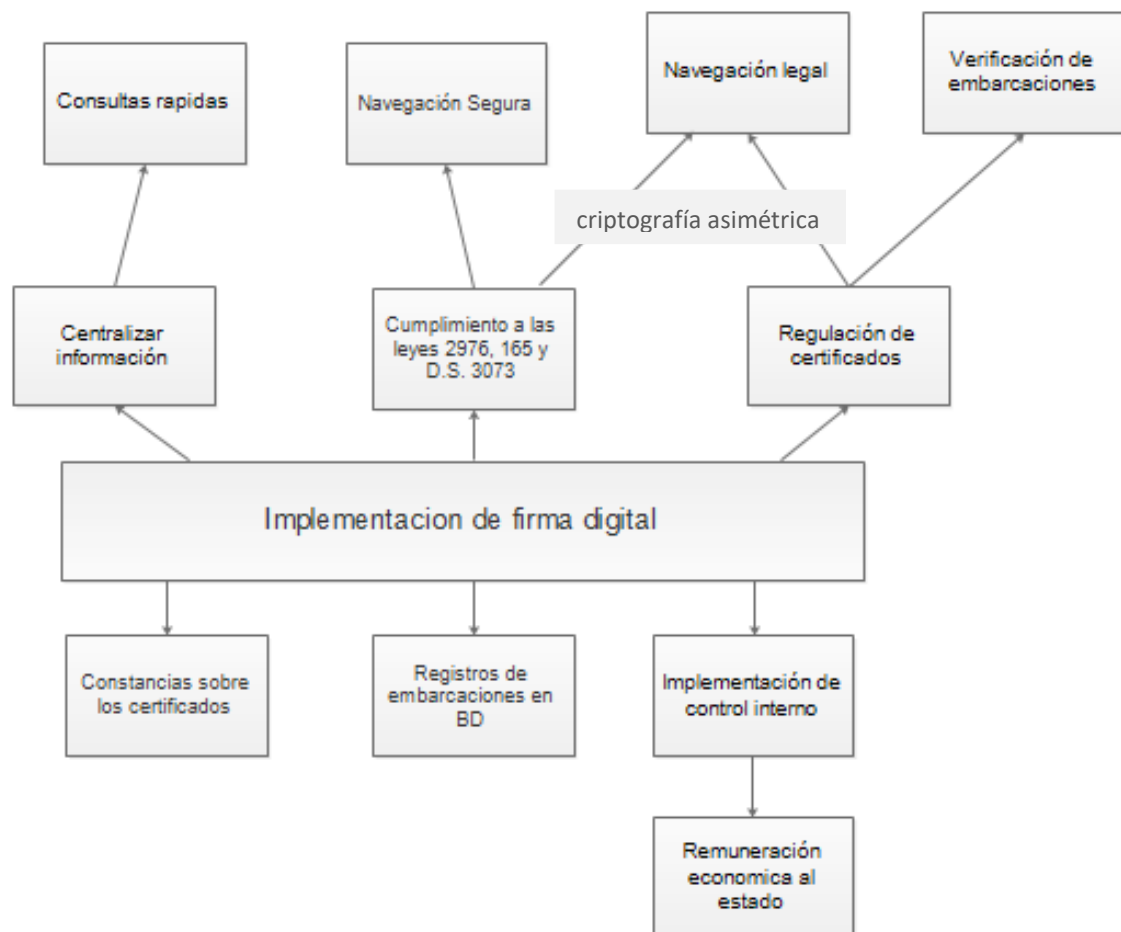
ANEXO A:

ÁRBOL DE PROBLEMAS



ANEXO B:

ÁRBOL DE OBJETIVOS



ANEXO C: FORMULARIO DE INSPECCIÓN

✓

Registro Nuevo

Ministerio de Defensa Nacional - DGIMFLMM.
Marina Mercante Nacional

FORM - SF - 002

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

1. PROPIETARIO/ARMADOR: Jose Luis Arana Chacque

2. CAPITAN/PATRÓN: Carlos B.

3. NOMBRE EMBARCACIÓN: Patron

4. TIPO DE EMBARCACIÓN: Patron

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

6. MATERIAL DE CONSTR: Aluminio

7. SERVICIO DE LA EMBARCACION: Patrullero

8. DOMICILIO DEL PROPIETARIO: Alfaro, Chaco

9. ESLORA: 6,25

10. MANGA: 1,50

11. PUNTAL: 0,50

12. CALADO: 0,50

13. N° DE CUBIERTAS: 1

14. N° REGISTRO: 1

15. N° MATRÍCULA: 1

16. T.R.B.: 1

17. T.R.N.: 1

18. CASCO

QUILLA	R/E
CUADERNAS	R/E
OBRA VIVA	R/E
OBRA MUERTA	R/E
PINTURA	R/E
CUBIERTA PRINCIPAL	NT
CALAFATEADO	NT
BANCADAS	NT
ENJARETADO	R/E
UNION D/CHAPAS	NT
ESPOSOR DE CHAPAS	NT

19. SISTEMA DE PROPULSIÓN

FUERA DE BORDA	✓
TANQUE COMBUSTIBLE	✓
MOTOR DE CENTRO	✓
MOTOR DE COLA	✓
BATERIA	✓
CABLEADO ELECTRICO	✓
MARCA	<u>PARSON</u>
POTENCIA	<u>15 HP</u>
NUMERO	<u>5-11010583</u>

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	NT
GUINDOLAS	NT
ESTINGUIDORES	NT
CAJA DE HERRAMIENTAS	NT
REMOS	✓
CINGA	✓
DEFENSAS	✓
BITAS/CORNAMUSAS	NT
CABLES/CABOS	✓

23. LUCES DE NAVEGACION

LUZ DE TOPE	✓
LUCES DE COSTADO	✓

24. COMPARTIMIENTOS

SALA DE PASAJEROS	NT
BASUREROS	NT

25. PRIMEROS AUXILIOS

BOTIQUIN	NT
LINTERNA	NT

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	Repe completo tanque combustible	
22	Repe completo chaleco salvavidas	
	Extintores	
25	Repe completo botiquin	

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

Lugar y fecha: Carabobo 07/10/19

[Firma]
CAPITAN O PROPIETARIO

[Firma]
INSPECTOR TÉCNICO

[Firma]
JEFE DE COMISION

ANEXO D:
FOTO DE EMBARCACIÓN



ANEXO E:

CERTIFICADO DE SEGURIDAD

N° 012199

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

N° REGISTRO
L - 10195487

CERTIFICADO DE SEGURIDAD DE LA NAVEGACIÓN

EXPEDIDO EN CUMPLIMIENTO AL D.S. N° 3073
REGLAMENTO TECNICO A LA LEY N° 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	1,55	0,50	1,08	1,00	---	
MTS.	MTS.	MTS.	UNIDAD DE REGISTRO	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.		
PARSUN		L-511010583	HP	ALTERNA: ---		
MATERIAL DEL CASCO		PESO Y ALTURA DE CUBERTADA	MERCANCIAS 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.

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



COACOLLO, 07 DE OCTUBRE DE 2019

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

ANEXO F:

REGISTRO DE EMBARCACIONES

N° 012198


 ESTADO PLURINACIONAL DE BOLIVIA
 MINISTERIO DE DEFENSA
 DIRECCION GENERAL DE INTERESES MARITIMOS
 FLUVIALES, LACUSTRES Y DE MARINA MERCANTE

	N° REGISTRO L - 10195487
--	------------------------------------

CERTIFICADO DE REGISTRO

EXPEDIDO DE CONFORMIDAD AL RECONOCIMIENTO
EFECTUADA POR LA DIRECCIÓN DE MARINA MERCANTE NACIONAL

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
BUPALO			EN TRAMITE		- - -
SERVICIOS DE LA EMBARCACIÓN			TIPO		AÑO DE CONSTRUCCIÓN
PESCA			BOTE AMOTOR		2016
ESLORA	MANGA	PUNTAL	ARQUEO BRUTO	ARQUEO NETO	FRANCOBORDO
6,05	1,55	0,50	1,08	1,00	- - -
MTS.	MTS.	MTS.	UNIDAD DE REGISTRO	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.
PARSUN		L-511010583	HP		ALTERNA: - - -
MATERIAL DEL CASCO		PESO Y ALTURA DE CUBERTADA	MERCANCIAS PELIGROSAS		NÚMERO MÁXIMO DE PASAJEROS
MADERA		- - -	NO		4

SE CERTIFICA:
 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.

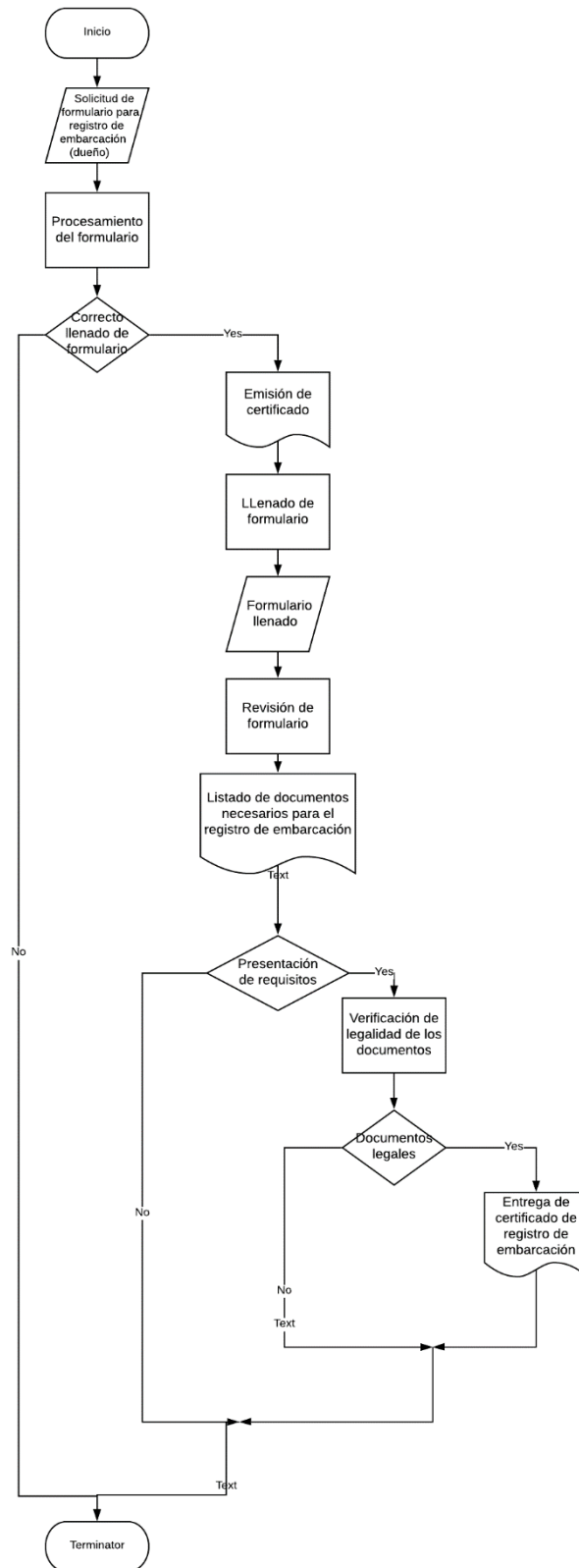
COACOLLO, 07 DE OCTUBRE DE 2019


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


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

ANEXO G:

PROCESO DE EMISIÓN DE CERTIFICADO DE REGISTRO



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

CAPÍTULO III

NORMAS PARA LA CONSTRUCCIÓN DE BARCAZAS TANQUE

Artículo 14º (Construcción de barcaza tanque). Para la construcción de barcasas tanque se sujetarán al cumplimiento del diseño, construcción y equipamiento de conformidad a las estipulaciones siguientes:

a) Características:

- La eslora mayor a 24 metros.
- Posee tanques de flotación de acuerdo a su estructura.
- El casco estará construido de chapas de acero resistentes, unidos por soldadura y remaches.
- La cubierta superior tiene que estar dotada de medios permanentes de cierre estanco de todas las aberturas.

b) Disposiciones de la estructura de tanques.

La estructura puede disponerse en forma longitudinal, transversal o adoptar una combinación de ambas distribuciones. La estructura longitudinal será soportada por cuadernas separadas regularmente, constituidos por fierros en forma de "U" que se extienden a través de las anteriores de los longitudinales o chapas pestañadas, con escotes para el pasaje de los longitudinales, unidos al enchapado del casco o de la cubierta.

c) Enchapado del costado y el casco.

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:

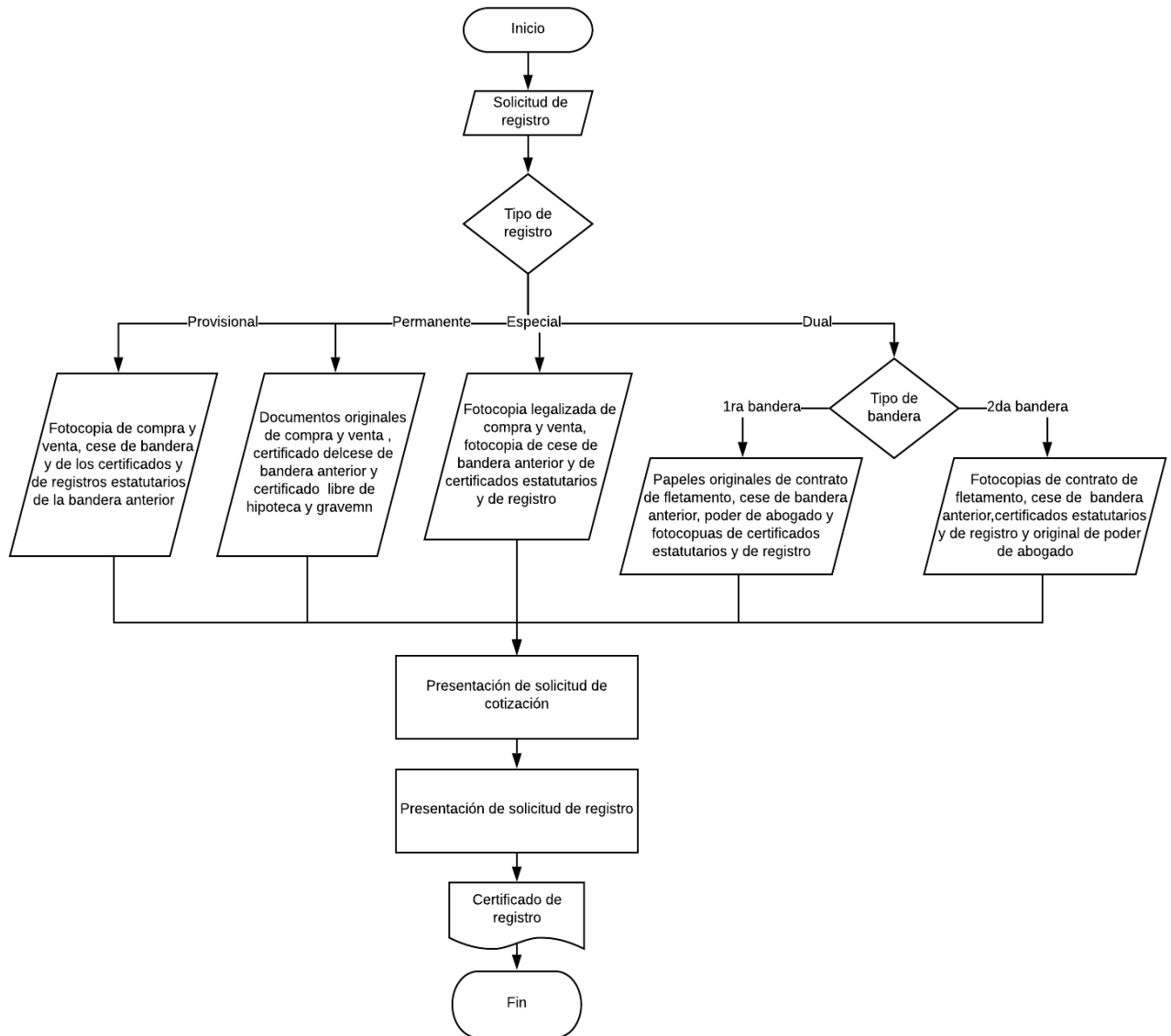
TAREAS DEL PERSONAL DE UNIDAD DE MARINA MERCANTE

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 de 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.

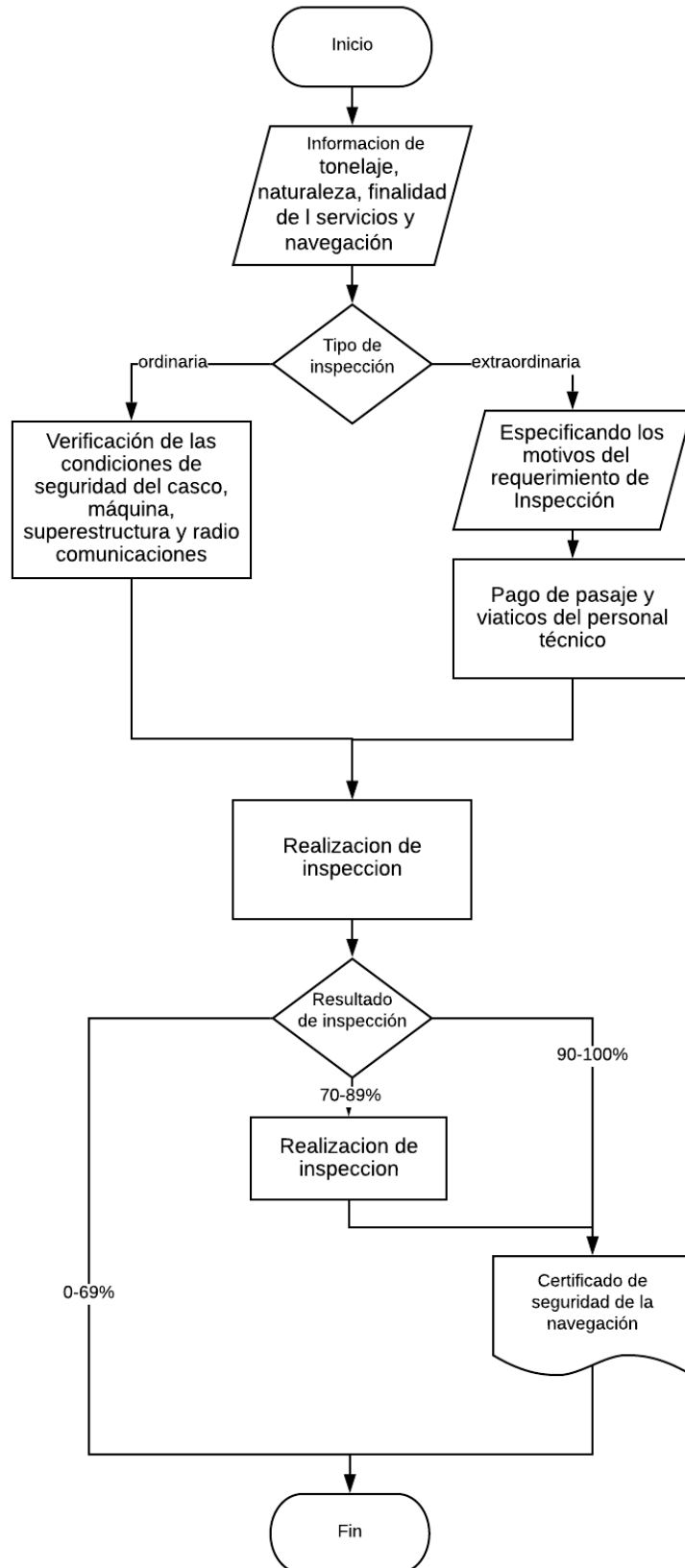
ANEXO J:

PROCESO DE REGISTRO DE EMBARCACIÓN



ANEXO K:

PROCESO DE INSPECCIÓN DE EMBARCACIÓN



ANEXO L:
REGLAMENTO NACIONAL PARA LA CONSTRUCCIÓN DE
EMBARCACIONES Y ARTEFACTOS NAVALES

CAPÍTULO I

OBJETO, AMBITO DE APLICACIÓN Y DEFINICIONES

Artículo 1° (Objeto). El presente Reglamento tiene por objeto regular las actividades de construcción de embarcaciones y artefactos navales para la navegación en los ámbitos fluvial y lacustre.

En la Hidrovía Paraguay – Paraná, se aplicará la Reglamentación del Acuerdo de Transporte Fluvial por la Hidrovía Paraguay – Paraná.

Artículo 2° (Ámbito de aplicación). El presente reglamento será aplicable para la construcción de embarcaciones mercantes conforme a la siguiente clasificación:

- Combustible líquido
- Carga general
- Transporte de pasajeros
- Transbordo de vehículos
- Turismo
- Otros

Artículo 3° (Definiciones) Para efectos del presente reglamento se aplicarán las siguientes definiciones:

- **BARCAZA TANQUE.** Embarcación con cubierta con cierres permanentes estancos, para el transporte de carga líquida.
- **BARCAZA ABIERTA.** Embarcación sin cubierta ni propulsión propia empleada para el transporte de carga general y transbordo de vehículos.
- **LANCHA MOTONAVE.** Embarcaciones de madera, con motor de centro equipadas para el transporte turístico.
- **LANCHA CHALANA.** Embarcación de aluminio, con motor fuera de borda equipadas para el transporte de pasajeros.
- **LANCHA CATRAYA.** Embarcación de madera, con motor fuera de borda equipadas para el transporte de pasajeros y carga.
- **CATAMARÁN.** Embarcación con el casco de acero, con sala de maquinas o motor de centro, destinada para el transporte de turismo y pasajeros.
- **ALISCAFO.** Embarcación con el casco de aluminio, con motores de centro, equipadas para el transporte de pasajeros y turismo.

ANEXO M: DETERMINACIÓN DE MENSAJES A ENCRYPTAR

