**FICHA TRABAJO DE GRADO EMI -2020\_II**

|  |  |
| --- | --- |
| **TITULO** | APLICACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA EN LOS CERTIFICADOS PARA EL SEGUIMIENTO Y CONTROL DE EMBARCACIONES  CASO: DIRECCIÓN GENERAL DE INTERESES MARÌTIMOS, FLUVIALES, LACUSTRE Y MARINA MERCANTE |
| **PROPONENTE** | LUIS RICARDO RIVAS GIWENCER |
| **TUTOR** | LIC. CYNTHIA RODRIGUEZ CANAVIRI |

|  |  |  |
| --- | --- | --- |
| **PROBLEMA** | **OBJETIVO PRINCIPAL** | **OBJETIVOS ESPECIFICOS** |
| 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. | 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. | 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. |

|  |  |
| --- | --- |
| **RESULTADO / PRODUCTO** | SISTEMA DE INFORMACIÓN, CON IMPLEMENTACIÓN DE SEGURIDAD |

|  |  |  |
| --- | --- | --- |
| **METODOLOGÍA DE INVESTIGACIÓN (general)** | | |
| TIPO (S) DE ESTUDIO | METODO (S) | INSTRUMENTO (S) |
| Estudio exploratorio | Inducción  Análisis | Cuestionario  Entrevista |

|  |  |
| --- | --- |
| **METODOLOGÍA DE LA INGENIERIA DE SISTEMAS** | |
| ENTIDAD RELACION | Base de datos normalizada, entidades y cardinalidad |
| UML | Diagrama de casos de uso, diagramas de actividades, diagramas de componentes, diagramas de caso de uso de alto nivel, diagrama de clases |
| DESIGN SPRINT | Entrevistas, Notas HMW, Boot up, Notetaking, Crazy 8s,Dot voting ,Heat map voting ,Storyboards,Prototipos ,Mock, Test de usabilidad |

|  |  |  |  |
| --- | --- | --- | --- |
| **TIPO APLICACIÓN / SISTEMA** | | | |
| DESCRIPCIÓN | MODULOS | SUBMODULOS | DESCRIPCIÓN |
| Sistema que incorpora criptografía asimétrica, en los certificados, para el seguimiento y control de embarcaciones a nivel nacional | Gestión de usuarios | Registro de nuevos usuarios y asignación de rol | Módulo que controle aquellas personas que puedan ingresar al sistema, dependiendo del rol se modificara, dar de alta y baja a los demás usuarios. |
| Edición de datos de usuario |
| Dar de baja a usuarios |
| Listado de usuarios |
| Registro de embarcaciones | Registro de nuevas embarcaciones | En este módulo se podrá realizar el registro de una embarcación nueva, llenando todos los campos que correspondan dependiendo de la embarcación. |
| Lista de embarcaciones existentes |
| Consultas de información de embarcaciones |
| Reportes | Generación de reportes de embarcaciones registradas | Este módulo facilitará la emisión de reportes de embarcaciones registradas e inspeccionadas, los cuales son emitidos hacia el Viceministerio de Defensa |
| Almacenamiento de reportes en el sistema |
| Seguridad: | Generación de llaves | Administra la parte criptográfica, este módulo es el cual nos permite generar el par de llaves (llave pública y llave privada) |
| Almacenamiento de llaves |
| Inspecciones | Generación de formulario de inspección | 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 |
| Asignación de formulario a inspecciones |
| Resultado de formulario de inspección |
| Almacenamiento de resultados en la base de datos |

|  |  |
| --- | --- |
| DATOS TECNICOS | |
| SOFTWARE | Amazon Web Service  Digital Ocean  Heroku  Laravel 7 |
| HARDWARE | Usuario PC procesador i5  Tablets |
| BASE DE DATOS | Gestor de base de datos MySql, con tablas: embarcaciones, usuarios, roles, pivote de usuario-rol, formularios, movimientos económicos y archivos |
| CONECTIVIDAD | Inalámbrica, 6 a 8 equipos |
| PROCESOS | Altas, bajas y modificaciones a usuarios, registro e inspecciones a embarcaciones, generación de certificados para embarcaciones, registro de formularios de inspección, generación de llaves criptográficas para corroborar la integridad de la información de los distintos certificados |
| USUARIOS | Administrador  Jefe de sección  Inspector de Buques  Cobrador |
| ARQUITECTURA | Arquitectura 3 capas |
| SERVICIOS | Internet |
| OTROS |  |

|  |  |
| --- | --- |
| **BENEFICIARIOS DIRECTOS** | **BENEFICIARIOS INDIRECTOS** |
| Dirección General de General de Intereses Marítimos, Fluviales, Lacustre y Marina Mercante, de manera que se automatiza los procesos de registro e inspección  Generación automática de certificados, implementando seguridad | Facilidad a los dueños de embarcaciones y empresas pequeñas, para poder registrar embarcaciones  Obtención digital de certificado |

|  |  |
| --- | --- |
| **APORTE DE LA INVESTIGACIÓN** | **IMPACTO ESPERADO** |
| Implementación de criptografía asimétrica | Resguardo de la integridad de la información de certificados de embarcaciones |