

UNIVERSIDAD AUTÓNOMA JUAN MISAEL SARACHO
FACULTAD DE CIENCIAS Y TECNOLOGÍA
INGENIERÍA INFORMÁTICA



**MEJORAMIENTO DE LA SEGURIDAD EN LAS APLICACIONES
WEB UTILIZANDO EL PROTOTIPO “SISTEMA DE GESTIÓN DE
PROYECTOS DE GRADO”**

Por:

JUAN CARLOS MALLEA GUTIERREZ

Proyecto de grado presentado a consideración de la **UNIVERSIDAD AUTÓNOMA JUAN MISAEL SARACHO**, como requisito para optar al Grado Académico de Licenciatura en Ingeniería Informática.

TARIJA – BOLIVIA
2022

MSc. Ing. Marcelo Segovia Cortez
DECANO FACULTAD DE
CIENCIAS Y TECNOLOGÍA

MSc. Lic. Clovis Gustavo Succi Aguirre
VICEDECANO FACULTAD DE
CIENCIAS Y TECNOLOGÍA

APROBADO POR:

TRIBUNAL

M. Sc. Ing. Silvana Sandra Paz Ramirez

M. Sc. Lic. Deysi Beatriz Arancibia Marquez

M. Sc. Ing. Raquel Ivonne Jalil Angulo

“El tribunal calificador no se solidariza con la forma, términos, modos y expresiones vertidas en el presente trabajo, siendo únicamente responsabilidad del autor”.

DEDICATORIA

Mi proyecto de grado va dedicado a mis padres Willy Mallea y Estela Gutierrez por todo el apoyo incondicional que me brindaron en el trayecto de la carrera. Fueron ellos mi principal fuente de motivación para seguir adelante.

A los docentes por transmitirme sus diversos conocimientos.

A todos los amigos y amigas quienes sin esperar nada a cambio compartieron su conocimiento, alegrías y tristezas.

AGRADECIMIENTOS

*A mis padres **Willy Mallea y Estela Gutierrez** por guiarme constantemente, por la comprensión y por su apoyo incondicional para concluir el presente proyecto de grado.*

A la Universidad Autónoma Juan Misael Saracho, Facultad de Ciencias y Tecnología, Carrera de Ingeniería Informática por haberme recibido y acogido durante mis estudios académicos. También un gran agradecimiento al personal docente, por todo el conocimiento brindado.

*A mis hermanos y hermanas **Ivan, Josue, Esther, Dennis y Cristhian** alentándome constantemente a culminar mis estudios universitarios.*

*A una persona muy especial **Elsa**, quien estuvo ahí para mí, en los momentos más difíciles eternizándose así en mi corazón.*

PENSAMIENTO

“En tiempos de cambio, quienes estén abiertos al aprendizaje se adueñarán del futuro, mientras que aquellos que creen saberlo todo estarán bien equipados para un mundo que ya no existe”.

Eric Hoffer

ÍNDICE

I.	CAPITULO I EL PROYECTO	1
I.1	Introducción	1
I.2	Descripción del proyecto	2
I.2.1	Antecedentes	2
I.2.2	Justificaciones	6
I.2.2.1	Justificación tecnológica.....	6
I.2.2.2	Justificación económica.....	7
I.2.2.3	Justificación social.....	7
I.2.3	Planteamiento del problema.....	7
I.2.4	Objetivos	8
I.2.4.1	Objetivo general.....	8
I.2.4.2	Objetivos específicos	8
I.2.5	Sistema de marco lógico (SML).....	8
I.2.5.1	Cuadro de involucrados	9
I.2.5.2	Árbol de problemas.....	10
I.2.5.3	Árbol de objetivos.....	11
I.2.5.4	Árbol de alternativas.....	12
I.2.5.5	Matriz de marco lógico (MML).....	13
I.2.6	Metodología de desarrollo.....	17
I.2.7	Resultados esperados.....	17
I.2.8	Beneficiarios.....	18
I.2.8.1	Beneficiarios directos.....	18
I.2.8.2	Beneficiarios indirectos	18
I.3	Cronograma de actividades.....	19
II.	CAPÍTULO II MARCO TEÓRICO DEL PROYECTO	20
II.1	Introducción	20
II.2	Seguridad informática.....	20
II.2.1	Seguridad física	21
II.2.2	Seguridad lógica	21
II.3	Seguridad de la información	22
II.3.1	ISO 27001	23
II.3.1.1	Cómo funciona la ISO 27001	25

II.3.1.2	Beneficios de ISO 27001	26
II.3.1.3	Aplicabilidad de la norma ISO 27001 para auditoria	27
II.4	Aplicación web	28
II.4.1	Estructura de una aplicación web	29
II.4.2	Arquitectura de una aplicación web	29
II.4.3	Servicios web.....	30
II.5	Seguridad de aplicaciones web	30
II.5.1	Validación de datos	30
II.5.2	Manejo de sesiones.....	30
II.5.3	Ataque a la aplicación web.....	30
II.5.4	Riesgos en una aplicación web.....	31
II.5.5	Vulnerabilidad	31
II.6	Sistema de detección de intrusos	32
II.6.1	Funciones de un IDS.....	33
II.6.2	Tipos de sistemas de detección de intrusos	34
II.6.2.1	Tipos de IDS en función del origen de los datos	35
II.6.2.1.1	HIDS: Host-based Intrusion Detection Systems	35
II.6.2.1.2	NIDS: Network Intrusion Detection Systems	36
II.7	Detección de riesgos en las aplicaciones web.....	38
II.7.1	Detección de riesgos del lado del cliente.....	39
II.7.2	Detección de riesgos del lado del servidor	42
II.7.3	Detección de riesgos en el canal de comunicación.....	45
II.8	Seguridad en Bases de Datos	46
II.8.1	Inyección de código.....	47
II.8.2	Inyección de código maliciosa	47
II.8.3	Inyección de código benéfico.....	47
II.8.4	Inyección de código inesperado	48
II.8.5	Inyección SQL.....	48
II.8.6	Encriptación de base de datos.....	49
II.8.6.1	Encriptación de datos en transito	49
II.8.7	Cross site scripting (XSS).....	50
II.9	Ataques DDOS.....	50
II.10	Mejores prácticas en el desarrollo.....	51
II.10.1	ITIL.....	51

II.10.2	COBIT	53
II.10.2.1	Adquisición e implementación.....	55
II.10.2.2	Entrega y soporte.....	56
II.10.2.3	Supervisión y evaluación	57
II.11	Modelo 4+1 vistas.....	58
II.12	Lenguaje de modelado unificado (UML)	59
II.13	Modelo de seguridad.....	62
II.14	Metodologías de desarrollo.....	62
II.14.1	RUP (Proceso Unificado de Racional)	62
II.14.2	XP (Programación Extrema)	63
II.14.3	MSF (Microsoft Solution Framework).....	63
II.14.4	SCRUM	63
II.15	Tecnologías de desarrollo	64
III.	CAPITULO III ESTUDIO DE VULNERABILIDADES EN	
APLICACIONES WEB	65
III.1	Introducción	65
III.2	Propósito	65
III.3	Objetivo general.....	65
III.4	Objetivos específicos	65
III.5	Web.....	65
III.5.1	XSS (Cross Site Scripting).	66
III.5.2	CSRF (Cross Site Request Forgery).....	68
III.5.3	Inyección de Código (Code Injection).....	70
III.5.4	Buffer Overflow.	72
III.6	Bases de datos.....	74
III.6.1	SQL Injection.	75
IV.	CAPÍTULO IV CASO DE ESTUDIO Y APLICACIÓN PRÁCTICA.....	83
IV.1	Introducción	83
IV.2	Propósito	84
IV.3	Objetivo general.....	84
IV.4	Objetivos específicos	84
IV.5	Arquitectura de las aplicaciones web mediante capas	84
IV.5.1	Capa de presentación visual	85
IV.5.1.1	Validación de datos con JavaScript.....	85

IV.5.1.2	Validación AntiSamy	85
IV.5.1.3	Tecnología Ajax	86
IV.5.1.4	Utilización del algoritmo de cifrado.....	87
IV.5.1.5	Control de actividades.....	87
IV.5.2	Capa lógica de negocio.....	87
IV.5.2.1	Validación de datos en el servidor	88
IV.5.2.2	Limitación de intentos durante la autenticación.....	88
IV.5.2.3	Cifrado de datos en servidor.....	88
IV.5.2.4	Transacción de los datos	88
IV.5.2.5	Proceso de datos en SQL.....	89
IV.5.3	Capa servicios de datos web.....	89
IV.5.3.1	Servicios web	89
IV.5.3.2	Credenciales de acceso.....	90
IV.5.3.3	Limitar las peticiones	90
IV.5.4	Capa de alojamiento web.....	90
IV.5.4.1	Balanceo en la carga de datos	91
IV.5.4.2	Componentes ORM.....	91
IV.5.4.3	Servidor de cache	91
IV.5.4.4	Corta fuegos como seguridad.....	91
IV.5.4.5	Implementación de SSL	92
IV.6	Seguridad mediante capas en las aplicaciones web	92
IV.7	Prototipo.....	93
IV.7.1	Caso de estudio 1	94
IV.7.1.1	Descripción.....	94
IV.7.1.2	Prueba.....	95
IV.7.1.3	Resultado.....	98
IV.7.1.4	Recomendación	99
IV.7.2	Caso de estudio 2.....	100
IV.7.2.1	Descripción.....	100
IV.7.2.2	Prueba.....	102
IV.7.2.3	Resultado.....	102
IV.7.2.4	Recomendación	102
IV.7.3	Caso de estudio 3.....	103

IV.7.3.1	Descripción.....	103
IV.7.3.2	Prueba.....	103
IV.7.3.3	Resultado.....	104
IV.7.3.4	Recomendación.....	104
IV.7.4	Caso de estudio 4.....	105
IV.7.4.1	Descripción.....	105
IV.7.4.2	Prueba.....	106
IV.7.4.3	Resultado.....	106
IV.7.4.4	Recomendación.....	108
V.	CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES.....	109
V.1	Conclusiones.....	109
V.2	Recomendaciones.....	110
	BIBLIOGRAFIA.....	112
	ANEXOS.....	115
	SISTEMA DE GESTIÓN DE PROYECTOS DE GRADO.....	115
	Modelo de análisis y diseño.....	115
	Diseño de la base de datos.....	115
	Modelo conceptual de la base de datos.....	115
	Diccionario de datos.....	116
	Capturas de pantallas del sistema.....	120
	Modelo de implementación.....	149
	Código fuente.....	149
	MANUAL DE INSTALACIÓN.....	152
	Manual de Instalación PostgreSQL.....	151
	Manual de instalación Herramientas para el Back - end.....	156
	Instalación JDK8 - JAVA.....	158
	Manual de instalación Herramientas para el Front - end.....	162
	Node JS.....	165
	Instalación de ANGULAR/CLI.....	168

ÍNDICE DE TABLAS

<i>Tabla 1: Cuadro de Involucrados.....</i>	9
<i>Tabla 2: Matriz de Marco Lógico.....</i>	16
<i>Tabla 3: Cronograma de Actividades.....</i>	19
<i>Tabla 4: Porcentaje de vulnerabilidad por tipo de sitio</i>	38
<i>Tabla 5: Detección de riesgos al lado del cliente</i>	42
<i>Tabla 6: Detección de riesgos del lado del servidor</i>	44
<i>Tabla 7: Detección de riesgos en el canal de comunicación</i>	46
<i>Tabla 8: Mapeo de vistas a diagramas UML</i>	59
<i>Tabla 9: Vulnerabilidad, ataque, descripción, recomendación y ejemplos</i>	82
<i>Tabla 10: Datos de la catalogo de la base de datos.....</i>	106
<i>Tabla 11: Personas</i>	116
<i>Tabla 12: Docentes</i>	116
<i>Tabla 13: Alumnos</i>	116
<i>Tabla 14: Procesos</i>	117
<i>Tabla 15: Menús</i>	117
<i>Tabla 16: Mepro</i>	117
<i>Tabla 17: Roles.....</i>	117
<i>Tabla 18: Rolme.....</i>	117
<i>Tabla 19: Datos</i>	117
<i>Tabla 20: Usurol.....</i>	118
<i>Tabla 21: Grupos</i>	118
<i>Tabla 22: Áreas</i>	118
<i>Tabla 23: Etapas.....</i>	118
<i>Tabla 24: Dicta.....</i>	119
<i>Tabla 25: Programación</i>	119
<i>Tabla 26: Proyectos.....</i>	119

ÍNDICE DE FIGURAS

<i>Figura 1. Árbol de Problemas.....</i>	10
<i>Figura 2. Árbol de Objetivos.....</i>	11
<i>Figura 3. Árbol de alternativas.....</i>	12
<i>Figura 4. Cantidad de certificados emitidos en Latinoamérica</i>	23
<i>Figura 5. Estructura de ISO 27001.....</i>	25
<i>Figura 6. Esquema general de un IDS.....</i>	33
<i>Figura 7. Clasificación del IDS</i>	35
<i>Figura 8. Sistema de detección de intrusos basado en host.....</i>	36
<i>Figura 9. Sistema de detección de intrusos basado en red</i>	37
<i>Figura 10. Figura 2-7: Modelo 4+1 vistas de la arquitectura</i>	59
<i>Figura 11. Modelo 4+1 vistas con UML.....</i>	60
<i>Figura 12. Tecnologías más usados para el desarrollo web</i>	64
<i>Figura 13. Modelo de seguridad en las aplicaciones web mediante capas.....</i>	92
<i>Figura 14. Interfaz general del prototipo</i>	93
<i>Figura 15. Conexión de la base de datos.....</i>	94
<i>Figura 16. Configuración de la base de datos.....</i>	95
<i>Figura 17. Autenticación.....</i>	95
<i>Figura 18. Formulario de inicio de sesión.</i>	96
<i>Figura 19. Inicio de sesión con datos correctos.</i>	97
<i>Figura 20. Inicio de sesión con inyección SQL.</i>	97
<i>Figura 21. Intento de inicio de sesión con inyección SQL, Front-end.</i>	98
<i>Figura 22. Intento de inicio de sesión con inyección SQL, Back-end.....</i>	98
<i>Figura 23. Proceso de autenticación</i>	99
<i>Figura 24. Aplicación vulnerable a ataques XSS</i>	101
<i>Figura 25. Vulnerabilidad XSS de Tipo-0.....</i>	102
<i>Figura 26. Comportamiento de la vulnerabilidad XSS de Tipo-1</i>	103
<i>Figura 27. Interfaz aplicación falsa Vulnerabilidad XSS de Tipo-1.....</i>	104
<i>Figura 28. Interfaz aplicación Original Vulnerabilidad XSS de Tipo-1.....</i>	104
<i>Figura 29. Vulnerabilidad XSS de Tipo-2.....</i>	107
<i>Figura 30. Comportamiento de la vulnerabilidad XSS de Tipo-2</i>	108
<i>Figura 31. Modelo Conceptual de la Base de Datos</i>	115
<i>Figura 32. Estructura General del prototipo la aplicación web “Sistema de gestión de proyectos de grado”</i>	120

<i>Figura 33. Pantalla de autenticación del sistema.</i>	121
<i>Figura 34. Pantalla Administrador del sistema.</i>	121
<i>Figura 35. Pantalla gestión de personas.</i>	122
<i>Figura 36. Adicionar nueva persona</i>	122
<i>Figura 37. Modificar Persona</i>	123
<i>Figura 38. Eliminar persona.</i>	124
<i>Figura 39. Recuperar o habilitar a la persona.</i>	124
<i>Figura 40. Imprimir datos de la persona</i>	125
<i>Figura 41. Asignar datos de acceso.</i>	125
<i>Figura 42. Modificar datos de acceso de la persona.</i>	126
<i>Figura 43. Gestión grupos.</i>	126
<i>Figura 44. Adicionar Grupos.</i>	127
<i>Figura 45. Modificar Grupo.</i>	128
<i>Figura 46. Eliminar grupo.</i>	128
<i>Figura 47. Recuperar o habilitar grupo.</i>	129
<i>Figura 48. Gestión áreas.</i>	129
<i>Figura 49. Adicionar nueva área.</i>	130
<i>Figura 50. Modificar área.</i>	130
<i>Figura 51. Eliminar área.</i>	131
<i>Figura 52. Habilitar área.</i>	131
<i>Figura 53. Gestión de proyectos.</i>	132
<i>Figura 54. Adicionar nuevo proyecto.</i>	132
<i>Figura 55. Selección Área:</i>	133
<i>Figura 56. Selección programación del estudiante:</i>	133
<i>Figura 57. Selección de tutor:</i>	134
<i>Figura 58. Modificar proyecto</i>	134
<i>Figura 59. Eliminar proyecto.</i>	135
<i>Figura 60. Recuperar o habilitar proyecto.</i>	136
<i>Figura 61. Gestión de roles.</i>	136
<i>Figura 62. Anadir nuevo rol.</i>	137
<i>Figura 63. Modificar Rol.</i>	138
<i>Figura 64. Eliminar rol.</i>	138
<i>Figura 65. Recuperar rol.</i>	139
<i>Figura 66. Gestión menús.</i>	139

<i>Figura 67. Adicionar nuevo menú.....</i>	140
<i>Figura 68. Modificar menú.</i>	140
<i>Figura 69. Eliminar menú.</i>	141
<i>Figura 70. Habilitar menú.</i>	141
<i>Figura 71. Gestión etapas.....</i>	142
<i>Figura 72. Anadir nueva etapa.</i>	142
<i>Figura 73. Modificar etapas</i>	143
<i>Figura 74. Eliminar etapa.....</i>	143
<i>Figura 75. Recuperar o habilitar etapa.</i>	144
<i>Figura 76. Gestión programación.</i>	144
<i>Figura 77. Selección grupos:</i>	145
<i>Figura 78. Selección Alumnos:</i>	145
<i>Figura 79. Adicionar nueva programación.</i>	146
<i>Figura 80. Modificar programación.....</i>	146
<i>Figura 81. Eliminar programación.....</i>	147
<i>Figura 82. Controles de formularios.</i>	147
<i>Figura 83. Autenticación Back - end:</i>	149
<i>Figura 84. Añadir personas</i>	149
<i>Figura 85. Crear proyectos.....</i>	150
<i>Figura 86. Modificar proyecto.....</i>	151
<i>Figura 87. Eliminar proyecto.....</i>	151
<i>Figura 88. Recuperar proyecto</i>	151
<i>Figura 89. Adicionar nueva programación.</i>	151
<i>Figura 90. Modificar programación.....</i>	151