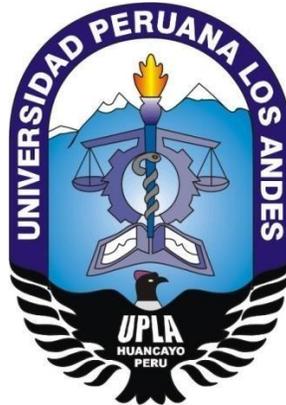


UNIVERSIDAD PERUANA LOS ANDES
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE
SISTEMAS Y COMPUTACIÓN



TESIS:

**IMPLEMENTACIÓN DE FIRMAS DIGITALES PARA EL CONTROL DE
LA INTEGRIDAD DE CERTIFICADOS DE ESTUDIOS**

Línea de Investigación Institucional:
Nuevas Tecnologías y Procesos

PRESENTADO POR:

Bach. MAYTA LLACUA, CARLOS ANDRES

**PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO DE SISTEMAS Y COMPUTACIÓN**

HUANCAYO – PERÚ

2019

DR. VICENTE RAMOS WAGNER ENOC
ASESOR METODOLÓGICO

MG. ARANA CAPARACHIN MAGLIONI
ASESOR TEMÁTICO

DEDICATORIA

El presente trabajo de investigación lo dedico a todas aquellas personas que con sus consejos basado en experiencias me impulsaron a seguir adelante a pesar de las adversidades y demostrarme que todos podemos ser mejores personas de lo que consideramos ser y que sobre todo la familia es el pilar que solidifica la realización personal.

AGRADECIMIENTOS

Agradezco a Dios por la salud que brinda día con día, esto fue de vital importancia para poder utilizarlo como sostén para cumplir mis objetivos planteados.

Agradezco a mis padres José y Eva, cada uno con su forma singular de demostrar cómo darle la cara a la vida y aprender de cada error para saber sobreponerse ante todo y ser mejor cada día.

Agradezco a mi sobrina Estefanny quien es para mí como una hija que entiende y acoge todas las correcciones que intento aplicar en su vida, apoyándome a su vez con su dulzura y alegría siendo así un motivo más para seguir.

Agradezco a una persona en especial, Karen a quien admiro mucho por su persistencia y deseo de superación, ella es quien me va apoyando a cada instante.

Agradezco a mis asesores personas admirables que demuestran el deseo de apoyar con sus enseñanzas y quienes ayudaron enormemente con la presente tesis.

DR. CASIO AURELIO TORRES LOPEZ
PRESIDENTE

.....
JURADO 01

.....
JURADO 02

.....
JURADO 03

SECRETARIO

ÍNDICE

DEDICATORIA	iii
AGRADECIMIENTOS	iv
ÍNDICE	vi
ÍNDICE DE TABLAS	ix
ÍNDICE DE FIGURAS.....	iv
ÍNDICE DE ANEXOS	xii
RESUMEN	xiii
ABSTRACT.....	xiv
INTRODUCCIÓN.....	xv
CAPÍTULO I.....	17
PROBLEMA DE INVESTIGACIÓN	17
Planteamiento del Problema	17
Formulación y sistematización del problema.....	23
1.2.1. Problema general.....	23
1.2.2. Problemas específicos.....	23
Justificación	23
1.3.1. Práctica o Social.	23
1.3.2. Científica o Teórica.	¡Error! Marcador no definido.
1.3.3. Metodológica.....	24
Delimitaciones	24
1.4.1. Espacial.....	24
1.4.2. Temporal.....	25
1.4.3. Económica.	25
Limitaciones.....	25
Objetivos.....	26
1.6.1. Objetivo General.	26
1.6.2. Objetivo(s) Específico(s).....	26
CAPÍTULO II.....	27
MARCO TEÓRICO	27

2.1. Antecedentes.....	27
2.1.1. Nacionales.	27
2.1.2. Internacionales.....	29
2.2. Marco Conceptual	30
2.2.1. SGSI.....	30
2.2.2. ISO 27001.....	30
2.2.3. Confidencialidad, integridad y disponibilidad.....	31
2.2.4. Control de la integridad.....	32
2.2.5. Firma digital.....	33
2.2.6. Firma Manuscrita.	34
2.2.7. Criptografía.	36
2.2.8. Base de Datos.....	37
2.2.9. Lenguaje de Programación.....	38
2.3. Definición de Términos.....	39
2.4. Hipótesis.....	45
2.4.1. Hipótesis general.	45
2.4.2. Hipótesis específicas.	45
2.5. Variables.....	45
2.5.1. Definición conceptual de variable.	45
2.5.2. Definición operacional de variable.	46
2.5.3. Operacionalización de la Variable.	47
CAPÍTULO III.....	48
METODOLOGÍA.....	48
Método de Investigación.....	48
Tipo de Investigación.....	48
Nivel de Investigación.....	48
Diseño de Investigación	49
Población y muestra	49
3.5.1. Población.	49

3.5.2. Muestra.....	50
Técnicas e Instrumentos de recolección de datos	51
3.6.1. Técnicas.....	51
3.6.2. Instrumentos.....	52
Procesamiento de la información	53
Técnicas y Análisis de datos	53
CAPITULO IV	54
RESULTADOS	54
4.1. Descripción.....	54
4.2. Trabajo de Campo.....	55
4.2.1. Modelado del Negocio.....	55
4.2.2. Desarrollo del Sistema.....	68
4.3. Resultados Descriptivos	90
4.3.1. Primer indicador.....	90
4.3.2. Segundo indicador.....	92
4.3.3. Tercer Indicador.....	93
4.4. Prueba de Hipótesis	95
4.4.1. Hipótesis Especifica 1:.....	95
4.4.2. Hipótesis Especifica 2:.....	98
4.4.3. Hipótesis Especifica 2:.....	100
4.4.3. Hipótesis General:.....	101
CAPÍTULO V	102
DISCUSIÓN DE RESULTADOS	102
CONCLUSIONES	104
RECOMENDACIONES.....	106
REFERENCIAS BIBLIOGRÁFICAS	107
ANEXOS.....	110

ÍNDICE DE TABLAS

Tabla 1_ <i>Cuadro de operacionalización de variables con las dimensiones, indicadores e ítems del trabajo de investigación</i>	48
Tabla 2_ <i>Descripción de cada icono de acuerdo a su estereotipo</i>	58
Tabla 3_ <i>Descripción de los casos de uso del negocio</i>	59
Tabla 4_ <i>Descripción de los trabajadores del negocio</i>	61
Tabla 5_ <i>Descripción de los actores</i>	66
Tabla 6_ <i>Información descriptiva del Pre y Post Test del primer indicador</i>	92
Tabla 7_ <i>Información descriptiva del Pre y Post Test del segundo indicador</i>	94
Tabla 8_ <i>Información descriptiva del Pre y Post Test del tercer indicador</i>	96
Tabla 9_ <i>Prueba de normalidad hipótesis específica 1</i>	98
Tabla 10_ <i>Prueba paramétrica de hipótesis específica 1</i>	99
Tabla 11_ <i>Prueba de normalidad hipótesis específica 2</i>	100
Tabla 12_ <i>Prueba paramétrica de hipótesis específica 2</i>	101
Tabla 13_ <i>Prueba de normalidad hipótesis específica 3</i>	102
Tabla 14_ <i>Prueba paramétrica de hipótesis específica 3</i>	102

ÍNDICE DE FIGURAS

Figura 1. <i>Certificados emitidos en el mes de julio</i>	20
Figura 2. <i>Estructura ISO 27001</i>	31
Figura 3. <i>Triada en seguridad de la información</i>	32
Figura 4. <i>Integridad de la información</i>	32
Figura 5. <i>La firma digital</i>	32
Figura 6. <i>La firma manuscrita</i>	32

Figura 7. Seguridad criptográfica	32
Figura 8. Tipos de base de datos	32
Figura 9. Lenguaje de programación	32
Figura 10. Diagrama de objetivos del negocio	59
Figura 11. Diagrama de objetivos del negocio	60
Figura 12. Diagrama de casos de uso	62
Figura 13. Diagrama actividades de la creación de la firma digital	63
Figura 14. Diagrama de actividad del cargado de certificados virtuales	64
Figura 15. Diagrama de actividad de la verificación del certificado	65
Figura 16. Interacción de actores del negocio	67
Figura 17. Diagrama general de casos de uso	67
Figura 18. Caso de uso en la creación de las firmas digitales	68
Figura 19. Caso de uso indicando la carga de certificados	69
Figura 20. Caso de uso con respecto a la verificación del certificado	69
Figura 21. Opciones de descargar del software Middleware	70
Figura 22. Dispositivo de autenticación con DNle marca Wiltron	71
Figura 23. Instalación inicial del software Middlware	71
Figura 24. Software Middlware instalado en el S.O.	72
Figura 25. Insertando el dispositivo de autenticación con DNle	72
Figura 26. Insertando el DNle para realizar la autenticación mediante la clave PIN	73
Figura 27. Software Middlware en ejecución solicitando DNle	73
Figura 28. Software con los certificados disponibles	74
Figura 29. Software ReFirma	74
Figura 30. Pantalla de instalación inicial del producto ReFirma	75
Figura 31. Configuración automática del software ReFirma	75
Figura 32. Términos de uso del software ReFirma (Reniec)	76

Figura 33. En el software se elige la opción abrir para acceder a los documentos	76
Figura 34. Se seleccionan los documentos a firmar	77
Figura 35. Configurando el nivel de visibilidad del logo de firma	77
Figura 36. Términos de uso para realizar la firma digital	78
Figura 37. Certificado obtenido con el aplicativo Middleware	78
Figura 38. Mostrando los parámetros de firma	79
Figura 39. Solicitud de la clave PIN para validar la firma digital	78
Figura 40. Verificada la firma digital se mostrara el proceso de validación	80
Figura 41. Solicitud de la clave PIN para validar la firma digital	80
Figura 42. Certificado de estudios con firma digital	81
Figura 43. Base de datos completa del Centro de Idiomas	82
Figura 44. Tabla alumno con los campos necesarios	82
Figura 45. Tabla alumno con el nuevo campo alucertificado	83
Figura 46. Vista del servidor con la carpeta contenedora de los certificados	83
Figura 47. Portal web del Centro de Idiomas	86
Figura 48. Ingresando credenciales de seguridad del asistente académico	86
Figura 49. Seleccionar la pestaña alumnado para actualizar la información	87
Figura 50. Búsqueda del alumno mediante datos o DNI	87
Figura 51. Se elige al interesado para subir el certificado	88
Figura 52. Seleccionar la opción Browse para abrir el explorador de archivos ..	88
Figura 53. Elegir el certificado firmado digitalmente	89
Figura 54. Elegido el certificado pulsar en el botón subir archivo	89
Figura 55. Vista previa con el documento cargado al servidor	89
Figura 56. Portal web con las diversas opciones académicas	90
Figura 57. Opciones de estudiante disponible	90
Figura 58. Vista previa del certificado de estudios mediante búsqueda	91

Figura 59. Vista previa con la opción de descarga disponible	92
Figura 60. Grafico estadístico del primer indicador	93
Figura 61. Grafico estadístico del segundo indicador	95
Figura 62. Grafico estadístico del tercer indicador	96
Figura 63. Curva de distribución “t” de cola izquierda - Hipótesis Especifica 1...99	
Figura 64. Curva de distribución “t” de cola izquierda - Hipótesis Especifica 2 .	101

ÍNDICE DE ANEXOS

Anexo N° 01: Matriz de Consistencia	116
Anexo N° 02: Ficha de Observación	117
Anexo N° 03: Instrumento de validación 1	118
Anexo N° 04: Instrumento de validación 2	119
Anexo N° 05: Instrumento de validación 3	120
Anexo N° 06: Tratamiento de datos Pre Test	121
Anexo N° 07: Promedio de Incidencias Post Test	122
Anexo N° 08: Tratamiento de datos Post Test	123
Anexo N° 09: Promedio de Incidencias Post Test	124
Anexo N° 10: Certificado de estudios adulterados	125
Anexo N° 11: Documento sobre adulteración	126
Anexo N° 12: Registro manual de certificados 1	127
Anexo N° 13: Registro manual de certificados 2	128
Anexo N° 14: Registro manual de certificados 3	129

RESUMEN

El presente trabajo inicio mediante el problema general: ¿Como influye la implementación de firmas digitales en el control de la integridad de los certificados de estudios del Centro de Idiomas de la UNCP? , luego se planteó el objetivo que consistió en determinar de qué manera la implementación de firmas digitales mejorará el control de la integridad de los certificados de estudios del Centro de Idiomas de la UNCP y luego fijar la hipótesis: la implementación de firmas digitales mejora significativamente el control de la integridad de los certificados de estudios del centro de Idiomas de la UNCP.

Esta investigación se realizo utilizando el método inductivo – deductivo de tipo aplicada, haciendo uso del nivel descriptivo – explicativo con el diseño pre experimental (pre y post test) y haciendo uso de una población de 305 certificados de estudios con una muestra de 170.

Se concluye que, la implementación de firmas digitales mejora significativamente el control de la integridad de los certificados ya que comparando los valores del Pre y Post Test se pudo validar la hipótesis.

Palabras claves: Firmas digitales, seguridad y control de la integridad.

ABSTRACT

The present work began with the general problem: How does the implementation of digital signatures influence the integrity control of the study certificates of the Language Center of the UNCP? The objective was to determine how the implementation of digital signatures will improve the integrity control of the study certificates of the Language Center of the UNCP and then set the hypothesis: the implementation of digital signatures significantly improves the Integrity control of the study certificates of the Language Center of the UNCP.

This research was carried out using the inductive method - deductive of applied type, using the descriptive level - explanatory with the pre-experimental design (pre and post test) and using a population of 305 certificates of studies with a sample of 170.

In conclusion, it was obtained that the implementation of digital signatures significantly improves the control of the integrity of the certificates since comparing the Pre and Post Test values the hypothesis could be validated.

Keywords: Digital signatures, security and integrity control.

INTRODUCCIÓN

A día de hoy la tecnología avanza a pasos agigantados, insertándose en todos los campos de actividad humana y los sistemas de información automatizada se hace cada día más indispensable, esto permite que podamos desarrollar y desenvolver mejor nuestras labores ya sea en el hogar o en el trabajo, aunque el avance es constante día con día existe aún la necesidad de difundirlo implementando e innovando los procesos que suelen llevarse a cabo en las organizaciones que más lo requieran, este es el caso del Centro de Idiomas de la UNCP el cual afronta un problema de seguridad como en cualquier organización con el control de la integridad de sus certificados los cuales requieren mayor confidencialidad, seguridad y disponibilidad al momento de ser emitidos al usuario final (alumno), este problema se ha evidenciado provocando conflictos en el desarrollo de los tramites académicos trayendo consigo insatisfacción en los distintos actores de proceso.

El presente trabajo de investigación se divide secuencialmente en 5 capítulos descritos como sigue a continuación:

El CAPITULO I “EL PROBLEMA DE INVESTIGACIÓN”. Se detalla el planteamiento del problema, formulación y sistematización del problema (problema general y problemas específicos), justificación (práctica o social, científica o teórica y metodológica), delimitaciones (espacial, temporal y económica), limitaciones y objetivos (general y específicos).

El CAPITULO II “MARCO TEORICO”. Se procede con la descripción de los antecedentes (nacionales e internacionales), marco conceptual, definición de términos, hipótesis (general y específicas), y variables (definición conceptual, definición operacional y operacionalización)

El CAPITULO III “METODOLOGÍA”. Se prosigue con el método de investigación, tipo de investigación, nivel de investigación, diseño de investigación, población, muestra,

técnicas e instrumentos de recolección de datos, procesamiento de la información para culminar el capítulo en las técnicas y análisis de datos.

El CAPITULO IV “RESULTADOS”. En este punto se desarrolló el trabajo de campo, modelado del negocio, desarrollo del sistema, resultados descriptivos (primer, segundo y tercer indicador) y la prueba de hipótesis.

El CAPITULO V “DISCUSION DE RESULTADOS”. Este último capítulo realizara la descripción de resultados obtenidos al final de la investigación.

Por último, se muestran las conclusiones, recomendaciones, referencias bibliográficas y anexos del trabajo desarrollado.

Bach. Carlos Andrés Mayta Llacua