UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS ECONÓMICO ADMINISTRATIVAS
DOCTORADO EN TECNOLOGÍAS DE INFORMACIÓN

Título:

Algoritmos y Protocolos de Seguridad para el Registro Civil del Ecuador

Trabajo recepcional para obtener el Grado de

Doctor en Tecnologías de Información

Presenta:

Segundo Moisés Toapanta Toapanta

Director:

Dr. José Antonio Orizaga Trejo

Co-Director:

Dr. Luis Enrique Mafla Gallegos

Lectores:

Dra. Ma. del Roció Maciel Arellano

Dr. Carlos Alberto Ochoa Ortiz

Dr. Edgar Cossio Franco

Dr. Jesús Raúl Beltrán Ramírez

Zapopan, Jalisco, abril de 2018

ZAPOPAN, JALISCO A 5 DE MARZO DE 2018

JUNTA ACADÉMICA DEL PROGRAMA DE
DOCTORADO EN TECNOLOGIAS DE INFORMACIÓN
PRESENTE

En mi carácter de **Director** del trabajo recepcional titulado: "**Algoritmos y Protocolos de Seguridad para el Registro Civil del Ecuador**", que presenta el C **SEGUNDO MOISÉS TOAPANTA TOAPANTA**, expongo que lo he revisado y que a mi juicio cumple con todos los requisitos académicos con el rigor teórico-metodológico y de contenido, además los resultados del análisis de similitud no muestra coincidencias relevantes, por lo puede ser sometido al examen de grado correspondiente al **Doctorado en Tecnologías de Información**.

Por lo antes expuesto, me permito emitir el presente oficio de: *liberación del trabajo recepcional*, en mi carácter de **Director**, con la finalidad de que pueda llevarse a cabo la defensa del mismo.

ATENTAMENTE
ZAPOPAN, JALISCO, MEXICO

DR. JOSÉ ANTONIO ORIZAGA TREJO
DIRECTOR DE TESIS Y PROFESOR INVESTIGADOR C 9605193

Zapopan, Jalisco a 5 de Marzo de 2018

Junta Académica del Programa de
Doctorado en Tecnologías de Información
Presente

En mi carácter de Co-Director del trabajo recepcional titulado: "ALGORITMOS Y PROTOCOLOS DE SEGURIDAD PARA EL REGISTRO CIVIL DEL ECUADOR", que presenta el C. SEGUNDO MOISES TOAPANTA TOAPANTA, expongo que lo he revisado y que a mi juicio cumple con todos los requisitos académicos con el rigor teórico-metodológico y de contenido, además los resultados del análisis de similitud no muestra coincidencias relevantes, por lo puede ser sometido al examen de grado correspondiente al Doctorado en Tecnologías de Información.

Por lo antes expuesto, me permito emitir el presente oficio de: liberación del trabajo recepcional, en mi carácter de Lector, con la finalidad de que pueda llevarse a cabo la defensa del mismo.

Atentamente

Dr. Luis Enrique Mafla Gallegos
Profesor Titular – Investigador
Facultad de Ingeniería en Sistemas
Escuela Politécnica Nacional

Zapopan, Jalisco a 09 de Marzo de 2018

Junta Académica del Programa de
Doctorado en Tecnologías de Información
Presente

En mi carácter de lectora del trabajo recepcional titulado: "ALGORITMOS Y PROTOCOLOS DE SEGURIDAD PARA EL REGISTRO CIVIL DEL ECUADOR", que presenta el C. SEGUNDO MOISES TOAPANTA TOAPANTA, expongo que lo he revisado y que a mi juicio cumple con todos los requisitos académicos con el rigor teórico-metodológico y de contenido, además los resultados del análisis de similitud no muestra coincidencias relevantes, por lo puede ser sometido al examen de grado correspondiente al Doctorado en Tecnologías de Información.

Por lo antes expuesto, me permito emitir el presente oficio de: liberación del trabajo recepcional, en mi carácter de Lectora, con la finalidad de que pueda llevarse a cabo la defensa del mismo.

Atentamente

Dra. Rocío Maciel Arellano
Universidad de Guadalaja – CUCEA
Profesora Investigadora

Zapopan, Jalisco a 15 de Marzo de 2018

Junta Académica del Programa de
Doctorado en Tecnologías de Información
Presente

En mi carácter de lector del trabajo recepcional titulado: "ALGORITMOS Y PROTOCOLOS DE SEGURIDAD PARA EL REGISTRO CIVIL DEL ECUADOR", que presenta el C. SEGUNDO MOISES TOAPANTA TOAPANTA, expongo que lo he revisado y que a mi juicio cumple con todos los requisitos académicos con el rigor teórico-metodológico y de contenido, además los resultados del análisis de similitud no muestra coincidencias relevantes, por lo puede ser sometido al examen de grado correspondiente al Doctorado en Tecnologías de Información.

Por lo antes expuesto, me permito emitir el presente oficio de: liberación del trabajo recepcional, en mi carácter de Lector, con la finalidad de que pueda llevarse a cabo la defensa del mismo.

Atentamente

Dr. Alberto Ochoa
Doctor en Tecnologìa
Universidad Autònoma de Ciudad de Juàrez
SIN Nivel 2

Zapopan, Jalisco a 12 de Marzo de 2018

Junta Académica del Programa de
Doctorado en Tecnologías de Información
Presente

En mi carácter de lector del trabajo recepcional titulado: "ALGORITMOS Y PROTOCOLOS DE SEGURIDAD PARA EL REGISTRO CIVIL DEL ECUADOR", que presenta el C. SEGUNDO MOISES TOAPANTA TOAPANTA, expongo que lo he revisado y que a mi juicio cumple con todos los requisitos académicos con el rigor teórico-metodológico y de contenido, además los resultados del análisis de similitud no muestra coincidencias relevantes, por lo puede ser sometido al examen de grado correspondiente al Doctorado en Tecnologías de Información.

Por lo antes expuesto, me permito emitir el presente oficio de: liberación del trabajo recepcional, en mi carácter de Lector, con la finalidad de que pueda llevarse a cabo la defensa del mismo.

Atentamente

Dr. Edgar Cossio Franco
Universidad Enrique Díaz de León
Profesor Investigador

Zapopan, Jalisco a 14 de Marzo de 2018

Junta Académica del Programa de
Doctorado en Tecnologías de Información
Presente

En mi carácter de lector del trabajo recepcional titulado: "ALGORITMOS Y PROTOCOLOS DE SEGURIDAD PARA EL REGISTRO CIVIL DEL ECUADOR", que presenta el C. SEGUNDO MOISES TOAPANTA TOAPANTA, expongo que lo he revisado y que a mi juicio cumple con todos los requisitos académicos con el rigor teórico-metodológico y de contenido, además los resultados del análisis de similitud no muestra coincidencias relevantes, por lo puede ser sometido al examen de grado correspondiente al Doctorado en Tecnologías de Información.

Por lo antes expuesto, me permito emitir el presente oficio de: liberación del trabajo recepcional, en mi carácter de Lector, con la finalidad de que pueda llevarse a cabo la defensa del mismo.

Atentamente

D. en .C Jesús Raúl Beltrán Ramírez
Universidad de Guadalajara - CUCEA

Agradecimiento

A Dios que es nuestro creador, que por él tenemos la oportunidad de vivir y cumplir objetivos, metas personales, profesionales y académicas.

A mi madre Diocelina Toapanta, Don Lorenzo Quilumba, Cecilia Pavón (esposa), Pamela Toapanta Pavón (hija), a la memoria de mi padre Segundo Manuel Toapanta Coyago y a todas (os) mis hermanas (os), sobrinas (os), cuñadas (dos), Jaime Pavón León (amigo y asesor jurídico), familiares y amigas (os) que siempre me han apoyado incondicionalmente para cumplir una etapa más en la vida.

A los académicos Dra. Roció Maciel, Dr. José Orizaga, Dr. Enrique Mafla, Dr. Leopoldo Gómez, Dr. Jesús Aramburo, Dr. Raúl Beltrán, Dr. Edgar Cossio, Dr. Alberto Ochoa y todo el personal administrativo y operativo del Programa Doctorado en Tecnologías de Información.

A todas las autoridades de la Universidad Politécnica Salesiana del Ecuador que hicieron posible el auspicio económico y administrativo en esta formación doctoral en especial al Dr. Javier Hérran, Rector; Eco. Andrés Bayolo, Vicerrector de la Sede Guayaquil, Compañeras (ros) de Trabajo y Senescyt.

Todos los imperios del futuro van a ser imperios del conocimiento, y solamente serán exitosos los pueblos que entiendan cómo generar conocimientos y cómo protegerlos; cómo buscar a los jóvenes que tengan la capacidad para hacerlo y asegurarse que se queden en el país.

Albert Einstein

La humildad es la virtud del ser humano pero no permitas que se convierta en conformismo en tu vida. Agradece a Dios sobre todas las cosas.

Moisés Toapanta

Algoritmos y Protocolos de Seguridad para el Registro Civil del Ecuador

Resumen:

Los registros de eventos civiles constituyen la infraestructura básica de la base de datos del Registro Civil del Ecuador; en particular el documento de identidad es un requisito indispensable para el acceso a servicios y beneficios públicos y privados. El Registro Civil de Identificación y Cedulación es una institución pública responsable de la captura, depuración, documentación, presentación, custodia, corrección, actualización y certificación de los actos y estadísticas vitales, entre otros. El objetivo es mitigar los riesgos y amenazas de la confidencialidad, integridad y autenticidad de la información del Registro Civil del Ecuador con la adopción de algoritmos, protocolos y modelos criptográficos de seguridad en modelos conceptuales. Resultó el diseño del sistema de seguridad para el Registro Civil; basados en la adopción de diseños de modelos, tecnologías de seguridad, adoptados en modelos conceptuales que es una alternativa para mitigar la base de datos con confidencialidad, integridad y autenticación. A partir de esta investigación se publicó varios artículos en diferentes conferencias y revistas científicas indexadas a ACM, Scopus, Web of Science, con impacto SJR, JCR unas registradas en línea otras en proceso de registro; con la finalidad que sea validada y certificada la investigación. Se concluyó que para el diseño del sistema de seguridad del Registro Civil con confidencialidad, integridad y autenticidad se debe considerar la misión, visión, objetivos operativos, tácticos estratégicos y procesos de la institución. La adopción en un modelo conceptual de los diseño de modelos y tecnologías de seguridad es una alternativa para mitigar la seguridad de la información. El impacto de este proyecto de investigación puede tener efecto en forma directa o indirecta para todas las personas de nacionalidad ecuatoriana o extranjera que estén registradas en la base de datos.

Palabras claves: Confidencialidad, integridad, autenticidad, seguridad de la información, modelos de seguridad, algoritmos y protocolos de seguridad.

Algorithms and Security Protocols for the Civil Registry of the Ecuador

Abstract:

The records of civil events constitute the basic infrastructure of the database of the Civil Registry of Ecuador; in particular, the identity document is an indispensable requirement for access to public and private services and benefits. The Civil Registry of Identification and Certification is a public institution responsible for the capture, debugging, documentation, presentation, custody, correction, updating and certification of vital acts and statistics, among others. The objective is to mitigate the risks and threats of confidentiality, integrity and authenticity of the information of the Civil Registry of Ecuador with the adoption of algorithms, protocols and cryptographic models of security in conceptual models. The design of the security system for the Civil Registry turned out; based on the adoption of model designs, security technologies, adopted in conceptual models that is an alternative to mitigate the database with confidentiality, integrity and authentication. From this research, several articles were published in different conferences and scientific journals indexed to ACM, Scopus, Web of Science, with impact SJR, JCR registered online others in process of registration; with the purpose that the investigation is validated and certified. It was concluded that for the design of the security system of the Civil Registry with confidentiality, integrity and authenticity should be considered the mission, vision, operational objectives, strategic tactics and processes of the institution. The adoption in a conceptual model of the design of security models and technologies is an alternative to mitigate the security of information. The impact of this research project can have direct or indirect effect for all persons of Ecuadorian or foreign nationality who are registered in the database.

Keyboard: Confidentiality, integrity, authenticity, information security, security models, algorithms and security protocols.

Índice

Índice de Figuras

Glosario de términos

UDI	Unique Identification for Indias
IAAA	Identidad, Autenticación, Autorización, Auditoria
CIA	Confidencialidad, Integridad, Autenticación
HIPAA	Ley de Portabilidad y Contabilidad de Seguros de Salud
CID	Confidencialidad, integridad, disponibilidad
CDIs	Elementos datos restringidos
UDIs	Elementos de datos no restringidos
IVP	Procedimientos de verificación de integridad
TP	Procedimientos de transformación
C	Reglas de certificación
E	Reglas de ejecución
C1	Certificación IVP
C2	Validez
E1	Ejecución de la validez
CW	Clark Wilson

Capítulo I

Introducción

La información que almacena la base de datos del Registro Civil del Ecuador es estratégica en vista, que es donde se genera el documento de identidad que es el documento habilitante para acceder a los servicios públicos y privados. Los problemas que se identifican son de confidencialidad, integridad y autenticidad de la información; entre su problemas podemos encontrar en los subregistro, sobreregistro, adulteración de nacimientos, personas que tienen doble nacionalidad, edades adulteradas, futbolistas con edades falsas, personas con doble registró, entre otros. El Registro Civil es el encargado para la entrega de la información con confidencialidad, integridad y autenticidad en forma directa a las personas ecuatorianas o extranjeros que están registradas en su base de datos y a las instituciones públicas y privadas que requieren de esta información para su gestión.

Con el fin de solucionar este inconveniente el Registro Civil tramitó un crédito ante el Banco Interamericano de Desarrollo (BID) en el años 2004 el mismo que fue aprobado en el año 2010 para realiza el proyecto "Modernization of the National Civil Registration, Identification, and Documentation System" con la premura de solucionar la inconsistencia de la seguridad de la información, el crédito fue tramitado ante el Banco Interamericano de Desarrollo (BID) por 78.000.000,00 (Setenta y ocho millones de dólares americanos 00/100) y realizó un aporte de su presupuesto por $ 15.550.000,00 (Quince millones quinientos cincuenta mil 00/100 dólares americanos) con esta inversión se busca reducir el subregistro tardío de nacimientos, la tasa de identificación civil y la mejora de la calidad y fiabilidad de los registros vitales y documentos de identidad civil. Según la figura1 de la referencia[1].

En la Figura 1-1 se presenta la evidencia de los valores asignados que fueron considerados para iniciar el proyecto de "Modernización del Registro Civil de