PROYECTO DE INVESTIGACIÓN
DATOS INFORMATIVOS

TIPO DE CONVOCATORIA

Proyecto Interno X	Proyecto Semilla ❑	Proyecto Junior ❑	Proyecto Multi e Interdisciplinario ❑

Fecha de presentación (dd/mm/aa): 25/08/2017

Título del proyecto: *(Revisar la guía para la presentación de las propuestas de los proyectos de investigación)*
Diseño de un sistema seguro de gestión de identidades para el registro civil del Ecuador

TIPOS DE INVESTIGACIÓN

Investigación básica ❑ Investigación aplicada X

DEPARTAMENTO(S) Y/O INSTITUCIÓN:
1. DICC
2.

LÍNEA(S) DE INVESTIGACIÓN (verificable en el SAEW):
1. **Seguridad y Privacidad**
2.

RESUMEN DE INFORMACIÓN DEL DIRECTOR Y COLABORADORES

Director

Apellidos y nombres	No. de Cédula	HSS	Departamento	Título de mayor nivel y mención.
Mafla Gallegos Luis Enrique TC	**1000933406**	**10**	**DICC**	**PhD en ciencias de la computación**

Codirector *(Se aplica para todos los proyectos, el codirector será a su vez colaborador)*

Apellidos y nombres	No. de Cédula	HSS	Departamento	Título de mayor nivel y mención.
Gallardo Carrera César Eduardo TC	1705121612	4	DICC	Diplomado Superior en Plataformas Operativas para Internetworking

Colaborador(es)

Apellidos y nombres	No. de Cédula	HSS	Departamento	Título de mayor nivel y mención.

Colaboradores Externos

Apellidos y nombres	No. de identificación	HSS	Institución	Título de mayor nivel y mención.

* HSS = Horas Semana Semestre

PROYECTO DE INVESTIGACIÓN

Proyecto Interno X	Proyecto Semilla ❑	Proyecto Junior ❑	Proyecto Multi e Inter Disciplinario ❑

Investigación Básica ❑	Investigación Aplicada X

DEPARTAMENTO(S) Y/O INSTITUTOS:
1. DICC
2.

LINEA(S) DE INVESTIGACIÓN:
1. **Seguridad y Privacidad**
2.

DISCIPLINA CIENTÍFICA ***(Marque X, solamente una opción)***	
Ciencias Naturales y Exactas	
Ingeniería y Tecnologías	X
Ciencias Médicas	
Ciencias Agrícolas	
Ciencias Sociales	
Humanidades	

OBJETIVO SOCIOECONÓMICO ***(Marque X, solamente una opción)***	
Exploración y explotación del medio terrestre	
Ambiente	
Exploración y explotación del espacio	
Transporte, telecomunicaciones y otras infraestructuras	
Energía	
Producción y tecnología industrial	
Salud	
Agricultura	
Educación	
Cultura, ocio, religión y medios de comunicación	
Sistemas políticos y sociales, estructuras y procesos	X
Defensa	
Avance general del conocimiento: I+D financiada con los Fondos Generales de Universidades (FGU)	
Avance general del conocimiento: I+D financiados con otras fuentes	

1 Proyecto de Investigación

Título:
Diseño de un sistema seguro de gestión de identidades para el registro civil del Ecuador

Resumen del proyecto (máximo 200 palabras)

El principal objetivo del proyecto es el diseño de un sistema seguro para la gestión de las identidades y actos civiles de los ciudadanos ecuatorianos.

El registro de los actos civiles de los ecuatorianos es fundamental para un sinnúmero de actividades, procesos y actos tanto personales como gubernamentales. Dicho registro es utilizado para la identificación, autenticación y autorización de los ciudadanos en todos los trámites y transacciones públicas. El gobierno utiliza el registro civil para la gestión de todas sus políticas y proyectos públicos. Lamentablemente, la Dirección General de Registro Civil, Identificación y Cedulación (DGRCIC) no ha podido implementar un sistema seguro para gestionar las identidades de los ecuatorianos. Los errores, inconsistencias y problemas que tiene el registro civil ecuatoriano son públicos y notorios.

En el proyecto que proponemos, analizaremos los requerimientos legales y tecnológicos para mitigar los mencionados problemas. Durante el proyecto desarrollaremos o adaptaremos algoritmos y protocolos de seguridad informática para garantizar la integridad, confidencialidad y disponibilidad del registro civil.
En el diseño tomaremos en cuenta las experiencias de otros países y de la propia DGRCIC; confiamos que dicho diseño podrá servir para implementar un sistema seguro y confiable.

Palabras clave (4-6): registro civil, gestión de identidades, criptografía, protocolos seguros

2 Objetivos, limitaciones, hipótesis y resultados esperados de esta propuesta de investigación

2.1 Objetivos

2.1.1 Objetivo General

- El principal objetivo del proyecto es el diseño de un sistema seguro y confiable de gestión de las identidades y actos civiles de los ciudadanos ecuatorianos.

2.1.2 Objetivos Específicos

a. Realizar un análisis técnico, científico y objetivo de la calidad de la información del registro civil ecuatoriano
b. Investigar algoritmos y protocolos criptográficos eficientes y seguros para proteger la información del registro civil durante todo su ciclo de vida
c. Diseñar un sistema seguro para gestionar las identidades y actos civiles de los ecuatorianos de una manera confiable y segura.

2.2 Limitaciones (Aspectos que quedan fuera del alcance del Proyecto de Investigación)

a. Implementación de los procedimientos, algoritmos y/o protocolos investigados

2.3 Hipótesis (Responden al problema de investigación)

a. Existen graves problemas de confidencialidad, integridad y disponibilidad en la información de identidad y del registro de los actos y hechos de carácter civil de los ciudadanos ecuatorianos.
b. Dichos problemas pueden ser mitigados con la utilización de algoritmos, protocolos y aplicaciones informáticas basadas en criptografía.

2.3 Detalle de los resultados esperados (con relación a los objetivos)

a. Definición científica del origen, alcance, tipos de los problemas de seguridad que afectan a la información de identidad y registro de los actos y hechos civiles.
b. Diseñar algoritmos, procedimientos y/o aplicaciones que permitan mitigar dichos problemas
c. Diseño formal del sistema seguro para la gestión de identidades y registro civil

3 Relevancia de la propuesta de investigación y su relación con la(s) líneas de investigación

El registro de identidades y actos civiles de los ciudadanos es fundamental para el desarrollo del país. Las implicaciones que tiene la falta de un registro civil confiable son graves; por ejemplo, los errores que contiene el registro civil se propagan al registro electoral, creando serios riesgos para los procesos electorales y para los derechos de elección y participación de los ciudadanos. Sin un registro civil confiable, el gobierno no puede planificar, definir, implementar y control las diferentes políticas públicas en salud, educación, asistencia social, trabajo, etc. A pesar de que la Dirección General de Registro Civil, Identificación y Cedulación ha realizado varios proyectos de modernización, estos no han llegado al núcleo del problema: la base de datos segura y confiable del registro civil.
El proyecto está enmarcado dentro de las dos líneas de investigación definidas para el DICC: "Gestión de Identidades" y "Seguridad en networking". La gestión del registro de los actos civiles de los ciudadanos es, fundamentalmente, un problema de gestión de identidades. Dicha gestión se realiza en las infraestructuras tecnológicas de información y redes de comunicación.

4 Productos esperados

Tipo de Producto:	Marcar con una "X"
a. Publicaciones científicas (obligatorio);	X
b. Disertación a la comunidad politécnica;	X
c. Trabajo de titulación de acuerdo a lo que establece el Reglamento de Régimen Académico y la Normativa Interna de la EPN;	X
d. Aplicación tecnológica construida o implementada;	
e. Patente presentada;	
f. Perfil de proyecto de mayor impacto científico, técnico, pedagógico o de innovación.	

5 Descripción, metodología y diseño del proyecto

5.1 Descripción, metodología y diseño del proyecto (Máximo dos carillas)

Los graves errores e inconsistencias del registro civil del Ecuador son públicos y notorios. Existe una gran demanda informal para alterar los contenidos de dicho registro. Es necesario, por lo tanto, desarrollar un sistema de gestión de identidades y actos civiles de los ciudadanos que sea resistente a los diferentes ataques y amenazas, especialmente a aquellos originados al interior de la DGRCIC.

Existen varios modelos, esquemas y propuestas para sistemas de gestión de identidades para aplicaciones institucionales [13, 14, 15, 16], pero los mismos no escalan eficientemente o no consideran las complejidades relacionadas a la gestión de identidades de los ciudadanos de un país como el nuestro, mismo que tiene flujos

migratorios muy dinámicos, sub registro o sobre registro de actos civiles como nacimientos o defunciones, etc.

Proponemos diseñar un sistema de gestión de identidades ajustado a la normativa vigente, a la realidad migratoria, social y cultural del pais y con los controles tecnológicos, físicos y administrativos que correspondan al nivel de riesgos de la seguridad de la información de registro civil.

5.1.2 Metodologia

Para el desarrollo del proyecto, aplicaremos una metodología sistémica, misma que considera los aspectos legales, tecnológicos, económicos y sociales y consiste de las siguientes fases:

Análisis de la situación actual del registro civil. Algunos problemas del registro civil son bien conocidos y han sido reportados extensivamente en la prensa; por ejemplo, el caso de las alteraciones de las fechas de nacimiento deportistas. Sin embargo, no existen resultados públicos de estudios formales sobre la calidad del registro civil. Realizaremos un control de calidad basado en una muestra estadísticamente representativa del registro civil para conocer con exactitud (estadística) el tipo y la magnitud de los problemas que tiene dicho registro. Para esto utilizaremos herramientas informáticas y estadísticas como las que se exponen en [1, 2, 12].

Análisis de requerimientos. Durante esta fase realizaremos el análisis de requerimientos legales relacionados a la seguridad de la información de registro civil. Tomaremos en cuenta la normativa sobre registro civil, acceso a la información, protección de datos personales, ciberespacio, etc.

Adaptación o desarrollo de algoritmos criptográficos y protocolos seguros de comunicación. Existe una gama extensa de algoritmos criptográficos, protocolos de comunicación y aplicaciones informáticas para proteger la seguridad de la información [4, 9, 10]. Estos algoritmos han sido desarrollados, principalmente, para aplicaciones comerciales que tienen lugar en Internet. Realizaremos un análisis de los mencionados algoritmos y protocolos para determinar su aplicabilidad a la gestión de identidades del registro civil. Trabajaremos en la adaptación o desarrollo de algoritmos y protocolos para que se ajusten a los requerimientos del proyecto.

Existen propuestas que consideran los problemas de seguridad de la información [7, 9, 11] para casos especiales de aplicación institucional. Dichas propuestas serán tomadas en cuenta para analizar su aplicabilidad al problema del proyecto.

Diseño del sistema de gestión de identidades. Para el diseño utilizaremos los principios básicos de diseño de sistemas de gestión de identidades [3, 5, 6], orientados a la solución de los requerimientos legales, tecnológicos, sociales y económicos identificados en las fases anteriores del proyecto.

5.1.3 Diseño del proyecto

Hemos estudiado extensivamente los problemas del registro electoral, mismos que se derivan en gran medida de los problemas que tiene el registro civil. En la metodología propuesta hemos aplicado la experiencia ganada en dichos estudios.

El análisis de calidad del registro electoral lo realizaremos con ayuda de un auxiliar de ciencias de la computación para llevar a cabo el desarrollo del proceso de análisis estadístico y su implementación en el lenguaje de programación estadística R.

El análisis de requerimientos legales, tecnológicos, económicos y sociales lo llevaremos a cabo con asistentes en las áreas correspondientes y en colaboración con los funcionarios del registro civil.

El diseño del sistema de gestión de identidades lo realizará el director del proyecto. Para la ejecución de las pruebas de validación del diseño se contará con la colaboración del auxiliar de ciencias de la computación. Planificamos publicar los resultados del análisis de calidad, adaptación de algoritmos y protocolos y diseño del sistema de gestión de identidades.

Referencias

1. Caffo, B (2016). *Advanced Linear Models for Data Science*. e-book, https://leanpub.com/lm.
2. Caffo, B (2016). *Regression Models for Data Science in R*. e-book, https://leanpub.com/regmods.
3. Dabrowski, M y Pacyna, P (2008). "Modular reference framework architecture for Identity Management," *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on*, Guangzhou, 743-749.
4. Feng, H y Anderson, R y Daugman, J (2006). "Combining Crypto with Biometrics Effectively". *IEEE Transactions on Computers*, 55(9), 1081-1088.

5. Ferdous, M S y Poet, R (2012). "A comparative analysis of Identity Management Systems". *High Performance Computing and Simulation (HPCS), 2012 International Conference on* Madrid. pp. 454-461.
6. Gao, F y Zhang, F y Xia, J y Ma, Z (2016). "General identity management model for big data analysis," *2016 18th International Conference on Advanced Communication Technology (ICACT)*, Pyeongchang, 197-200.
7. Khattak, Z A y Sulaiman, S y Manan, J L A (2010). "A study on threat model for federated identities in federated identity management system," *2010 International Symposium on Information Technology*, Kuala Lumpur, 618-623.
8. Lee, H y Jeun, L y Jung, H (2009). "Criteria for Evaluating the Privacy Protection Level of Identity Management Services". *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, Athens, Glyfada, 155-160.
9. Maarof, A y Senhadji, M y Labbi, Z y Belkasmi, L (2014). "Security analysis of low cost RFID systems". *Codes, Cryptography and Communication Systems (WCCCS), 5th Workshop on*, El Jadida, 11-16.
10. McClure, S y Scambray, J y Kurtz, G. (2012). *Hacking Exposed 7: Network Security Secrets and Solutions*. 7ma Edición. Columbus, E.U.: McGraw-Hill.
11. Ouakasse, F y Rakrak, S (2014). "A new mechanism for RFID clustering and identification," *Codes, Cryptography and Communication Systems (WCCCS), 5th Workshop on*, El Jadida, 6-10.
12. Peng, R (2016). *R Programming for Data Science*. 5ta Edición. e-book, https://leanpub.com/rprogramming.
13. Thakur, M A y Gaikwad, R (2015). "User identity & lifecycle management using LDAP directory server on distributed network," *Pervasive Computing (ICPC), 2015 International Conference on*, Pune, pp. 1-3.
14. Thomas, I y Meinel, C (2009). "Enhancing Claim-Based Identity Management by Adding a Credibility Level to the Notion of Claims," *Services Computing, 2009. SCC '09. IEEE International Conference on*, Bangalore, 243-250.
15. Zhang, Y y Chen, J L (2010). "Universal Identity Management Model Based on Anonymous Credentials," *Services Computing (SCC), 2010 IEEE International Conference on*, Miami, E.U., 305-312.
16. Zhang, Y y Chen, J L (2011). "A Delegation Solution for Universal Identity Management in SOA". *IEEE Transactions on Services Computing*, 4(1), 70-81.

6 Infraestructura, equipos y fondos adicionales.

6.1 Infraestructura y equipos

- *N/A. El investigador utilizará la computadora personal asignada por la EPN.*

Infraestructura	Equipos	
Laboratorio	**Nombre del Equipo**	**Ubicación del Equipo**
		Laboratorio Departamento

6.2 Breve justificación del equipo requerido

- *Justificar la infraestructura y equipos **solicitados** para la ejecución del proyecto e indicar el departamento en el cual se ubicará dicho equipamiento.*

6.3 Fondos Adicionales

- *N/A*

Investigación y Proyección Social

ESCUELA POLITÉCNICA NACIONAL

Proyecto de Investigación Interno

CRONOGRAMA DE ACTIVIDADES DEL PROYECTO

ESCUELA POLITÉCNICA NACIONAL

Título del Proyecto: Diseño de un sistema seguro de gestión de identidades para el Registro Civil del Ecuador

AÑO 1

Nº	Actividad	Presupuesto de la Actividad	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6				Mes 7				Mes 8				Mes 9				Mes 10				Mes 11				Mes 12			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Análisis del problema	$ -																																															
1,1	Recoleción de información y datos																																																
1,2	Analisis de la informacion y datos																																																
2	Adaptación de algoritmos, protocolos y/o aplicaciones	$ -																																															
2,1	Analisis de los algoritmos y protocolos criptográficos relevantes																																																
2,2	Diseño de soluciones criptográficas																																																
3	Diseño del sistema seguro	$ 2.352,00																																															

VICERRECTORADO DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

UNIDAD DE INVESTIGACIÓN

PRESUPUESTO PROYECTOS DE INVESTIGACIÓN

AÑO 1

Director del proyecto	Título del proyecto
Enrique Mafla	Diseño de un sistema seguro de gestión de identidades para el registro civil del Ecuador

	Lista de Items	Cantidad	Unidad	Precio Unitario Referencial	Precio Total Referencial	Precio Unitario Referencial +Aporte IESS	Precio Total Referencial con IVA + Aporte del IESS
1	**Contratación de servicios personales por contrato**						
1.1	Ayudantes de investigación		mes	$ -	$ -	$ -	$ -
1.2	Prestación de servicios profesionales (Homologado Escala de remuneración de servidores publicos)		mes	$ -	$ -	$ -	$ -
	Subtotal 1			$ -	$ -	$ -	$ -
	Lista de Items	**Cantidad**	**Unidad**	**Precio Unitario Referencial sin IVA**	**Precio Total Referencial sin IVA**	**Precio Unitario Referencial con IVA**	**Precio Total Referencial con IVA**
2	**Maquinaria equipos**						
2.1	Item 1 (Detallar nombre de la maquinaria y equipos solicitado)			$ -	$ -	$ -	$ -
2.2	Item 2 (Detallar nombre de la maquinaria y equipos solicitado)			$ -	$ -	$ -	$ -
2.3	Item 3 (Detallar nombre de la maquinaria y equipos solicitado)			$ -	$ -	$ -	$ -
2.4	Item 4 (Detallar nombre de la maquinaria y equipos solicitado)			$ -	$ -	$ -	$ -
2.5	Item 5 (Detallar nombre de la maquinaria y equipos solicitado)			$ -	$ -	$ -	$ -
	Subtotal 2			$ -	$ -	$ -	$ -
3	**Reactivos y materiales de laboratorio**						
3.1	Item 1 (Detallar nombre de los insumos y reactivos)			$ -	$ -	$ -	$ -
3.2	Item 2 (Detallar nombre de los insumos y reactivos)			$ -	$ -	$ -	$ -
3.3	Item 3 (Detallar nombre de los insumos y reactivos)			$ -	$ -	$ -	$ -
3.4	Item 4 (Detallar nombre de los insumos y reactivos)			$ -	$ -	$ -	$ -
3.5	Item 5 (Detallar nombre de los insumos y reactivos)			$ -	$ -	$ -	$ -
	Subtotal 3			$ -	$ -	$ -	$ -
4	**Literatura especializada**						
4.1	Item 1 (Detallar nombre del libro)			$ -	$ -	$ -	$ -
4.2	Item 2 (Detallar nombre del libro)			$ -	$ -	$ -	$ -
4.3	Item 3 (Detallar nombre del libro)			$ -	$ -	$ -	$ -
4.4	Item 4 (Detallar nombre del libro)			$ -	$ -	$ -	$ -
4.5	Item 5 (Detallar nombre del libro)			$ -	$ -	$ -	$ -
	Subtotal 4			$ -	$ -	$ -	$ -
5	**Viajes técnicos y de muestreo**						
5.1	Pasajes al interior			$ -	$ -	$ -	$ -
5.2	Viaticos al interior			$ -	$ -	$ -	$ -
	Subtotal 5			$ -	$ -	$ -	$ -
6	**Presentación de ponencias en congresos internacionales y publicaciones**						
6.1	Pasajes al exterior	1			$ 1.200,00		$ 1.344,00
6.2	Viaticos al exterior	1			$ 400,00	$ -	$ 448,00
6.3	Pago de inscripción y publicaciones				$ 500,00	$ -	$ 560,00
	Subtotal 6			$ -	$ 2.100,00	$ -	$ 2.352,00
	TOTAL				$ 2.100,00		$ 2.352,00

VICERRECTORADO DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

UNIDAD DE INVESTIGACIÓN

PRESUPUESTO PROYECTOS DE INVESTIGACIÓN

Director del proyecto	Título del proyecto
Enrique Mafla	Diseño de un sistema seguro de gestión de identidades para el registro civil del Ecuador

Presupuesto consolidado sin IVA

AÑO	Contratación de servicios personales por contrato	Maquinaria y equipo	Reactivos y materiales de laboratorio	Literatura especializada	Viajes técnicos y de muestreo	Presentación de ponencias en congresos intrenacionales y publicaciones	Total sin IVA
1	$ -	$ -	$ -	$ -	$ -	$ 2.100,00	$ 2.100,00
2	$ -	$ -	$ -	$ -	$ -	$ -	$ -
3	$ -	$ -	$ -	$ -	$ -	$ -	$ -
TOTAL	$ -	$ -	$ -	$ -	$ -	$ 2.100,00	$ 2.100,00

Presupuesto consolidado con IVA

AÑO	Contratación de servicios personales por contrato	Maquinaria y equipo	Reactivos y materiales de laboratorio	Literatura especializada	Viajes técnicos y de muestreo	Presentación de ponencias en congresos intrenacionales y publicaciones	Total con IVA
1	$ -	$ -	$ -	$ -	$ -	$ 2.352,00	$ 2.352,00
2	$ -	$ -	$ -	$ -	$ -	$ -	$ -
3	$ -	$ -	$ -	$ -	$ -	$ -	$ -
TOTAL	$ -	$ -	$ -	$ -	$ -	$ 2.352,00	$ 2.352,00

DECLARACIÓN FINAL

TIPO DE PROYECTO

Proyecto Interno X Proyecto Semilla ❑ Proyecto Junior ❑ Proyecto Multi e Interdisciplinario ❑

TIPO DE INVESTIGACIÓN

Investigación básica ❑ Investigación aplicada X

TÍTULO DEL PROYECTO

Diseño de un sistema seguro de gestión de identidades para el registro civil del Ecuador

DECLARACIÓN DEL DIRECTOR DEL PROYECTO

El equipo de investigadores, representado por el Director del Proyecto declara lo siguiente:

- Que el presente proyecto es una obra original de este equipo de investigadores y por tanto, asumimos la completa responsabilidad legal en caso de que un tercero alegue la titularidad de los derechos intelectuales del proyecto, exonerando a la EPN de cualquier acción legal que se derive por esta causa.
- Que el presente proyecto no ha sido presentado en ninguna convocatoria de otra institución pública o privada solicitando el financiamiento total del presupuesto. El incumplimiento será causal para que el proyecto no sea tomado en consideración.
- Que, todos los bienes adquiridos en el proyecto permanecerán bajo la custodia y responsabilidad del director de proyecto.
- Que, aceptamos que si el proyecto genera algún producto o procedimiento susceptible de obtener de derechos de propiedad intelectual, de los cuales se deriven beneficios, estos serán compartidos entre los investigadores y las instituciones participantes en el proyecto.

Firma del Director del Proyecto
Nombre: Enrique Mafla
C.I.: 1000933406

DECLARACIÓN DEL JEFE DE DEPARTAMENTO

Esta propuesta ha sido aprobada y avalada por el Consejo del Departamento de Informática y Ciencias de la Computación, en sesión del día 29 de agosto de 2017 mediante resolución No. 118.032.29-08-2017.

Las instalaciones, incluyendo personal, edificios, equipo y recursos financieros están a disposición del proponente y sus colaboradores de acuerdo con las especificaciones que se encuentran en esta propuesta.

Firma del Jefe del Departamento
Nombre: MSc. Myriam Guadalupe Peñafiel Aguilar
C.I.: 1705828711

ESCUELA POLITECNICA NACIONAL
DEPARTAMENTO DE INFORMATICA Y CIENCIAS DE LA COMPUTACION
DICC
Quito