PTI-15

ESCUELA POLITÉCNICA NACIONAL
VICERRECTORADO DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

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: **"Detección de Ransomware a gran escala por medio de seguridad cognitiva"**

TIPOS DE INVESTIGACIÓN

Investigación básica ☐ Investigación aplicada ☐X

DEPARTAMENTO(S) Y/O INSTITUCIÓN:
1. INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN
2.

LÍNEA(S) DE INVESTIGACIÓN (verificable en el SAEW):
1. DICC-A2-L2: Seguridad y Privacidad
2. DICC-A1-L2: Machine learning

RESUMEN DE INFORMACIÓN DEL DIRECTOR Y COLABORADORES

Director

Apellidos y nombres	No. de Cédula	HSS	Departamento	Título de mayor nivel y mención.
Hernández Álvarez Myriam Beatriz	1705009304	**6**	Informática y Ciencias de la Computación	Doctora en Aplicaciones de la Informática

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.
Yoo Sang Guun	1306853720	4	Informática y Ciencias de la Computación	Ph.D. in Computer Science and Engineering

Colaborador(es)

Apellidos y nombres	No. de Cédula	HSS	Departamento	Título de mayor nivel y mención.
Herrera Silva Juan Alberto	1709122889	6	Informática y Ciencias de la Computación	Magister en Ingeniería Eléctrica – Mención en Conectividad y Redes de Telecomunicaciones, M.Sc.

Colaboradores Externos

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

* HSS = Horas Semana Semestre

HOJA DE VIDA DEL DIRECTOR DEL PROYECTO

Datos Personales					
Nombre completo:	**Hernández Álvarez Myriam Beatriz**				
No. de identificación:	1705009304	**Nacionalidad:**	Ecuatoriana		
Fecha de nacimiento:	21/07/2017	**Celular:**	0992715620	**Ext. EPN:**	4700
Correo institucional:	myriam.hernandez@epn.edu.ec				
Cargo actual en la EPN:	Profesor Principal				
Facultad:	Ingeniería en Sistemas				
Departamento:	Informática y Ciencias de la Computación				

Educación universitaria. Proveer el nombre de los títulos de pregrado y postgrado (Ing., M.Sc., Ph.D.)				
Título	**Año**	**Institución/Universidad**	**Ciudad/ País**	**Área o línea de investigación de la tesis**
Doctora en Aplicaciones de la Informática	2015	Universidad de Alicante	España	Sistemas Inteligentes
Especialista Superior en Dirección de Empresas Mención Mercadeo	2002	Universidad Andina Simón Bolívar	Ecuador	N/A
Magister en Ciencias	1987	The Ohio University	Estados Unidos	Ciencias de la Computación
Ingeniería en Electrónica y Telecomunicaciones	1982	Escuela Politécnica Nacional	Ecuador	Microprocesadores

Experiencia investigativa y en ejecución de proyectos (cite los tres más relevantes)		
Año	**Título del proyecto**	**Cargo /Actividades realizadas**
2010	Estudio de acuíferos utilizando técnicas de teledetección y procesamiento digital	Director
2015	Uso de aprendizaje automático en el análisis de citas bibliográficas	Director
2016	Propuesta de valoración del impacto para citas bibliográficas tomando en cuenta criterios cualitativos	Director

Publicaciones, patentes, prototipos o productos (cite las más relevantes dentro de los últimos cinco años y que se encuentren alineados al proyecto de investigación)	
1.	HERNÁNDEZ-ALVAREZ, MYRIAM, & GOMEZ, J.M. (2016). Survey about citation context analysis : Tasks, techniques, and resources. *Natural Language Engineering*, 22(03), 327-349
2.	Hernández-Alvarez, MY., & Gómez, J.M. (2015, October). Citation Impact Categorization: For Scientific Literature. *In Computatonal Science and Engineering (CSE)*. 2015 IEEE 18th *International Conference on* (pp. 307-313). IEEE.
3.	Hernández-Alvarez, MY., & Gómez Soriano, J.M. (2015). Esquema de anotación para categorización de citas en bibliografía científica

4.	Hernández, N.B., & Gómez, J.M. (2014). Análisis de Sentimientos Aplicado a Referencias Bibliográficas. *Revista Politécnica,* 33(1)
5.	Hernández, N.B., & Gómez, J.M. (2013). Aplicaciones de Procesamiento de Lenguaje Natural. *Revista Politécnica,* 32

Experiencia profesional, otros trabajos científicos y técnicos (cite lo más relevante o las más recientes)

Hernández, M., & Gómez, J. M. (2014, June). Survey in sentiment, polarity and function analysis of citation. In Proceedings of the First Workshop on Argumentation Mining ACL (pp. 102-3).

Álvarez, M. H., & Soriano, J. G. Corpus annotation methodology for citation classification in scientific literature. Processing in the 5th Information Systems Research Working Days (JISIC 2014), 7.

HERNÁNDEZ-ALVAREZ, MYRIAM. (2015). Concit-Corpus: Análisis de contexto de citas para detectar Función, Polaridad e Influencia. In Actas del XXXI Congreso de la Sociedad Española para el Procesamiento del Lenguaje Natural ISBN (Vol. 978, pp. 84-608).

Hernández-Álvarez, M., Gómez Soriano, J., & Martínez-Barco, P. (2016). Annotated Corpus for Citation Context Analysis. Latin American Journal of Computing Faculty of Systems Engineering National Polytechnic School Quito-Ecuador, 3(1), 35-42.

DIRECTORA DEL PROGRAMA DOCTORAL EN INFORMÁTICA, FIS. EPN, MARZO 2016-PRESENTE FECHA

DECANA FACULTAD DE INGENIERIA DE SISTEMAS. DICIEMBRE 2013–PRESENTE FECHA

HOJA DE VIDA DEL CODIRECTOR DEL PROYECTO

Datos Personales					
Nombre completo:	Sang Guun Yoo				
No. de identificación:	1306853720	**Nacionalidad:**	Corea del Sur		
Fecha de nacimiento:	2 de octubre de 1978	**Celular:**	0999496897	**Ext. EPN:**	4708
Correo institucional:	sang.yoo@epn.edu.ec				
Cargo actual en la EPN:	Profesor titular agregado nivel 1 grado 3 - tiempo completo				
Facultad:	Facultad de Ingeniería de Sistemas				
Departamento:	Departamento de Informática y Ciencias de la Computación				

Educación universitaria. Proveer el nombre de los títulos de pregrado y postgrado (Ing., M.Sc., Ph.D.)

Título	Año	Institución/Universidad	Ciudad/País	Área o línea de investigación de la tesis
Ing.	2002	Escuela Politécnica del Ejército	Sangolquí/ Ecuador	Comunicaciones y Seguridades
M.S.	2010	Sogang University	Seúl/Corea del Sur	Comunicaciones y Seguridades
Ph.D.	2013	Sogang University	Seúl/Corea del Sur	Comunicaciones y Seguridades

Experiencia investigativa y en ejecución de proyectos (cite los tres más relevantes)

Año	Título del proyecto	Cargo /Actividades realizadas
2016 - 2017	Mecanismos de Autenticación para Redes de Sensores Inalámbricos orientados a Servicios de Salud	Director / Dirección y ejecución del proyecto
2009 - 2010	Trusted Execution Environment (Proyecto con Samsung Electronics en Corea del Sur)	Director e investigador / Dirección y ejecución del proyecto

2008-2009	Sistema de seguridad para plataforma Baseband (Proyecto con Samsung Electronics en Corea del Sur)	Director e investigador / Dirección y ejecución del proyecto

Publicaciones, patentes, prototipos o productos (cite las más relevantes dentro de los últimos cinco años y que se encuentren alineados al proyecto de investigación)	
1.	S. Yoo. (2017). 5G-VRSec: Secure Video Reporting Service in 5G Enabled Vehicular Networks. *Wireless Communication and Mobile Computing*. Vol. 2017, Article ID 7256307 (JCR y Scopus/Scimago Q2)
2.	S. Yoo, J. Barriga. (2017). Privacy-aware User Authentication System for Indoor Positioning System. *Communications in Computer and Information Science*. CCIS 719, pp. 201-213 (Scopus)
3.	S. Kim, S. Yoo, J. Kim. (2017). Privacy Protection Mechanism for Indoor Positioning Systems. *International Journal of Applied Engineering Research*. Vol. 12, Number 9, pp. 1082-1086 (Scopus)
4.	X. Campaña, R. Arroyo, S. Yoo. (2017). Experience in Applying Data Mining Techniques to Musical Content Database to Identify Personality Traits. *International Journal of Applied Engineering Research*. Vol 12, Number 12, pp. 3298-3304 (Scopus)
5.	S. Yoo, J. Kim. (2017). IT-Dependent Strategic Initiative to Increase the Marketing Performance of Mobile Security Solutions. *International Journal of Applied Engineering Research*. Vol. 12, Number 6, pp. 1084-1092 (Scopus)
6.	S. Yoo. (2016). Cryptanalysis of Several Authentication Schemes for Healthcare Applications using Wireless Medical Sensor Networks. Proceedings of the Fifth International Conference on Network, Communication and Computing. pp. 282-286 (Scopus)
7.	S. Yoo, F. Castro. (2016). Enhanced BSN-Care: Cryptanalysis of BSN-Care and Proposal of Improved Authentication System. Proceedings of 2016 IEEE International Symposium on Robotics and Intelligent Sensors. (Scopus)
8.	S. Yoo. (2016). E-SAS: Enhanced Secure Authentication System for Healthcare Applications using Wireless Medical Sensor Networks. *WSEAS Transactions on Systems*. Vol. 15, pp. 309-320.
9.	S. Yoo, S. Kang, J. Kim. (2014). SERA: A Secure Energy-Reliability Aware Data Gathering for Sensor Networks. *Multimedia Tools and Applications*. Vol. 73, Issue 2, pp. 617-646, November, 2014. (JCR y Scopus/Scimago Q1 en Media Technology y Q2 en Computer Networks and Communications)
10.	S. Yoo, H. Lee, J. Kim. (2013). A Performance and Usability Aware Secure Two-Factor User Authentication Scheme for Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*. Vol. 2013, Article 543950 (JCR y Scopus/Scimago Q2 en Engineering y SJR Q3 en Computer Networks and Communications)
11.	S. Kang, K. Park, S. Yoo, J. Kim. (2013). DDoS avoidance strategy for service availability. *Cluster Computing*. Vol. 16, Issue 2, pp. 241-248. (JCR y Scopus/Scimago Q2 en Computer Networks and Communications)

Experiencia profesional, otros trabajos científicos y técnicos (cite lo más relevante o las más recientes)

1) Mayo 2017 – Presente:
- **Institución:** Escuela Politécnica Nacional (Quito, Ecuador)
- **Cargo:** Docente Investigador

2) Agosto 2016 – Presente:
- **Institución:** Universidad de las Fuerzas Armadas ESPE (Sangolquí, Ecuador)
- **Cargo:** Docente Investigador

3) Diciembre 2007 – Julio 2016
- **Institución:** CAD & Security Lab. de Sogang University (Seúl, Corea del Sur)
- **Cargo:** Investigador y personal académico

4) Marzo 2014 – Julio 2014:
- **Institución:** LG Electronics (Seúl, Corea del Sur)

- **Cargo:** Chief Research Engineer

5) Septiembre 2011 – Marzo 2012
- **Institución:** SICA: Sistema de la Integración Centroamericana (San Salvador, El Salvador)
- **Cargo:** Becario del Ministerio de Asuntos Exteriores y Comercio de Corea en SICA

6) Octubre 2005 – Julio 2007
- **Institución:** Universidad Internacional del Ecuador (Quito, Ecuador)
- **Cargo:** Docente

7) Mayo 2006 – Junio 2007:
- **Institución:** Dirección de Inteligencia del Ejército (Quito, Ecuador)
- **Cargo:** Asesor tecnológico

8) Agosto 2001- Mayo 2006
- **Institución:** Extremosoftware S.A. (Microsoft Gold Certified Partner) (Quito, Ecuador)
- **Cargo:** Gerente del departamento de tecnología y co-fundador

HOJA DE VIDA DEL COLABORADOR DEL PROYECTO

Datos Personales					
Nombre completo:	**Herrera Silva Juan Alberto**				
No. de identificación:	1709122889	**Nacionalidad:**	Ecuatoriana		
Fecha de nacimiento:	25/01/1971	**Celular:**	0996021505	**Ext. EPN:**	
Correo institucional:	juan.herrera@epn.edu.ec				
Cargo actual en la EPN:	Profesor Principal a Tiempo Parcial (Doctorante en Programa de Doctorado en Informática – Seguridad Informática – Fase Investigación – Tesis Doctoral)				
Facultad:	Ingeniería en Sistemas				
Departamento:	Informática y Ciencias de la Computación				

Educación universitaria. Proveer el nombre de los títulos de pregrado y postgrado (Ing., M.Sc., Ph.D.)				
Título	**Año**	**Institución/Universidad**	**Ciudad/País**	**Área o línea de investigación de la tesis**
Magister en Ingeniería Eléctrica con mención en Conectividad y Redes de Telecomunicaciones	2006	ESCUELA POLITÉCNICA NACIONAL	QUITO-ECUADOR	Ingeniería Eléctrica, Conectividad y Redes de Telecomunicaciones
Diplomado Superior en Plataformas Operativas para Internetworking	2004	ESCUELA POLITÉCNICA NACIONAL	QUITO-ECUADOR	Plataformas Operativos para Internetworking
Ingeniero de Sistemas de Computación e Informática	1996	ESCUELA POLITÉCNICA NACIONAL	QUITO-ECUADOR	Computación e Informática

Experiencia investigativa y en ejecución de proyectos (cite los tres más relevantes)		
Año	**Título del proyecto**	**Cargo /Actividades realizadas**

Publicaciones, patentes, prototipos o productos (cite las más relevantes dentro de los últimos cinco años y que se encuentren alineados al proyecto de investigación)	
1.	Seguridad en la Nube - El Comercio – SEGURINFO 2011- 07/2011- Quito
2.	Auditoría y Seguridad de Sistemas de Información en la Nube - Jornadas de Sistemas JISIC 2014 - 11/2014 – Quito
3.	
4.	
5.	

Experiencia profesional, otros trabajos científicos y técnicos (cite lo más relevante o las más recientes)

Responsable líder de servicios de Auditoría Informática y Consultoría en Seguridad de la Información, Ethical Hacking, Gestión de TI y Riesgos Tecnológicos.

- *Tiene 20 años de experiencia en Auditoría Informática y Seguridad de la Información, en importantes empresas nacionales y multinacionales de los sectores bancario, manufacturero, comercial y servicios.*
- *Actualmente está cursando el Doctorado en "Seguridad Informática" en la EPN-FIS.*
- *Es MSc. en Ingeniería Eléctrica con mención en Conectividad y Redes de Telecomunicaciones.*
- *Certificación como Auditor Líder en Sistemas de Gestión de Seguridad ISO 27001*
- *Posee Certificación COBIT 5 Foundation y Ciberseguridad Fundamentos (CSXF)*
- *Formación PMP y en Pruebas de Calidad de Software (ISTQB)*
- *Obtuvo en el 2005 el Certified Information System Auditor, CISA y en el 2011 el Certified Risk Information System and Control, CRISC, dados por ISACA Internacional.*
- *Trabajó por 5 años en Deloitte como Auditor Informático y Consultor de Riesgo Empresarial.*
- *Es especialista en gestión y seguridades de plataformas tecnológicas y Ethical Hacking.*
- *Posee un Diplomado Superior en Plataformas Operativas para Internetworking.*
- *Es Ingeniero de Sistemas graduado en la Escuela Politécnica Nacional.*
- *Profesor Principal a Tiempo Parcial de la Escuela Politécnica Nacional y ex-Presidente miembro fundador del Capítulo Quito, Ecuador - Information Systems Audit and Control Association (ISACA).*
- *Es Microsoft Certified Systems Administrator en ambientes de Redes Windows Server 2000, MCSA.*

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. INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN
2.

LINEA(S) DE INVESTIGACIÓN:
1. DICC-A2-L2: Seguridad y Privacidad
2. DICC-A1-L2: Machine learning

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	
Defensa	
Avance general del conocimiento: I+D financiada con los Fondos Generales de Universidades (FGU)	X
Avance general del conocimiento: I+D financiados con otras fuentes	

1 Proyecto de Investigación

Título: "Detección de Ransomware a gran escala por medio de seguridad cognitiva"

Resumen del proyecto (máximo 200 palabras)

Los ataques de Ransomware están aumentando cada día. Este tipo de subprocesos explota las vulnerabilidades del sistema, especialmente aquellas que tienen una base en MS-Windows. A partir de mayo de 2017, millones de computadoras de todo el mundo experimentaron este virus. Por esta razón, la necesidad de crear diferentes mecanismos que actúen de manera proactiva, para evitar altos niveles de propagación. La investigación propuesta creará un modelo para la detección y prevención de ransomware.

Se analizarán los datos no estructurados almacenados en los registros del EcuCERT (Centro de Respuesta a Incidentes Informáticos del Ecuador). Con esta información, se creará un corpus que contenga atributos o características necesarias para detectar patrones de comportamiento de las principales vulnerabilidades relacionadas con ransomware, que se encuentran en Microsoft Windows Systems.

Se utilizarán métodos para selección de variables relevantes dentro de logs para decidir qué características representan mejor a los datos que configuran la amenaza. Estas variables conformarán el corpus y serán entrada de algoritmos de aprendizaje automático. Los algoritmos modelarán patrones que servirán para detectar tempranamente el ransomware, antes de secuestren los datos.

Finalmente se realizará un reporte del rendimiento de los modelos obtenidos en la detección de la amenaza.

Palabras clave (4-6):

Classification, data mining, logs, Machine Learning, Ransomware.

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

2.1 Objetivos

2.1.1 Objetivo General

- Diseñar un modelo de detección y prevención de Ransomware, mediante la identificación de patrones y comportamientos sospechosos a través de herramientas que interpretan, aprenden y procesan la inteligencia de seguridad.

a.1.2 Objetivos Específicos

a. Recolectar datos a gran escala estructurados y no estructurados para analizar su comportamiento utilizando algoritmos de aprendizaje automático.

b. Evaluar los patrones de comportamiento de Ransomware en grandes volúmenes de datos del EcuCERT (Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de Telecomunicaciones del Ecuador) y su impacto en las organizaciones públicas.

c. Utilizar algoritmos de aprendizaje automático para desarrollar un nuevo modelo de detección y prevención que brinde seguridad informática a las instituciones públicas.

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

a. Diseño y desarrollo y de nuevos algoritmos y modelos matemáticos para detección de ransomware
b. Detección y prevención de cualquier otro tipo de malware que no sea ransomware

2.3 Hipótesis (Responden al problema de investigación)

¿Es posible desarrollar modelos de detección y prevención de Ransomware mediante la identificación de tendencias basadas en patrones de comportamiento detectados y la aplicación de técnicas de aprendizaje automático sobre la información histórica de incidentes en logs obtenidos de EcuCERT durante los últimos tres años?

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

Actualmente, los datos de ECUCERT (Centro de Respuesta a Incidentes Informáticos de la Agencia Reguladora y de Control de Telecomunicaciones de Ecuador) tienen alertas reactivas a incidentes de seguridad causados por diversas amenazas a la seguridad de la información. Sin embargo, no tiene metodologías para la detección y prevención de Ransomware en sus registros (grandes volúmenes de datos ECUCERT), por lo que la investigación contribuirá con modelos para hacerlo.

Para ello, teniendo en cuenta los últimos ataques de ransomware causados por Petya y WannaCry, se identificarán las vulnerabilidades más significativas que actúan sobre los sistemas Windows y así prevenir el ataque de los ransomware.

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

El definir y establecer patrones de comportamiento de secuestros digitales en grandes volúmenes de datos del ECUCERT (Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador), permitirá anticiparse a temas de secuestros digitales y fraude, mediante el análisis de riesgos y su impacto en las organizaciones.

Además, la identificación de estos patrones de comportamiento de secuestros digitales permitirá a los entes de control establecer mecanismos de monitoreo y cumplimiento apegados al marco regulatorio de las Telecomunicaciones dado por la ARCOTEL del Ecuador, que específicamente aún no ha desarrollado específicamente este tema de Ciberseguridad para el sector público.

4 Productos esperados

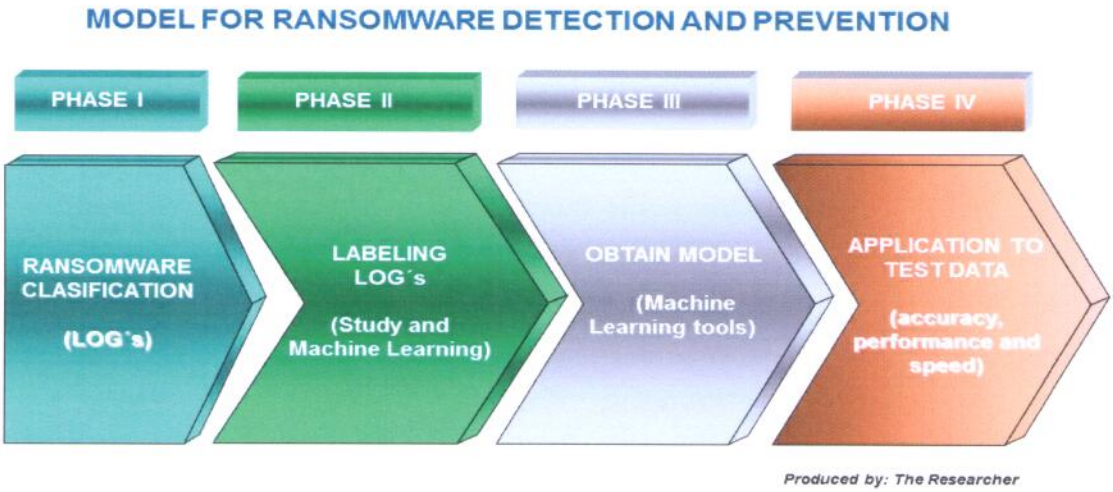
Tipo de Producto:	Marcar con una "X"
a. Publicaciones científicas (obligatorio);	X
b. Disertación a la comunidad politécnica;	
c. Trabajo de titulación de acuerdo a lo que establece el Reglamento de Régimen Académico y la Normativa Interna de la EPN;	
d. Aplicación tecnológica construida o implementada;	X
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)

El presente Proyecto Interno de Investigación será realizado principalmente por el M.Sc. Juan Herrera en su calidad de Doctorante dentro del Programa de Doctorado en Informática, especialización Seguridad Informática, ya que actualmente se encuentra en la Fase de Investigación para su Tesis Doctoral.

Esta propuesta presenta una solución al problema actual de crear un modelo para la detección de Ransomware y la prevención utilizando algoritmos de aprendizaje de máquina. Este trabajo aplicó un gran volumen de información para analizar datos estructurados y no estructurados. Se creará un corpus recopilando datos de los registros de EcuCERT para estudiar el comportamiento de las amenazas. Se expondrá la recomendación para detectar ransomware por adelantado antes de que tengan tiempo para dañar la información del usuario. Así, el proyecto integrará paradigmas cualitativos y cuantitativos. El modelo propuesto para la detección y prevención de Ransomware se basa en lo siguiente:



Para el efecto se revisará la diferente documentación relacionada con fraude y ransomware en el sector público - telemática del Ecuador en los últimos 3 años y adicionalmente, se realizarán relevamientos con responsables de las áreas de Riesgo y Seguridad de Información de la agencia de regulación y control de telecomunicaciones del Ecuador.

Se utilizará el muestreo estadístico para la selección de las instituciones públicas que usan telemática a considerar para el estudio de investigación doctoral y se revisará la información relacionada con marcos de referencia para Gestión de Riesgos como la ISO 31000 y 27005 específicamente enfocados con temas de riesgos aplicados a la seguridad de la información y se evaluará las diferentes técnicas de análisis de riesgo con su aplicación en Seguridad Cognitiva.

Se utilizará herramientas de análisis en big data con aplicación de máquinas de aprendizaje a fin de identificar patrones de comportamiento del Ransomware antes de su ataque a las redes públicas y se realizará el desarrollo de una aplicación práctica.

Complementariamente, se analizará el alcance del marco regulatorio para instituciones públicas que usan la telemática a fin de ver su aplicabilidad y se revisará bibliografía (papers, books, etc.) y toda fuente de información relacionada con las temáticas de Detección de Ransomware, Gestión de Riesgo y Seguridad Cognitiva de los últimos 3 años.

6 Infraestructura, equipos y fondos adicionales.

6.1 Infraestructura y equipos

- *Indicar la infraestructura y equipos **disponibles** para la ejecución del proyecto, con la ubicación actual de los mismos*

Infraestructura	Equipos	
Laboratorio	**Nombre del Equipo**	**Ubicación del Equipo**
EPSILON - DOCTORADO	EPS-01	Laboratorio EPSILON-DOCTORADO, Departamento Informática y Ciencias de la Computación
EPSILON - DOCTORADO	EPS-02	Laboratorio EPSILON-DOCTORADO, Departamento Informática y Ciencias de la Computación

6.2 Breve justificación del equipo requerido

- *Equipos necesarios para la investigación y revisión de LOGs a gran escala, así como para utilización de herramientas como WEKA*

6.3 Fondos Adicionales

- *NO APLICA*

Investigación y Proyección Social

ESCUELA POLITÉCNICA NACIONAL

Proyecto de Investigación Interno

CRONOGRAMA DE ACTIVIDADES DEL PROYECTO

ESCUELA POLITÉCNICA NACIONAL

Título del Proyecto: "Detección de Ransomware a gran escala por medio de seguridad cognitiva"

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	**Objetivo específico 1: Recolectar datos a gran escala estructurados y no estructurados para analizar su comportamiento utilizando algoritmos de aprendizaje automático.**	$ -	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X																																
1,1	Revisión del Estado del Arte		X	X	X	X	X	X	X	X	X	X	X	X																																				
1,2	Investigación						X	X	X	X	X	X	X	X																																				
1,3	Experimentación									X	X	X	X	X	X	X	X	X																																
2	**Objetivo específico 2: Evaluar los patrones de comportamiento de Ransomware en grandes volúmenes de datos del EcuCERT (Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de Telecomunicaciones del Ecuador) y su impacto en las organizaciones públicas.**	$ 330,40													X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
2,1	Investigación	$ 330,40													X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
2,2	Experimentación														X	X	X	X	X	X	X	X	X	X	X	X																							
3	**Objetivo específico 3: Utilizar algoritmos de aprendizaje automático para desarrollar un nuevo modelo de detección y prevención que brinde seguridad informática a las instituciones públicas.**	$ 1.308,13																	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X										
3,1	Manejo de Herramientas de Data Mining	$ 1.308,13																	X	X	X	X	X	X	X	X	X	X	X	X																			
3,2	Generación de aplicación para detección de ransonware	$ -																					X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X										
4	**Producto esperado:**	$ 3.360,00																									X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4,1	Elaboración de Paper para Publicación	$ 360,00																									X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
4,2	Presentación de Paper en Conferencia Internacional	$ 3.000,00																																									X	X	X	X	X	X	X	X
		$ 4.998,53																																															

VICERRECTORADO DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

DIRECCIÓN DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

PRESUPUESTO PROYECTOS DE INVESTIGACIÓN

AÑO 1

Director del proyecto	Título del proyecto
Dra. Myriam Hernández	"Detección de Ransomware a gran escala por medio de seguridad cognitiva"

	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
1	**Contratación de servicios personales por contrato**						
1.1	Ayudantes de investigación ($ 366 + 9,15%IESS)	3	mes	$ 399,49	$ 1.198,47	$ 436,04	$ 1.308,13
1.2	Prestación de servicios profesionales (Homologado Escala de remuneración de servidores publicos)		mes	$ -	$ -	$ -	$ -
	Subtotal 1			**$ 399,49**	**$ 1.198,47**	**$ 436,04**	**$ 1.308,13**
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	1		$ 190,00	$ 190,00	$ 212,80	$ 212,80
5.2	Viaticos al interior	1		$ 105,00	$ 105,00	$ 117,60	$ 117,60
	Subtotal 5			**$ 295,00**	**$ 295,00**	**$ 330,40**	**$ 330,40**
6	**Presentación de ponencias en congresos internacionales y publicaciones**						
6.1	Pasajes al exterior	1		$ 1.500,00	$ 1.500,00	$ 1.680,00	$ 1.680,00
6.2	Viaticos al exterior	1		$ 1.200,00	$ 1.200,00	$ 1.344,00	$ 1.344,00
6.3	Pago de inscripción y publicaciones	1		$ 300,00	$ 300,00	$ 336,00	$ 336,00
	Subtotal 6			**$ 3.000,00**	**$ 3.000,00**	**$ 3.360,00**	**$ 3.360,00**
	TOTAL				**$ 4.493,47**		**$ 4.998,53**

VICERRECTORADO DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

DIRECCIÓN DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

PRESUPUESTO PROYECTOS DE INVESTIGACIÓN

Director del proyecto	Título del proyecto
Dra. Myriam Hernández	"Detección de Ransomware a gran escala por medio de seguridad cognitiva"

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	$ 1.198,47	$ -	$ -	$ -	$ 295,00	$ 3.000,00	$ 4.493,47
2	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!
3	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!
TOTAL	**#¡REF!**	**#¡REF!**	**#¡REF!**	**#¡REF!**	**#¡REF!**	**#¡REF!**	**#¡REF!**

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	$ 1.308,13	$ -	$ -	$ -	$ 330,40	$ 3.360,00	$ 4.998,53
2	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!
3	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!	#¡REF!
TOTAL	**#¡REF!**	**#¡REF!**	**#¡REF!**	**#¡REF!**	**#¡REF!**	**#¡REF!**	**#¡REF!**

Firma

Nombre del director del proyecto

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

"Detección de Ransomware a gran escala por medio de seguridad cognitiva"

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: Dra. Myriam Hernández
C.I.: 1705009304

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. 122.032.29-08-2017

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 Peñafiel Aguilar
C.I.: 1705828711

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