ESCUELA POLITÉCNICA NACIONAL
VICERECTORADO DE INVESTIGACIÓN Y EXTENSIÓN

PROYECTOS DE INVESTIGACIÓN: Multidisciplinario

Área del proyecto: Ciencias Básicas ☐ Ciencias Aplicadas ☒

FACULTAD: Ingeniería Eléctrica y Electrónica - FIEE

DEPARTAMENTO: Electrónica, Telecomunicaciones y Redes de Información - DETRI

LINEA DE INVESTIGACIÓN: Sistemas de Seguridades

1 **Proyecto de Investigación**

Título:

Desarrollo de Prototipos para la Investigación en Seguridad de la Información

Resumen del proyecto (máximo 200 palabras)

La información es actualmente uno de los activos más importantes para cualquier institución. Sin embargo, debe almacenarse y transportarse utilizando múltiples protocolos, tecnologías, dispositivos, redes y aplicaciones, que pueden tener errores y son inherentemente vulnerables.
Aunque la información siempre ha sido crítica, recién ahora puede estar en todos lados gracias al Internet y a la masificación de su uso. Como es de esperarse, además, esta información se genera en todo proceso, mucho más si es tecnológico, y la tecnología abarca un espectro sumamente amplio de estudio.
La seguridad de la información comprende temas referentes a las amenazas, vulnerabilidades y riesgos vinculados a la infraestructura, los servicios y las aplicaciones que procesan datos, así como los mecanismos para prevenir y protegerse frente a posibles ataques.
La seguridad es, consecuentemente, transversal a muchas disciplinas y carreras, cuando en sus aplicaciones se utiliza información sensible.
Este proyecto propone desarrollar prototipos de laboratorio y documentación didáctica, que impulsen la investigación y la difusión en aspectos relacionados con la Seguridad de la Información, tanto en la EPN como en el país.
Se pretende recrear distintos entornos de redes telemáticas donde la información pueda ser vulnerada y los sistemas atacados, con el fin de desagregar estos ataques y poder realizar una evaluación y pruebas sobre infraestructuras no críticas.
Para justificar en nuestro entorno la investigación en Seguridad de la Información, se plantea además la recopilación de estadísticas relacionadas con la seguridad y las vulnerabilidades en nuestro país, a través de la cooperación con entidades externas y la implementación de herramientas de monitoreo.

Palabras clave (3-5): seguridad, información, marco regulatorio, vulnerabilidades, prototipos

4	**Objetivos, hipótesis y resultados esperados de esta propuesta de investigación**

Objetivo General

Desarrollar prototipos para la investigación en seguridad de la información en el Ecuador

Objetivos específicos

- Generar, recopilar y analizar estadísticas relacionadas con vulnerabilidades y ataques a la seguridad de la información en el Ecuador.
- Colaborar con al menos dos instituciones para la obtención de muestras que permitan investigar las principales vulnerabilidades en las redes telemáticas de nuestro país.
- Desarrollar prototipos de laboratorio para la investigación en seguridad informática y en redes de telecomunicaciones.
- Analizar las necesidades del marco regulatorio del país con relación a la seguridad de la información.
- Elaborar material didáctico de apoyo que incentive y facilite el tratamiento de temas de seguridad de la información a nivel de pregrado y postgrado.
- Difundir los conocimientos adquiridos durante el desarrollo de la investigación mediante cursos, seminarios y conferencias.

Resultados y productos esperados

- Estadísticas que permitan tener una idea de las vulnerabilidades y ataques a la seguridad de la información en el país.
- Una infraestructura de red y aplicaciones informáticas simuladas, que servirán como entorno de pruebas de vulnerabilidades y ataques a la seguridad de la información.
- Dos o más prototipos de laboratorio, que contribuyan a la enseñanza de la seguridad en redes para distintas asignaturas de las carreras del Departamento de Electrónica, Telecomunicaciones y Redes de Información (DETRI).
- Se organizarán grupos de estudiantes interesados en estas áreas para su formación académica.

- Documentación didáctica para la realización de prácticas de laboratorio que aporten a la enseñanza de asignaturas relacionadas con la seguridad de la información como: Comunicaciones Inalámbricas, Seguridad en Redes, Telemática, Redes WAN, Redes LAN, Sistemas Operativos, Telefonía y Desarrollo de Software.
- Documentación sobre el proceso seguido para implementar los prototipos y las pruebas realizadas.
- Se propondrán distintas actividades de difusión y participación de la comunidad académica, relacionadas con este proyecto.
- Artículos científicos a nivel nacional
- Documentos como parte de los proyectos de titulación de estudiantes de pregrado
- Formación de masa crítica interesada en investigar en seguridad de la información, mediante tareas de difusión como charlas técnicas, conferencias y seminarios.

Usuarios/Beneficiarios

- Profesores e investigadores universitarios de las facultades de Eléctrica y Electrónica y Sistemas, que estén interesados en actualizar el pensum de las asignaturas a su cargo, para incluir detalles relacionados con la seguridad de la información en las distintas tecnologías que estudian.
- Estudiantes, universitarios interesados en investigar el estado del arte de la seguridad de la información.
- Entidades gubernamentales, como la Superintendencia o el Ministerio de Telecomunicaciones, interesadas en conocer la situación actual de los sistemas telemáticos, con respecto a sus vulnerabilidades y ataques en el país, así como en la promoción de conciencia respecto a la seguridad de la información desde el sector académico y hasta el entorno ciudadano.
- Empresas públicas y privadas que deseen conocer los riesgos a los que se están enfrentando las infraestructuras críticas de las que dependen sus datos.

5 Relevancia de esta propuesta de investigación con los objetivos científicos del departamento y su Línea de Investigación.

Los objetivos científicos del Departamento de Electrónica, Telecomunicaciones y Redes de Información (DETRI) están enmarcados en 11 líneas de investigación orientadas a promover la docencia, la investigación y la extensión en las áreas de conocimiento relacionadas con la Electrónica, las Telecomunicaciones y las Redes de Información.

Como se justificó previamente, la Seguridad de la Información y, consecuentemente, los sistemas que intentan implementarla son relevantes en un espectro **multidisciplinario** ya que las fuentes, tecnologías, infraestructuras y aplicaciones involucradas con la información, están relacionadas con múltiples disciplinas tecnológicas, que incluso trascienden las telecomunicaciones, los sistemas informáticos y las redes de información.

Bajo esta perspectiva, nuestro proyecto plantea la implementación de prototipos para la investigación en seguridad de la información, que es relevante para las siguientes líneas de investigación, definidas por el DETRI: **Sistemas de Seguridad, Sistemas de Comunicaciones Inalámbricas, Conectividad y Software de Comunicación de Datos**. Además, y destacando este carácter multidisciplinar de la temática que se propone, debemos indicar que existen varias líneas de investigación íntimamente ligadas en la Facultad de Ingeniería en Sistemas, tales como: **Redes y Seguridad de la Información, y Computación Forense.**

Adicionalmente, los tópicos que se desarrollarán en este proyecto están relacionados con varias asignaturas de las carreras de Electrónica y Redes de Información, Telecomunicaciones y en algunos casos con la de Automatización y Control, y el único Departamento de la Facultad de Sistemas.

La seguridad de la información despierta un enorme interés en la opinión pública y en los ámbitos académico y comercial en todo el mundo. Sin embargo, en nuestro país apenas se le está dando cabida. A pesar de esto, otras universidades como la ESPOL o la UTPL ya tienen entidades administrativas y grupos de investigación formados en esta temática y cuya influencia trasciende las barreras académicas. Además, aunque la Seguridad de la Información es un campo de estudio transversal, hay muy pocas asignaturas en las carreras en la EPN que permitan a los estudiantes especializarse en esta temática.

Este vacío justifica nuestro proyecto, especialmente considerando que la investigación y la formación en Seguridad de la Información son muy valoradas en el campo profesional y puede darle mucha visibilidad a la EPN por la colaboración que se generaría con entidades gubernamentales estratégicas.

Nuestro equipo de investigación estará formado por investigadores especializados en distintas áreas parte de las disciplinas de Ingeniería en Telecomunicaciones, Redes de Información y Sistemas Informáticos, tales como:

- *Privacidad y Hacking Ético*
- *Auditoría Informática*
- *Gestión de la Seguridad de la Información*
- *Sistemas Operativos*
- *Comunicaciones Inalámbricas*
- *Telefonía IP*
- *Desarrollo de Software*

6 Descripción del proyecto, metodología, cronograma de trabajo y justificación del equipo requerido

Descripción y justificación del proyecto

Todos los sistemas tecnológicos que se conectan a las redes de datos son vulnerables pues en su desarrollo siempre pueden existir errores. La masificación del acceso a Internet y del uso de dispositivos móviles para la utilización de redes sociales ha ido en ascenso durante los últimos años [1], y estos fenómenos han estimulado la utilización más frecuentemente de recursos, aplicaciones y servicios altamente inseguros. Esta tendencia no es distinta en el Ecuador [2].Todos los datos personales que se comparten por estos medios son de fácil obtención para los atacantes debido a lo poca consciencia que existe en los usuarios sobre los riesgos del uso de estas tecnologías.
La información, que para ser útil debe ser transmitida y procesada, está siempre a merced de atacantes cibernéticos y esto, más o menos, lo comprende todo el mundo. Sin embargo, esta consciencia sobre el riesgo se dispersa en la mayoría de los administradores de infraestructuras tecnológicas al tratar de resolver problemas aparentemente más urgentes del día a día.

En nuestro proyecto proponemos, en principio, recopilar y generar estadísticas sobre las vulnerabilidades y ataques en aplicaciones y servicios comunes en el país. Estas estadísticas pueden ayudar a la comunidad académica a comprender mejor la grave situación de vulnerabilidad de los distintos sistemas de información en nuestro entorno. Además, nos permitirá dotar de elementos de decisión para investigaciones futuras mucho más específicas en el vasto campo de la seguridad.
Con el fin de incentivar la colaboración con entidades del medio externo, se propone trabajar en conjunto con instituciones públicas y privadas en el proceso de investigación de ataques y vulnerabilidades.
Adicionalmente, se propone desarrollar escenarios virtualizados y físicos para la recreación de ataques a la seguridad de la información relacionados con múltiples ámbitos de la tecnología, como los sistemas informáticos y las redes telemáticas. Estos escenarios serán utilizados para elaborar documentación de soporte como guías didácticas de laboratorios de seguridad de la información, orientándolos, de manera especial, a los recientes ataques a sistemas que se han llevado a cabo en los últimos años. Estos laboratorios estarán enfocados al contenido de varias asignaturas de las carreras del DETRI, tales como: Comunicaciones Inalámbricas, Telemática, Redes WLAN, Redes LAN, Redes WAN, Sistemas Operativos, Sistemas Operativos Linux, Telefonía, Programación, Aplicaciones Distribuidas y, desde luego, Seguridad en Redes.

También se propondrán ideas para estimular el estudio de la seguridad en sistemas de Control Industrial, que forman parte de infraestructuras sumamente críticas y que recientemente han sido atacadas en el mundo como parte de la guerra electrónica que al parecer se libra entre EE.UU y algunos países de Oriente[3].
Uno de los graves problemas relacionados con la seguridad de la información en nuestro país es el deficiente y casi nulo marco regulatorio al respecto [4] (no existe una ley de protección de datos, por ejemplo). Esto deja a las posibles víctimas en un estado de indefensión, en un contexto en el que los cuerpos de seguridad del estado apenas están estructurándose [5] para dar protección a los ciudadanos y a las instituciones frente a un fenómeno que lleva con nosotros, al menos, desde que apareció Internet. Así, analizaremos el estado del arte del marco regulatorio con respecto a la seguridad de la información en el Ecuador, para proponer normativa y metodologías que persigan la protección de la información.

Finalmente, se realizará actividades de difusión con el fin de formar una masa crítica que pueda abordar temáticas de seguridad en cursos, seminarios, charlas técnicas y eventos académicos nacionales.

Cabe resaltar, además, que en caso de aprobarse este proyecto, se dará un gran impulso para la formación del grupo de investigación de Seguridad de la Información de la Facultad de Ingeniería Eléctrica y Electrónica, ya que se dispondrá de equipamiento, capacitación especializada para los investigadores, y documentación de respaldo para fortalecer las cátedras antes mencionadas. Existen además otros proyectos vinculados con el grupo de investigación y la seguridad de la información que se plantearán como proyectos internos en el DETRI.

Procedimiento - Metodología

Consulta y análisis de información sobre los aspectos teóricos, técnicos y funcionales de los dispositivos y aplicaciones que se utilizarán para la generación y recopilación de estadísticas relacionadas con las seguridad de la información en el país.

Instalación y configuración de aplicaciones de detección que monitoreen la existencia de vulnerabilidades y ataques a la seguridad de la información.

Instalación y preparación del sistema operativo de los equipos que servirán de base para la simulación y pruebas de los entornos de red para la recreación de vulnerabilidades, ataques y sistemas de protección de la información.

Implementación de dos o más prototipos de escenarios de red con aplicaciones y servicios que permitan recrear vulnerabilidades y ataques contra la seguridad de la información.

Análisis y estudio del estado del arte de la normativa técnica existente referente a la seguridad de la información y los sistemas en el Ecuador.

Elaboración de documentación técnica que describa los procesos realizados para cumplir los objetivos de este proyecto, así como de documentación didáctica que pueda ser utilizada en laboratorios de las distintas asignaturas de las carreras de Telecomunicaciones, Redes de Información y Sistemas Informáticos.

Cronograma de trabajo anual

Actividades	Meses											
	1	2	3	4	5	6	7	8	9	10	11	12
Consulta bibliográfica y tratamiento de información relacionada con el estado del arte de la seguridad de la información, con énfasis en el Ecuador como caso de estudio												
Adquisición de equipos, configuración inicial del software y del hardware.												
Creación y puesta en marcha de herramientas para la detección y monitoreo de vulnerabilidades y ataques a la seguridad de la información												
Instalación y configuración de los equipos que servirán de base para los prototipos y escenarios de red vulnerables donde se recrearán vulnerabilidades y ataques a la seguridad de la información												
Implementación del primer prototipo para la recreación de vulnerabilidades y ataques a la seguridad de la información.												
Implementación del segundo prototipo para la recreación de vulnerabilidades y ataques a la seguridad de la información.												
Evaluación de los resultados de la generación y recopilación de estadísticas de vulnerabilidades y ataques a la seguridad de la información												
Documentación de procesos seguidos para la implementación de los prototipos y análisis de resultados.												
Realización de artículos científicos para publicación a nivel nacional.												
Informe semestral de actividades.												
Difusión de los materiales bibliográficos recopilados, de la información y de los resultados obtenidos para implementación de futuras aplicaciones.												

Justificación del equipo requerido

Para este proyecto se requiere un servidor que será utilizado para simular los distintos escenarios de red y sus correspondientes aplicaciones donde se recrearán los entornos vulnerables y los ataques a la seguridad de la información antes mencionados, mediante herramientas de virtualización. Cabe destacar que se proyecta que este equipo pueda ser utilizado concurrentemente por varios usuarios mientras realizan una práctica para determinada asignatura, por ello las altas prestaciones requeridas.

Con el fin de monitorear la actividad relacionada con ataques y vulnerabilidades de al menos dos instituciones, se requiere dos computadores, uno para cada institución. En estos equipos se adquirirá y procesará la información del tráfico de red que recibe la red de la institución, con el fin de obtener estadísticas sobre los riesgos de seguridad de las distintas infraestructuras.

Adicionalmente, para recrear esquemas de red que no pueden ser virtualizados, tales como redes inalámbricas, redes móviles de segunda, tercera y cuarta generación; y para representar distintos escenarios de vulnerabilidad y ataque que no corresponden a las redes virtualizadas, se requiere de los siguientes dispositivos:

- 2 computadores que permitan la conexión de los escenarios de red a la red de telefonía pública (PSTN) y a la red de telefonía celular
- 2 computadores que permitan construir una *honeynet*, una infraestructura de red en la que funcionan servicios vulnerables que atraen atacantes para monitorear su actividad cuando el ataque se lleva a cabo.
- 3 bases de conexión a la red celular que permitan interacción de nuestros escenarios con infraestructuras de telefonía móvil.
- 4 *routers* inalámbricos que permitan desplegar escenarios no cableados y representar los posibles ataques y vulnerabilidades en esta tecnología de capa 2. Se requieren 4 *routers*
- 1 *switch* de 24 puertos para interconectar todos los dispositivos de los escenarios físicos de red
- 1 mini-rack para fijar los equipos de conmutación y el servidor
- 1 rollo de cable UTP categoría 6 para realizar el cableado estructurado entre los dispositivos de red
- 20 *patch-cords* para conexión itinerante de dispositivos en los distintos escenarios físicos de red que se recrearán

Tal como se puede intuir, los equipos que requerimos funcionan con varias de las tecnologías de comunicaciones que actualmente existen ya que nuestro objetivo, en ese sentido, es recrear varios de los escenarios usando dichas tecnologías con el fin de mostrar que todas ellas pueden ser sujetas de ataques en determinadas circunstancias.

Bibliografía

[1] Internet Live Stats, URL:http://www.internetlivestats.com/internet-users/
[2] *Smartphones*: 3,7 millones con Internet, URL:http://www.hoy.com.ec/noticias-ecuador/smartphones-3-7-millones-con-internet-596364.html
[3] Stuxnet, virus de sistemas de control industriales, URL: http://www.symantec.com/es/mx/page.jsp?id=stuxnet
[4] Proyecto de Ley de Telecomunicaciones, URL: http://www.asambleanacional.gob.ec/noticia/proyecto_de_ley_de_telecomunicaciones_requiere_varios_ajustes_fabian_jaramillo
[5] El contexto de la Ciberseguridad, URL: http://www.supertel.gob.ec/index.php?option=com_content&view=article&id=554&Itemid=50
[6] Harris, S., Harper, A., Eagle, C., & Ness, J. (2007). Gray hat hacking. McGraw-Hill, Inc..
[7] Spitzner, L. (2003). The honeynet project: Trapping the hackers. IEEE Security & Privacy, 1(2), 15-23.
[8] Endler, D., & Collier, M. (2006). Hacking exposed VoIP: voice over IP security secrets & solutions. McGraw-Hill, Inc..
[9] Chandra, P. (2011). Bulletproof Wireless Security: GSM, UMTS, 802.11, and Ad Hoc Security. Elsevier.

7 Fecha de inicio

Lunes 7 de julio de 2014.

8 Tiempo dedicación docentes, infraestructura, equipamientos y fondos adicionales.

- **Tiempos de dedicación semestral del Director de proyecto, de los docentes participantes y otros colaboradores.**

  Director de proyecto: el máximo que permite el reglamento de la convocatoria (300 horas). Es muy probable que se dedique más tiempo.

  Docente colaborador: el máximo que permite el reglamento de la convocatoria (210 horas). Es muy probable que se dedique más tiempo.

- **Infraestructura y equipos disponibles para la ejecución del proyecto**
  Equipos de cómputo, infraestructura física y servicios de red e Internet disponibles para el DETRI.

- **Otros fondos de otros organismos (si los hubiere)**
  No existen