Introducción de la tesis

Ing. Felipe de Jesús Miramontes Romero

Centro de Investigación en Matemáticas A.C.,
Maestría en Ingeniería de Software,
Avenida Universidad 222, La Loma, 98068, Zacatecas, México.
felipemiramontesr@gmail.com
http://www.ingsoft.mx

Resumen Keywords: Seguridad cibernetica, Delincuencia informática, México, Técnicas, Estrategias, Planes, Herramientas, Mejora de la Seguridad informática

1. Introducción de la tesis

De acuerdo con [1] el cibercrimen o delincuencia informática es el área de mas rápido crecimiento dentro de la gama de crímenes punibles de carácter internacional, es perseguida por varias agencias del globo, entre ellas la Interpol y la National Security Agency (NSA) de los Estados Unidos. Los criminales cibernéticos o criminales informáticos aprovechan las potentes capacidades de la tecnología emergente en combinación con técnicas fraudulentas; cometen un diverso rango de actividades criminales, que rompen fronteras e impactan en los aspectos sociales, económicos y políticos del mundo. Se afirma que no existe una definición universal de cibercrimen. Legalmente la ley hace dos distinciones entre los crímenes relacionados a Internet: el primero de ellos es conocido como cibercrimen avanzado ese incluye los crímenes de alta tecnología; por otra parte la llamada ciberdelincuencia habilitada o "Cyber-Enabled-Crime" que se enfoca en crímenes de carácter general en los cuales el cibercrimen solo es una herramienta mas para lograr su objetivo: la trata de personas, los crímenes financieros, el narcotráfico y el terrorismo. La Interpol menciona que nuevas tendencias en delincuencia informática están surgiendo todo el tiempo. De acuerdo con [2] los costos estimados para la economía mundial por estos crímenes están entre los 375 y los 575 mil millones de dolares al año.

De acuerdo con la Interpol [1] hace algunos años los delitos cibernéticos eran cometidos principalmente por individuos o grupos pequeños. Hoy en día existen redes complejas de criminales que pretenden reunir a personas de todo el mundo en tiempo real para cometer crímenes en una escala sin precedentes.

En México, Enrique Galindo Ceballos, comisionado general de la Policía Federal de México en 2015 ha declarado en conferencia de prensa [2] que es fundamental controlar la integridad y confidencialidad de la información pues la

mayoría de los sectores de economía y gobierno del país basan su completa operación en la afamada red mundial. Durante la presentación de los resultados de la estrategia nacional de ciberseguridad, el funcionario declaró que con el desarrollo de las tecnologías de información, los gobiernos han establecido al ciberespacio como un nuevo entorno operativo, por lo que actualmente controlar la integridad, disponibilidad y confidencialidad de la información se vuelve un tema fundamental en lo económico y político de las naciones. Ademas se dijo que del 1 de diciembre del 2012 al 1 de febrero del 2015 se emitieron más de 1,000 alertas de seguridad que permitieron prevenir y mitigar incidentes cibernéticos gracias a la colaboración internacional, así mismo se lograron atender de diciembre de 2012 a enero 2015, aproximadamente 59,236 incidentes cibernéticos. Así mismo se hizo referencia a la siguiente información de de alto impacto:

1. El 53 % de los incidentes cibernéticos identificados fueron en contra de los tres órdenes de gobierno, 26 % al ámbito académico y 21 % al privado.

2. Las principales afectaciones son, 68 % suplantación y robo de identidad, 17 % fraude cibernético, 15 % ataques a sitios web.

3. A pesar de la complejidad para la persecución de estos delitos, se cumplimentaron 47 órdenes de cateo y fueron detenidos 36 probables responsables.

4. El patrullaje virtual de la Policía Federal (PF) identificó y desactivó 5,549 sitios web apócrifos usurpadores de instancias financieras y de gobierno.

De acuerdo a Kapellmann y Reyes [3], la consultora The Competitive Intelligence Unit (CIU) afirma que, "por medio de la Reforma en Materia de Telecomunicaciones [4] y la Estrategia Digital Nacional [5] se ha dado prioridad a la digitalización de la población y los servicios públicos, pero el tema de la ciberseguridad no ha recibido el mismo ímpetu". Ademas se dice que en 2014 México contó con una calificación global en seguridad informática de 32.4 sobre 100, lo cual implica que se encuentra 12.3 puntos por debajo del promedio global. A nivel latinoamérica México se ubica por encima de países como Paraguay y Venezuela, pero muy por debajo de otros como Brasil, Uruguay, Argentina, Costa Rica, Chile y Colombia. Según el reporte "Tendencias de Seguridad en América Latina y el Caribe" [6], de la Organización de los Estados Americanos (OEA), en México los costos anuales generados por ciberdelitos en 2014 ascendieron a 3 mil millones de dólares, afectando a los sectores público, privado y civil. ABI Research [7] afirma que el Índice Mundial de Ciberseguridad (IMC) es una medida del nivel de desarrollo de la ciberseguridad de cada estado nación y ha sido creado con el fin de fomentar una cultura mundial en pro de la seguridad informática y de la integración de las Tecnologías de Información y Comunicaciones (TIC) como elemento catalizador. Brahima Sanou [7] menciona que el IMC ha sido calculado en colaboración con ABI Research, institución especializada en análisis estadísticos y evaluación comparativa de las industrias, quienes han desarrollado cuestionarios especializados para la extracción de información; y sus

resultados fueron presentados a todos los Estados Miembros de la Unión Internacional de Telecomunicaciones (UIT). Dentro de su metodología se realizaron encuestas a nivel de país, complementadas con una investigación cualitativa a fondo; se recopilo información sobre leyes, reglamentos; Computer Emergency Response Team (CERT) y Computer Incident Response Team (CIRT), políticas, estrategias nacionales, normas, certificaciones, formación profesional, sensibilización, y asociaciones de colaboración. Otorgando una calificación a cada país miembro. Para la calificación se tomaron en cuenta 5 áreas especificas: medidas jurídicas, medidas técnicas, medidas de organización, creación de capacidades y cooperación.

A continuación es presentado un resumen de resultados del IMC 2015 (Figuras 1 y 2), en el cual son presentados los 5 países con mejor calificación, los 5 países con peor calificación y un rango de 5 países en el cual aparece México. Los datos mostrados hacen referencia a la calificación denominada Índice la cual se compone de la ponderación de las áreas mencionadas anteriormente, además se muestra la clasificación de cada país la cual indica su posición en la tabla general de calificaciones. Los detalles del estudio IMC se encuentran en [7].

País	IMC	Clasificación
Estados Unidos de América	0,824	1
Canadá	0,794	2
Australia	0,765	3
Malasia	0,765	3
Omán	0,765	3
Emiratos Árabes Unidos	0,353	17
Burkina Faso	0,324	18
México	0,324	18
Perú	0,324	18
Vietnam	0,324	18
Lesoto	0	29
Islas Marshall	0	29
Namibia	0	29
San Vicente y las Granadinas	0	29
Timor Oriental	0	29

Figura 1. Indice Mundial de Ciberseguridad

En “Retos de Ciberseguridad para México” [3] , se dice que es de suma importancia comenzar con la pronta elaboración e implementación de estrategias y planes nacionales que agilicen la transición hacia un ciberespacio seguro, donde sea posible aprovechar los beneficios que generan las tecnologías de información y comunicaciones. En este documento es presentado un modelo de trabajo que pretende satisfacer las necesidades actuales de los principales afectados por me-

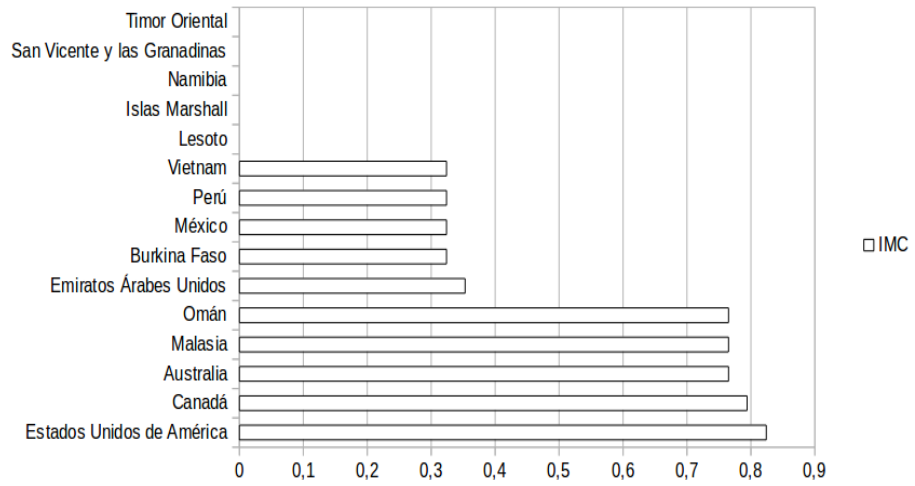

Figura 2. Comparativa del Indice Mundial de Ciberseguridad (IMC).

dio de la supresión de la mayor cantidad de vulnerabilidades durante el ciclo de vida de desarrollo de sistemas web basados en plataformas Content Management System (CMS), Learning Management System (LMS), Learning Content Management System (LCMS) y e-Commerce. Para lograr un correcto entendimiento de la panorámica general se han realizado en este trabajo actividades y experimentos con el fin de comprender la simbiosis cibernética existente entre los mecanismos que actualmente son utilizados en pro de la mejora de la seguridad de la información en los sistemas web localizados geográficamente en México.

El presente trabajo se encuentra estructurado de una manera simple y en el se encuentran contenidas las siguientes secciones:

- Antecedentes; en esta sección es posible encontrar la información necesaria para comprender el panorama tecnológico actual de México; es decir, los resultados obtenidos de los experimentos y estudios realizados para responder la interrogante: ¿Qué se ha hecho a favor de la construcción de sistemas web seguros en México? Ademas de ello, es posible encontrar el planteamiento del problema que se ha identificado, los objetivos generales, específicos y la justificación del desarrollo de la propuesta.

- Estado de arte; según Molina [8] en esta sección se aborda la información que da respuesta a la interrogación: ¿Cómo fue realizado el estudio del conocimiento acumulado (escrito en textos)? Dicha información pertenece a la rama de la tecnología denominada seguridad informática, en la especialidad de desarrollo de sistemas web seguros.

- Propuesta; en esta sección se aborda a detalle la información relacionada al modelo de trabajo propuesto.

- Caso de estudio; en esta sección es posible localizar la información concerniente al desarrollo de un sistema web seguro utilizando el modelo de trabajo propuesto, esto con el fin de poder evaluar el impacto del mismo en un entorno real.

- Resultados; en esta sección es posible encontrar los datos obtenidos de la evaluación de la propuesta, así como la información relacionada con la medición del impacto en la seguridad de la información en México.

- Conclusiones; en esta sección es posible encontrar los aprendizajes generales de la interacción y el desarrollo de los mecanismos incluidos en la propuesta, así como el trabajo hacia el futuro, así como la áreas de oportunidad de la aplicación para el presente trabajo.

Acronyms

CERT Computer Emergency Response Team. 2
CIRT Computer Incident Response Team. 2
CIU The Competitive Intelligence Unit. 2
CMS Content Management System. 3

IMC Índice Mundial de Ciberseguridad. 2, 3

LCMS Learning Content Management System. 3
LMS Learning Management System. 3

NSA National Security Agency. 1

OEA Organización de los Estados Americanos. 2

PF Policía Federal. 2

TIC Tecnologías de Información y Comunicaciones. 2

UIT Unión Internacional de Telecomunicaciones. 2

Referencias

1. Interpol, "Cybercrime." `http://www.interpol.int/es/Crime-areas/Cybercrime/Cybercrime`. Fecha de acceso: 3-3-2016.
2. Forbes, "Cibercrimen en México." `http://www.forbes.com.mx/10-datos-sobre-cibercrimen-en-mexico-que-debes-conocer`. Fecha de acceso: 3-3-2016.
3. D. Kapellmann and B. Reyes, "Retos de Ciberseguridad para México." `http://the-ciu.net/nwsltr/381_1Distro.html`. Fecha de acceso: 4-14-2016.
4. G. de los Estados Unidos Mexicanos, "Reforma en Materia de Telecomunicaciones," Marzo 2014.
5. G. de los Estados Unidos Mexicanos, "Estrategia Digital Nacional," Noviembre 2013.
6. OEA, "Tendencias de Seguridad Cibernética en América Latina y el Caribe," Junio 2014.
7. A. Research, "Global Cybersecurity Index and Cyberwellness Profiles," Abril 2015.
8. P. Molina, "¿Qué es el estado del arte?." `http://revistas.lasalle.edu.co/index.php/sv/article/view/1666`. Fecha de acceso: 5-3-2016.