

# Resumen de 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. Resumen de tesis

En [1] se dice que 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 al rededor del globo, entre ellas la Interpol y la National Security Agency (NSA) de los Estados Unidos de América (EE.UU). Los criminales cibernéticos o criminales informáticos aprovechan las potentes capacidades de la tecnología emergente en combinación con técnicas fraudulentas para cometer un diverso rango de actividades criminales que rompen fronteras e impactan de manera profunda en los aspectos sociales, económicos y políticos del mundo. En [1] 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 este incluye los crímenes de alta tecnología, es decir; ataques sofisticados a Software o Hardware, por otra parte la coloquialmente llamada ciberdelincuencia habilitada o formalmente “Cyber-enabled crime ” se enfoca en crímenes inclusivos de carácter general que no tienen como fin principal cometer ataques sofisticados pues son aquellos en los cuales el cibercrimen solo es una herramienta mas para lograr el principal objetivo, entre ellos se destacan: la trata de personas, los crímenes financieros, el narcotráfico y el terrorismo. En [1] se menciona que nuevas tendencias en delincuencia informática están surgiendo todo el tiempo y los costos estimados para la economía mundial por estos crímenes están entre los 375 y los 575 mil millones de dolares al año, así lo manifiesta [2]. Segun [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.

Por otra parte en México, Enrique Galindo Ceballos, comisionado general de la Policía Federal de México en 2015 ha declarado en [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. En [2] se dice 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. En [2] se hace referencia a la siguiente información 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 cumplieron 47 órdenes de cateo y fueron detenidos 36 probables responsables.
4. El patrullaje de la Policía Federal (PF) identificó y desactivó 5,549 sitios web apócrifos usurpadores de instancias financieras y de gobierno.

De acuerdo con [3], la consultora The Competitive Intelligence Unit (CIU) afirma que, “por medio de las reformas en materia de telecomunicaciones y la Estrategia Digital Nacional 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”. Según [3] México cuenta 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”, de la Organización de los Estados Americanos (OEA), en México los costos anuales generados por ciberdelitos en 2014 ascendió a 3 mil millones de dólares, afectando a los sectores público, privado y civil.

En el reporte denominado “Retos de Ciberseguridad para México”, 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 correctamente los enormes beneficios que generan las nuevas tecnologías de información y comunicaciones.

## Acronyms

**CIU** The Competitive Intelligence Unit. 2

**EE.UU** Estados Unidos de América. 1

**NSA** National Security Agency. 1

**OEA** Organización de los Estados Americanos. 2

**PF** Policía Federal. 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. OEM, “México se rezaga en materia de seguridad cibernética.” <http://www.oem.com.mx/elsoldezacatecas/notas/n3827524.htm>. Fecha de acceso: 3-3-2016.