Antecedentes

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

En esta sección es posible encontrar la información referente a los estudios y experimentos realizados para dar respuesta a la interrogante; ¿Cuál es el panorama general de la ciberseguridad en México? Para dar respuesta a la anterior cuestión y con el fin de realizar una propuesta en pro de la seguridad informática en el país se ha considerado identificar la información relacionada con las áreas de estudio utilizadas por la International Telecomunication Union (ITU) y ABI Research para la construcción Índice Mundial de Ciberseguridad (IMC) [1], cabe mencionar que la información de cada área de estudio sera enriquecida por medio de datos emanados de actividades y experimentos personales desarrollados con el objetivo de proveer un mayor nivel de detalle en el estudio. Ademas de lo mencionado anteriormente también es posible encontrar el planteamiento del problema, los objetivos generales y específicos así como la justificación de la presente propuesta.

1. Marco teórico

1.1. Indice Mundial de Ciberseguridad (IMC)

ABI Research [1] menciona que las Tecnologías de Información y Comunicaciones (TIC) son el catalizador que impulsa la evolución de las sociedades modernas pues sustentan el crecimiento social, económico y político de las personas, organizaciones y gobiernos. De igual manera se menciona que la tecnología y la Internet están ingresando de manera sistemática tanto en el ámbito publico como en el privado ya que estas proveen ventajas considerables en productividad, velocidad, reducción de costes y flexibilidad. Se menciona también que la ciberseguridad es de máxima importancia para el sostenimiento de cualquier modelo tecnológicamente aceptable pues los cibercriminales son numerosos, están bien organizados y ademas cuentan con medios de persuasión políticos, terroristas, hacktivistas (ver hacktivismo), etc. Para lograr el progreso tecnológico, la

ciberseguridad debe formar parte integral de cualquier proceso relacionado con la tecnología, sin embargo sigue sin formar parte fundamental de las estrategias tecnológicas nacionales e industriales, aunque en la actualidad es posible apreciar de manera táctil el avance tecnológico los esfuerzos en materia de seguridad informática siguen siendo eclécticos y dispersos. Se menciona que la solución se encuentra en la inserción de mecanismos de ciberseguridad en todos los estratos sociales, sin embargo a nivel global la diferencias económicas, políticas y de concientización entre Estados nación son una limitante, para remediar dicha situación es necesario realizar una comparativa entre las capacidades de la seguridad de cada país y la publicación de una clasificación efectiva de la situación pues de tal manera es posible revelar la deficiencias existentes y tomar un acicate para que se intensifiquen los esfuerzos en la materia. ABI Research [1] manifiesta que solo se puede sopesar el valor real de la capacidad de ciberseguridad de un país, por comparación y que el IMC tiene como principal objetivo medir de manera efectiva el nivel de compromiso con la ciberseguridad de cada Estado nación, este se fundamenta en el mandato actual de la ITU pues esta es un facilitador de la linea de acción C5 [2] de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) la cual tiene como propósito crear confianza y seguridad en la utilización de las TIC a nivel nacional, regional e internacional. Se menciona también que el Dr. Hamadoun I. Touré Secretario General de ITU en 2007, presento la Global Cibersecurity Agenda (GCA) como marco de cooperación entre las todas las partes interesadas en la construcción de una sociedad de la información mas segura. De acuerdo a Stein Schjolberg [3] la GCA es un marco de referencia para la cooperación internacional dirigida a la mejora de la confianza y seguridad en una sociedad de la información, se basa en 5 áreas de trabajo: medidas jurídicas, medidas técnicas, medidas de organización, creación de capacidades y cooperación.

El modelo estadístico utilizado para la asignación del IMC se inspira en el Análisis Multicriterios (MCA) así lo menciona ABI Research [1], el MCA establece la preferencia entre alternativas por referencia a un grupo explícito de objetivos para los que se han definido criterios de evaluación del grado en el que sean alcanzados dichos objetivos, se aplica un modelo de evaluación lineal aditiva, la matriz de rendimiento describe las alternativas y las columnas el rendimiento de las alternativas en relación a los criterios. La puntuación de la evaluación comparativa se apoya en indicadores ponderados de manera equitativa, se otorgan 0 puntos cuando no existen actividades; 1 cual la medida posee carácter parcial; y 2 puntos para medidas de alto alcance. La puntuación para cada categoría es la siguiente (véase tabla 1).

1.2. Medidas Jurídicas

De acuerdo con [1] la legislación es una medida para la habilitación de un marco para la estandarización de un reglamento común, permite además que un Estado nación establezca los mecanismos de respuesta a las infracciones: mediante la investigación y la persecución de los delitos y la imposición de sanciones por

Tabla 1. Puntuación total atribuida a cada una de las categorías del Indice Mundial de Ciberseguridad (IMC).

Área	**Puntos**
Medidas jurídicas	
Legislación penal	2
Reglamentación y conformidad	2
Medidas técnicas	
CERT/CIRT/CSIRT	2
Normal	2
Certificación	2
Medidas organizativas	
Política	2
Hoja de ruta de gobernanza	2
Organismo responsable	2
Evaluación comparativa nacional	2
Creación de capacidades	
Desarrollo de normas	2
Desarrollo laboral	2
Certificación profesional	2
Certificación del organismo	2
Creación de capacidades	
Cooperación interestatal	2
Cooperación entre organismos	2
Asociaciones entre los sectores publico y político	2
Cooperación internacional	2
Total	34

falta de conformidad o incumplimiento de la ley. En ultima instancia su objetivo es armonizar supranacionalmente las practicas y medidas interoperables que facilite la lucha contra la ciberdelincuencia. El entorno legal puede ser medido a partir de la existencia de varias instituciones y marcos jurídicos, dicho subgrupo consta de propios indicadores de rendimiento; legislación penal y reglamento y conformidad.

Legislación penal La legislación del cibercrimen debe contener las leyes sobre el acceso, la interferencia, la intercepción de sistemas y datos, sin autorización (sin derecho). Estas leyes puedes ser clasificadas por su nivel de completitud; no existente, parcial o de amplio alcance. La legislación parcial contiene textos alusivos a la informática en una ley o código penal, por otra parte la legislación de amplio alcance se refiere a la promulgación puntual que aborda los aspectos específicos del delito informático. De acuerdo con [1] México posee la siguientes leyes de carácter especifico:

- Código Criminal Federal (CCF)

- Ley de Firma Electrónica Avanzada (LFEA)

Glossary

hacktivismo Es un acrónimo de hacker y activismo, se entiende normalmente "la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software".. 1

Acronyms

CCF Código Criminal Federal. 3
CMSI Cumbre Mundial sobre la Sociedad de la Información. 1

GCA Global Cibersecurity Agenda. 1

IMC Índice Mundial de Ciberseguridad. 1, 2
ITU International Telecomunication Union. 1

LFEA Ley de Firma Electrónica Avanzada. 3

MCA Análisis Multicriterios. 2

TIC Tecnologías de Información y Comunicaciones. 1

Referencias

1. A. Research, "Global Cybersecurity Index and Cyberwellness Profiles," Abril 2015.
2. ONU, "World Summit on the Information Society," Enero 2002.
3. S. Schjolberg, "ITU Global Cibersecurity Agenda," Mayo 2007.
4. G. de los Estados Unidos Mexicanos, "Estrategia Digital Nacional," Noviembre 2013.