INSTITUTO DE INVESTIGACIONES ESTRATÉGICAS DE LA ARMADA DE MÉXICO

DA 35/18
15/06/18

Cap. Nav. CG. DEM.
M. Jorge Luis García Cancino

Hacia un modelo de protección al ciberespacio en México para las instituciones del Consejo de Seguridad Nacional

RESUMEN

Los índices de desarrollo de los países van acompañados del empleo de sus Tecnologías de la Información y Comunicaciones (TIC) y el ciberespacio. El Gobierno, la Defensa Nacional, las empresas y la sociedad dependen del funcionamiento de las nuevas tecnologías, los servicios electrónicos y las redes de comunicación. Sin embargo, existen amenazas que aprovechan las debilidades que se presentan en ese espacio operacional intangible y sin fronteras donde las TIC se comunican: el ciberespacio. Ejemplos como la información que brinda el portal de Wikileaks[1] y la información ofrecida por el exfuncionario de la CIA, Edward Snowden (BBC Mundo, 2013), hacen reflexionar a las naciones sobre la protección al Ciberespacio. En México, las Instituciones que conforman el Consejo de Seguridad Nacional (CSN) emplean las TIC para el desarrollo de sus procesos administrativos y operativos y por ello es necesario unir esfuerzos para proteger este espacio creado por el hombre y aprovechar las capacidades que el Estado ha hecho para fortalecer la protección al ciberespacio; Esta investigación pretende mostrar un modelo como resultado del análisis y experiencia del autor para mejorar la protección del ciberespacio en México para las Instituciones del Consejo de Seguridad Nacional aprovechando las capacidades que el Estado ha realizado.

ABSTRACT

The development indexes of the countries are accompanied by the use of their Information and Communication Technologies (ICT) and Cyberspace. The Government, National Defense, companies and society depend on the functioning of new technologies, electronic services and communication networks. However, there are threats that take advantage of the weaknesses that arise in this intangible and borderless operational space where ICTs communicate: Cyberspace Examples such as the information provided by the Wikeleaks portal and the information provided by the former CIA official. Edward Snowden (BBC World, 2013), makes nations reflect on the protection of Cyberspace. In Mexico, the Institutions that make up the National Security Council (CSN) use ICT for the development of their administrative and operational processes and

[1] Organización Internacional sin lucro que publica documentos filtrados de interés al público.

therefore it is necessary to unite efforts to protect this space created by man and take advantage of the capacities that the State has made to strengthen the protection of Cyberspace; This research aims to show a model resulting from the author's analysis and experience to improve the protection in Cyberspace in Mexico for the Institutions of the National Security Council taking advantage of the capacities that the State has made.

> En los siglos XIX y XX el poder derivaba del control de las rutas de navegación y en el futuro derivará de la habilidad de manejar las líneas de información del Ciberespacio y de influir en el discurso social que conforman las opiniones públicas. (Joseph S. Nye)

EL CIBERESPACIO EN MEXICO Y SUS IMPLICACIONES

Aunque los antecedentes de las ciencias computacionales en México tienen sus orígenes en el año de 1955 en la Universidad Nacional Autónoma de México, al instalarse el primer equipo de cómputo para la resolución de sistemas de ecuaciones simultáneas complejas (CINVESTAV, 2008). El Centro de Investigación y de Estudios Avanzados (CINVESTAV) en 1961 introduce la primera minicomputadora y en el año de 1983 adquiere 7 más por la importancia que estos sistemas tenían a nivel de los países desarrollados para la resolución de problemas complejos.

En ese mismo año; en 1983, pero en los Estados Unidos de América (EUA), se interconectaron tres redes denominadas ARPANET[2], CSNET[3] y MILNET[4] que dieron origen al Internet a través del protocolo de comunicación TCP/IP[5] que fue la clave que permitió comunicarse con los sistemas de cómputo de diferentes entornos; fue hasta el año de 1989 cuando el Internet empieza en México a través de un convenio hecho por el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM) con la Universidad de Texas en San Antonio al interconectarse ambas universidades con fines académicos y de investigación y es ahí donde inicia la era del Ciberespacio en México.

Actualmente se pueden interconectar al Internet los sistemas satelitales, los equipos de transmisión de comunicaciones en voz y datos, los equipos de cómputo, las televisiones, los teléfonos celulares, las agendas personales, videojuegos; es decir, todo equipo o sistema que este comprendido en las TIC y empleen el protocolo TCP/IP para enlazarse y emplearse en cualquier área del conocimiento, desafortunadamente también puede mal emplearse.

De acuerdo al Instituto Nacional de Estadística y Geografía (INEGI); en el año 2012 en nuestro país, el 84% del sector productivo emplean el Internet para la transferencia, búsqueda y acopio de información; 53.9 millones de mexicanos tienen un equipo de cómputo, teléfono inteligente o similar con acceso a Internet.

[2] Red de computadoras creadas por encargo del Departamento de Defensa de los Estados Unidos creada en 1969.
[3] Red de ciencias de la computación con fines académicos y de investigación financiada por la *National Science Foundation* y creada en 1981.
[4] Red de comunicación militar de las Fuerzas Armadas de los Estados Unidos de América creada en 1983.
[5] Protocolo de control de transmisión/Protocolo de Internet que sustituye al protocolo NCP para enrutado de datos.

Solo para hacernos una idea de la interconexión que puede tener un sistema con servicio de Internet hoy en día, el hombre ha creado el Protocolo de Internet versión 6 (IPV6) y es quizás el protocolo con la mayor cifra en número que se conoce en direcciones IP: 340 sextillones (340 mil millones de millones de millones), es decir, por cada milímetro cuadrado de la superficie de la tierra existen 670 mil billones de direcciones de IP.

El ciberespacio es el único espacio de los cinco existentes (Tierra, Aire, Mar, Espacio y Ciberespacio)[6] que está completamente construido por el hombre; por lo que también puede ser modificado a su conveniencia y aprovechar de él todas las oportunidades que este pueda brindar. Sin embargo, también en él se pueden presentar amenazas que, aprovechando la ventaja que da su diseño basado en las TIC, el empleo del Internet y del espectro electromagnético; se puede explotar la información que viaje en él.

Países como China, Rusia y los EUA, han sido objeto de blancos por *hackers*[7] a través del ciberespacio, quienes han obtenido información de asuntos de carácter militar o de Seguridad Nacional de esas naciones para hacer públicas su información sensible o robándolas en forma secreta, afectando con ello los intereses nacionales de estas naciones.

Así mismo, gobiernos de algunos países, han modificado el actuar del "espionaje"[8]; aprovechándose del ciberespacio para penetrar los sistemas informáticos y robar información de las actividades de Seguridad Nacional incluyendo los desarrollos tecnológicos con el fin de beneficiarse al reducir gastos en investigación, mejorar sus sistemas de armas y conocer las acciones de los países con quienes tienen conflictos de intereses.

En el año 2011, grupos hacktivistas como Anonymous[9] y LulZsec[10] dirigieron ataques informáticos diversos y de frecuencia creciente a las infraestructuras tecnológicas del país a través del correo electrónico para robo de información personal y financiera, suplantación de identidad, denegación de servicios (José Reyes, 2016) distribuidos (DDoS)[11], entre otros. Diversos estudios realizados por empresas especializadas en seguridad de la información como *McAfee, Kaspersky y Symantec*[12] identificaron que México es uno de los países menos preparados para resistir ataques cibernéticos. En este sentido, el periódico Milenio Diario (2018) destacó que nuestro país presenta un mayor número de ciberataques en los últimos años.

[6] En México, el Ciberespacio es considerado como la cuarta dimensión de operaciones después del aire, tierra y mar. Sin embargo, algunos países consideran al espacio separado del ciberespacio.
[7] Persona experta en alguna rama de la Tecnología a menudo informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.
[8] Actividad secreta que consiste en tratar de conseguir información confidencial especialmente de un país extranjero.
[9] Seudónimo utilizado mundialmente por diferentes grupos e individuos para realizar acciones de protesta a favor de la libertad de expresión, de la independencia de Internet y en contra de diversas organizaciones.
[10] Grupo o individuos hackers responsables de ataques a varias instituciones gubernamentales.
[11] *Distributed Denial of Service* (DDoS) es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
[12] Empresas líderes en solución de problemas informáticos producidos por virus, troyanos, gusanos, etcétera.

En el año 2014, la empresa *GData* de Alemania informó que cada segundo México sufre 12 ataques cibernéticos, de los cuales el 60 por ciento son contra el gobierno. Su finalidad es tratar de extraer información proveniente principalmente de complejas redes de piratas de Rusia y Estados Unidos (*Excelsior*, 2014); por otra parte el *Diario Sin Límites* informó que el robo de la información es el fraude más común en nuestro país.

En este sentido, la Agenda Nacional de Riesgo en México, en el periodo 2014-2015 consideró a la ciberseguridad como una amenaza a atender respecto a los riesgos que afectan a la nación mexicana. Así también, la última agenda registrada en el Centro de Investigación y Seguridad Nacional la tiene contemplada dentro de una zona moderada a nivel transnacional.

Tabla 1: Agenda de Riesgo 2014 y 2015

	Año 2014	Año 2015
1	Desastres naturales y pandemias	Desastres naturales y pandemias
2	Delincuencia organizada	Delincuencia organizada
3	Conflictos agudos focalizados	Conflictos agudos focalizados
4	Anarquismo	Anarquismo
5	Subversión	Subversión
6	Flujos migratorios descontrolados	Flujos migratorios descontrolados
7	Ciberseguridad	Ciberseguridad
8	Tráfico ilícito de mercancías: fronteras y mares	Tráfico ilícito de mercancías: fronteras y mares
9	Corrupción e impunidad	Desastres naturales y pandemias
10	Terrorismo y armas no convencionales	Subversión

Fuente: Centro de Información y Seguridad Nacional

En la actualidad, y debido a que casi la totalidad de la información esta digitalizada y almacenada en los sistemas de información en apego a las políticas establecidas por la Unidad de Gobierno Digital de la Secretaria de la Función Pública (SFP) referente al objetivo de: Instrumentar, fomentar y promover la utilización de las TIC en los procesos de la Administración Pública Federal, para fortalecer la gestión pública y mejorar la entrega de servicios a la sociedad (Estrategia Digital Nacional, 2013); El empleo del ciberespacio

es un requisito indispensable en el desarrollo de los procesos de información de las Instituciones del Gobierno Federal.

REGULACIONES DEL CIBERESPACIO.

El ciberespacio y la Seguridad Nacional esta soportada bajo ordenamientos jurídicos, algunos de carácter internacional que incluyen a nuestro país por tratados celebrados y otros de carácter nacional que a medida que se han suscitados cibercrimenes[13] y ciberataques[14] en el ciberespacio se han reformado jurídicamente. Cada país y de acuerdo a sus necesidades, han normado su legislación al interior de sus naciones en el ámbito de sus instituciones gubernamentales, financieras, comerciales o para la protección de la integridad de sus connacionales protegiéndolos de las amenazas cibernéticas.

En el ámbito internacional, México ha celebrado convenios relacionados con el ciberespacio, entre ellos están el de la Organización de Cooperación y Desarrollo Económico sobre delitos de informática y normas para la seguridad de los sistemas de información; además, está el convenio sobre la "ciberdelincuencia" del Consejo de Europa celebrado en Budapest del 23 de Noviembre de 2001, donde los países miembros están convencidos de la necesidad de aplicar con carácter prioritario una política penal para proteger a la sociedad frente a la ciberdelincuencia.

La Constitución Política de los Estados Unidos Mexicanos, explícitamente no establece lineamientos para el ciberespacio. Sin embargo, en materia de protección de datos personales, inviolabilidad de las comunicaciones personales, la investigación del delito, funciones del congreso en materia de TIC y la facultad del presidente de la República para disponer de la Fuerza Armada para mantener la Seguridad Nacional quedan establecidas en los artículos 16, 21, 25, 29 y 89.

El Código Penal Federal, establece en los Arts. 210, 211, 214 y 220, las sanciones aplicables a los servidores públicos que revelen información secreta que comuniquen, sustraigan o utilicen ilícitamente citada información secreta para su beneficio.

La Ley de Seguridad Nacional, en el artículo tercero define la Seguridad Nacional, en el quinto establece las amenazas a la Seguridad Nacional y en el capítulo I, en los artículos del 9 al 12 establecen todo lo relativo al Consejo de Seguridad Nacional y las instancias que lo componen.

La Ley Federal del Derecho de Autor en el capítulo IV, establece la protección de los programas de computación y las bases de datos; y la Ley Federal de Transparencia y Acceso a la Información Pública

[13] Actividades delictivas efectuadas con herramientas informáticas.
[14] Daños o perjuicios hechos a personas, grupos de ellos o Instituciones ejecutados generalmente por equipos de cómputo conectados al Internet.

Gubernamental (2014) en los Arts. 3, 13, 14 y 20, establece la definición de la Seguridad Nacional, los lineamientos a considerar en la información reservada y la protección de los datos personales.

Por otra parte; en el Plan Nacional de Desarrollo 2013-2018, publicado por el Ejecutivo Federal, reconoce por primera vez en México que el ciberespacio debe protegerse; por lo que dentro de las metas nacionales y estrategias transversales para lograr que la productividad lleve al País a su objetivo general de: Llevar a México a su máximo potencial.

La primera meta "México en Paz", contempla en uno de sus objetivos: garantizar la Seguridad Nacional (Presidencia de la República, 2014); y para ello se apoya en sus estrategias, de la cual, una de ellas es la: Estrategia 1.2.3. fortalecer la inteligencia del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la Seguridad Nacional, considerando la línea de acción de impulsar, mediante la realización de estudios e investigaciones, iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para fortalecer la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad.

Además; el Programa para la Seguridad Nacional 2014-2018 plantea el fortalecimiento de la cuarta dimensión de las operaciones de seguridad: La ciberseguridad; en este sentido cabe aclarar que, en México, el ciberespacio está considerado como la cuarta dimensión de las operaciones siendo el aire, mar y tierra los otros tres.

OPORTUNIDADES Y AMENAZAS EN EL CIBERESPACIO.

El ciberespacio representa un sinfín de oportunidades que hacen muy atractivo su uso, las más significativas identificadas a través de encuestas fueron: Bajo costo de operación, continuidad en la comunicación ante eventos catastróficos, facilidad en la búsqueda de información y contribución al desarrollo del conocimiento; así mismo, en este sentido también se identificaron algunas amenazas: ciberterrorismo, ciberataques, dependencia tecnológica y cibercrimen.

1. Las Oportunidades en el Ciberespacio.

a. Bajo costo en el servicio de operación.- Las TIC al emplear el ciberespacio intercomunicado al Internet y cualquier red que se encuentre intercomunicada para viajar en ella la información que se desea transmitir, hace reducir los costos de operación y con ello se beneficia a la población en general reduciendo los gastos en estos servicios y contribuyendo directamente en su economía; tal es el objetivo de la Agenda Digital Nacional[15] con su lema "Por un México conectado".

[15] Agenda impulsada en el año 2013 por diversos grupos de la sociedad mexicana y ejecutada por el Ejecutivo Federal, que busca el bien común y resolver problemas en materia de innovación y competitividad en materia del uso de las TIC´s, internet y la banda ancha.

b. Continuidad en la comunicación ante eventos catastróficos.- Al inicio de la creación del Internet en los EUA; la columna vertebral que dio origen a este servicio fue ARPANET (creado por el departamento de defensa de los EUA) y su función principal era mantener comunicados a las Fuerzas Militares de los Estados Unidos ante un ataque nuclear por estar diseñada para recorrer la información por múltiples caminos para llegar a su destino. En la actualidad esta bondad de múltiples interconexiones que tienen las TIC en el ciberespacio y de acuerdo al estudio de investigación efectuado, sigue siendo una oportunidad para el Estado Mexicano.

c. Facilidad en la búsqueda de información.- La gran capacidad de interconexión en el ciberespacio brinda la oportunidad de acopio de información para hacer del conocimiento a sus empleadores de los aconteceres del ámbito internacional y nacional a través de los medios periodísticos, redes sociales, foros, etc; aunque esta oportunidad representa un desafío a los gobiernos represivos y dictaduras, donde la fortaleza de esos gobiernos es la obscuridad de la información y la prohibición a la libre expresión; esta facilidad de interconexión brinda a la población el medio para formular criterios con una visión más holística antes las eventualidades que existan a su alrededor y sus propios intereses.

d. Contribuye al desarrollo del conocimiento.- Como el subíndice anterior, también el empleo del ciberespacio brinda la oportunidad de poder accesar a un mundo virtual de información digital de las múltiples bibliotecas que están interconectadas, aplicaciones educativas y que proporcionan información académica a la comunidad internacional en cualquier área del conocimiento; así mismo, se puede accesar a platicas (Chats) donde se facilita la información para la solución de problemas de cualquier índole.

2. Las amenazas en el ciberespacio.

Aunque en su entorno global las amenazas que existen en el ciberespacio, la gran mayoría que se identifican son las que van enfocadas al cibercrimen; existen otras que por la naturaleza de su complejidad se están llevando a cabo y la victima desconoce que la están vulnerando en sus sistemas de información; a continuación, se hace una clasificación de estas amenazas que fueron identificadas y que afectan o pueden afectar a nuestro país.

a. Ciberterrorismo.- Una de las principales preocupaciones de los países desarrollados son las actividades que grupos extremistas hacen con las tecnologías de información, comunicación, informática, electrónica o similar, con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente (Díaz García Pedro, 2014). Nuestro país no está exento de sufrir algún atentado de esta naturaleza; de hecho el pasado 24 de noviembre del 2015, el Estado Islámico lanzo una amenaza a los países que integran “La coalición global contra el

Estado Islámico" conformada por los EUA el 10 de Septiembre del 2014 y en la que México decidió ser parte de él; por lo que nuestro país debe estar alerta ante cualquier ataque terrorista de este grupo Islámico radical y que podría perpetrar su ataque incluso a través del Ciberespacio.

b. Ciberataques a las Instituciones de Seguridad Nacional o Infraestructuras Criticas por hacktivistas o Gobiernos extranjeros.- Las redes informáticas del Gobierno pueden ser comprometidas por: fuga de información sensible, intrusión a las TIC´s por grupos criminales, negación de servicios de las infraestructuras críticas del país. (Suministro de energía, agua, combustibles; transporte masivo, redes de telecomunicaciones y servicios financieros, entre otros) o cualquier otra actividad que emplee el Ciberespacio como plataforma para perpetrar su ataque ya sea por hacktivistas como Anonimuos o Gobiernos extranjeros para crear un ambiente inestable o satisfacer algún interés. Nuestro país ya ha sido víctima de esos grupos o incluso es posible que algunos se desconozcan por no haber sido pública la información o simplemente nunca supieron que fueron víctimas.

c. Dependencia Tecnología.- Al ser nuestro país dependiente de tecnología extranjera en el área de las TIC; las Instituciones, empresas, centros educativos, comercio, bancos, etc., se ven comprometidas ante sus desarrolladores porque conocen la tecnología y sus vulnerabilidades, los que nos hace dependientes a esas empresas desarrolladoras o gobiernos extranjeros ante un ataque de destrucción de información contenida en bases de datos gubernamentales sensibles (Fuerzas Armadas, Bolsa Mexicana de Valores, Renapo, INE, CFE, Telmex, Conagua, etc); exposición pública de información confidencial; alteración de procesos informáticos críticos o cualquier actividad que pueda afectar al Sector público o privado.

d. Cibercrimen.- La suplantación de identidad con propósitos criminales e inhabilitación de servicios esenciales de los bancos, sistemas de transporte masivo o suministro de energía; las actividades de fraude, extorsión, espionaje informático, amenazas, robo, acoso a través de las TIC´s reciben el nombre de "Cibercrimen". La atención a este delito es competencia de las policías cibernética dependiente de la Comisión Nacional de Seguridad; en México, cerca del 61% de la población adulta ha sido víctima del Cibercrimen; anualmente se han recibido alrededor de 5000 a 7000 reportes de ciudadanos y los Estados con mayor reporte son: el Distrito Federal, Estado de México, Jalisco, Veracruz y Puebla; por lo que este delito aunque no representa aun un riesgo a la Seguridad Nacional por ser competencia de Seguridad Publica, esta puede escalar a un nivel superior dependiendo el grado de afectación y hacia donde este dirigida (Policía Federal División Científica, 2015).

EL CONSEJO DE SEGURIDAD NACIONAL Y SU RELACIÓN CON EL CIBERESPACIO

El Consejo de Seguridad Nacional (CSN) en México es una instancia deliberativa, la cual fue creada por instrucciones del Presidente Vicente Fox Quesada el 2 de febrero de 2005 y sustentada en la Ley de

Seguridad Nacional (LSN) en sus artículos 12 y 13. Citado consejo está encabezado por el titular del Ejecutivo Federal, cuya finalidad consiste en establecer y articular las acciones y políticas en materia de Seguridad Nacional, conociendo lo siguiente:

- La integración y coordinación de los esfuerzos y medidas orientadas a preservar la Seguridad Nacional, los programas de cooperación internacional, y los lineamientos que permitan el establecimiento de políticas generales;
- El Programa para la Seguridad Nacional y la evaluación de sus resultados;
- La definición anual de la Agenda Nacional de Riesgos y su seguimiento;
- Los lineamientos para que el Centro de Investigación y Seguridad Nacional (CISEN) preste auxilio y colaboración en materia de Seguridad Pública, procuración de justicia y en cualquier otro ramo de la Administración Pública que acuerde el Consejo;
- Los procesos de clasificación y desclasificación de información en materia de Seguridad Nacional, y
- Los demás que establezca el Presidente de la República en el marco de las disposiciones aplicables.

Los demás representantes de este Consejo son de las Secretarías de: Gobernación (Secretario Ejecutivo), Defensa Nacional (SEDENA), Marina (SEMAR), Hacienda y Crédito Público (SHCP), Comunicaciones y Transportes (SCT), Función Pública (SFP) y Relaciones Exteriores (SRE); quienes con base al artículo 16 de la LSN serán convocados por el Presidente del Consejo con la periodicidad que este determine cuando menos bimestralmente.

En la presenta administración, en el Programa para la Seguridad Nacional 2014-2018; se estableció como los principales riesgos y amenazas en primer lugar a los desastres naturales y pandemias, después a la delincuencia organizada transnacional y en tercer lugar definió a la ciberseguridad (Presidencia de la República, 2014); ya que en los últimos años, se ha incrementado las amenazas vinculadas con la gestión del Ciberespacio y esto se ha convertido en una fuente de preocupación para todos los países; a continuación se describen algunas capacidades que el CSN ha logrado en conjunto o a través de las Instancias que la componen:

A. Las Capacidades del Estado Mexicano.

1. Presidencia de la República Mexicana.

a. Estrategia Nacional de Seguridad de la Información.

Durante el sexenio 2007-2012, el Presidente Felipe Calderón Hinojosa, a través del Consejo de Seguridad Nacional ordenó la integración del Comité Especializado en Seguridad de la Información (CESI) como órgano

asesor de citado consejo en el ámbito de la ciberseguridad y la ciberdefensa, citado comité fue integrado con personal especialista de la SEMAR, SEDENA, CISEN y de la SFP.

Este Comité está compuesto por dos grupos: el técnico y el de armonización legislativa; el técnico, es el responsable de elaborar y trabajar la metodología de seguridad de la información bajo la cual se debe regir la Administración Pública Federal; así mismo, debe elaborar y poner en ejecución la Estrategia Nacional de Seguridad de la Información (ENSI), y el grupo de armonización legislativa es el encargado de proponer las leyes y las reformas necesarias para regular el uso del ciberespacio en materia de Seguridad Nacional**.** La Estrategia de Nacional de Seguridad de la Información fue concluida en su primera parte en noviembre de 2011; quedando pendientes su publicación.

b. Estrategia Digital Nacional.

Como una fortaleza en materia de digitalización y explotar las oportunidades descritas anteriormente, en junio del 2013, el Ejecutivo Federal promulgó el decreto de reforma a la CPEUM en materia de Telecomunicaciones y competencia económica; como parte de esta reforma y con la finalidad de hacer efectivo este derecho se creó la “Estrategia Digital Nacional”, la cual permitirá mayor disponibilidad y calidad en los servicios de las TIC, Internet y banda ancha, lo que permitirá insertar a la sociedad mexicana en la información y conocimiento, lo que dará una posibilidad de mayor desarrollo del país; está planeada para ser implementada en el transcurso de los años 2013-2018. Esta estrategia solamente contempla la interconectividad y digitalización y no la protección al ciberespacio.

c. Estrategia Nacional de Ciberseguridad.

Es un documento realizado por la Policía Federal a través de la División Científica que define objetivos y ejes transversales, plasma los principio rectores, identifica a los diferentes actores involucrados y da claridad sobre la articulación de esfuerzos entre individuos, sociedad civil, organizaciones privadas y públicas en materia de ciberseguridad; además señala el modelo de gobernanza para la implementación, seguimiento y evaluación de la Estrategia en materia de Ciberseguridad.

2. Secretaría de Gobernación.

Durante el sexenio del Presidente Felipe Calderón Hinojosa en el año del 2010; la SEGOB a través de la Comisión Nacional de Seguridad, creo en la Policía Federal el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX) en las áreas de Seguridad Pública como un organismo acreditado para atender amenazas de ciberseguridad en México, su misión es proporcionar soporte en la respuesta y defensa en contra de incidentes de seguridad de la información en el dominio.mx e infraestructuras de TIC criticas del país.

El 6 de Julio del 2012, en el Diario Oficial de la Federación se comunica el nuevo Manual de organización general órgano administrativo desconcentrado de la Policía Federal, donde se establece en su orgánica la División Científica con 3 coordinaciones: 1.- Para la prevención de delitos electrónicos, 2.- Innovación tecnológica y 3.- criminalística; siendo esta División científica la que impulso la impulso la creación de una Estrategia Nacional en Ciberseguridad para fortalecer, entre otros la concientización social sobre el uso responsable de las TIC y establecer la visión del Estado mexicano en materia del reconocimiento a los riesgos asociados al empleo de las TIC. (Gobierno de México, 2017).

3. Secretaría de Marina.

El 16 de julio del 2004, la SEMAR fue de las pioneras en materia de protección al Ciberespacio al crear por instrucciones del Alto Mando de la SEMAR, la Comisión de Seguridad de la Información con la misión de: Establecer la política institucional en materia de Seguridad de la Información, para administrar los riesgos en el procesamiento de la información, coadyuvando en la conducción y apoyo a la toma de decisiones de las operaciones navales; actualmente esta Comisión se denomina Unidad de Ciberseguridad (UNICIBER); por otra parte en el Centro de Estudios Superiores Navales se especializa personal de esta Institución e invitados de la Administración Pública Federal. (Presidencia de la República, 2004).

La SEMAR ha fortalecido sus capacidades para la protección al ciberespacio por la información sensible que esta maneja en materia de Seguridad Nacional y ha sido una de las Secretarias del CSN que más activamente ha participado en la capacitación y fomentar la Cultura de Seguridad de la Información en el Ciberespacio de manera prospectiva y reactiva.

4. Secretaria de la Defensa Nacional.

La SEDENA en la presente administración en materia de protección al Ciberespacio, elaboró “el programa para generar el desarrollo de la ciberdefensa en el Ejército y Fuerza aérea Mexicana” con la finalidad de desarrollar capacidades de defensa de la integridad, independencia y soberanía de la nación, así como garantizar la seguridad interior en el ámbito del Ciberespacio. Dicho programa planteó cuatro estrategias:

a. Creación de un Centro para las Operaciones del Ciberespacio (COC)
b. Capacitación de personal en las áreas de tecnologías de la información y seguridad de la información, enfocados a la ciberdefensa y ciberseguridad.
c. Coadyuvar en las políticas públicas para la defensa del Estado Mexicano en el Ciberespacio.
d. Generación de doctrina en materia del ciberespacio.

Así mismo, la SEDENA, tiene en proyecto un memorándum de entendimiento con Perú y se llevan a cabo diversos trabajos entre la SEMAR para unificar la visión de las Fuerzas Armadas Mexicana en el ámbito de Seguridad al Ciberespacio. (SEDENA, 2015).

5. Secretaria de Relaciones Exteriores.

La SRE ha participado y promovido el fortalecimiento al Ciberespacio con el CSN y ha fungido de enlace ante otras naciones tal fue la visita en mayo del 2015 de la Coordinadora Adjunta para Asuntos de Seguridad Cibernética del Departamento de EUA, Michele Markoff, donde sostuvo encuentros con los miembros del Comité Especializado de Seguridad de la Información y con funcionarios del Secretariado Técnico del Consejo de Seguridad Nacional y la Secretaría de Relaciones Exteriores, a fin de explorar áreas de cooperación bilateral en materia de ciberseguridad que tomen en cuenta los retos comunes y la seguridad regional (Secretaria de Relaciones Exteriores, 2015).

6. Secretaría de Comunicaciones y Transporte.

La Agencia Espacial Mexicana (AEM) representa una oportunidad para potencializar el empleo del ciberespacio del Estado Mexicano por la gran capacidad de interconexión que se obtendrá al materializarse esta agencia; la AEM como órgano descentralizado de la SCT la cual tiene la misión de utilizar la ciencia y la tecnología espacial para atender las necesidades de la población mexicana y generar empleos de alto valor agregado, impulsando la innovación y el desarrollo del sector espacial, contribuyendo a la competitividad y al posicionamiento de México en la comunidad internacional, en el uso pacífico, eficaz y responsable del espacio.

La actual administración, ha incluido en el Plan Nacional de Desarrollo 2013-2018, en el objetivo 4.5 “Democratizar el acceso a servicios de telecomunicaciones”, estrategia 4.5.1 “Impulsar el desarrollo e innovación tecnológica de las telecomunicaciones que amplíe la cobertura y accesibilidad para impulsar mejores servicios y promover la competencia, buscando la reducción de costos y la eficiencia de las comunicaciones” el concepto de “Infraestructura Espacial” en una de sus líneas de acción.

Por otra parte, la SCT ha impulsado varios proyectos de conectividad de redes digitales hacia los estados y Municipios para brindar servicios de Internet; reducir costos y apoyar al desarrollo nacional: el autor cuestionó al licenciado Gerardo Ruiz Esparza titular de esa dependencia referente a las estrategias o capacidades que han desarrollado para proteger estos servicios de conectividad en el Ciberespacio, respondiendo que solamente han actuado hacia la conectividad.

7. Secretaria de la Función Pública.

Durante el periodo 2006-2012, la SFP, como parte del proyecto de mejores prácticas, elaboró 9 Manuales de Administración y Aplicación General; el Consejo de Seguridad Nacional instruyó al Comité Especializado en Seguridad de la Información para participar con la SFP en la elaboración del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información “MAAGTICSI” (Presidencia de la República, 2014). Este manual establece procesos uniformes,

acciones y medidas coordinadas en materia de seguridad de la información, mediante la identificación de infraestructura crítica de tecnologías, elaboración de análisis de riesgos y definición de esquemas de respuesta a incidentes de seguridad en tecnologías de la información.

8. Secretaria de Hacienda y Crédito Público

Durante el año 2004, el Sistema de Administración Tributaria (SAT) implementó un mecanismo alternativo en su inicio y obligatorio para el año 2005, después de una serie de reformas al Código Fiscal de la Federación, el SAT presentó este primer esfuerzo como la sustitución de la firma autógrafa del firmante con los mismos efectos y alcances que la firma autógrafa (Izquierdo León, 2011), denominada "**firma electrónica"**[16]. Además de autentificar al contribuyente, la firma electrónica permite la expedición de facturación fiscal electrónica que junto su Clave de Identificación Electrónica Confidencial (CIEC), dio inicio a la actual Firma Electrónica (FIEL).

Este logro de la SHCP a través del SAT ha brindado seguridad a las transacciones electrónicas de los contribuyentes, con su uso se puede identificar al autor del mensaje y verificar que no haya sido modificado (SAT, 2005), lo que representa un avance a la protección de datos en el ciberespacio

PROSPECTIVA DE LA PROTECCIÓN DEL CIBERESPACIO EN MÉXICO

¿Que sería en la actualidad un mundo sin interconexión en el Ciberespacio?, sería como un país sin carreteras. Las grandes ventajas que existen en la interconexión sobre el empleo del ciberespacio es que une fronteras, abre ventanas al conocimiento, incrementa la cultura, la economía, el comercio, apoya la salud, etc; lo que propicia que cada año más gente busque interconectarse a esta red como lo muestran las estadísticas actuales. En México según datos de la Agencia mexicana de Internet (AMIPIC), el 59.8% de la población esta interconectada al ciberespacio y cada año aumenta la cantidad; es un hecho, que la interconexión de las TIC al ciberespacio llego para quedarse ante una población ávida de información global.

Sin embargo, también se espera que las amenazas evolucionen, no solo al robo de los números de tarjetas de crédito y sus contraseñas por la Delincuencia Organizada Transnacional (DOT), sino a influir en la vida política de los países convirtiéndose en un arma universal capaz de destruir social, política económica o militarmente a una nación.

Motivado por lo anterior, conlleva a hacer estrategias que permitan proteger ante cualquier adversidad la información sensible de quienes emplean el ciberespacio como su medio de comunicación. Países como EUA, Rusia, Corea del Sur, Japón, Kenia y países de la Unión Europea son algunos de los numerosos países que han declarado a los ciberataques contra sus gobiernos y ciudadanos como una amenaza para la

[16] La Firma Electrónica es un archivo digital que te identifica al realizar trámites por internet en el SAT e incluso en otras dependencias del Gobierno de la República.

seguridad nacional y, por lo tanto, han desarrollado estrategias o iniciativas de ciberseguridad nacional (BBC, 2017); incluso algunos han creado Cibercomandos al interior de sus Fuerzas Armadas.

En Latinoamérica; países como Argentina, Perú, Colombia , Brasil e incluso México han adoptado planes en ciberseguridad que posteriormente han dado lugar a la creación de Grupos de Respuesta a Emergencias Cibernéticas (CERT); en el Ejército Brasileño, junto al sector nuclear y el espacial están formalizando la Estrategia Nacional de Defensa, sobre las políticas de ciberseguridad y la creación de órganos para su ejecución.

Tabla 2. Matriz comparativa de paises europeos y asiaticos que cuentan con Estrategias en Ciberseguridad.

		Paises Europeos					Paises Asiaticos		
		Alemania	Francia	España	Estonia	Gran Bretaña	Japon	Rusia	China
Protección	Infraestructuras Criticas	✓	✓	✓	✓	✓	✓	✓	✓
	Economía	✓		✓		✓	✓		✓
	Seg. Nac.	✓	✓	✓		✓	✓		
	Biesnestar social	✓			✓	✓	✓	✓	✓
Enfoque	Concientización				✓	✓			
	Conocimiento.					✓		✓	✓
	Educación.				✓	✓			
	Capacidades Ciberneticas Militares.	✓	✓			✓		✓	✓
Sector Público	Liderazgo.	✓	✓	✓	✓	✓	✓		✓
	Marco Jurídico	✓	✓			✓	✓	✓	✓
Sector Privado	Parcipación en la Estrategía.		✓	✓	✓	✓	✓	✓	✓
CooperaciónInternacional	Cooperación en su grupo.	✓	✓	✓					
	Cooperación con otros paises.	✓	✓	✓	✓	✓	✓	✓	

Fuente: Leyva, 2015

Tabla 3. Matríz comparativa de paises de America que cuentan con Estrategías en Ciberseguridad.

		Paises de America integrantes de la OEA					
		Estados Unidos	Canada	Colombia	Brasil	Chile	Argentina
Protección	Infraestructuras Criticas	✓	✓	✓	✓	✓	✓
	Economía	✓			✓		
	Seg. Nac.	✓	✓		✓		
	Biesnestar social	✓	✓	✓	✓		
Enfoque	Concientización	✓	✓	✓	✓	✓	
	Conocimiento	✓					
	Educación	✓		✓	✓	✓	
	capacidades Ciberneticas Militares.	✓		✓			
Sector Público	Liderazgo	✓	✓	✓	✓	✓	✓
	Marco Juridico	✓		✓			✓
Sector Privado	Parcipación en la Estrategía.	✓	✓	✓	✓	✓	
Cooperación Internacional	Cooperación en su grupo.	✓	✓	✓	✓	✓	✓
	Cooperación con otros paises.	✓	✓	✓	✓	✓	✓

Fuente: Leiva, 2015.

Por lo tanto, nuestro país debe realizar esfuerzos conjuntos entre las Instituciones y la iniciativa privada para proteger el ciberespacio ante una eventualidad de cualquier índole trátese de robo a instituciones bancarias, robo de información a las farmacéuticas, a las instituciones del gobierno incluyendo a las de Seguridad y Defensa del país.

HACIA UN MODELO DE PROTECCIÓN

A. Consideraciones del Modelo.

1. La SEDENA y la SEMAR para la protección de su activo de información emplean los conceptos de **ciberseguridad** (controles, procedimientos y normas para proteger los activos en el Ciberespacio) **y ciberdefensa** (Acciones, recursos y mecanismos del Estado en materia de Seguridad Nacional para

prevenir, identificar y neutralizar toda ciberamenaza o ciberataque que afecte a la infraestructura crítica Nacional); las demás Instituciones del CSN solamente tratan el concepto ciberseguridad.

2. Actualmente la única instancia del CSN que hace labores de **ciberseguridad** para afrontar la cibercriminalidad en México es la División Científica de la Policía Federal perteneciente a la SEGOB; citada División está basado en su Estrategia Nacional en Ciberseguridad.

3. La SFP, SCT y la Oficina de la Presidencia de la República han focalizado esfuerzos para hacer del Estado Mexicano, un país digitalizado a través de la Estrategia Digital Nacional misma que busca la interconexión a todos los sectores para el desarrollo y competitividad; y ha considerado la protección al ciberespacio a través de la Estrategia Nacional de Ciberseguridad y el Manual de Administración y Aplicación General en Tecnologías de la Información y seguridad de la Información (MAAGTICSI).

B. Organización del Modelo.

De manera sistemática, el modelo que se propone está organizado en dos bloques: el primero denominado las “fronteras del modelo” y el segundo denominado “el núcleo del modelo”:

1. **Fronteras del Modelo**.

Las fronteras del modelo representan el entorno general de lo que se pretende proteger y da respuesta a ¿Quién? y ¿Qué? se debe realizar:

a. Actores Principales.- Las Instituciones que integran el CSN serán los actores principales, quienes tendrán la responsabilidad de velar por la seguridad del Ciberespacio; siendo el titular del Ejecutivo Federal quien presida este modelo.

b. Cultura de Protección al Ciberespacio.- La educación y la concientización al personal de las Instituciones del Gobierno Federal, así como a la población en general, desde los planteles escolares es básico crear una cultura informática sobre todo del uso adecuado en la protección de sus datos personales y de la información que manejen en el Ciberespacio.

c. Marco Normativo del Ciberespacio.- No se puede concebir un modelo de protección si se carece de un marco normativo que regule la actuación de las personas por el mal empleo del ciberespacio en asuntos que implique al Gobierno, Defensa, Empresas y Sociedad; por lo que se debe realizar una revisión de la legislación nacional actual en materia de protección al ciberespacio y fortalecer las lagunas existentes para la aplicación del modelo propuesto.

2. Núcleo del Modelo.

El núcleo del modelo es la parte medular de las acciones a seguir de manera escalonada para que de forma transversal los actores, la cultura y el marco normativo se conjunten y se materialice el modelo propuesto, da respuesta al ¿Cómo se debe proteger?:

a. Estrategia Digital Nacional.- Como parte de una iniciativa presidencial y ser la estrategia que da soporte a la Infraestructura digital en nuestro país, deberá considerarse en el modelo planteado como punto inicial de las TIC interconectadas al ciberespacio.

b. Estrategias Nacionales que impliquen la protección del ciberespacio.- Se incluirán las dos estrategias en Ciberseguridad (La ya existente) y Ciberdefensa que aún no ha sido desarrollada pero es necesaria que se desarrolle además, se debe incluir la Estrategia Nacional de Seguridad de la Información.

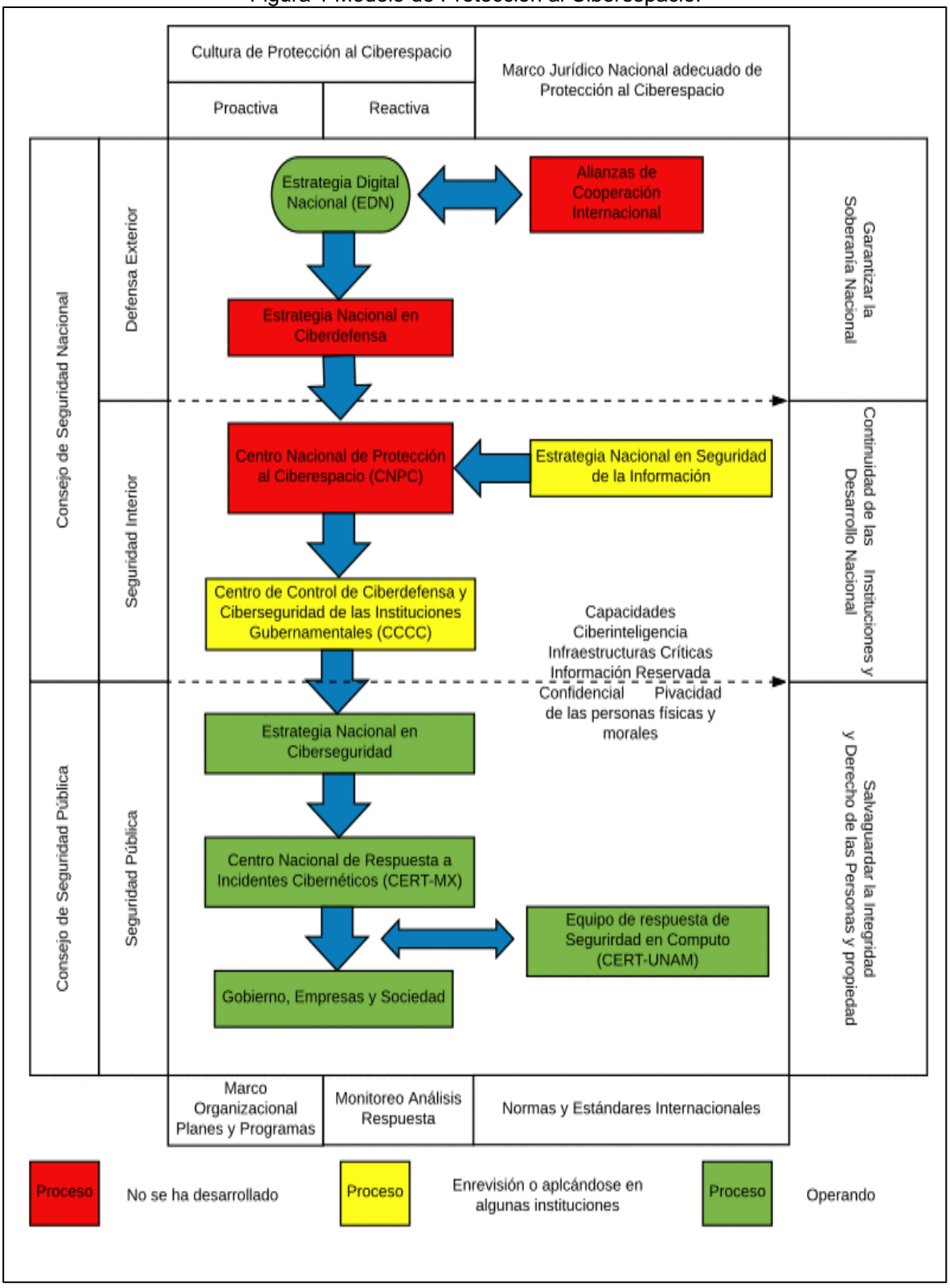
c. Centro Nacional de Protección al Ciberespacio-MX (CNPC-MX) y CERT´s Institucionales.- El CNPC-MX es la Instalación estratégica propuesta integrado con material y personal pertenecientes a las Instituciones que integran el CSN y coadyuvará con los Centros de Control de Ciberdefensa y Ciberseguridad de las Instituciones para contener cualquier incidentes que se suscite en el Ciberespacio y con el CERT-MX o los CERT´s académicos o empresariales.

d. Alianzas de Cooperación Internacional.- Son aquellos tratados y convenios gubernamentales, académicos y de Investigación en materia de protección al Ciberespacio con países extranjeros.

C. Diagrama del Modelo de Protección al Ciberespacio.

A continuacion se presenta la propuesta de modelo de protección en el Ciberespacio, desarrollado con base a los resultados obtenidos; citado modelo puede ser empleado como base y guia para el desarrollo de las estrategias planteadas.

Figura 1 Modelo de Protección al Ciberespacio.



Fuente: elaboración propia.

CONCLUSIONES

La evolución de las TIC en México ha jugado un papel importante en nuestro país para la comunicación y el desarrollo. Los Sistemas de Cómputo y el Internet, han permitido hacer esa relación "TIC-Internet" en la cual el empleo del ciberespacio en México estadísticamente ha incrementado de una manera muy significativa y actualmente es un modo de vida de la población nacional; además, la Estrategia Digital Nacional (ADN) que el Presidente de la República ha impulsado en esta administración, constituye un reto para el país ya que brinda oportunidades que benefician al desarrollo, bajo costo de operación y comunicación, continuidad en las comunicaciones ante eventos catastróficos, facilidad de búsqueda de la información y del conocimiento en general.

Sin embargo, en este trabajo de investigación se identifico que nuestro país esta vulnerable ante las amenazas cibernéticas y esto puede traer consecuencias graves al país, por lo que se concluye:

Se carecen de una "Cultura de protección al Ciberespacio"; en este aspecto: no existe concientización en este ámbito en el personal de las Instituciones del gobierno y de la población en general, se requiere de personal especializado que afronte el compromiso de capacitar, enseñar y actuar de forma proactiva en la protección de activos de información sensibles e infraestructuras criticas; a nivel poblacional y que apoye a diseminar una cultura informática a nivel básico y superior que enfoque esfuerzos a la protección de datos personales y concientización en el uso del ciberespacio.

La Policía Federal a través de la División Científica ha desarrollado una Estrategia Nacional de Ciberseguridad basada en fortalecer la concientización social sobre el uso responsable de las TIC y establecer la visión del Estado mexicano en materia del reconocimiento a los riesgos asociados al empleo de las TIC que su empleo está enfocado al cibercrimen y Seguridad Publica; sin embargo, el Estado mexicano no cuenta con una estrategia en Estrategia Nacional en Ciberdefensa enfocada a la Seguridad Nacional.

Por último, se requiere contar con un "Organismo o Centro Especializado para protección del Ciberespacio que en este estudio fue denominado Centro Nacional de Protección al Ciberespacio CNPC" que englobe esfuerzos conjuntos de las Instituciones del CSN para afrontar amenazas cibernéticas de mayor escala (Ciberterrorismo) y que coordine con Gobiernos de Países u Organizaciones Internacionales en materia de protección al ciberespacio y este enlace con la División Científica y los Centros de Operaciones de Ciberespacio de las Instituciones del gobierno y de las académicas.

BIBLIOGRAFÍA

Álvarez C. L. (2008). Historia de las Telecomunicaciones. México: UNAM.

Cintra, José Thiago (1998). Seguridad Nacional, poder nacional y desarrollo. México: UNAM.

D.O.F. (6 julio 2012). Manual de Organización General Órgano Administrativo Desconcentrado Policía Federal. México

CPEUM. (2014). Constitución Política de los Estados Unidos Mexicanos. Ley Suprema. Secretaría de Gobernación.

Eduardo Alfredo Leyva. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en enfoque Top-Down desde una visión global a una visión local. Argentina

El Diario sin limite. (2018, Mayo). Robo de información, el fraude cibernético más común | 24 Horas. *5 Mayo 2018*. Recuperado de http://www.24-horas.mx/2018/02/19/robo-informacion-fraude-cibernetico-comun/

El hombre que revelo la amplia red de vigilancia en EE.UU. (2013). BBC Mundo, recuperado de: http://www.bbc.com/mundo/noticias/2013/06/130610_edward_snowden_espionajes_eeuu_mr

Excelsior. (2014). México sufre 12 ataques cibernéticos cada segundo: GData | excelsior. March 5, 2018, Recuperado de http://www.excelsior.com.mx/hacker/2014/04/20/95487

García Benavides R. (2013). Las Telecomunicaciones en México. México: UNAM.

Gobierno de España. (2013). Estrategia de Ciberseguridad Nacional. Madrid, España; Presidencia del Gobierno.

Gobierno de México. (2013). Estrategia Digital Nacional. México.

Gobierno de México. (2017). Estrategia Nacional de Ciberseguridad. México.

Hernández Sampieri, Roberto (2010). Metodología de la investigación. Perú: MacGraw Hill.

Ley SEGNAL. (2005). Ley de Seguridad Nacional. México. Diario Oficial de la Federación. 31/01/2005.

LFCDO. (1996). Ley Federal Contra la Delincuencia Organizada. Diario Oficial de la Federación. 7/11/1996.

LFTAIPG. (2014). Ley de Transparencia y Acceso a la Información Pública Gubernamental. México. Diario Oficial de la Federación. 14/07/2014.

Milenio. (2018). México es el país con más ciberataques - Grupo Milenio. Retrieved March 5, 2018, from http://www.milenio.com/negocios/ciberseguridad-empresas-prevencion-web-ataques-peligro-red-ftmercados_0_1097290427.html

Miklos, T.& Tello,M.E. (2007). Planeación Prospectiva. México: Limusa.

Presidencia de la República. (2013). Plan Nacional de Desarrollo 2013-2018. México.

Presidencia de la República. (2014). Programa para la Seguridad Nacional 2014-2018. México.

Secretaria de Relaciones Exteriores. (2015). Tercer informe de labores 2014-2015. México.

Secretaria de la Defensa Nacional. (2015). Tercer informe de labores 2014-2015. México.