Perspectiva de la Seguridad Nacional de México en el Ciberespacio

Mexico´s National Securiti Pespective in Ciberspace

Resumen

En México se entiende por Seguridad Nacional a las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a la ley en la materia, que conlleven entre otras cosas la protección de la nación mexicana frente a las amenazas y riesgos que enfrenta nuestro país, amenazas que pueden tener lugar en el ciberespacio. De esta forma, el presente documento tiene como finalidad, determinar qué bienes nacionales se tienen que cuidar de las amenazas en el ciberespacio para proteger la seguridad nacional, a través de un estudio científico basado en el análisis documental y entrevistas a encargados de la ciberseguridad en diferentes dependencias del gobierno mexicano que pertenecen al Consejo de Seguridad Nacional, así como contribuir a dar elementos para ampliar el tema en el país en este entorno virtual denominado ciberespacio.

Palabras clave

Ciberseguridad en la Seguridad Nacional, Seguridad Nacional, Ciberespacio, Ciberesguriad.

Abstract

In Mexico, National Security is understood like the actions intended immediately and directly to maintain the integrity, stability and permanence of the Mexican State, in accordance with the law on the matter, which entails, among other things, the protection of the Mexican nation against threats and risks that our country faces, threats that can take place in cyberspace. In this way, the purpose of this document is to determine which national assets have to be protected of threats in cyberspace in order to protect national security, through a scientific study based on documentary analysis and interviews with cybersecurity officers in charge of cybersecurity in different dependencies of the Mexican government, which belong to the National Security Council, as well as contributing to give elements to expand the theme in the country in this virtual environment called cyberspace.

Keywords

Cybersecurity in National Security, National Security, Cyberspace, Cybersecurity.

Doctor Jaime Romero Galicia

Egresado de la Facultad de Ingeniería de la UNAM, Maestro en Seguridad de la Información (CESNAV), Doctor en Defensa y Seguridad Nacional (CESNAV).

Funcionario de la Secretaría de Gobernación, Área de Gestión de Seguridad de la Información.

Dirección: Camino Real a Contreras No. 35, Col. La Concepción, C.P.10840, Alcaldía La Magdalena Contreras, Ciudad de México.

Correo: jaime0rg@gmail.com

El autor de este artículo, hace del conocimiento de los editores, que el presente manuscrito es original y de mí autoría, no ha sido publicado parcial o completamente en ninguna parte con anterioridad y

actualmente no se encuentra en revisión en ninguna otra revista.

Artículo recibido el 15 de marzo de 2020.

Los errores remanentes son responsabilidad del autor.

Aprobado el 16 de diciembre de 2020.

El contenido de la presente publicación refleja el punto de vista del autor, que no necesariamente coinciden con el del Alto Mando de la Armada de México o la Dirección de este plantel.

Introducción

Durante el siglo XX, la seguridad nacional fue definida en términos de protección contra amenazas militares externas, ahora en esta última década, el término considera amenazas a la seguridad física y cultural, seguridad territorial, seguridad financiera, seguridad ecológica, seguridad física de los ciudadanos, estabilidad social y política (Ballesteros Martín y Aguilar Joyanes, 2011).

Sin embargo la seguridad nacional en general tiende a ser definida como una «condición» que debe brindar el Estado para el desarrollo de la sociedad a la que sirve (Orozco, 2005). Las definiciones actuales son influenciadas en gran medida por el surgimiento del concepto de seguridad humana (que se centra más en la seguridad del individuo), así como por el fenómeno de la globalización, los factores económicos y la importancia de las Tecnologías de Información y Comunicaciones (Ballesteros Martín y Aguilar Joyanes, 2011).

En México el concepto de Seguridad Nacional todavía es un terminó en discusión (Medina Martínez, 2012), sin embargo, existen varios instrumentos que la definen y refieren, entre los que destacan la Ley de Seguridad Nacional creada en 2005, que establece en su artículo tercero que: «por Seguridad Nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano» (Ley de Seguridad Nacional, 2005, p. 1). Como se observa el concepto se centra en la seguridad del Estado. Además, los retos son bastantes en un mundo cambiante y tal como menciona Valdés Castellanos (2009) «la seguridad nacional… Al igual que el resto de los conceptos políticos no tienen, ni tendrá una definición universalmente aceptada. Su contenido ha variado en función del periodo histórico y del país. No puede ser de otra manera«(pág. 21).

Por otro lado, las tecnologías de la información y de las comunicaciones (TIC) tienen gran relevancia, ya que se han convertido en los últimos años, en un catalizador del progreso humano y también son un instrumento fundamental en las nuevas estrategias de seguridad nacional, y un factor clave en la estabilidad y la seguridad internacional (OECD, 2012). Al respecto el sociólogo canadiense McLuhan (1993) anticipó que los avances de la informática y de las telecomunicaciones convertirían al mundo en una «aldea global», y siendo así, las TIC hoy en día son ubicuas y han sido útiles para el desarrollo de las naciones, así como han originado un entorno denominado ciberespacio[1], que constituye un medio de comunicación mundial entre las personas y las organizaciones.

Así mismo, si bien muchas actividades que se suscitan en el ciberespacio tiene un impacto positivo, también se desarrollan actividades ilícitas, por lo que ahora el ciberespacio se ha convertido en un campo de actuación de la delincuencia organizada cuyas actividades pueden afectar tanto a particulares como a gobiernos enteros (Nye,2010). Es por ello que, el ciberespacio se ha convertido en un nuevo campo de batalla, el cual es global, sin límites formales, sin regulación, anónimo, de fácil

1 El ciberespacio es un dominio creado por el hombre, global, dinámico y en constante cambio, que se encuentra dentro del entorno de información, y el cual consiste de redes interdependientes de infraestructuras de tecnologías de información, incluyendo el Internet, redes de telecomunicaciones, sistemas industriales de control y cualquier otro tipo de sistema tecnológico que contenga procesadores y controladores embebidos capaces de ser accedidos a de forma remota

acceso y barato para ejecutar ataques (Lord y Sharp, 2011), por lo que militarmente al ciberespacio se le conoce en la mayoría de los países como el quinto dominio de la guerra, aunado a los dominios de tierra, mar, aire, y espacio exterior (Murphy, 2010; Clarke y Knake, 2011 ;Schreie, Weekes y Winkler, 2015).

De esta forma, existe la necesidad de proteger el ciberespacio de acciones ilícitas y potencialmente dañinas, a lo que se le conoce como ciberseguridad. En este caso, la ciberseguridad se puede definir como «la colección de herramientas, políticas, conceptos de seguridad, salvaguardas, guías, enfoques de gestión de riesgos, acciones, entrenamiento, mejores prácticas, seguridad y tecnologías, que pueden ser usadas para proteger los activos de la organización y de los usuarios dentro del ciberespacio» (Global Forum on Cyber Expertise, 2016, p. 8).

Así, en el ciberespacio se pueden realizar actividades en contra de Estados nación, por ejemplo, actos como ciberespionaje, ciberterrorismo y ciberguerras (Instituto Español de Estudios Estratégicos, 2011), por ello la ciberseguridad del ciberespacio ya se ha convertido en un asunto de seguridad nacional, por lo que se han desarrollado Estrategias Nacionales de Ciberseguridad, en varios países del mundo que contemplan también la protección de la seguridad nacional en el ciberespacio (ENISA,2016). A las estrategias que sólo se dedican a temas de seguridad nacional las llamaremos Estrategias de Ciberseguridad para la Seguridad Nacional (ECS-SN), a diferencia de una Estrategia Nacional de Ciberseguridad cuyo ámbito es más amplio y trata temas de seguridad nacional y de otros que no los son.

Además, otro tema inherente a la ciberseguridad son los marcos legales que por una parte son necesarios para hacer legítima la actividad de ciberseguridad ante la población, y por otra, permiten castigar los ilícitos cometidos dentro del ciberespacio (ENISA,2012).

Para proteger la seguridad nacional de las amenazas en el ciberespacio, se tiene que identificar primero qué es necesario proteger y a partir de ahí cuáles son esos bienes, servicios o instalaciones nacionales que se tienen que cuidar para lograr este fin. De acuerdo a buenas prácticas la protección de la seguridad nacional en el ciberespacio tiene que ver con la identificación y protección de infraestructuras críticas de información (ICI), por lo que en las condiciones de México es necesario determinar qué y cuáles son esas ICI, pero para realizar esto siempre se tiene que tener en mente cuál es el concepto de seguridad nacional establecido en la ley respectiva.

La importancia de proteger la seguridad nacional de México en el ciberespacio también es evitar que el país sufra ciberataques como los que ha experimentado en los últimos años, ya que el costo de los ciberdelitos en 2016 para México fue de 5,500 millones de dólares (Symantec Corporation, 2016). Por otro lado, se ha encontrado también que los ciberataques de tipo financiero crecen de forma directa al crecimiento del PIB de una nación, y en el caso de México, en los últimos años se ha tenido un crecimiento sólido de su PIB, por lo que también se han incrementado casi en la misma proporción los ciberataques (Control Risk, 2015; Parragez Kobek, 2017). De igual forma de acuerdo con el reporte «Pérdidas Netas: Estimando los Costos Globales de los Ciberdelitos», el costo de los ciberdelitos en México como porcentaje de su Producto Interno Bruto es de 0.17% (McAfee, 2014). De esta forma, las amenazas en el ciberespacio son muchas, por lo que se tienen que tomar las

medidas pertinentes para que no se materializa alguna amenaza que pueda afectar a la seguridad nacional de nuestra nación.

Por otra parte, la Estrategia Nacional de Ciberseguridad (ECSN) publicada en noviembre del 2017 en México, establece el objetivo estratégico número 5 relacionado con Seguridad Nacional y un eje transversal 6 referente a infraestructuras críticas, lo que indica la necesidad de atender el tema de proteger la seguridad nacional en el ciberespacio. De igual forma la ECSN establece que:

> Las acciones necesarias para dar cumplimiento al objetivo estratégico de seguridad nacional deberán ser aprobadas en el seno del Consejo de Seguridad Nacional, y su implementación estará a cargo del Comité Especializado en Seguridad de la Información, en coordinación con la Subcomisión de Ciberseguridad, en el ámbito de su competencia (2017, p. 26).

De esta forma se asienta que para proteger la seguridad nacional de amenazas en el ciberespacio será el Consejo de Seguridad Nacional (CSN) a través del Comité Especializado de Seguridad de la Información (CESI) quién establezca e implemente las medidas necesarias.

Infraestructuras Críticas de Información

Las Infraestructuras Críticas de Información (ICI) se definen como «aquellas infraestructuras de información y comunicaciones interconectadas que son esenciales para mantener funciones societales vitales (bienestar social, económico, de seguridad o salud de la gente)» (Global Forum on Cyber Expertise, 2016, p. 9).

A su vez, la Protección de Infraestructuras Críticas de Información (PICI) se deriva de la anterior definición como «todas las actividades dirigidas a asegurar la funcionalidad, continuidad e integridad de las ICI para disuadir, mitigar y neutralizar las amenazas, riesgos o vulnerabilidades, o minimizar el impacto de un incidente» (Global Forum on Cyber Expertise, 2016, p. 9).

Por otra parte, los potenciales desastres naturales o ataques terroristas, que amenazan las infraestructuras críticas (IC) y las ICI también se están incrementando dramáticamente en nuestros días, por ejemplo, en los últimos años, los apagones en Norteamérica y algunas partes de Europa son una evidencia de vulnerabilidades serias de IC e ICI, sin embargo, la protección de ICI, y principalmente su metodología de identificación, han sido aplicadas a muchos países con serios retos. Hay muchas preguntas no respondidas aún: ¿Qué es lo más crítico entre las infraestructuras de información? ¿Cómo pueden identificarse y priorizarse? (László, 2009).

De acuerdo con el Libro Verde de la Unión Europea sobre un programa europeo para la protección de infraestructuras críticas (Comisión de las Comunidades Europeas, 2005), las ICI son:

- Sistemas TIC que son infraestructuras críticas en sí mismas, y que está basada en sistemas de información, principalmente redes de computadoras.
- TIC que son esenciales para la operación de las infraestructuras críticas (telecomunicaciones, computadoras/software, internet, satélites, etc.), que está basada en redes de computadoras y además en sistemas de info-comunicación

Ejemplos de ICI son los servicios de comunicación móvil, los puntos de intercambio de Internet, los servicios de nombre de dominio, así como los sistemas críticos ciber-físicos y sistemas administrativos clave. Los sistemas críticos ciber-físicos son principalmente los sistemas de control industrial que se utilizan para monitorean y controlan, en general remotamente, sistemas físicos como válvulas, compuertas o switch eléctricos para el control del flujo del agua, de gas, petróleo o la electricidad (Global Forum on Cyber Expertise, 2016). De igual forma el libro Verde de la Unión Europea lista un conjunto de infraestructuras críticas que se pueden tomar como base para determinar las ICI. La relación entre ICI e IC se muestra en la figura 1.

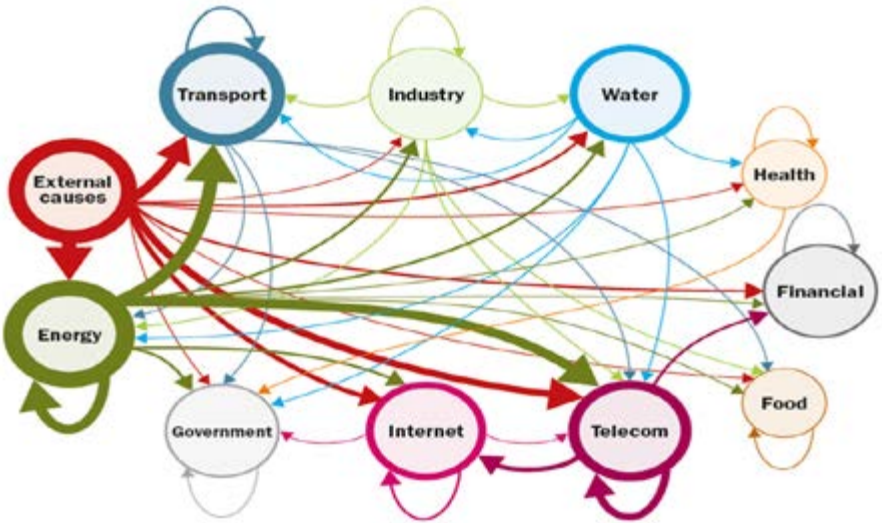
Figura 1 Relación entre IC e ICI

Fuente: Global Forum on Cyber Expertise, 2016.

Como se puede ver, las TIC juegan un doble papel como ICI, por una parte son ICI en sí mismas porque son servicios de comunicación e información entre IC, pero por parte están embebidas en los procesos de IC.

Por otra parte, para empezar a determinar las IC primero se debe definir que es una IC, y después se deben adoptar metodologías para la identificación sistemática de sectores de IC (comunicaciones, energía, salud, transporte, agua, etc.) y servicios, que incluya criterios específicos para evaluar las áreas, la criticidad, las dependencias y los criterios de evaluación transversal. La figura 2 muestra las dependencias transversales y directas de los sectores de IC para la evaluación de riesgos.

Figura 2 Dependencias transversales y directas de los sectores de IC



Fuente: Fuente: Global Forum on Cyber Expertise, 2016.

Posteriormente se recomienda identificar los operadores de las ICI (Públicos, Público-Privado, Privado), y las dependencias entre ICI y cadenas de suministro de información. También es necesario tener conocimiento de aquellas dependencias que no se pueden controlar, por ejemplo, los servicios de comunicación que están en otro país cuya falla puede producir una falla en las IC propias. Con la información anterior se puede realizar una administración de riesgos nacionales y contemplar también una administración de crisis nacionales creando experiencia en el manejo de crisis de ICI, por lo que es recomendable empezar a coordinar un cuerpo de PICI para realizar ejercicios de administración de crisis público-privado involucrando a los sectores/operadores de ICI, para aprender de los errores, y como parte fundamental se recomienda realizar acciones de monitoreo y mejora continua, para crear resiliencia o rapidez de recuperación ante un evento que impacte de forma negativa en las ICI nacionales, así como también es buena práctica tener diálogos internacionales y ser receptivo a la publicación de vulnerabilidades (Global Forum on Cyber Expertise, 2016).

Infraestructuras Críticas de Información en México

El concepto de infraestructuras críticas de información en México no está establecido en una ley, sin embargo en la Constitución Política de los Estados Unidos Mexicanos (2017) se mencionan áreas estratégicas las cuales son: «correos, telégrafos y radiotelegrafía; minerales radiactivos y generación de energía nuclear; la planeación y el control del sistema eléctrico nacional, así como el servicio público de transmisión y distribución de energía eléctrica, y la exploración y extracción del petróleo y de los demás hidrocarburos» (p. 34).

De igual forma en la Ley General del Sistema de Seguridad Pública (2016) señala que:

> se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación, de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, así como de aquellas que tienden a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de la Ley de Seguridad Nacional» (p. 55).

Sin embargo en el Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones, y de Seguridad de la Información (MAAGTICSI), establece que infraestructuras críticas de información son «las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional, en términos de la Ley en la materia» (Diario Oficial de la Federación, 2014, p. 4). De igual forma el MAAGTICSI presenta una metodología para identificar infraestructuras críticas de información en las dependencias del gobierno federal, que está definida en el formato ASI F2.

Por otra parte, derivado de que las empresas buscan reducir costos, están optando por contratar servicios de almacenamiento en la nube, esto es, en empresas que brindan el servicio remoto de almacenamiento y hospedaje de sitios web corporativos (hosting), y si en estas empresas de hosting se manejan infraestructuras críticas de información, es necesario considerarlas porque un ataque a ellas puede poner en riesgo la seguridad nacional del país.

Siendo así, se consideran inicialmente como Infraestructuras críticas de Información de México las siguientes:

- TIC de procesos clave de Instalaciones estratégicas (agua, energía, petróleo, electricidad, nucleares, transporte, salud, militares, principalmente)
- TIC del sector privado considerados como IC (sistema financiero, telecomunicaciones, aeropuertos, etc.)
- TIC de la Estrategia Digital Nacional
- TIC que soportan la Información confidencial de la Presidencia
- TIC que soportan la Información de seguridad nacional (LSN art. 51)
- Servicios en la nube que soportan servicios esenciales para el país

Con esta definición previa de lo que son ICI se procedió determinar aquellos bienes que se tienen que proteger para cuidar la seguridad nacional del país en el ciberespacio.

Materiales y Métodos

El objetivo del estudio fue determinar qué son infraestructuras críticas de información nacionales, y cuáles proteger prioritariamente, para resguardar la seguridad nacional, a través del análisis de entrevistas a actores encargados de la ciberseguridad en diferentes instituciones de gobierno federal en México. Considerando la

naturaleza del objeto de estudio y el objetivo establecido se eligió un enfoque de investigación cualitativo, con un enfoque filosófico pragmático, utilizando técnicas de teoría fundamentada, con métodos de investigación basados en entrevistas de preguntas abiertas y cerradas (encuesta semi-estructurada), análisis estadístico y de texto utilizando para ello los programas de MS Excel y Atlas-Ti.

La Teoría Fundamentada es «una estrategia de indagación en la cual el investigador deriva de una teoría general, teorías abstractas de un proceso, acción o interacción fundamentada en los puntos de vista de los participantes» (Creswell, 2009, pág. 21) e involucra varias etapas de recolección de datos y el refinamiento e interrelación de categorías de información. En este caso, la teoría fundamentada se utilizó como un instrumento de análisis de datos, usando la codificación e interpretación de patrones (Saldaña, 2009), para derivar los conceptos relacionados con las infraestructuras criticas de información que se tienen que proteger de acuerdo a la codificación de respuestas de los entrevistados.

Podemos reconocer cuatro etapas durante la aplicación de la teoría fundamentada, la primera está en el planteamiento de la pregunta de investigación, a la que se sigue la recolección de datos, y después se pasa a la codificación que puede ser de dos tipos, abierta o axial, para terminar en el proceso de validación de la teoría. Estas etapas no son secuenciales, pues el tratamiento de la teoría fundamentada es no lineal en consonancia con lo que es la metodología habitual de la investigación cualitativa (Creswell, 2009).

Con el propósito de encontrar las respuestas a las pregunta de investigación, referente a ¿qué es una infraestructura crítica?, y ¿cómo se puede identificar de acuerdo a una perspectiva basada en de la realidad nacional?, se realizó una entrevista semiestraucturada con la guía de entrevista de preguntas abiertas de la Tabla 1, dejando que el entrevistado proporcionara toda la información posible de acuerdo a su experiencia.

Tabla 1. Guía para entrevista semi-estructurada

Tema	Preguntas
Identificación de infraestructuras críticas de información nacionales	1.1 ¿Cuáles son las infraestructuras críticas de información que usted identifica en México? 1.2 ¿Cómo se pueden identificar las infraestructuras críticas de información del país? ¿Cuáles son los criterios para su identificación?

De igual forma se realizó una pregunta cerrada para que los entrevistados calificaran ICI ya predefinidas de acuerdo a estándares como se muestra en la Tabla 2.

Tabla 2. Pregunta Cerrada 1.3. Calificación de ICI.

Tomando en cuenta que las Infraestructuras Críticas de Información (ICI) son las TIC o Activos de Información, cuya afectación, interrupción o destrucción tendría un impacto negativo en la salud, la seguridad, y el bienestar económico de la mayor parte de la población o en el funcionamiento del Estado, califique cada elementos citado abajo con un valor de 1 a 10 de acuerdo a la importancia de las siguientes (ICI) siendo 1 la menor calificación y 10 la calificación más alta, así como califique con 0, aquel elemento que no considere una ICI.	
Elemento	**Calificación**
TIC y/o Información del Sector de Energía	
TIC y/o Información del Sector de Petrolero	
TIC y/o Información del Sector de Transportes	
TIC y/o Información del Sector de Telecomunicaciones	
TIC y/o Información del Sector de Militar	
TIC y/o Información del Sector de Financiero	
TIC y/o Información del Sector de Salud	
TIC y/o Información del Sector de Agua	
TIC y/o Información de los Aeropuertos	
TIC y/o Información de Plantas Nucleares	
TIC y/o Información de la Presidencia de la República	
TIC y/o Información que soporta la Estrategia Digital Nacional	
Información de Seguridad Nacional señalada en el Artículo 51 de la Ley de Seguridad Nacional	
Otros (si identifica otras ICI no mencionadas, por favor escríbalas):	
1.	
2.	
3.	

Los actores clave para las entrevistas fueron 12 funcionarios responsables de la ciberseguridad en dependencias de gobierno federal, cuyas Secretarias de Estado integran el Consejo de Seguridad Nacional de México. Las dependencias de adscripción de los entrevistados fueron en orden aleatorio: SHCP, SEGOB, SEDENA, Banco de México, RENAPO, Comisión Nacional de Seguridad Nuclear y Salvaguardas (CNSNS), Comisión Nacional de Seguridad (CERT-MX), CISEN, Agencia de Investigación Criminal de la PGR, SEMAR, SENER y PEMEX. Para las entre-

vistas se utilizó un código con la forma PC-ACGF-NN, que tiene el significado abreviado de «Persona Clave, Actor de la Ciberseguridad en el Gobierno Federal». La lista de estos funcionarios fue la siguiente:

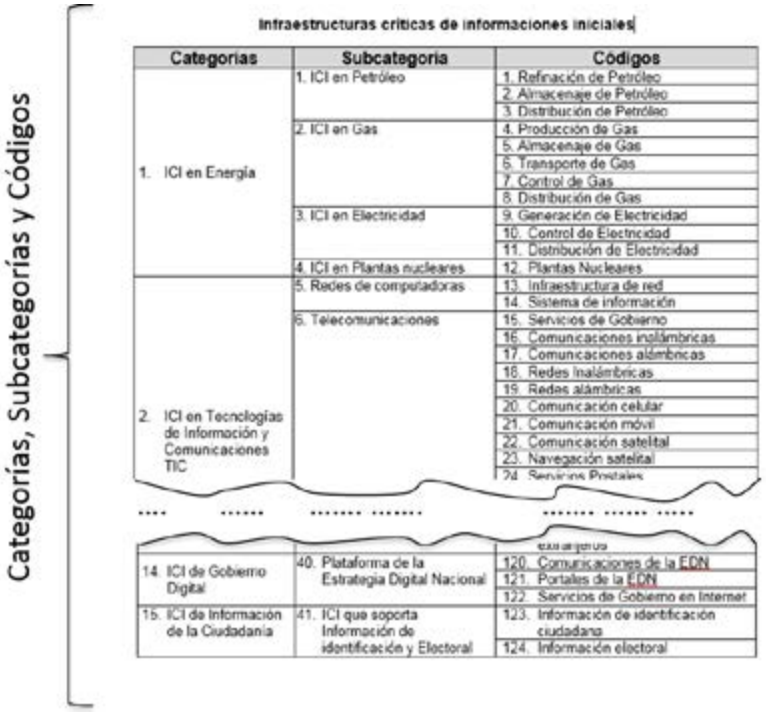
Tabla 3. Lista de funcionarios del Gobierno Federal entrevistados

No.	Clave	Dependencia
1	PC-ACGF-01	D-01
2	PC-ACGF-02	D-02
3	PC-ACGF-03	D-03
4	PC-ACGF-04	D-04
5	PC-ACGF-05	D-05
6	PC-ACGF-06	D-06
7	PC-ACGF-07	D-07
8	PC-ACGF-08	D-08
9	PC-ACGF-09	D-09
10	PC-ACGF-10	D-10
11	PC-ACGF-11	D-11
12	PC-ACGF-12	D-12

Fuente: Elaboración Propia.

Por otra parte, con base al libro Verde de la Unión Europea sobre un programa europeo para la protección de infraestructuras críticas, se construyó una tabla inicial de 14 categorías, 41 subcategorías y 124 códigos, para codificar los datos de entrevistas, como se muestra en la figura 3.

Figura 3. Categorías, Subcatgorías y Códigos



Fuente: Elaboración Propia.

Resultados

Criterios para identificar Infraestructuras Críticas de Información

La problemática de definir de forma clara las ICI lo menciona uno de los entrevistados de la siguiente manera:

> Aquí tenemos que visualizar bien, tenemos que definir un concepto, que es una infraestructura crítica, porque si bien en el MAAGTICSI se manejan infraestructuras críticas de información, en mi concepto personal, infraestructura crítica de información es un concepto que puede ser acotado como infraestructuras críticas. Una infraestructura crítica puede ser considerada como toda aquella infraestructura que permite la vida cotidiana, que permite el desarrollo cotidiano, que permite la armonía, que no altera la vida productiva de un país, el llamarle infraestructura crítica de información es obvio, porque todos los sistemas manejan información, el software es información, los datos que se manejan a través de los sistemas tecnológicos, es información, pero todo eso forma parte de una infraestructura crítica mayor, la infraestructura critica desde el punto

de vista de cómo yo lo veo, es la infraestructura critica, una infraestructura crítica es el sector energético, una infraestructura crítica es el sector económico, una infraestructura crítica es el sector salud, esas son como tal infraestructuras críticas, y cada una de esas infraestructuras críticas se pueden subdividir ya sea en instalaciones estratégicas que son a las que componen a cada una de esas infraestructuras críticas, entonces desde ese punto de vista, nosotros debemos de empezar a trabajar en definir los conceptos y a meterlos en la ley y es eso lo que nosotros estamos tratando de hacer. (…) las infraestructuras críticas de información son todas aquellas infraestructuras que manejan información, ya sea en forma digital o en forma física, inclusive también el factor humano, porque finalmente el factor humano maneja información también, tiene conocimiento también, forman parte de una infraestructuras críticas, entonces, yo siempre he evitado usar el término infraestructura crítica de información, yo lo manejo como infraestructura crítica, y para mí una infraestructura crítica es aquella que en caso de ser dañada puede afectar la vida cotidiana de un país, la vida cotidiana de los ciudadanos, altera de forma grave la vida diaria de los ciudadanos. La infraestructura crítica de información puede estar inmersa en la infraestructura crítica (PC-ACGF-01)

Otro de los problemas a la hora de identificar ICI es determinar cómo considerar aquellas que se comparten con empresas privadas que, por ejemplo, ganaron una concesión en sectores como el petróleo. Uno de los entrevistados señala el tema cuando las infraestructuras críticas de información también están compartidas con la iniciativa privada.

(…) no todas las estructuras están a resguardo del estado...exactamente, si claro, actualmente como el esquema de PEMEX y CFE, la parte energética estaba monopolizada, por eso hoy podemos hablar de las dependencias de PEMEX y CFE, tenían el 90% del mercado, pero ahora con la reforma hay una apertura en la que la iniciativa privada va a ir entrando y que eso además nos pone en una situación con la seguridad nacional, en un paradigma porque lo que se resguarda es lo que pertenece a la nación, en el caso del petróleo es una situación complicada porque la parte del suelo pertenece a la nación, por lo tanto las fuerzas armadas tendrían que estarlo protegiendo, aunque parte de la situación es que la iniciativa privada debería de pagar (…) entonces quien debe de proteger este tipo de infraestructura, para evaluarlo se tendría que hacer una normatividad para estas infraestructuras criticas ya que van a empezar a combinarse o ser mezcladas (PC-ACGF-02).

Los criterios de los entrevistados para determinar qué es una infraestructura crítica de información, fueron dispares y dependieron del enfoque de la organización a la que pertenecen o a su propio criterio, así por ejemplo hubo algunas personas que señalaron que los criterios ya están definidos en el MAAGTICSI o por el CESI, como se indica a continuación

el CESI recientemente ha emitido unas directivas, o una indicaciones de que manera debemos llevar a cabo una identificación de infraestructuras críticas en

cada una de las dependencias, y todo eso se va a unir para tener un inventario nacional sobre las infraestructuras críticas (PC-ACGF-01).

Otros comentaron que un análisis de riesgos a nivel nacional pudiera dar la pauta para determinar cuáles de las infraestructuras de información son críticas para el país, sin embargo la mayoría sí determinó algunos criterios y entre los más importantes están los siguientes

- El uso y el fin que se le da a la información.
- Impacto Económico
- Impacto Social
- Impacto negativo a la imagen del país
- Impacto en la cadena de suministro en la que participan las industrias.

Sin embargo, para la mayoría de los entrevistados el principal criterio para determinar si una infraestructura de información es crítica o no, es el impacto hacia el bienestar de las personas, si afecta a la gente es una infraestructura crítica de información como lo quedo expresado en algunos entrevistados de la siguiente forma:

> [una infraestructura crítica de información es aquella que está en] cualquier proceso que provea lo esencial a la nación, a los habitantes de un país, como es los alimentos, educación, salud, seguridad, incluso educación yo creo que son los elementos fundamentales para que una nación subsista (PC-ACGF-04)
>
> [una] infraestructuras critica de información] es cualquier cosa que le pegue a la sociedad tanto a nivel personal o nivel económico, esos son los dos valores importantes para determinar esas infraestructuras críticas, adicionalmente esta la parte del control por medio de sensores, sobre todo para los sistemas de control industrial (PC-ACGF-02)
>
> Bueno, tomando en cuenta que la seguridad en su más alto nivel ha ido evolucionando y ahora se habla como uno de los aspectos más relevantes de seguridad lo que es la Seguridad Humana, ya la ONU lo maneja en ese nivel, la seguridad humana, entonces el impacto que puede haber por el daño de una infraestructura crítica de información en vidas humanas me parece que es un aspecto que se debe de considerar como el primero. Otro aspecto que es relevante es el impacto financiero, también es muy importante el número de bajas que puedes tener y ya alrededor puedes ir teniendo otro tipo de aspectos que pongan en riesgo al estado como por ejemplo un tema de orden de equilibrio social o de gobernabilidad (PC-ACGF-08).

De igual forma cabe destacar que se hizo énfasis en un punto importante, que consistió en que para determinar si una infraestructuras es crítica o no, es necesario determinar su impacto desde un punto de vista económico o con alguna otra variable que pueda dar un valor, como lo comentó uno de los entrevistados:

> (..) todo esto tendría que llevar una cuantificación desde el punto de vista económico, en cuanto a que si un día no esté funcionando la red eléctrica o que no se tenga producción petrolera o que no exista suministro de agua o que no exista una recaudación fiscal, pues cuanto impacta en la economía del país (PC-ACGF-03)

De igual forma existió una observación muy interesante con respecto a la determinación de infraestructuras críticas, que tiene que ver con cómo la ICI está interconectada con otras industrias, porque puede ser que individualmente se califique como no critica, pero al ver que es un factor importante dentro de una cadena de suministros de varios procesos industriales, puede cambiar su estatus como lo comentó uno de los entrevistados:

> [un criterio para identificar una ICI es el] impacto en la cadena de suministro en la que participan estas industrias, qué tanto está relacionada esta infraestructuras con los procesos productivos de otra índole (PC-ACGF-03)

Pero sin embargo, para identificar ICI, se tiene que referir a la ley de seguridad nacional y a la Agenda Nacional de Riesgos, aunque en México este instrumento es de carácter reservado y únicamente pueden acceder quienes constituyen el Consejo de Seguridad Nacional, por lo que en última instancia, es este organismo el que deberá validar las infraestructuras críticas de información, inicialmente identificadas por los organismos públicos y privados, a través de los comités especializados del Consejo de Seguridad Nacional como lo es el CESI. Al respecto uno de los entrevistados comento lo siguiente:

> Identificar las infraestructuras criticas es un trabajo muy grande, tenemos que primero voltear a ver la agenda nacional de riesgos, tenemos que ver todos los riesgos que presenta el país, ver que sectores pueden verse afectados, ver cuáles son los componentes principales de esos sectores, y en base a eso catalogarlos por niveles, ver cuáles son los que afectarían grandemente a nuestro país, cuáles afectarían menos y así sucesivamente, para poder nosotros definir una estrategia con líneas de acción que nos permitan atender las problemáticas que surgieran en esas infraestructuras críticas de acuerdo a su nivel de importancia (PC-ACGF-01).

Por último, un aspecto muy relevante es que la identificación de infraestructuras críticas de información debe ser un proceso continuo, pues debido a la incorporación creciente de las TIC en diversos sectores, muchas de las infraestructuras físicas o industrias que en este momento no son críticas, podrían con el paso del tiempo volverse críticas debido a la incorporación de TIC dentro de su proceso de modernización, como lo expuso uno de los entrevistados

> también vamos haciendo una transición hacia allá, vemos la red inteligente de CFE que se está proyectando, a medida de eso los esquemas son más vulnerables porque mientras sean más analógicos, no tan comunes, hasta cierta manera están protegidos, pero como vamos hacia una transición hacia la digitalización, hacia los sensores y el internet de las cosas creo que este tema de la ciberseguridad se vuelve mucho más crítico, entonces vamos avanzando en el internet de las cosas, sucede que el ámbito de competencia se vuelve más fuerte, hacia el sistema financiero, hacia ciertas infraestructuras o información pero a medida que la participación del internet de las cosas vaya aumentando, creo que es un punto que hay que ir reforzando. Entonces creo que la parte de la ciberseguridad va a ir

> creciendo por que los elementos digitales cada vez forman mas parte de nuestra vida y al suceder esto, la ciberseguridad es más importante.. (PC-ACGF-02)

De esta forma vemos que la identificación de ICI es un proceso dinámico, que no es sencillo debido a que no solo se deben determinar las ICI de forma individual, sino también de una manera interconectada e integral para ver si de ahí surge otras ICI o industrias que en primera instancia no eran relevantes, así como también hay que revisar los riesgos que están planteados por el Consejo de Seguridad Nacional, que es la última instancia que debería ver si lo que en un determinado momento se ha clasificado como ICI lo es en base a los riesgos plasmados en la Agenda Nacional de Riesgos, por último no hay que olvidar que la identificación es un proceso dinámico, por las constantes innovaciones de las nuevas tecnologías y las modernizaciones que se están haciendo a diferentes industrias, que desde el punto de vista de TIC pueden ser no críticas en este momento pero que en el futuro lo pudieran ser.

Del análisis de las entrevistas el concepto de ICI puede ser establecido como: Las TIC no sustituibles que soportan las infraestructuras críticas del país, y que a su vez son imprescindibles para brindar servicios esenciales a la población para vivir, y cuyo daño provocaría un perjuicio profundo en el bienestar de las personas y en el funcionamiento de las instituciones del Estado.

Identificación de Infraestructuras Críticas de Información

En la identificación de las de ICI del país, que realizaron los entrevistados cuando se hizo la pregunta 1.1, la cual demandaba una respuesta espontánea de los participantes sin mostrarles algún catálogo de ICI diseñado previamente, se obtuvieron los resultados de la figura 4.

Figura 4. Codificación de las entrevistas para identificación de ICI

Fuente: Elaboración propia.

De esta lista se observa que hay descripciones muy globales y algunas más precisas. Esta diferencia en definiciones refleja la forma tan diversa de conceptualizar las ICI, ya que no hay una homologación, incluso para poder determinar la misma infraestructura crítica. Cabe aclarar, que la gráfica muestra las categorías en lugar de los códigos, debido a que las infraestructuras críticas de información determinadas en las entrevistas fueron descritas de forma muy general, así como algunos códigos fueron creados al vuelo para tratar de adaptarse a las respuestas obtenidas de los entrevistados.

Los conceptos que más se repitieron con las preguntas abiertas fueron las siguientes, indicando entre paréntesis la frecuencia en que se repitieron.

- Sector financiero (5)
- Energía eléctrica (4)
- Defensa nacional (3)
- Petróleo (2)
- Bancos (2)
- Transporte (2)
- Telecomunicaciones (2)

Es importante señalar que las dos ICI más señaladas durante las entrevistas fueron la infraestructuras del sector energía y las del sector financiero, la primera porque la energía eléctrica es indispensable para que funcionen prácticamente todos los sectores del país, y la segunda porque el flujo de dinero es indispensable para poder realizar cualquier actividad de compra de bienes y servicios, ya que en las actividades sociales, el flujo de dinero es tan indispensable que una interrupción en este sector provocaría daños a nivel internacional. Es por ello que en caso de una ciberguerra, como la ocurrida en Estonia o en Georgia uno de los primeros objetivos fue afectar al sector financiero del país objetivo (Klimburg, 2011).

La siguiente tabla muestra la calificación promedio para cada ICI que los funcionarios entrevistados proporcionaron:

Tabla 4 Calificación de Infraestructuras Críticas de Información

Infraestructuras críticas de información	Promedio Calificación
TIC y/o Información del Sector de Energía	9.13
TIC y/o Información del Sector de Petrolero	9.63
TIC y/o Información del Sector de Transportes	8.50
TIC y/o Información del Sector de Telecomunicaciones	9.38
TIC y/o Información del Sector de Militar	9.13
TIC y/o Información del Sector de Financiero	9.38
TIC y/o Información del Sector de Salud	9.00
TIC y/o Información del Sector de Agua	9.25
TIC y/o Información de los Aeropuertos	9.00

Infraestructuras críticas de información	Promedio Calificación
TIC y/o Información de Plantas Nucleares	8.00
TIC y/o Información de la Presidencia de la República	7.50
TIC y/o Información que soporta la Estrategia Digital Nacional	6.75
Información de Seguridad Nacional señalada en el Artículo 51 de la Ley de Seguridad Nacional	8.13
Otros:	
1 Banco de México	10.00
2. Fondo Mexicano del Petróleo	9.00
3. Infraestructuras del Ciberespacio, como redes sociales, internet de las cosas y cómputo en la nube	9.00
4. Marítimo (OMI-Ciberseguridad, Puertos, buques)	8.00
5. Identidad de las personas	9.00
6. Alimentario	6.00
7. Sistema Electoral	5.00

Fuente: Elaboración propia, con base a las entrevistas realizadas a funcionarios públicos.

De acuerdo con la pregunta 1.3 que se les hizo a los entrevistados, las cinco principales ICI identificadas (sin considerar el rubro de otros debido a que la calificación solo fue de quien lo propuso), en orden de prioridad, son:

1) Petrolero
2) Telecomunicaciones
3) Financiero
4) Agua
5) Energía

Cabe señalar que en el rubro de otros, los entrevistados brindaron ICI adicionales que para ellos eran fundamentales, y en ellas cabe destacar que se identificó al Banco de México y el Fondo Mexicano del Petróleo como infraestructuras críticas de información importantes.

Con los resultados obtenidos de las entrevistas, y análisis de datos se determinó que las ICI del país que se deben de cuidar para proteger las Seguridad Nacional en el Ciberespacio son las siguientes en orden de prioridad:

Tabla 5 Identificación de ICI para la protección de lSeguridad Nacio

Elementos del modelo	Valores
Infraestructuras críticas de información	**Más importantes** 1. Banco de México 2. Sector de Petrolero 3. Telecomunicaciones 4. Sector de Financiero 5. Agua 6. Energía 7. Militar 8. Salud 9. Aeropuertos 10. Fondo Mexicano del Petróleo 11. Infraestructuras del Ciberespacio (redes sociales, Internet de las cosas y cómputo en la nube) 12. Identidad de las personas **Importantes** 13. Transportes 14. TIC que soportan Información de Seguridad Nacional señalada en el Artículo 51 de la Ley de Seguridad Nacional 15. Plantas Nucleares 16. Sector Marítimo (OMI-Ciberseguridad, Puertos, buques) 17. TIC que soporta Información confidencial de la Presidencia de la República 18. TIC que soportan la Estrategia Digital Nacional

Por otra parte los actores de la ciberseguridad que señalaron que en sus dependencias manejan infraestructuras críticas de información del país fueron de SEMAR, PEMEX, BANXICO, RENAPO, CISEN, SHCP y SEDENA, siendo la información de esas ICI reservada.

Discusión

Las principales ICI que se identificaron fueron las del Banco de México y Sector Petrolero, resultado que es congruente con lo que han establecido algunos estudios sobre las mayores amenazas en el ciberespacio en México, los cuales señalan que los bancos son los objetivos principales de los ciberataques porque la finalidad es obtener un beneficio monetario, y estos ataques son perpetrados principalmente por el crimen organizado (Control Risk, 2015). Esto también es correspondiente con los últimos problemas que se han tenido en el país relacionado con la gran cantidad de fraude bancario a través de medios electrónicos reportado frecuentemente por la CONDUCEF o los últimos problemas relacionados con el robo de 300 millones de pesos de diversos bancos que se conectaban al SPEI ocurrido en el año en curso (Mares, 2018).

En contraste las ICI correspondientes a las TIC que soportan la Estrategia Digital Nacional (EDN) y la información de la Presidencia de la República no fueron consideradas tan importantes en principio porque la EDN a pesar de sus avances, todavía no se consolida como un servicio esencial para la población, y en el caso de la información de la Presidencia, sus implicaciones iniciales son de daño de imagen.

Un hallazgo importante que se detectó durante el estudio es que a pesar que la mayoría de los funcionarios de gobierno entrevistados han participado en el CESI, manejan diferentes conceptos de ICI, así como diferentes criterios para identificar las mismas, además la mayoría de los entrevistados no han considerado las interdependencias entre ICI, esto es, no hay una homologación de criterios aunque prácticamente todos tienen un grado de formación muy bueno sobre ciberseguridad.

Además, los participantes identificaron las ICI de una forma muy general, incluso no por el nombre de la industria, sino por el nombre de las instituciones que las manejan, por lo que la tabla de categorías, subcategorías y códigos para codificar y analizar la información fue demasiado exhaustiva obligando a utilizar códigos más genéricos. Esto puede deberse principalmente que los participantes no han tenido la oportunidad de revisar a detalle los estándares para protección de IC y de ICI, que tienen que ver más con la ciberseguridad de un país más que con la de una institución.

Una de las aportaciones importantes de los participantes cuyas dependencias administran ICI es que la ciberseguridad para proteger esas infraestructuras tiene varios matices y va evolucionando, por ejemplo, debido a la reforma energética en donde varias empresas privadas han entrado a industrias que antes eran exclusivas del gobierno, las protección de ICI es más difícil, pues tendrá que ser una mezcla de iniciativas publico privadas para proteger ICI en un sector determinado. Esto sin dejar de lado las ICI que están exclusivamente en propiedad de la iniciativa privada, y los continuos cambios de ICI derivados de la evolución tecnológica.

Conclusiones

Las ICI es el principal activo de una nación que se tiene que proteger en el ciberespacio para proteger la Seguridad Nacional, pues ataques a estas infraestructuras causarían un gran impacto negativo a la mayor parte de la población y al funcio-

namiento de las instituciones gubernamentales, lo que prácticamente pondría en peligro inminente la integridad, estabilidad y permanencia del Estado.

Las principales ICI identificadas en México fueron: 1. Banco de México, 2. Sector de Petrolero, 3.Telecomunicaciones, 4. Sector de Financiero, 5. Agua, 6. Energía, 7. Militar, 8. Salud, 9. Aeropuertos, 10. Fondo Mexicano del Petróleo, 11. Infraestructuras del Ciberespacio (redes sociales, Internet de las cosas y cómputo en la nube), y 12. Identidad de las personas.

De igual forma, se comprobó lo que establece el Plan Sectorial de Defensa Nacional 2013-2018 (2013) que señala que la ciberseguridad no se ha visto desde un punto de vista de la defensa nacional ni de seguridad nacional, sino que solamente desde un punto de vista de seguridad institucional, ya que las dependencias de gobierno que fueron consultadas nada más se restringen a cuidar su propia ciberseguridad pero no ven la ciberseguridad de aquellos organismos públicos y privados a quienes pueden afectar o de quienes pueden ser afectados, por lo que todavía falta mucho trabajo para que se constituya un esfuerzo nacional de ciberseguridad en donde todas las instituciones trabajen coordinadamente para proteger las ICI del país y no solamente las que les corresponda administrar.

Es imprescindible recalcar que cuando hablamos de ICI estamos hablando de activos de la nación, no de activos de una institución, aunque al final las instituciones u organizaciones son quienes las administran, y que el documento adecuado para coordinar los esfuerzos para proteger las ICI de un país es una Estrategia de Ciberseguridad para la Seguridad Nacional, la cual está única y exclusivamente enfocada a la Protección de las Infraestructuras Críticas de Información y cuyo propósito es cuidar la seguridad nacional en el ciberespacio.

Teniendo claro cuáles son las ICI que se deben cuidar, se puede empezar a trabajar en una Estrategia de Ciberseguridad para la Seguridad Nacional la cual debe desprenderse de la Ley de Seguridad Nacional y debe de operarse a través del CESI, atendiendo también al objetivo estratégico 5 y eje transversal 6 de la Estrategia Nacional de Ciberseguridad.

Bibliografía

- Ballesteros Martín, M. A.; Aguilar Joyanes, L. (Julio-Diciembre 2011). Los efectos de la globalización en el ámbito de la seguridad y defensa. México: Inteligencia y Seguridad, pags. 11-28
- Clarke, R. y Knake, R. (2011). Guerra en la Red, Los nuevos campos de batalla. Barcelona: Ariel
- Comisión de las Comunidades Europeas (2005). Libro Verde, Sobre un programa Europeo para la protección de infraestructuras críticas: Bruselas.
- Constitución Política de los Estados Unidos Mexicanos (2017): DOF 24-02-2017. Cámara de Diputados del Honorable Congreso de la Unión de México.
- Creswell, J. W. (2009). Research Design Qualitative, Quantitative and Mixed Methods Approaches (3a ed.). EU: SAGE Publications.
- Comisión de las Comunidades Europeas (2005). Libro Verde: Sobre un Programa Europeo para la Protección de Infraestructuras Críticas. Bruselas.
- Control Risk. (2015). Cyber Threats to the Mexican Financial Sector. UK. Disponible en:https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/2015-09-09-cyber-mexico-whitepaper-WEB.pdf
- Diario Oficial de la Federación. (8 de mayo de 2014). ACUERDO que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de información y comunicaciones, y en la seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.
- ENISA. (2016). National Cyber Security Strategies in the World. Bruselas Belgica. the European Union Agency for Network and Information Security (ENISA). Recuperado de: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world
- ENISA. (2012). National Cyber Security Strategies, Practical Guide on Development and Execution. Bruselas Belgica. the European Union Agency for Network and Information Security (ENISA). Recuperado de: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
- Estrategia Nacional de Ciberseguridad (2017). Presidencia de la República. Unidad de Innovación y Estrategia Tecnológica de la Oficina de la Presidencia de la República: México.
- Global Forum on Cyber Expertise. (Noviembre de 2016). The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection.
- Instituto Español de Estudios Estratégicos (2011), Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio. Cuaderno de Estrategia 149. España: Ministerio de Defensa.
- Klimburg, A. (2011). Mobilising cyber power. Survival, 53(1), 41-60.
- Ley de Seguridad Nacional (2005). Diario Oficial de la Federación. Cámara de Diputados del Honorable Congreso de la Unión de México.
- Ley General del Sistema de Seguridad Pública (2016). Diario Oficial de la Federación Cámara de Diputados del Honorable Congreso de la Unión de México.
- László, K. (Septiembre de 2009). Possible Methodology for protection of Critical Information Infrastructures. Hadmérnök, IV(3), 13.
- Lord, K., y Sharp, T. (2011). America's Cyber Future Security and Prosperity in the Information Age

volume II. Washington: Center for New American Security (CNAS).

- Mares M. A. (15 de mayo de 2018). Robo electrónico del siglo. El economista. Recuperado de https://www.eleconomista.com.mx/opinion/Robo-electronico-del-siglo-20180515-0034.html
- McAfee. (2014). Net Losses: Estimating the Global Cost of Cybercrime. Santa Clara California, USA: McAfee Inc.
- Medina Martínez, F. (2012). La transformación del concepto de seguridad nacional en México. Nueva Epoca, 218-235.
- Murphy, Matt (2010). Cyberwar: War in the fifth domain. Economist, July,3.
- McLuhan, M. y Powers, B.R.(1993). La aldea Global, Transformaciones en la vida y los medios de comunicación mundiales en el siglo XXI, Barcelona España: Editorial GEDISA S.A.
- Nye, Joseph S. Jr (May, 2010) Cyber Power. Estados Unidos: Harvad Kennedy School.
- OECD. (2012). Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.
- Orozco, G. (2005). El concepto de la seguridad en la Teoría de las Relaciones Internacionales. Revista CIDOB d'afers internacionals, 161-180.
- Parragez Kobek, L. (2017). The State of Cybersecurity in Mexico: An Overview. México: Wilson Center's Mexico Institute.
- Programa Sectorial de Defensa Nacional 2013-2018 (2013). Diario Oficial de la Federación. Presidencia de la Republica.
- Schreie F., Weekes B. y Winkler T. H. (2015). Cyber Security: The Road Ahead. Ginebra Suiza: The Geneva Centre for the Democratic Control of Armed Forces (DCAF).
- Symantec Corporation. (2016). Informe Norton Sobre Ciberseguridad 2016: Comparaciones Globales Recuperado el 7 de marzo de 2017, de https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf
- Valdés Castellanos, G. (2009). La Inteligencia para la Seguridad Nacional en el Siglo XXI. En ESISEN, Inteligencia y Seguridad Nacional (págs. 21-29). México: ESISEN.