Revista Internacional de Ciencias Sociales y Humanidades SOCIOTAM
Vol. XXVIII, N. 2 (2018), pp. 69-93.

CONCEPTUALIZACIÓN DE UNA ESTRATEGIA DE CIBERSEGURIDAD PARA LA SEGURIDAD NACIONAL DE MÉXICO

Jaime ROMERO GALICIA
Secretaría de Gobernación, México

RESUMEN

Las estrategias de ciberseguridad pueden tener diferente ámbito de acción. Pueden ser empresariales, institucionales, nacionales o regionales, entre otras, pero una estrategia de ciberseguridad para la seguridad nacional, es específicamente un instrumento para atender las amenazas a la seguridad nacional en el ciberespacio.

Su principal función es establecer una adecuada coordinación de los diferentes sectores públicos y privados, que controlan y administran aquellos servicios que dependen de las Tecnologías de Información y Comunicaciones (TIC) para su operación, y que son esenciales para el bienestar de la población y el funcionamiento de las instituciones del Estado.

Las TIC que soportan estos servicios esenciales son conocidas como Infraestructuras Críticas de Información (ICI) y su protección es el principal propósito de una estrategia de ciberseguridad para la seguridad nacional.

Palabras clave: seguridad nacional, estrategia de ciberseguridad para la seguridad nacional, ciberseguridad para la seguridad nacional, ciberseguridad nacional, infraestructuras críticas de información, protección de infraestructuras críticas de información.

CONCEPTUALIZATION OF A CYBERSECURITY STRATEGY FOR MEXICO´S NATIONAL SECURITY

ABSTRACT

Cybersecurity strategies can have different action contexts such as business, institutional, national, or regional related, among others. Having a cybersecurity strategy for national security is considered an instrument to address threats of national security in cyberspace. Their main function is to establish an adequate coordination among different sectors, both public and private, that control and manage

all services that depend on ITC to operate, and that are essential for the wellbeing of the society and the performance of State institutions.

ITC´s that support basic services are known as Critical Information Infrastructures and their main purpose is to protect a cybersecurity strategy for national security.

Keywords: National security, cybersecurity strategy, cybersecurity for national security, national cybersecurity, critical information infrastructures, protection.

SEGURIDAD NACIONAL Y SU RELACIÓN CON LA CIBERSEGURIDAD

En 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 y estabilidad social y política (Ballesteros Martín y Aguilar Joyanes, 2011).

En particular, el factor económico tiene gran preponderancia, porque si un país tiene una economía fuerte tendrá mejores condiciones para hacer frente a las amenazas a la seguridad nacional, que tiene a su vez la principal finalidad de que el Estado brinde las condiciones adecuadas a los ciudadanos para su desarrollo individual, que les permita contribuir de forma importante al desarrollo económico del país (OECD, 2012), dando como resultado la ecuación: A mayor fortaleza económica, mayor seguridad para la Nación (Vizarretea Rosales, 2003).

Siendo así, 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 (TIC) en las estrategias de seguridad nacional (Ballesteros Martín y Aguilar Joyanes, 2011).

En este sentido, Cintra menciona que:

> *en el marco de la acelerada transformación del mundo contemporáneo, la expresión política del Poder Nacional se encuentra profundamente afectada por el factor Ciencia y Tecnología (…) el desarrollo tecnológico ha obligado al Estado a asumir nuevos retos de decisión y acción (…) bajo los objetivos nacionales al político le cabe decidir qué hacer en función del logro de aquellos objetivos; al técnico le queda reservado indicar cómo hacer* (1991:13).

De esta forma, las tecnologías han creado nuevos problemas a la seguridad nacional que antes no existían y que, por lo tanto, el Estado debe atender.

Por otro lado, las TIC tienen gran relevancia, ya que se han convertido en los últimos años en un catalizador del desarrollo humano y también son un instrumento fundamental en las nuevas estrategias de seguridad nacional e internacional, y un factor clave en la estabilidad y la seguridad internacional.

Al respecto, McLuhan (1993) anticipó que los avances de la informática y de las telecomunicaciones convertirían al mundo en una "aldea global".

En México, el concepto de Seguridad Nacional todavía es un término en discusión (Medina Martínez, 2012). Sin embargo, existen varios instrumentos que la definen y refieren, entre los que destacan la Ley de Seguridad Nacional (LSN) 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" (2005:1). Como se observa, el concepto se centra en la seguridad del Estado.

Así, los retos son bastantes en un mundo cambiante, y tal como menciona Valdés Castellanos:

> *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* (2009:21).

De esta forma, la Ciberseguridad para la Seguridad Nacional (CSSN) es un concepto que debe estar estrechamente ligado a la definición legal de Seguridad Nacional del país, pues en la LSN se definen cuáles son las amenazas que implica el concepto, lo que permite determinar qué cuidar en el ciberespacio, para que los efectos negativos en contra de la seguridad nacional no se materialicen en el mundo físico.

En el caso de México, se consideran amenazas a la seguridad nacional que se pueden realizar dentro del ciberespacio, entre otras:

> *I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional; (…) V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada; (…) XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos* (Ley de Seguridad Nacional, 2005:1).

EL CONCEPTO DE CIBERESPACIO

Las TIC han sido un catalizador para el desarrollo de los países y las sociedades, y constituyen un entorno virtual denominado ciberespacio. El término ciberespacio originalmente fue introducido primero en el mundo de la ciencia ficción en 1984, por William Gibson, autor de la novela *Neuromante*. De acuerdo con Gibson, el ciberespacio es una red espacial de almacenamiento de datos digitales con conectividad para acceso e interacción a través de una conexión de computadora (2008).

La primera referencia indirecta que se hizo del término en el mundo real fue en la Directiva de Decisión Presidencial 63 de Estados Unidos en 1998, para proteger las infraestructuras críticas, en don-

de se habló en términos de ataques en sistemas "basados en ciber" (Hare, 2010).

Sin embargo, el ciberespacio se afianzó en el lenguaje de ciberseguridad con la publicación de la *National Strategy to Secure Cyberspace,* publicada por la administración Bush en 2003 (Bush, 2003). Pero no fue hasta el año final de la administración Bush que el término fue completamente definido por el Gobierno federal como "Las redes interdependientes de infraestructuras de tecnologías de información incluyendo Internet, redes de telecomunicaciones, sistemas de cómputo y procesadores, y controladores embebidos en industrias críticas" (Hare, 2010:13). Esta definición deja en claro que el ciberespacio es considerado más grande que Internet.

Lo que hace que el ciberespacio sea único es que es hecho por el hombre y, por lo tanto, está en un continuo estado de flujo, es simultáneamente lineal y no lineal, y su inmensidad y alcance desconocido impide la precisa identificación de sus límites (Hall, 2011).

> *Es importante señalar que el ciberespacio constituye un campo de desarrollo, en el cual se transfiere información económica, social y gubernamental, que debe ser cuidada y es la base de muchos servicios actuales de la sociedad, por lo que es necesario crear políticas que aseguren que este campo esté disponible para que los servicios se establezcan con normalidad y fuera de riesgos o acciones contrarias que puedan perjudicar a personas, empresas o gobiernos. Es por ello que se han creado políticas y medidas de seguridad del ciberespacio para proteger este campo* (Weiss, 2008:103).

Sin embargo, el ciberespacio también ha sido un entorno en donde se desarrollan actividades delictivas que afectan a individuos, organismos públicos y privados e incluso a países enteros, por lo que el ciberespacio también se ha constituido como un campo de conflicto.

De esta forma, el ciberespacio es tan importante hoy en día y su protección tan fundamental, porque ahí tienen lugar muchos procesos productivos y se establece la comunicación de las sociedades, que ha sido considerada militarmente por 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; Schreie *et al.,* 2015).

El ciberespacio está siendo utilizado cada vez más como un teatro de conflicto político, económico y militar, en donde los conflictos son campañas paralelas en Internet de acciones hostiles en el mundo real. Además, el ciberespacio carece de identidad y espacio físico cuando lo comparamos con los otros dominios de la guerra; esto es, no tiene extensión definida (Lanzendorfer y Spangler, 2015).

Por otra parte, frecuentemente se considera que el ciberespacio solamente son las infraestructuras de las TIC que soportan los procesos de negocios. Sin embargo, uno de los principales componentes del ciberespacio son los Sistemas Industriales de Control (ICS por sus siglas en inglés: *Industrial Control Systems*) que forman parte integral de la infraestructura industrial que es un bien nacional. Estos sistemas incluyen Sistemas de Control Distribuido (DCS), Sistemas de Adquisición de Datos y Control de Supervisión (SCADA), Controladores Lógicos Programables (PLC) y dispositivos tales como Unidades de Telemetría Remota (RTU), medidores inteligentes e instrumentos de campo inteligentes, incluidas válvulas programadas remotamente y relevadores electrónicos inteligentes. Así mismo, los ICS son técnica, administrativa y funcionalmente más complejos y únicos, en comparación con los sistemas de negocios de TIC (Bolongna *et al.,* 2013).

Resumiendo, el ciberespacio es un dominio creado por el hombre, global, dinámico y en constante cambio, que se encuentra dentro del entorno de información. 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 de forma remota.

El ciberespacio también implicará un cambio de poder económico, dependiendo de cómo se muevan las situaciones comerciales en el mundo, por lo que:

> *A pesar de que Estados Unidos en el presente es la fuerza dominante en términos de Internet y el ciberespacio, la tecnología se propaga ampliamente a todo el mundo y el menor número de usuarios se concentra en el mundo occidental, y el cambio del poder (económico, político y estratégico) se está moviendo de América a Asia* (Ventre, 2014:16).

Siendo así, el ciberespacio es un nuevo dominio para los estudios de seguridad con muchas preguntas por resolver. Además, el ciberespacio presenta todas las condiciones para una tormenta perfecta: es abierto, global e inseguro; se usa ampliamente por individuos, corporaciones y Gobiernos, todos utilizando el mismo medio de transmisión e igual exposición a vulnerabilidades inherentes. Con estas condiciones, los Gobiernos están en negociaciones incipientes y lentas para resolver los problemas en el ciberespacio, al mismo tiempo que el número de ataques con objetivos político-militares va en aumento, lo que lleva a una militarización constante del ciberespacio con muchos países, formando comandos cibernéticos para emprender acciones ofensivas en este nuevo dominio (Ventre, 2014).

DEFINICIÓN DE CIBERSEGURIDAD

El *National Institute of Standards and Technology* define a la ciberseguridad como el "proceso de proteger información, previniendo, detectando y respondiendo a ataques" (2014:37).

Por otra parte, la ciberseguridad se puede definir también 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, 2016:8).

Pero la definición que aquí se considera más completa es la que establece el Departamento de Defensa de Estados Unidos, quien define a la ciberseguridad como:

> *la prevención de daños para la protección y restauración de computadoras, sistemas electrónicos de comunicación, servicios de comunicación electrónica, comunicaciones alámbricas y comunicación electrónica, incluyendo información contenida en ellos, para asegurar su disponibilidad, integridad, autenticidad, confidencialidad y no repudio* (U.S. Office of the Chairman of the Joint Chiefs of Staff, 2015:57).

De igual forma, la ciberseguridad tiene que ver con un concepto más amplio, que es la seguridad de la información, definida como la protección de la integridad, confidencialidad y disponibilidad de datos, independientemente de dónde se procesen, transmitan o almacenen (Bayuk *et al*., 2012). Estos tres conceptos se definen como sigue:

> *Disponibilidad es la propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada; Confidencialidad es la propiedad de que la información no sea disponible o rebelada a individuos, entidades o procesos no autorizados; y la Integridad es la propiedad de salvaguardar la precisión y totalidad de los activos* (ISO, 2005:1).

Por otra parte, la ciberseguridad está evolucionando hacia la gestión de riesgos del ciberespacio *(Information Assurance),* que consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados, basándose en estándares internacionalmente aceptados (Fojón Chamorr y Sanz Villalba, 2010).

De este modo, la ciberseguridad, similar a la seguridad de la información desde el punto de vista de los riesgos, es un asunto que tiene que ver con tres dimensiones. Por un lado, con la protección de la integridad, confidencialidad y disponibilidad de la información, aunque existen otras características como la confiabilidad y el no repudio; en segundo término la ciberseguridad tiene que ver con proteger la información desde su procesamiento, transmisión y almacenamiento; y finalmente la ciberseguridad es un asunto que tiene que ver desde el punto de vista de la gestión con gente, procesos y tecnología. Así se logra tener un cubo de tres dimensiones de la seguridad en tér-

minos de riesgos, como se muestra en la figura 1, al cual se le conoce como el Cubo de McCumber (McCumber, 2005).

Figura 1. Dimensiones de la ciberseguridad (Cubo de McCumber).

Como vemos, la ciberseguridad tiene que ver con muchos aspectos de riesgo, que son la combinación de los nueve elementos que se presentan en las dimensiones del cubo.

Es necesario entender todas las posibilidades, pues en la literatura y otros medios de información siempre se expresan los problemas de ciberseguridad como ataques a infraestructuras producidos por agentes-amenaza externos, pero la mayor parte de los problemas de ciberseguridad o de seguridad de la información son producidos por incidentes provocados voluntaria o involuntariamente por personal interno (Ponemon Institute, 2015).

EL PERFIL DE LA CIBESEGURIDAD EN MÉXICO

De acuerdo con el reporte de McAfee denominado "Pérdidas netas: estimando los costos globales de los ciberdelitos" (McAfee, 2014), se realiza una estimación del impacto económico de los ciberdelitos de algunos países como porcentaje del PIB, como se observa en la siguiente tabla:

Tabla 1. Ciberdelitos como porcentaje del PIB.			
País	**%**	**País**	**%**
Alemania	1.60	Reino Unido	0.16
Holanda	1.50	Colombia	0.14
Noruega	0.64	Sudáfrica	0.14
Estados Unidos	0.64	Vietnam	0.13
China	0.63	Francia	0.11
Unión Europea	0.41	Emiratos Árabes Unidos	0.11
Singapur	0.41	Rusia	0.10
Brasil	0.32	Nueva Zelanda	0.09
India	0.21	Australia	0.08
Irlanda	0.20	Nigeria	0.08
Zambia	0.19	Turquía	0.07
Malasia	0.18	Italia	0.04
Canadá	0.17	Japón	0.02
México	0.17	Kenia	0.01
Sudáfrica	0.17		
Fuente: McAfee, 2014.			

Este estudio encontró que los países más afectados fueron Alemania, Holanda y Noruega y, en general, los mayores costos en términos de porcentaje del PIB se localizan en los países desarrollados como Alemania, Estados Unidos y China, que son economías que generan mucho dinero y están altamente desarrolladas. En contraste, Kenia, Nigeria y Turquía son países con menor costo por ataques cibernéticos, en primera instancia porque son economías poco atractivas para los delincuentes en términos financieros y, por otra parte, porque no tienen el suficiente desarrollo tecnológico.

Con relación a México, se muestra que la pérdida es de 0.17 % del PIB. Asimismo, de acuerdo con Norton, el costo de los ciberdelitos en 2016 para México fue de 5500 millones de dólares (Symantec Corporation, 2016). Por otro lado, se ha encontrado también que los ciberataques de tipo financiero crecen de forma directa al PIB de una

nación, y en el caso de México, que en los últimos años ha tenido un crecimiento sólido de su PIB, también se han incrementado casi en la misma proporción los ciberataques (*Control Risk,* 2015).

Se puede decir que en esta época México se ha convertido en un objetivo atractivo para los cibercriminales, y que la mayoría de los ataques que buscan un beneficio monetario, son perpetrados directa o indirectamente en el sector financiero por organizaciones de la delincuencia organizada, por lo que es muy importante incrementar la ciberseguridad en el país para evitar un riesgo económico de alto impacto (*Control Risk,* 2015; Parragez Kobek, 2017).

Es importante señalar que en México existen algunos esfuerzos importantes de ciberseguridad, pero todos ellos están enfocados principalmente a la seguridad de cada institución de Gobierno y no a coordinar la ciberseguridad nacional, por lo que el Programa Sectorial de Defensa Nacional 2013-2018 señala que:

> *La seguridad en el ciberespacio en México no se ha abordado desde el punto de vista de la defensa nacional, ya que sólo se ha atendido desde el ámbito de la seguridad institucional y persecución del delito, no obstante que en la agenda nacional de riesgos 2012 se planteó que la vulnerabilidad cibernética puede impactar en la defensa del Estado mexicano (2013:21).*

De ahí que en el país se tenga una necesidad primordial de una Estrategia de Ciberseguridad para la Seguridad Nacional (ECSSN), que atienda los temas de defensa y seguridad nacional en el ciberespacio.

DEFINIENDO INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN EN MÉXICO

El principal objetivo de la ciberseguridad a nivel nacional es la Protección de las Infraestructuras Críticas de Información (PICI) que están íntimamente vinculadas con las Infraestructuras Críticas (IC) y la Protección de Infraestructuras Críticas (PIC) de una nación. Las Infraestructuras Críticas de Información (ICI) se definen como "aquellas infraestructuras de información y comunicaciones interco-

nectadas que son esenciales para mantener funciones societales vitales (bienestar social, económico, de seguridad o salud de la gente)" (*Global Forum on Cyber Expertise,* 2016:6).

De esta forma, la 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, 2016:6).*

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 monitorear y controlar –en general de forma remota–, sistemas físicos como válvulas, compuertas o interruptores eléctricos para el control del flujo de agua, gas, petróleo o electricidad (*Global Forum on Cyber Expertise,* 2016). La relación entre ICI e IC se muestra en la figura 2.

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 otra parte, están embebidas en los procesos de IC.

Figura 2. Relación entre Infraestructuras Críticas de Información e Infraestructuras Críticas (*Global Forum on Cyber Expertise,* 2016).

Para elaborar una Estrategia de Ciberseguridad para la Seguridad Nacional (ECSSN) es necesario partir de la PICI, y de la disposición de una legislación o regulación de las IC que contemple las ICI, porque en caso contrario las estrategias pueden llegar a ser de poca aplicabilidad o ser usadas sólo en casos de emergencia. De esta manera, la PICI es el núcleo vital para la elaboración de una ECSSN, como se muestra en la figura 3.

Figura 3. Relación y cobertura entre la PIC, PICI y la ciberseguridad (*Global Forum on Cyber Expertise*, 2016).

Una ECSSN debe además contemplar problemas de privacidad y derechos humanos, y temas económicos del ciberespacio, por lo que es necesario considerar elementos como la gobernanza, la legislación, los grupos de interés, incentivos, regulaciones y las comunidades de IC/ICI.

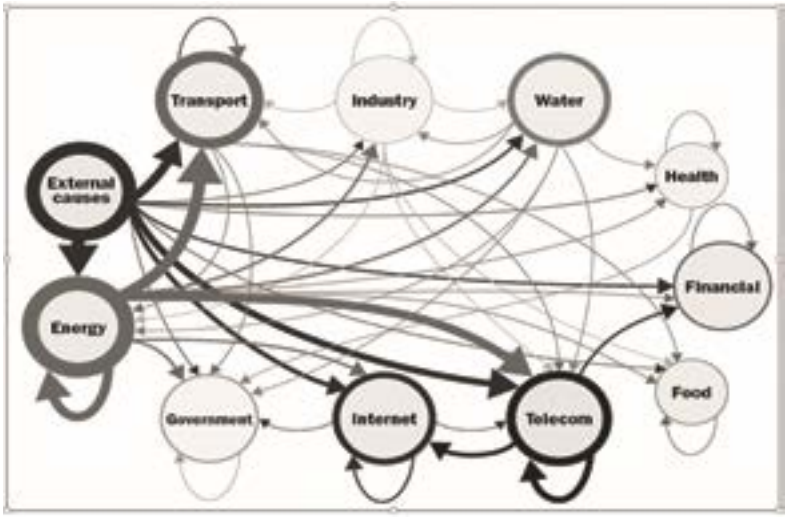
Una buena práctica para elaborar una ECSSN es empezar con una perspectiva nacional trabajando con las ICI, realizando una evaluación nacional de riesgos y la creación de un perfil nacional. Sin embargo, hay que tener en cuenta que no se puede entender e identificar las ICI si no se identifican las IC nacionales y se entiende cómo se ven y operan (Global Forum on Cyber Expertise, 2016).

Posteriormente se tienen que realizar evaluaciones de riesgo, tanto en la IC como en las ICI, para obtener un perfil de riesgo. Además, para empezar a determinar las IC, primero se debe definir qué es una IC, y después se deben adoptar metodologías para la identificación sistemática de sectores de IC (comunicaciones, energía, salud, transporte, agua, etc.) y criterios específicos para evaluar las áreas, criticidad, dependencias y criterios de evaluación transversal.

Posteriormente se recomienda identificar los operadores de las ICI (públicos, público-privados, privados), y las dependencias entre ICI y cadenas de suministro de información.

La figura 4 muestra las dependencias transversales y directas de los sectores de IC para la evaluación de riesgos.

Figura 4. Dependencias transversales y directas de los sectores de IC (*Global Forum on Cyber Expertise,* 2016).



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. Es recomendable empezar a coordinar un cuerpo de PICI para realizar ejercicios de administración de crisis público-privadas, involucrando a los sectores/operadores de ICI, para aprender de los errores.

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).

Es conveniente establecer redes de confianza para compartir información relacionada con amenazas, iniciativas y estándares de PICI, y construir lazos de cooperación pública y privada, interna y externa, para la protección de IC e ICI.

En un escenario más avanzado se recomienda crear un Consejo de Ciberseguridad a nivel nacional, en el cual exista la participación de las partes pública y privada para desarrollos relevantes de ciberseguridad y que esté a cargo de la implementación y ejecución de una ECSSN, así como de realizar investigaciones científicas dentro de una Agenda de Investigación de Ciberseguridad Nacional y crear protocolos para el intercambio de información confidencial entre las organizaciones públicas y privadas.

Una ECSSN tiene que enfocarse prioritariamente en la protección de ICI, porque si éstas fallan, no sólo se afectará a la población y al Gobierno, sino implicará cuantiosas pérdidas materiales e incluso pérdidas de vidas humanas, así como los servicios finales o particulares no se podrían llevar a cabo. Es por ello que se tiene que tener plena conciencia de que la protección de ICI tiene la primera prioridad, y es por ello que es un tema de seguridad nacional, sin dejar de soslayar los delitos que pueden afectar a organizaciones o personas particulares, cuya atención corresponde a policías cibernéticas que forman parte de la seguridad pública de un país, y obedece más a una Estrategia Nacional de Ciberseguridad (ENCS) de ámbito más amplio, la cual atiende amenazas de seguridad nacional y de aquéllas que no lo son.

Con relación a México, no existe una definición legal de ICI. Sin embargo, la Constitución define "áreas estratégicas" (*Constitución Política de los Estados Unidos Mexicanos,* 2017), y la Ley General del Sistema de Seguridad Pública define "instalaciones estratégicas" (2016).

Por otra parte, el Programa para la Seguridad Nacional 2013-2018 señala que:

> *México cuenta con alrededor de 3000 instalaciones estratégicas, de las cuales el 47 por ciento corresponden a Petróleos Mexicanos (PEMEX), el 17 por ciento a la Comisión Nacional del Agua (CONAGUA) y el 13 por ciento a la Comisión Federal de Electricidad (CFE). De igual forma, el país cuenta con 16 puertos de altura, 40 puertos de cabotaje y 56 aeropuertos internacionales* (2013:60).

Es así que, a partir de las instalaciones estratégicas definidas, se pueden identificar las IC e ICI del Gobierno, faltando determinar aquéllas que son privadas. Solamente el *Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y de Seguridad de la Información* (MAAGTICSI) –que emana del Ejecutivo Federal– define lo que es ICI como:

> *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 de la materia* (Diario Oficial de la Federación, 8 de mayo de 2014:24).

Además, el MAAGTICSI señala que todas las dependencias deben detectar las ICI nacionales que administran (*Diario Oficial de la Federación,* 22 de agosto de 2012), quedando la ciberseguridad sólo en el ámbito institucional, pues el manual no es un instrumento para coordinar las acciones de protección de esas ICI a nivel nacional.

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 (*hosting*) de sitios web corporativos.

Estas empresas proveedoras de servicios de almacenamiento pueden estar en cualquier parte del mundo, y si bien tienen ciertos

niveles de servicio en cuanto a disponibilidad, no es una garantía absoluta de que los datos están totalmente seguros en cuanto a confidencialidad.

Siendo así, si las organizaciones-clientes que controlan ICI directa o indirectamente utilizan servicios administrados en la nube, el ataque a estas empresas de hosting y almacenamiento puede provocar la paralización de muchas organizaciones-clientes, por lo que también se tienen que considerar a estas empresas de hosting como críticas, pues almacenan información de gran cantidad de organizaciones, que por su variedad y tamaño pueden impactar de forma importante a la economía y seguridad nacional del país si son afectadas.

Se consideran inicialmente como ICI de México las siguientes:

- TIC de procesos clave de instalaciones estratégicas (agua, energía, petróleo, electricidad, transporte, salud, militares y nucleares, principalmente)
- TIC del sector privado considerados como IC (sistema financiero, telecomunicaciones y aeropuertos)
- TIC de la Estrategia Digital Nacional (Presidencia de la República, 2013)
- 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.

ESTRATEGIA DE CIBERSEGURIDAD PARA LA SEGURIDAD NACIONAL

La necesidad de seguridad y de su institucionalización en una estrategia nacional, junto con sus documentos asociados, es un factor importante para las países, y esta necesidad requiere del desarrollo de estrategias a nivel nacional que sean diseñadas con objeti-

vos, que si son alcanzados, puedan garantizar las condiciones necesarias de seguridad dentro de un sistema internacional (Stolberg, 2012).

Una Estrategia de Ciberseguridad para la Seguridad Nacional (ECSSN), que también puede llamarse Estrategia de Ciberseguridad Nacional (ECN) delinea una visión y articula prioridades, principios y enfoques para entender y administrar riesgos a un nivel nacional (ENISA, 2012).

Las estrategias nacionales más exitosas comparten tres importantes características. Primero, están embebidas en documentos vivos que se han estado desarrollando e implementando en compañía o en conjunto con partes interesadas clave privadas y públicas; segundo, están basadas en principios claramente articulados que reflejan los valores societales, tradiciones y principios legales, ya que los programas creados por el Gobierno en el nombre de la seguridad pueden potencialmente infringir esos derechos y valores si no se articulan e integran como principios guía; tercero, las estrategias están basadas en un enfoque de administración de riesgos, en el cual los socios de Gobierno y los sectores privados están de acuerdo en los riesgos que deben manejar o mitigar, y aun aquéllos que deben ser aceptados.

Así, una estrategia nacional, si se desarrolla correctamente, puede cubrir muchas necesidades de Gobierno, sector privado y ciudadanos del país (Goodwin y Nicholas, 2013).

De esta forma, la ECSSN esta única y exclusivamente orientada a ciberamenazas que atenten directamente a la defensa y seguridad nacional. Esto es, se enfoca a proteger de ciberataques a las infraestructuras críticas de información del país que puedan poner en riesgo la integridad, estabilidad y permanencia del Estado y afectar de manera importante a gran cantidad de la población del país. La figura 5 muestra el alcance de la Estrategia de Cibeseguridad para la Seguridad Nacional, enfocada a la Protección de Infraestructuras Críticas de Información.

El objetivo de una estrategia de ECSSN es incrementar la resiliencia y la seguridad de los activos de TIC nacionales, que soportan

las funciones críticas del Estado o de la sociedad como un todo. Poner los objetivos claros y las prioridades es, por tanto, de primordial importancia para el éxito en alcanzar esta meta.

Figura 5. Ámbito de la Estrategia de Ciberseguridad para la Seguridad Nacional.

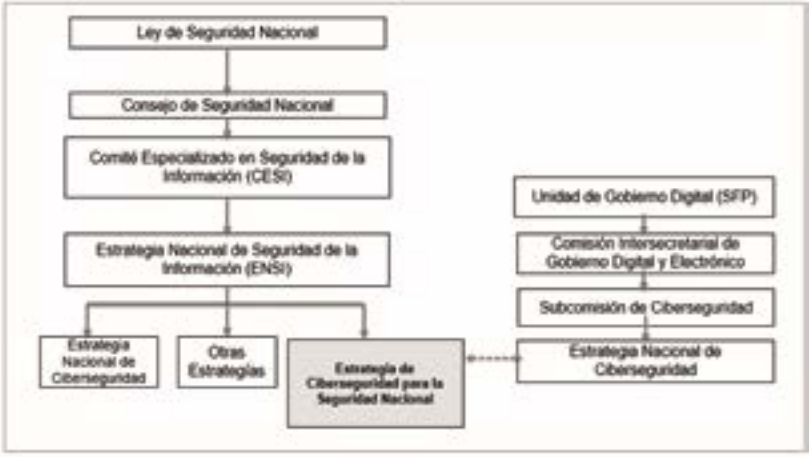
Para crear una estrategia como política pública en el caso de México, primero se tiene que tomar en cuenta que existen, por un lado, las leyes y, por otro, los programas. Las leyes emanan de la Constitución y definen las obligaciones y las acciones coercitivas derivadas de su incumplimiento. Además, existen los programas, tanto el Plan Nacional de Desarrollo, como los programas sectoriales que definen la forma en cómo se van a cumplir esas leyes. Pero la relación entre las leyes y los programas es mutua, ya que a partir de los programas se pueden derivar leyes, y las leyes, para su cumplimiento, derivan programas.

Siendo así, en el caso de México la Estrategia de Ciberseguridad para la Seguridad Nacional (ECSSN) debe emanar de la Ley de Seguridad Nacional, que entre otras cosas define la constitución del Consejo de Seguridad Nacional (CSN) y del Programa para la Seguridad Nacional, y debe operarse a través del Comité de Seguridad de la Información (CESI), creado por el CSN. De igual forma, debe procurar tener compatibilidad con la Estrategia Nacional de Ciber-

seguridad (ENCS) que se emitió en noviembre de 2017, la cual está a cargo de la Subcomisión de Ciberseguridad de la Comisión Nacional de Seguridad, que en este momento es la entidad encargada de coordinar los esfuerzos de ciberseguridad en el país.

Cabe señalar que la ENCS establece cinco objetivos estratégicos, y el número cinco se refiere a seguridad nacional, así como se definen ocho ejes transversales, siendo el seis el relacionado a infraestructuras críticas. La ENCS establece precisamente lo mencionado anteriormente, que para materia de seguridad nacional será el CESI quien aborde el tema (Estrategia Nacional de Ciberseguridad, 2017). La ubicación de la ECSSN se esquematiza en la siguiente figura 6.

Figura 6. Ubicación de la Estrategia de Ciberseguridad Nacional enfocada a ICI.



CONCLUSIONES

El tema de ciberseguridad es un asunto de seguridad nacional debido a que, de acuerdo con largas discusiones, afecta a bienes públicos usados por personas, organizaciones y Gobiernos, y muchos de esos bienes públicos son clasificados como ICI, cuya interrupción o daño pueden causar destrucciones inconmensurables (CACI, 2010; Danicu, 2014).

Una ECSSN tiene el objetivo de atender las amenazas a la seguridad nacional en el ciberespacio, de tal forma que se garantice la estabilidad, integridad y permanencia del Estado mexicano, de acuerdo con la ley en la materia.

Para desarrollar esta ECSSN hay que pasar de los esfuerzos institucionales actuales a los esfuerzos nacionales, para identificar las ICI, y que se controlen y monitoreen con una visión de Estado, independientemente de la organización pública o privada que directamente las administre.

Para ello es conveniente crear un organismo de Ciberseguridad Nacional con autonomía legal y presupuestal que coordine, norme, dirija y audite los esfuerzos de todas las partes, para proteger las ICI del país.

Una ECSSN debe incluir la creación de un Centro Nacional de Protección de Infraestructuras Criticas de Información y un Centro Nacional de Respuesta a Incidentes Tecnológicos, entre otros, así como promover la cooperación internacional con los demás países, pues el ciberespacio es un entorno sin límites y la ciberseguridad en esas condiciones no puede ser controlada por un solo país dentro de la comunidad internacional.

Por último, la ECSSN debe ser un instrumento dinámico que responda de forma adecuada a las vulnerabilidades y posibles ataques a infraestructuras críticas de información del momento, derivados de los constantes cambios tecnológicos (*National Institute of Standards and Technology*, 2014; Caudle, S., 2009).

BIBLIOGRAFÍA

BALLESTEROS MARTÍN, M.A. y AGUILAR JOYANES, L. (2011). "Los efectos de la globalización en el ámbito de la seguridad y defensa", *Inteligencia y Seguridad Nacional,* México, julio-diciembre, pp. 11-28

BOLONGNA, S.; FASSANI, A. y MARTELINI, M. (2013). *The Importance of Securing Industrial Control Systems of Critical Infrastructures*, Como, Italia, Landau Network-Centro Volta, General Secretariat.

BUSH, G.W. (2003). *The National Strategy to Secure Cyberspace*, EUA, The White House.

BAYUK, J.L.; HEALY, J.; ROHMEYER, P.; SACHS, M.H.; SCHMIDT, J. y WEISS, J. (2012). *Cyber Security Policy Guidebook,* EUA, A John Wiley & Sons, Inc.

CACI (2010). *Cyber Threats to National Security Symposium Four: Countering Challenges to the Global Supply Chain,* Arlington, Virginia, CACI International Inc.

CAUDLE, S. (2009). "National Security Strategies: Security from What, for Whom, and by What Means", *Journal of Homeland Security and Emergency Management*, 6(1), pp. 1-25. Recuperado el 23 de octubre de 2018, desde doi:10.2202/1547-7355.1526

CINTRA, J.T. (1991). *Seguridad nacional, poder nacional y desarrollo*, México, Centro de Investigación y Seguridad Nacional, Secretaría de Gobernación.

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS (2017). DOF 24-02-2017, México, Cámara de Diputados del Honorable Congreso de la Unión de México.

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

DINICU, A. (2014). "Cyber Threats to National Security. Specific Features and Actors Involved", *Scientific Bulletin-Nicolae Balcescu Land Forces Academy*, 19(2), pp. 109-113.

DIARIO OFICIAL DE LA FEDERACIÓN (2005). *Ley de Seguridad Nacional,* México, Cámara de Diputados del Honorable Congreso de la Unión de México.

DIARIO OFICIAL DE LA FEDERACIÓN (2005). *Programa para la Seguridad Nacional 2014-2018,* México, Presidencia de la República.

DIARIO OFICIAL DE LA FEDERACIÓN (2013). *Programa Sectorial de Defensa Nacional 2013-2018,* México, Presidencia de la República.

DIARIO OFICIAL DE LA FEDERACIÓN (2014, 8 de mayo). *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.

DIARIO OFICIAL DE LA FEDERACIÓN (2016). *Ley General del Sistema de Seguridad Pública,* México, Cámara de Diputados del Honorable Congreso de la Unión de México.

ENISA (2012). *National Cyber Security Strategies, Practical Guide on Development and Execution,* Bruselas, Bélgica, 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

FOJÓN CHAMORR, E. y SANZ VILLALBA, Á.F. (2010, junio 18). *Ciberseguridad en España: una propuesta para su gestión*. Recuperado de http://www.realinstitutoelcano.org/wps/wcm/connect/c1360e8042e4fcf49e51ff5cb2335b49/ARI102-2010_Fojon_Sanz_ciberseguridad_Espana.pdf?MOD=AJPERES&CACHEID=c1360e8042e4fcf49e51ff5cb2335b49

GIBSON, W. (2008), *Neuromante,* México, Minotauro.

GLOBAL FORUM ON CYBER EXPERTISE (2016, noviembre). *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection.*

GOODWIN C.F. y NICHOLAS J.P. (2013). *Developing a National Strategy for Cybersecurity,* Estados Unidos de América, Microsoft.

HALL, C. (2011). *Operational Art in the Fifth Domain*, Newport, R.I., Faculty of the Naval War College, Department of Joint Military Operations.

HARE, F. (2010). *The Interdependent Nature of National Cyber Security: Motivating Private Action for a Public Good*, Ann Arbor, George Mason University.

ISO (2005). *ISO/IEC 27001:2005 Information Technology-Security Techniques-Information Security Management Systems-Requirements*, Ginebra, International Organization for Standarization.

LANZENDORFER, Q.E. y SPANGLER, S.C. (2015). "Innovating Knowledge Management in Cyber Warfare", *Issues in Information Systems,* 16(2).

McAFEE (2014). *Net Losses: Estimating the Global Cost of Cybercrime*, Santa Clara California, EUA, McAfee Inc.

McCUMBER J. (2005). *Assessing and Managing Security Risk in IT Systems. A Structured Methodology,* Boca Raton, Florida, Auerbach Publications.

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.

MEDINA MARTÍNEZ, F. (2012). *La transformación del concepto de seguridad nacional en México*, Nueva Época, pp. 218-235.

MURPHY, M. (2010). "Cyberwar: War in the Fifth Domain", *Economist*, julio, 3.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2014). *Framework for Improving Critical Infraestructure Cybersecurity*, EUA, NIST.

OECD (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy, OECD Publishing.*

OROZCO, G. (2005). "El concepto de la seguridad en la Teoría de las Relaciones Internacionales", *Revista CIDOB d'Afers Internacionals*, pp. 161-180.

PARRAGEZ KOBEK, L. (2017). *The State of Cybersecurity in Mexico: An Overview,* México, Wilson Center's Mexico Institute.

PONEMON INSTITUTE LLC (2015). *2015 Cost of Cyber Crime Study,* Michigan, EUA, Ponemon Institute.

PRESIDENCIA DE LA REPÚBLICA (noviembre de 2013). *Estrategia Digital Nacional. México*, México.

PRESIDENCIA DE LA REPÚBLICA (2017). *Estrategia Nacional de Ciberseguridad* México, Unidad de Innovación y Estrategia Tecnológica.

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).

STOLBERG, A.G. (2012). *How Nation-States Craft National Security Strategy Documents*, EUA, U.S. Army War College Strategic Studies Institute.

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

U.S. OFFICE OF THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF (2015, 15 de noviembre). *Department of Defense Dictionary of Military and Associated Terms (JP 1-02*), Washington, CJCS.

VALDÉS CASTELLANOS, G. (2009). "La inteligencia para la seguridad nacional en el siglo XXI", *Lecturas Básicas de Inteligencia, Vol. 1: Inteligencia y Seguridad Nacional*, México, Escuela de Inteligencia y Seguridad Nacional (ESISEN), pp. 21-29.

VENTRE, D. (2014). *Chinese Cybersecurity and Defense*, Londres, John Wiley & Sons Inc.

VIZARRETEA ROSALES, E. (2003). *Seguridad y poder nacional*, México, SEMAR.

WEISS, J. (2008). *Assuring Industrial Control System (ICS) Cyber Security*, Center for Strategic & International Studies. Recuperado de http://csis.org/publication/assuring-industrial-control-system-ics-cyber-security

JAIME ROMERO GALICIA

Funcionario de la Secretaría de Gobernación, Doctor en Defensa y Seguridad Nacional, Maestro en Seguridad de la Información. Participante en grupos de trabajo para la generación de políticas públicas relacionadas con seguridad nacional y ciberseguridad por parte de la SEGOB.

Líneas de investigación: defensa y seguridad nacional, inteligencia, ciberseguridad, infraestructuras críticas de información.

Correo electrónico: jaime0r@gmail.com