Revista Internacional de Ciencias Sociales y Humanidades SOCIOTAM
Vol. XXX, N. 2 (2020), pp. 107-127

GESTIÓN ESTRATÉGICA DE LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS NACIONALES

Alberto RAMOS TOXTLE
Centro de Estudios Superiores Navales (CESNAV), México

RESUMEN

La ciberseguridad es un factor primordial de la seguridad nacional, ya que de su buena implementación y gestión depende el nivel de protección de las infraestructuras críticas nacionales.

La gestión de la ciberseguridad en estas infraestructuras debe llevarse al nivel estratégico y otorgarle la relevancia apropiada. Asimismo, deben considerarse los diversos factores que originan las vulnerabilidades de los sistemas, ya que en caso de ser afectadas por un ataque, se perdería la continuidad de los servicios que prestan, ya sea energéticos, económicos, de telecomunicaciones, financieros o militares.

Palabras clave: ciberseguridad, seguridad nacional, infraestructuras críticas, gestión estratégica.

STRATEGIC MANAGEMENT OF CYBER SECURITY IN NATIONAL CRITICAL INFRASTRUCTURES

ABSTRACT

Cybersecurity is a primary factor in national security since the level of protection of critical national infrastructures depends on its proper implementation and management.

The management of cybersecurity in these infrastructures must be taken to the strategic level and given the appropriate relevance. Likewise, the various factors that originate the vulnerabilities of the systems must be considered, in case of being affected by an attack, the continuity of the services they provide, be it energy, economic, telecommunications, financial, or military, would be lost.

Keywords: Cybersecurity, national security, critical infrastructure, strategic management.

I. INTRODUCCIÓN

Las tecnologías de la información (TICs) han evolucionado mucho y muy rápido desde su inicio. De esta manera, el ciberespacio, basado en esas tecnologías, ha tenido un crecimiento exponencial y se ha expandido a todo el mundo.

Las infraestructuras críticas nacionales son sistemas o instalaciones que brindan apoyo o servicios, o que procesan productos que son esenciales para la sobrevivencia de un Estado.

Estos servicios, en el ámbito del ciberespacio y la ciberseguridad, pueden incluir bases de datos personales, sistemas de control de supervisión y adquisición de datos, redes de control de energía, servicios de apoyo militar, económicos o financieros, de salud y telecomunicaciones.

La ciberseguridad en estas infraestructuras críticas debe ser cuidadosamente atendida, ya que aún existen vulnerabilidades que deben ser corregidas, para evitar que sus datos puedan ser explotados y afectar la seguridad nacional. Por eso la ciberseguridad debe gestionarse de manera estratégica, enfocada a solventar los problemas de inseguridad, que disminuyan las áreas desprotegidas y se fortalezca la seguridad nacional.

II. DISCUSIÓN

Evolución de la ciberseguridad

Desde la aparición de las computadoras, la dependencia tecnológica se ha venido incrementando. La integración de ésta con los sistemas de información y comunicaciones ha potenciado la capacidad para la transmisión e intercambio de datos entre naciones, empresas y personas.

El Internet es una estructura de información extendida a nivel global y su influencia alcanza muchos campos, tanto en lo técnico como en lo social. En su organización y funcionamiento abarca aspectos que van de los tecnológicos a los organizativos y comunitarios.

Su antecedente se ubica en agosto de 1962, cuando en los memorandos escritos por J.C.R. Licklider en el MIT (Massachusetts Institute of Technology) describe su concepto de "red galáctica" e imagina un conjunto de computadoras interconectadas globalmente y la posterior conexión de la computadora TX-2 en Massachusetts con la Q-32 en California mediante una línea telefónica conmutada, lo que dio lugar a la primera red de área amplia en el mundo. Fue a finales de 1969, cuando se unieron la Universidad de California y la Universidad de Utah, que oficialmente se sitúa el origen del proyecto de Internet, el cual no ha detenido su desarrollo, hasta la actualidad (Leiner *et al.*, 1997).

Este universo intangible, que muchos apenas empezamos a comprender, pero que es esencialmente humano, fue inventado, desarrollado y validado por el ser humano, mediante la codificación, decodificación, cifrado y descifrado de grandes cantidades de información a una velocidad extraordinaria, a través de infraestructuras creadas para ello. Por demás está decir que está en evolución constante y que día a día se encuentran formas para mejorarlo; también es un hecho que cada día incrementa la cantidad de personas que lo emplean en sus actividades rutinarias.

El término "Internet" sustituyó al de "Ciberespacio" a partir de 1984, acuñado en el libro de ciencia ficción *Neuromante* (Gibson, 1984) y definido como:

> *"Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseñan altos conceptos matemáticos [...] Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable. Líneas de luz clasificadas en el no-espacio de la mente, conglomerados y constelaciones de información."*

Ciberespacio también se define en el glosario de términos unificados de seguridad nacional como un "Ámbito intangible, de naturaleza global, soportado por las tecnologías de la información y la comunicación (TICs), que es utilizado para la interacción entre individuos y entidades públicas y privadas" (SEMAR-SEDENA, 2018).

Por supuesto, así como existen personas que se preocupan por la evolución del ciberespacio con fines productivos, educativos, entre otros, también existe la contraparte que busca emplearlo para fines criminales.

A diferencia de los entornos naturales como tierra, mar, aire y espacio exterior, que no tenemos manera de controlarlos, el ciberespacio, como se mencionó anteriormente, es producto del ser humano y es quien debe estar a cargo de su control y seguridad, así como de tomar las decisiones adecuadas para su protección (Bossomaier, D'Alessandro y Bradbury, 2020).

El crecimiento exponencial del Internet o Ciberespacio y su expansión en casi todos los países del mundo nos ha demostrado ser una de las revoluciones tecnológicas más importantes. En un inicio, esta integración de sistemas operativos, programas y redes de computadoras se hizo sin tener en consideración la seguridad de la información que se intercambiaba a través de ellas, lo cual es capitalizado por personas que se valen del desconocimiento de los usuarios para robar datos, explotarlos, alterar sistemas o crear caos en las bases de datos de los estados, servicios y empresas.

Los efectos de estos actos, como intrusión, manipulación, interrupción de los sistemas o de las redes de los sistemas que son el soporte, pueden afectar su funcionamiento, con consecuencias catastróficas.

Además, los medios, herramientas y aplicaciones que actualmente se emplean para vulnerar los sistemas, engañar a las personas y dañar redes y bases de datos son más sencillas y fáciles de usar, de forma que no se necesita ser un experto en cómputo o software para poder explotar sus cualidades (Instituto Español de Estudios Estratégicos, 2010).

Si bien es cierto que la tecnología ha cambiado la forma en que vivimos, trabajamos y convivimos en sociedad, también es cierto que está vinculada con un gran número de amenazas en el ciberespacio.

Por ello, se debe tener presente que la información para el Estado mexicano es un activo invaluable, y cualquier forma que ésta adquiera, ya sea escrita, almacenada electrónicamente, transmitida por correo o por medios electrónicos, presentada en imágenes, expuesta en una conversación o distribuida por cualquier medio, siempre debe ser protegida en forma adecuada, para preservar sus características fundamentales de disponibilidad, autenticidad, confidencialidad e integridad, con el fin de minimizar los riesgos que existen en el ciberespacio, y que son considerados factores importantes que pueden atentar contra la seguridad nacional y en el logro y mantenimiento de los objetivos nacionales.

Asimismo, el ciberespacio actualmente está considerado como el quinto dominio de la guerra, además de que la seguridad, la prosperidad y estabilidad económica dependen grandemente de él, y su seguridad depende de su resiliencia (Zeadally y Gruyter, 2014). Es el ciberespacio quien nos permite y mejora el comando y control, del mismo modo que permite y mejora nuestras capacidades. Nos da esa condición de ubicuidad en las operaciones diarias en el Gobierno y empresas, por lo que se le debe dar la importancia correspondiente (Blacker, 2018).

Muchas actividades y operaciones del día a día dependen del ciberespacio, tanto de las infraestructuras que proporcionan los servicios a los ciudadanos comunes, como de las instituciones relacionadas con la seguridad nacional, sin ser necesariamente parte del gabinete conformado para este fin. Más aún, con el rápido desarrollo de las tecnologías basadas en el uso de redes estamos siendo testigos de la proliferación desmedida de equipos y sistemas en todos los espacios: hogares, escuelas, hospitales, campus universitarios, áreas urbanas y rurales, lo que representa un verdadero reto encontrar métodos adecuados de control e integración en las actividades diarias (Xhafa, Barolli y Hussain, 2013).

De esta gama de actividades que se realizan en el ciberespacio surge la necesidad de proteger todos los componentes activos y pasivos que interactúan en las operaciones, de forma tal que se efectúen con la mayor de las certezas. De aquí es de donde surge la necesidad de establecer un esquema de ciberseguridad.

La ciberseguridad se ocupa de evitar, administrar y mitigar el riesgo, así como minimizar el daño que podría ocurrir como resultado de un incidente provocado por el descuido de un individuo, acciones de la delincuencia, espionaje industrial o, en el extremo de la escala, ataques incapacitantes contra las infraestructuras críticas de un país (Chávez, 2015).

La ciberseguridad tiene varias dimensiones y características; la principal y más obvia es que se ocupa de proteger un entorno que tampoco es natural, sino producto de la creación del ser humano, como lo es el ciberespacio (Instituto Español de Estudios Estratégicos, 2010).

Un incidente de ciberseguridad es un evento o una serie de eventos que afecta a cualquiera de las propiedades básicas de la información, como son su confidencialidad, integridad y disponibilidad, así como sus sistemas, servicios o redes, y que incide sobre uno o más de sus activos. El impacto en infraestructuras cibernéticas críticas puede tener efectos devastadores para la seguridad nacional, ya que afectaría al desarrollo económico, con daños colaterales claves en los otros campos del poder.

Estos incidentes pueden ser provocados por fallas en los propios sistemas, los cuales no son infalibles a errores de proceso o a descuidos del personal que los opera, aceptables hasta cierto nivel, porque existen factores que afectan al recurso humano en cualquier situación. Sin embargo, existen los incidentes de seguridad que son provocados por agentes externos que pueden tener diferentes orígenes, los cuales son denominados ciberataques, y que tienen varias finalidades, desde sólo conseguir un acceso a los sistemas de cómputo de las instituciones, hasta llegar a causar un daño muy grave a las infraestructuras críticas de un Estado.

En la actualidad, los ciberataques que se han llevado a cabo contra los intereses nacionales han incrementado el interés de los Estados en esta área, quienes están reaccionando a las nuevas condiciones y naturaleza de las amenazas, a fin de minimizar el riesgo de que alguna se materialice y provoque un impacto de dimensiones catastróficas para el Estado, lo cual pondría en peligro a las personas y a los activos de información crítica e infraestructuras del mismo tipo (Carlini, 2016).

Las infraestructuras críticas nacionales son sistemas o instalaciones que brindan apoyo o servicios o que procesan productos esenciales para la sobrevivencia de un Estado. Estos servicios, en el ámbito del ciberespacio y la ciberseguridad, pueden incluir bases de datos personales, sistemas de control de supervisión y adquisición de datos, redes de control de energía, servicios de apoyo militar, económicos o financieros, sanitarios y de telecomunicaciones.

Algunas de estas infraestructuras están bajo el control del Gobierno o de empresas nacionales; sin embargo, podrían considerarse otras que son controladas por organizaciones de otra nación (Dijkstra, 2011).

Para el caso de México, de acuerdo con un análisis y evaluación, se determinaron como infraestructuras críticas de información las de los sectores petróleo, telecomunicaciones, financiero, energía y militar. Éstas, en caso de un ciberataque, pueden tener consecuencias terribles para la seguridad del país (Romero, 2018).

Esta dependencia del ciberespacio representa al mismo tiempo una gran vulnerabilidad, ya que los delincuentes buscan de manera permanente la oportunidad de obtener beneficios con sus actividades criminales, o de causar daño a las infraestructuras críticas de información de los Estados.

Esto es, eventos hostiles se han venido dando desde el origen de Internet, pero que en la actualidad son mucho más sofisticados y también tienen diversos propósitos, como se ve en los siguientes ejemplos de ataques que se han perpetrado.

La ciberseguridad y la Seguridad Nacional

El concepto de Seguridad Nacional ha evolucionado de manera constante en México. Uno es la garantía de la prevalencia de la integridad territorial, independencia, soberanía, estabilidad política, social y económica, así como la consecución de los objetivos nacionales (SEMAR-SEDENA, 2018). Otra concepción es la que se menciona en el artículo 3.0 de la *Ley de Seguridad Nacional*, que la establece como las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano (Diario Oficial de la Federación (DOF), 26 de diciembre de 2005).

Dentro de las consideraciones de la seguridad nacional se encuentra el aspecto tecnológico, en el cual la ciberseguridad forma parte de ella como quinto dominio y relacionado con el ciberespacio, lo cual ha llevado a conflictos entre países en este plano, y que es intangible, al buscar tener acceso a las infraestructuras críticas de información de otro país para poder infligir daños que socaven su seguridad nacional. Es decir, ciberataques con propósitos militares perpetrados por grupos afiliados a países con programas activos de armas cibernéticas, además de iniciativas y programas en materia de ciberejércitos como China, India, Irán, Pakistán y Rusia (Acosta *et al.*, 2009).

Aunque no es necesario que existan intereses de carácter militar para que la ciberseguridad de las infraestructuras críticas de información de un país estén en riesgo, ya que la ciberdelincuencia y los hackers están siempre al acecho para aprovechar cualquier oportunidad para llevar a cabo ataques que pueden vulnerar la seguridad nacional y obtener beneficios económicos. Es decir, son ciberataques con motivaciones monetarias y están dirigidos a cualquier entidad, ya sea del Estado o de particulares.

Ciberataques en el mundo

Las amenazas a la ciberseguridad de estas infraestructuras son más tangibles en los años recientes, como lo demuestran los siguientes ciberataques ocurridos en diferentes países y que pusieron en riesgo no sólo a la infraestructura en la que se llevó a cabo el ata-

que, sino que pudieron ser de consecuencias devastadoras para el mundo (Mullane, 2019):

- *Un ciberataque en 2010 logró detener la planta nuclear de Natanz, Irán, en el cual se empleó por primera vez el malware "Stuxnet". Este software malicioso fue diseñado para dañar los motores que se usan comúnmente en las centrifugadoras para enriquecer uranio, y fue capaz de hacerlas perder el control y deshabilitar temporalmente 1000 centrifugadoras.*
- *En diciembre de 2015 Ucrania sufrió un ciberataque a su red eléctrica que causó el corte general. Fue dirigido a tres compañías energéticas que tuvieron que detener temporalmente su producción en tres regiones de Ucrania, dejando a casi un cuarto de millón de personas sin electricidad hasta por seis horas en pleno invierno. Se presume que el software se distribuyó mediante correos electrónicos de phishing personalizado oculto en archivos adjuntos falsos de Microsoft Office.*
- *En agosto de 2017, un grupo de ciberterroristas tomaron el control del sistema de seguridad instrumentado de una estación remota de una empresa petroquímica en Arabia Saudita, empleando un nuevo tipo de programa malicioso llamado "Tritón", según los investigadores, para sabotear el equipo de la empresa y desencadenar una explosión en toda la planta. El programa malicioso se configuró específicamente para sistemas de control industrial, también conocidos como tecnología operativa (TO).*
- *El 8 y 13 de diciembre de 2020, la compañía de ciberseguridad FireEye dio a conocer que el software de administración de redes empleado por organismos gubernamentales de los Estados Unidos, como el Buró Federal de Investigaciones (FBI), la Agencia de Seguridad Nacional, el Pentágono, el Ejército, la Marina, el Departamento de Energía, el Departamento de Seguridad Nacional, el Comando de Operaciones Especiales, el Departamento de Infraestructuras Críticas y otros sufrieron un ciberataque altamente sofisticado, del cual no se han cuantificado las consecuencias o su alcance.*

De acuerdo con el análisis inicial, el ataque fue realizado por el Grupo de Amenazas Persistentes Avanzadas (APT Group, por sus siglas en inglés), mediante la infección con malware tipo troyano a las actualizaciones del software empresarial, el cual fue llamado "Sunburst".

El ataque pudo haber iniciado desde la primavera y ser financiado por algún país, entre los que inicialmente se consideró a Rusia (Mandia, 2020). (*FireEye*, 2020).

El subdirector adjunto de la división cibernética del FBI, en su momento, declaró que la amenaza terrorista en los Estados Unidos se estaba expandiendo rápidamente y que los grupos terroristas podían desarrollar o contratar a hackers, sobre todo con el objetivo de cumplir ataques físicos más grandes con la ayuda del ciberespacio (Verton, 2004).

Ciberataques en México

En México, como a nivel internacional, hay muchos casos registrados de ciberataques exitosos a sistemas de infraestructuras críticas, las que se han tratado de proteger contra atentados físicos y sabotaje, ya que actualmente dependen de infraestructura informática, por lo que han sufrido asaltos o sólo intentos. De ello se puede inferir que la causa principal de su éxito fue porque el recurso humano no aplicó las medidas de protección necesarias o, en el peor de los casos, que no tenía el conocimiento para ello (Burnett, 2015).

En este sentido, hay muchos esfuerzos por parte de la iniciativa privada para promover la cultura de la ciberseguridad, al igual que se hace en diferentes países. Por este motivo es importante que el Gobierno tome en consideración los posibles ataques que logren impactar en las infraestructuras críticas de información que soportan procesos vitales para el mantenimiento de la soberanía y la estabilidad nacionales.

En México, a manera de ejemplos, los siguientes ciberataques:

- *En 2011, el sitio de Internet de la Secretaría de la Defensa Nacional sufrió un ataque distribuido de denegación de servicio (DoS, Denial of Service, por sus siglas en inglés), el cual generó indisponibilidad del sitio y de los servicios asociados a él (Godoy, 2017).*
- *En enero de 2013, la página web de la Secretaría de la Defensa Nacional padeció una desfiguración de su contenido (defacement, en inglés), desactivándola durante varias horas. Además, detectó una*

convocatoria para participar en la operación "#ADIOSNARCOGOBIERNO", organizada por el grupo hacktivista "Mexican Hackers", que indicó 12 posibles objetivos y que iniciaría a las 16 horas del 15 de febrero de 2015 (Godoy, 2017).

- *De acuerdo con la agencia de información Bloomberg, en 2014 Petróleos Mexicanos (PEMEX) fue blanco de un ciberataque a nivel mundial ligado a Teherán, y aunque no hubo información pública, una investigación de la empresa de ciberseguridad Cylance fue quien encontró esta notificación (Onofre, 2017)*
- *El ataque al sistema de pagos y transferencias electrónicas que está bajo control del Banco de México, sucedido a finales del mes de abril de 2018, en el cual se vieron involucradas al menos cinco instituciones financieras, entre las que se encuentran tres bancos, una casa de bolsa y una caja de ahorro popular, y que produjo una afectación económica por alrededor de 400 millones de pesos.*
- *A PEMEX, llevado a cabo el 10 de noviembre de 2019, y que según la empresa de seguridad ESET*[1] *fue un ataque dirigido mediante un malware*[2] *del tipo ransomware*[3] *que habría infectado a menos del 5 % de los equipos de cómputo de la empresa productiva del Estado mexicano. Asimismo, la comercializadora Innova Petromex reportó que había suspendido operaciones con Pemex desde el 8 de noviembre, lo que indica que cualquier ataque de esa naturaleza puede afectar a Pemex y, en determinado momento, a todas sus operaciones y producir un colapso (Garay, 2019).*
- *En abril de 2020, el Banco de México (Banxico) reportó un ciberataque que, de acuerdo con su versión, no tuvo afectaciones económicas y que consistió en un secuestro de datos que involucró a la banca por Internet y las transferencias interbancarias (Banxico, 2020).*

Es un hecho que el sector financiero o bancario es el principal blanco de ataques cibernéticos, dados los beneficios económicos que produce; sin embargo, eso lo ha obligado a tomar la ciberseguridad más en serio, por lo que la delincuencia también se está enfocando a empresas particulares que, si bien no representan un riesgo para la seguridad nacional, sí afectan a la sociedad.

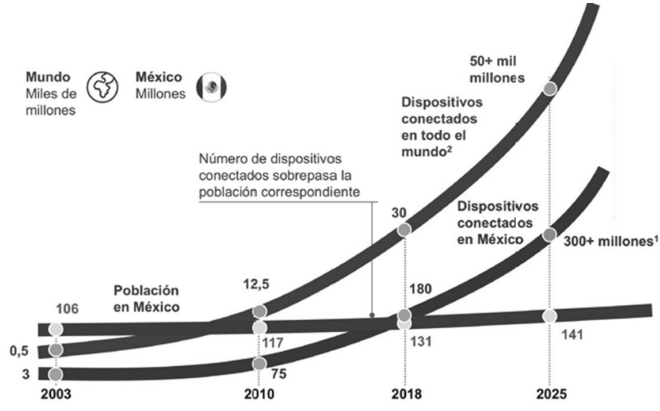
Como ejemplo de esta tendencia existe un ciberataque efectuado en 2018 contra la empresa minorista Liverpool, que le costó a la compañía aproximadamente 100 millones de pesos (Lara, 2019).

Si bien es cierto que la cantidad de atacantes sigue en aumento, también lo es que la ciberseguridad sigue incrementando fortalezas, aunque en menor grado. Es necesario considerar que el entorno de las ciberamenazas ha crecido sustancialmente, desde pequeños delincuentes e intrusos que piratean para su propia diversión, hasta empresas delictivas organizadas. La capacidad de atacar a gran escala desde muchos lugares a la vez les da a los delincuentes la oportunidad de la ubicuidad y resta a los encargados de la ciberseguridad medios de defensa. Asimismo, el entorno tecnológico ha atraído más atención en los últimos años por el incremento de la condición que aporta a los delincuentes de un mayor campo de acción, por las grandes posibilidades de obtener una ganancia.

Estos ciberataques hacen patente la necesidad de mejorar los estándares de seguridad, con el fin de reducir el riesgo en los activos de información y, en este caso, de afectaciones económicas a instituciones, empresas y a particulares (Valdelamar, 2018).

Los riesgos en la ciberseguridad seguirán en aumento, de acuerdo con la prospectiva de conectividad, en la que se incluyen las infraestructuras críticas de información, que se puede apreciar en la siguiente gráfica.

Gráfica 1. Prospectiva de conectividad en México y el mundo.



Fuente: Perspectiva de seguridad en México (McKinsey & Company, 2018).

Estadísticas y datos sobre ciberataques

Existen estadísticas que muestran las tendencias sobre los ciberataques, pero también hay estudios que señalan las posibles causas de su éxito. Por ejemplo, los resultados de una encuesta global efectuada a 3100 directores de Tecnologías de la Información de 12 países por la empresa Sophos4 muestran varios puntos interesantes (Sophos[4], 2019):

- *Los ataques proceden de múltiples direcciones, son coordinados, mixtos y constan de varias fases.*
- *El 44 % de los encuestados considera que los humanos somos una de las tres principales preocupaciones en materia de seguridad.*
- *Dos de cada tres empresas fueron víctimas de un ciberataque en 2018.*
- *En México, los ciberataques se dieron a través de un sitio web malicioso, del correo electrónico, o de memorias USB y dispositivos externos.*
- *Por otro lado, diversas encuestas realizadas por firmas de ciberseguridad publicadas en varios periódicos en México, el país fue uno de los más afectados por ciberataques en 2018. Se registró que más del 55 % de las empresas mexicanas fueron víctimas de los ciberdelincuentes, quienes se valieron de phishing propagado por medio de correos electrónicos y por sitios web maliciosos. Del mismo modo, menciona que uno de cada cuatro incidentes se dio a través de memorias USB y dispositivos externos.*
- *También, en noviembre de 2018 se dio a conocer que México es el segundo país más vulnerable a ciberataques en América Latina, lo cual representó un costo para comerciantes y empresas financieras por transacción fraudulenta en un 3.39 % superior al monto que perdió en el año anterior y representó el 1.75 % de los ingresos anuales (Forbes, 2018). Esto indica la importancia de mejorar las medidas que pueden ayudarnos a incrementar el nivel de ciberseguridad.*
- *Las razones o motivos de los criminales para realizar ciberataques son varias, sobre todo, porque les dan muchas ventajas, entre las cuales se pueden mencionar (Carlini, 2016):*
- *Sólo se necesita una computadora y una conexión a Internet.*
- *Se aprovecha el anonimato y la capacidad de realizar ataques remotos.*
- *Se puede atacar a varios objetivos simultáneamente.*
- *Daña el prestigio de las entidades gubernamentales.*

Es también remarcable que la pandemia de COVID-19 ha sido un terreno fértil para este tipo de ataques, ya que muchas empresas, instituciones financieras y de Gobierno se encuentran trabajando a distancia, empleando el ciberespacio y manejando información delicada sin las medidas de protección adecuadas, videollamadas sin cifrar y una serie de usos que representan casi un paraíso para la comisión de ciberdelitos. Asimismo, el incremento de dominios en Internet relacionados con el coronavirus podría ser utilizado para actividades maliciosas.

De acuerdo con la firma de seguridad ESET, en 2019 el 56 % de las empresas en México sufrieron algún tipo de ataque cibernético, colocando a México en América Latina sólo detrás de Perú como el que más agresiones sufrió (Turton y Soto, 2020).

Los ciberataques a las infraestructuras críticas de información no son nuevos y aumentan cada día. Este tipo de acciones ponen en peligro la seguridad de la sociedad, de la Nación, del propio Estado, así como de su territorio e instituciones. Por eso, la seguridad nacional debe garantizarse permanentemente en todos los ámbitos o espacios estratégicos y, desde ellos, o a partir de ellos, buscar alcanzar sus objetivos y aspiraciones nacionales, considerando las hipótesis de conflictos con posibles adversarios cuyos objetivos sean incompatibles con los propios (Ágreda, 2012).

Casi el 100 % de las infraestructuras críticas emplean Internet para su operación, haciéndolas susceptibles de ataques que las dañen. Estos incidentes resaltan los peligros que plantean los ataques bien coordinados a infraestructuras críticas, pero también el hecho de que los usuarios de los sistemas son engañados con métodos como el *phishing* o correos electrónicos, es decir, técnicas de ingeniería social.

Aunque en México se han presentado incidentes de ciberseguridad, ninguno de los dirigidos a infraestructuras críticas ha provocado pérdidas considerables o daños físicos, pero es necesario mantener la vigilancia y mejorar las capacidades para enfrentarse a las amenazas en la materia, siendo que muchos sistemas críticos del país están expuestos.

En relación con la implementación de la ciberseguridad, en las infraestructuras críticas de información es hasta cierto punto complicado conocer la forma en que se lleva a cabo, ya que la mayoría de ellas tiene clasificada la información relacionada con ese tema. Es conocido que las instituciones de Gobiernos y las que se consideran infraestructuras críticas tienen arquitecturas o esquemas de ciberseguridad diseñados con base en los diferentes estándares que al respecto han emitido los organismos especializados, cuya principal actividad es la elaboración de normas técnicas internacionales, tales como la Organización Internacional de Normalización (ISO, International Organization for Standardization, por sus siglas en inglés)[5], el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)[6], el Grupo de Trabajo de Ingeniería de Internet (IETF, Internet Engineering Task Force, por sus siglas en inglés)[7]. A pesar de ello, los ciberataques siguen siendo exitosos y las estadísticas y estudios realizados indican al recurso humano como el eslabón más débil en la implementación de la ciberseguridad.

Es necesario resaltar que corresponde al Estado fomentar la innovación y promover la adopción de las medidas adecuadas para asegurar la convergencia nacional en relación con la protección que se debe realizar a las infraestructuras críticas. Los ataques mencionados son una amenaza a la seguridad nacional y han evolucionado a la par que el ciberespacio. Los actores, además del Estado, que busca ser garante de la seguridad, son los delincuentes y organismos que apoyan a grupos dedicados a tratar de vulnerar la ciberseguridad de las infraestructuras y que pueden causar daños a la Nación (Instituto Español de Estudios Estratégicos, 2010).

Para la seguridad nacional es de gran relevancia la protección de las infraestructuras críticas de información y, en este sentido, la ciberseguridad es primordial. Actualmente, el control del ciberespacio no sólo cambia el poder relativo de las fuerzas sociales, sino que también afecta el poder de los Estados. Quien tiene más capacidades en este ámbito puede obtener ventajas sobre otro que no las tenga, y actualmente la mayoría de los sistemas son manejados con apoyo casi total de los mecanismos informáticos, y las ventajas estratégicas para cada uno de ellos es básica (Kirshner, 2006).

La gestión estratégica

El vocablo "gestión" se ha empleado como sinónimo de administración, aunque, diferenciándolo de ésta, se puede conceptuar como la articuladora de los recursos humanos, financieros, técnicos, organizacionales y políticos para la producción de bienes y servicios que satisfagan las demandas de la sociedad, enfatizando la eficiencia y la eficacia, y donde se pone en relación el aparato estatal con la sociedad (Galinelli y Migliore, 2015).

Hablando de gestión estratégica, podemos entenderla como un proceso continuo dentro de la organización para la toma de decisiones, así como la interacción que existe entre las capacidades de la organización y de su entorno, con el fin de conseguir los objetivos, teniendo como premisa la eficiencia y la eficacia. Y su principio es maniobrar en el espacio delimitado por las condiciones que establece el entorno (Prieto, 2003).

De ahí que la estrategia que se emplee para la gestión de la ciberseguridad debe ser desde un nivel estratégico, ya que las amenazas se ciernen sobre infraestructuras críticas y pueden causar un gran daño a la seguridad nacional si son afectadas por un ataque.

III. CONCLUSIONES

No existe un entorno adecuado de ciberseguridad, ya que cambia constantemente, como puede constatarse cuando las nuevas tecnologías son vulneradas por la delincuencia. Se ha convertido en un tema fundamental para nosotros como individuos, en el trabajo y, en el caso que nos ocupa, para el Gobierno, ya que actualmente constituye uno de los factores relevantes para la supervivencia.

Las infraestructuras críticas en México requieren tener un nivel máximo de protección en todos los ámbitos y, para ello, es de vital importancia que se gestione la ciberseguridad de manera estratégica, de forma tal que se actúe de manera proactiva, con el objetivo de que los riesgos se minimicen y se consiga un nivel adecuado de seguridad.

Se requiere gestionar la ciberseguridad desde un nivel estratégico, a través de los mecanismos más adecuados para que aminoren las fallas del recurso humano encargado de ésta en las infraestructuras críticas nacionales, para reducir los riesgos y amenazas.

La gestión estratégica de la ciberseguridad es fundamental para afrontar las amenazas que, de llegar a concretarse, podrían causar mucho daño a la información y a las infraestructuras críticas de México, con afectación directa a la seguridad nacional.

NOTAS

1. *ESET es una compañía de seguridad informática establecida en Bratislava, Eslovaquia. Fundada en 1992, es pionera en protección antivirus y en el desarrollo de software para la detección de amenazas.*
2. *Malware es la abreviatura en inglés de "Malicious Software" o software malicioso, por su significado en español.*
3. *Ransomware es una forma de malware que bloquea los archivos o dispositivos del usuario y luego reclama un pago online para restaurar el acceso.*
4. *Sophos es una empresa de servicios de ciberseguridad con presencia en más de 150 países.*
5. *La Organización Internacional para la Normalización es una agencia internacional sin ánimo de lucro con sede en Ginebra (Suiza), cuyo objetivo es el desarrollo de normalizaciones que abarcan un amplio abanico de materias.*
6. *La IEEE es la mayor asociación profesional para el avance de la innovación y la excelencia tecnológica en busca del beneficio de la humanidad.*
7. *La IETF es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.*

BIBLIOGRAFÍA

ACOSTA, Ó.P.; RODRÍGUEZ, J.A.P.; TORRE, D.A.D.L. y BALLESTEROS, P.T. (2009). *Seguridad Nacional y Ciberdefensa* (Vol. 6).

ÁGREDA, Á.G.D. (2012). El Ciberespacio como escenario de conflicto. Identificación de las amenazas. En C.S.d.E.d.l.D.Nacional (Ed.), *El ciberespacio. Nuevo escenario de confrontación* (Vol. 126).

BANXICO (2020). *Banxico reporta incidente cibernético*. Recuperado de https://www.eluniversal.com.mx/cartera/banxico-reporta-incidente-cibernetico

BLACKER, N. (2018). *The Cyber Defense Review.*

BOSSOMAIER, T.R.J.; D'ALESSANDRO, S. y BRADBURY, R.H. (2020). *Human Dimensions of Cybersecurity.* Boca Raton: CRC Press.

BURNETT, P. (2015). *El vital papel de la protección de la infraestructura de información crítica (CIIP) en la seguridad cibernética. Trend Micro.* Organización de Estados Americanos, 55.

CARLINI, A. (2016). *Ciberseguridad: un nuevo desafío para la comunidad internacional.* Instituto Español de Estudios Estratégicos, 67/2016(67), 17. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO67-2016_Ciberseguridad_Desafio_ComunidadInt_ACarlini.pdf

CHÁVEZ, J.D. (2015). *Seguridad informática personal y corporativa* (segunda parte). Venezuela: IEASS Editores.

DIJKSTRA, E.W. (2011). *Cyber Attacks. Protecting National Infraestructure.*

FIREEYE (2020). *Highly Evasive Attacker Leverages Solar Winds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor.* Recuperado de https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages- solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

FORBES (2018). *México, segundo país más vulnerable a ciberataques en América Latina.* Recuperado de https://www.forbes.com.mx/mexico-segundo-pais-mas-vulnerable-a-ciberataques-en-america-latina/

GALINELLI, B. y MIGLIORE, A. (2015). Administración y gestión pública ¿De qué hablamos cuando hablamos de

gestión? En *Estudios sobre Gestión Pública.* Argentina: Comisión de Investigaciones Científicas.

GARAY, K.G. (2019). *El ciberataque a Pemex fue una acción dirigida: ESET.* Recuperado de https://www.eleconomista.com.mx/tecnologia/El-ciberataque-a-Pemex-fue-una-accion- dirigida-ESET-20191112-0089.html

GIBSON, W. (Ed.) (1984). *Neuromante.* Canadá: Minotauro.

GODOY, E. (2017). *Fuerzas armadas, vulnerables a ciberataques.* Recuperado d e https://www.proceso.com.mx/reportajes/2017/6/10/fuerzas-armadas-vulnerables- ciberataques-185880.html

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (2010). *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio* (p. 352).

KIRSHNER, J. (2006). *Globalization and National Security.* United States: Taylor & Francis Group.

LARA, P. (2019). *Los errores de un ciberataque. Dinero en Imagen.* Recuperado de https://www.dineroenimagen.com/paul-lara/los-errores-en-un-ciberataque/116424

LEINER, B.M.; CERF, V.G.; CLARK, D.D.; KAHN, R.E.; KLEINROCK, L.; LYNCH, D.C.; POSTEL, J.; ROBERTS, G.L. y WOLFF, S. (1997). *Breve historia de Internet.* Recuperado de https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/

MANDIA, K. (2020). *FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community.* Recuperado de https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

McKINSEY & COMPANY (2018). *Perspectiva de ciberseguridad en México. Consejo Mexicano de Asuntos Internacionales, Anual.* Recuperado de https://consejomexicano.org/multimedia/1528987628-817.pdf

MULLANE, M.A. (2019). Ciberataques dirigidos a infraestructuras críticas. *La Revista de la Normalización Española.* Recuperado de https://revista.une.org/downloads/revistas/15.pdf

ONOFRE, J.S. (2017). *Las infraestructuras críticas de México ya están bajo ciberataques.* Recuperado de https://www.eleconomista.com.mx/tecnologia/-Las-infraestruc-

turas-criticas-de-Mexico-ya-estan-bajo-ciberataques-20171002-0165.html

PRIETO, A.d.G. (2003). *Gestión estratégica.* Recuperado de: http://www.laplazahumana.com/mod%202/mod%202%20tema%201.pdf

ROMERO, J. (2018). *Factores para una aproximación de estrategia de ciberseguridad nacional enfocada a la protección de infraestructuras críticas de información de México.* (Doctorado Cualitativa). México: Centro de Estudios Superiores Navales.

SEMAR-SEDENA (2018). *Glosario de términos unificados de seguridad nacional.* En SEMAR_SEDENA (Ed.), (Vol. único). México.

SOPHOS (2019). El rompecabezas imposible de la ciberseguridad. *Monográficos de Sophos.*

TURTON, W. y SOTO, G. (2020). *Lo que nos enseñó el secuestro cibernético a Pemex. 6 agosto 2020.* Recuperado de https://www.elfinanciero.com.mx/bloomberg-businessweek/los-hackers-secuestraron-sus-datos-que-no-te-pase-a-ti

VALDELAMAR, J. (2018). *5 entidades y 300 mdp involucrados en ciberataque: Banxico.* 1. Recuperado de https://www.elfinanciero.com.mx/economia/5-entidades-fueron- afectadas-por-ciberataque-banxico

VERTON, D. (2004). *CIA to Publish Cyberterror Intelligence Estimate.* Recuperado de https://www.computerweekly.com/news/2240054743/CIA-to-publish-cyberterror- intelligence-estimate?amp=1

XHAFA, F.; BAROLLI, L. y HUSSAIN, O. (2013). Special Issue on Cyber Physical Systems. *Computing,* 95. DOI:10.1007/s00607-013-0318-0

ZEADALLY, S. y GRUYTER, D. (2014). Special ISSUE on Cibersecurity, Cybercrime, Cyberwar. *HOMELAND SECURITY,* 11(4).

Alberto RAMOS TOXTLE
Contralmirante de la Secretaría de Marina, Maestro en Seguridad Nacional, Maestro en Administración Naval, Maestro en Seguridad de la Información, Especialista en Administración Naval, Especialista en Comunicaciones Navales e Ingeniero en Ciencias Navales. Se ha desempeñado como docente en el Centro de Estudios Superiores Navales. Sus líneas de investigación son la defensa y seguridad nacional, ciberseguridad e infraestructuras críticas de información.
Correo E: artoxs1@gmail.com