AMERICAN CHAMBER MEXICO

100 Years Connecting Business 1917•2017

Estrategia de Ciberseguridad en México

Por un futuro ciberseguro

Índice

Introducción

Nos encontramos en una era digital en la que las personas no únicamente se comunican e interactúan aprovechando las tecnologías de la información, sino que también aumenta el número de operaciones comerciales en el ámbito digital, lo cual expande las oportunidades de negocios a nivel global. Esto se traduce en un crecimiento constante en el flujo de información personal, económica, política, social, etc.

Además de oportunidades, la evolución del mundo digital vislumbra retos a las naciones y ciudadanos para prevenir, proteger y reparar los actos lesivos realizados por medio de internet[1]. Los negocios, servicios, infraestructura básica, redes sociales y la economía global requieren de seguridad cibernética.

En las últimas dos décadas[2], miles de millones de personas de todo el mundo se han beneficiado del crecimiento exponencial y constante de las tecnologías de la información y las comunicaciones[3] (**TIC**), lo que ha generado oportunidades económicas y de interacción social global. Es indudable que el incremento en esta interacción beneficia el desarrollo humano en todos los aspectos; sin embargo, presenta importantes desafíos pues las oportunidades para la ciberdelincuencia crecen en igual proporción, por lo que es cada vez más necesario contar con estrategias de ciberseguridad efectivas.

Por ciberseguridad comprendemos "*… el conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, acciones, formaciones, prácticas idóneas, garantías y tecnologías que pueden utilizarse para proteger la disponibilidad, integridad y confidencialidad de los activos de la infraestructura conectada pertenecientes al gobierno, a las organizaciones privadas y a los ciudadanos; estos activos incluyen los dispositivos informáticos conectados, el personal, la infraestructura, las aplicaciones, los servicios, los sistemas de telecomunicaciones y los datos en el mundo cibernético*"[4].

La ciberseguridad considerada globalmente, requiere una estrategia integral que deben implementar los gobiernos al unísono, precisando objetivos y prioridades, que les permitan integrar a los sectores público, privado y social, con la finalidad de establecer un protocolo de prevención, acción y respuesta ante cualquier amenaza doméstica o internacional. Todo Estado debe contar con un óptimo nivel de prevención y respuesta a este problema global, puesto que podría verse afectada la infraestructura económica[5].

Es muy relevante que los Derechos Humanos sean la base de toda política pública de ciberseguridad, puesto que el uso de, y acceso a, medios electrónicos e internet[6] ha evolucionado para convertirse en un verdadero Derecho Humano. Por ello, al igual que todo derecho humano, la estrategia de ciberseguridad debe regirse por los principios de universalidad, interdependencia, indivisibilidad y progresividad.

Es prioritario que en México se implemente y ejecute una Estrategia Nacional de Ciberseguridad[7] que considere objetivos socioeconómicos y el mecanismo para lograrlos, con un enfoque estructural basado en la educación, el progreso económico y el fortalecimiento de la interacción social, y comprender todos los ámbitos de la vida privada y pública, y el ejercicio del gobierno[8]. Además, la Estrategia Nacional de Ciberseguridad debe ser una política pública vinculada a la protección de la seguridad nacional[9] ya que inclusive la seguridad del Estado está en juego[10]. De hecho, parte importante del funcionamiento óptimo de la infraestructura crítica del Estado[11] depende de la ciberseguridad. Además del permanente diálogo intersecretarial el sector privado, académico, sociedad civil deben ser partícipes activos en el diseño de esta estrategia.

Es evidente que existe una evolución de las ciberamenazas, como el fraude electrónico, el robo de la propiedad intelectual, robo de la información personal de identidad, la interrupción de los servicios, daños o la destrucción de la propiedad y la generación de noticias falsas[12]. Por ello, es importante que la Estrategia tenga el suficiente espacio de actualización para evolucionar al unísono con la constante evaluación de riesgos, incluidas las catástrofes[13].

En esa tesitura, el presente documento se constituye en una propuesta razonable para el reconocimiento, establecimiento y ejecución de la política y la **ENCI**, en la que participen los sectores público, privado y social.

Panorama y Realidad Cibernética en México

De conformidad con la *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares ENDUTIH 2019*[14], en México cada vez hay más usuarios de internet[15] que realizan más operaciones comerciales en línea e intercambian mayor información[16].

Problemas más comunes que enfrentan los usuarios de internet

Problemática	*Número de personas que sufren este problema*	*Porcentaje del universo total de usuarios de internet en México*
Exceso de información no deseada	*20.5 millones de usuarios*	*25.5%*
Violación a la privacidad	*2.5 millones de usuarios*	*3.1%*
Mensajes de personas desconocidas	*16.4 millones de usuarios*	*20.3%*
Infección por virus	*10.6 millones de usuarios*	*13.1%*
Fraudes con información financiera, personal	*3.2 millones de usuarios*	*4.0%*

Además, la recesión económica ocasionada por la actual emergencia sanitaria mundial, nos genera una oportunidad e invita a ver de una nueva forma la realidad y futuro de las relaciones humanas, profesionales y el comercio doméstico y global. El comercio electrónico es cada vez más un medio de supervivencia de grandes, medianas y pequeñas empresas, porque permite reducir costos y ser más eficientes en la producción y suministro de bienes, así como acceder a más clientes y mercados. En la vida pública, jefes de gobierno[17], autoridades regulatorias del máximo nivel[18] y procesos judiciales[19] ya suceden también en el ciberespacio.

El sector financiero en México es un caso que merece una mención particular, porque ha enfrentado grandes desafíos en ciberseguridad. Del total de eventos de ciberataques que sufrieron las organizaciones financieras en 2018, un 43% resultó exitoso.

Los ataques más comunes fueron a través de software malicioso o malware (56%) y phishing (47%), que es la suplantación de identidad. Aún cuando este sector suele tener medidas de ciberseguridad altas, así como regulación al respecto, las instituciones financieras son de los principales objetivos de los hackers[20] o ciberdelincuentes, al ser las plataformas de internet de esas organizaciones las que generan, recogen, administran y dirigen activos. Los centros de respuesta a incidentes *Computer Emergency Response Team* (CERT) y *Computer Security Incident Response Team* (CSIRT) podrían formar parte de esta cooperación binacional toda vez que han tomado relevancia para contar con gestión de incidentes y coordinación entre países para lograr interactuar los sistemas de control con los sistemas de gestión financieros y operacionales de la población en común.

Los delitos cibernéticos no sólo generan costos para el sistema financiero, también afectan la inclusión financiera, ya que los eventos de ciberataques que se difunden, dañan la reputación de las instituciones y con ello, merman la confianza de la población. Según cifras de la Encuesta Nacional de Inclusión Financiera 2018[21], entre 2% y 7% de la población no adquiere un producto financiero, como seguro, crédito, afore o cuenta, por falta de confianza en las instituciones financieras.

Finalmente, la entrada en vigor del Tratado de Libre Comercio entre México, Estados Unidos y Canadá (T-MEC) desde el 01 de julio de 2020, incluye disposiciones en materia de ciberseguridad. En el tratado, los tres países acordaron construir sus capacidades de respuesta a incidentes cibernéticos y fortalecer la colaboración para identificar y contrarrestar códigos maliciosos, por lo que se requiere un mapa de ruta entre los países de América del Norte para implementar la cooperación en tan relevante tema. Además, se acordó que, en vez de promover regulaciones severas que entorpezcan los intercambios comerciales, la construcción y colaboración se centre en la identificación y gestión de riesgos, así como encontrar soluciones prácticas.

Los tres países también acordaron hacer cumplir las protecciones del consumidor, garantizar la privacidad de los datos y restringir la capacidad de sus gobiernos para exigir la divulgación del código fuente patentado. Lo anterior demuestra que los tres gobiernos comparten una visión y un compromiso común en la gestión eficaz del riesgo cibernético.

Estrategia Nacional de Ciberseguridad México

En México el cibercrimen genera pérdidas entre 3,000 y 5000 millones de dólares anuales. Si bien ha habido esfuerzos anteriores por crear una Estrategia Nacional de Ciberseguridad **(ENCI)**, los resultados han sido insuficientes para inhibir las conductas de los ciberdelincuentes, puesto que observamos que los delitos cibernéticos van a la alza. Creemos que el diseño de una Estrategia robusta y transversal debe retomarse y replantearse para convertirse en una verdadera política de gobierno en la que descanse toda interacción de los entes oficiales, privados y sociales, para un óptimo ejercicio de gobierno, desarrollo económico y social.

Un buen referente para replantear la **ENCI** es la "Guía para la elaboración de una Estrategia Nacional de Ciberseguridad, participación estratégica en la ciberseguridad"[22] **(GUIA)**, elaborada en 2018 por la Unión Internacional de Telecomunicaciones **(UIT)**, que comprende las siguientes fases estratégicas:

Fase I – Iniciación. Como punto de partida se establece a una autoridad, existente o nueva, como responsable del proyecto, se crea un comité directivo y se identifican a las partes que participarán;
Fase II - Inventario y análisis. Su objetivo es conocer y evaluar el presente y futuro del panorama nacional de la ciberseguridad, a fin de obtener información trazable y auditable para la elaboración de la estrategia;
Fase III – Producción. Su finalidad es la creación del texto de la estrategia, con la participación del sector público, del sector privado y de la sociedad civil por medio de consultas públicas y grupos de trabajo, que culminan con su publicación y fuerza obligatoria;
Fase IV – Ejecución. Es la observancia y desarrollo de la estrategia trazada; y,
Fase V - Seguimiento y evaluación. Comprende la acción gubernamental para asegurar que la estrategia cumple su finalidad y determinar si es óptima con base en el análisis de la evolución de los riesgos.

El eje sobre el que debe establecerse la regulación e implementación de la **ENCI** tendría que basarse en el enfoque de **Gestión de Riesgos**, debido a que los procesos tecnológicos están en constante evolución, por lo cual, para evitar establecer reglas que puedan quedar desactualizadas o restringir la capacidad de las empresas para innovar, el criterio que debe prevalecer es desde la visión de gestionar los riesgos cibernéticos. Asimismo, este modelo debe estar alineado con las **mejores prácticas** sobre ciberseguridad, tales como los lineamientos del *National Institute of Standards and Technology*[23].

Para el funcionamiento de la **ENCI**, el mecanismo de **gobernanza** resulta fundamental, ya que la ciberseguridad y los ciberataques afectan de forma transversal a cualquier país, desde el usuario con necesidades básicas del internet, pasando por el uso de internet para la operación de empresas, escuelas, instituciones privadas y entes gubernamentales administrativos, hasta las labores de seguridad nacional y de cooperación internacional, incluyendo el intercambio de información entre todos estos actores.

Autoridades Cibernéticas en México

Se torna indispensable la asignación de entes de gobierno específicos encargados de la regulación, administración y observancia de ejercicios de gobierno, interacción de los ciudadanos, actos de comercio y delitos realizados en la web. La autoridad a cargo de la coordinación e implementación de la ENCI debe contar con facultades y atribuciones suficientes para enfrentar los desafíos ante la actuación de la ciberdelincuencia. Por ello, es indispensable que exista una clara asignación de responsabilidades y canales efectivos de coordinación entre autoridades federales y con las autoridades locales, bajo reglas de cooperación, confidencialidad y comunicación efectiva.

En el ámbito de procuración de justicia, se estima necesaria la creación de fiscalías especializadas en delitos cibernéticos en los fueros federal, local y militar de acuerdo a sus competencias, mismas que podrían definirse en las leyes orgánicas de las fiscalías, así como en la normatividad que regula a las policías, con el propósito de establecer la especialización que se requiere tanto de las fiscalías como de las policías. Todo lo anterior, bajo la delimitación de sus respectivas competencias, de tal manera que la investigación de los delitos esté cubierta en todas las formas de expresión y espacios donde se presente.

En materia de impartición de justicia, también se torna necesario el establecimiento de jueces especializados en el ámbito cibernético, a nivel federal y estatal. Por lo que hace a controversias jurídicas en materia cibernética, se requiere que las mismas puedan ser resueltas a través de medios electrónicos, priorizando aquellas en materia mercantil y penal, dada la naturaleza de ese tipo de controversias.

La ley procesal penal mexicana contempla la posibilidad legal de que el procedimiento penal funcione a través del uso de las **TIC** desde su inicio y hasta su conclusión, con algunas salvedades en cuanto a las notificaciones de las partes. Estas mismas reglas podrían incorporarse en las materias civil, mercantil, familiar, administrativa, etc. realizando los ajustes legislativos correspondientes.

La competencia en materia de delitos[24], será federal o local, considerando los siguientes factores;

a) Si se trata de delincuencia organizada transnacional[25] en donde se requerirá colaboración de las instituciones de otros países o de la Interpol;

b) Si se trata de delincuencia organizada nacional;

c) Si se trata de asociación delictuosa o pandilla;

d) El tipo de delito específico cometido, si afecta el interés público o particular;

e) Lugar de inicio y ejecución del delito;

f) Si afecta una infraestructura de gobierno federal o local;

g) Si afecta a autoridades federales o locales; y,

h) Si afecta a, o es cometido por, servidores públicos federales o locales.

Propuestas en la Estrategia Nacional de Ciberseguridad

En este contexto, sugerimos que la **ENCI** comprenda los siguientes elementos:

1. **Protocolo nacional para compartir información** de ataques cibernéticos, que establezca esquemas de colaboración entre autoridades, organizaciones, empresas y usuarios, al mismo tiempo que garantice la confidencialidad de la información de los sujetos que fueron víctimas del ciberataque, para evitar la afectación a la reputación;
2. **Boletín público, periódico e informativo de los riesgos y eventos cibernéticos que publique la autoridad coordinadora.** Es importante que se conozcan los ataques ya perpetrados para conocimiento de potenciales afectados y prevenir que vuelvan a suceder;
3. Generación de **estadísticas oficiales**, con datos que provengan de instituciones públicas y privadas de los tipos de riesgos en ciberseguridad que refleje lugares, periodicidad e incidencia, así como instrumentos de vigilancia de dichos riesgos para su seguimiento;
4. **Simulacros** en ciberseguridad en el ámbito público y privado guiados en todo momento por reconocidos expertos en la materia;
5. Reglas de atención y sanciones en materia de ciberseguridad para el **caso de catástrofes naturales, pandemias, epidemias, etc.;**
6. Desarrollo de **infraestructura tecnológica** como las Redes Privadas Virtuales (VPN), en colaboración público-privada, ante el uso constante de servicios de nube que derivan en una mayor exposición a posibles ciberataques.

Además, para su correcto diseño e implementación, es necesario considerar:

a) En materia legislativa:

- Crear una Ley específica en materia de ciberseguridad que:

i) Comprenda un catálogo de delitos en la materia, que permita tipificar, detectar, disuadir, investigar y enjuiciar eficazmente los delitos cibernéticos, así como armonizar el marco jurídico y reglamentario respectivo;

ii) Incluya la intención o tentativa de daño tecnológico dentro de este catálogo de delitos aún y cuando no logre realizar la acción delictiva de vulnerar el sistema tecnológico porque los controles sean eficientes para la contención del ataque;

iii) Defina, delimite y establezca facultades, derechos, obligaciones y responsabilidades de los sectores público, privado y social en materia de ciberseguridad;

iv) Homologue los términos ciberespacio, cibergobierno, ciberpolicía, ciberempresa, cibercompra, ciberproducto, ciberservicio, ciberusuario, cibertrabajo, cibertrabajador, ciberdelincuencia organizada, ciberdelincuente y ciberseguridad; de delitos de esta índole.

- Siguiendo las mejores prácticas de países como Alemania o Francia, se recomienda crear o en su caso, designar a una autoridad competente que se encargue de la coordinación y ejecución de la **ENCI**. Es fundamental que dicha autoridad tenga las capacidades legales y administrativas para coordinar a todas las partes interesadas. A nivel estatal también debe existir esa autoridad con atribuciones específicas para garantizar que la Estrategia Nacional tenga una implementación efectiva tanto a nivel nacional como local;

- Actualizar la legislación y lineamientos en materia de datos personales a la realidad de los riesgos del ciberespacio;

- Reformar los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y al Código Nacional de Procedimientos Penales, a fin de que sea obligatorio para los concesionarios de telecomunicaciones y los concesionarios y autorizados que presten el servicio de acceso a Internet –artículo 145-, el colaborar con las instituciones de procuración e impartición de justicia, y de seguridad pública, en todo lo relacionado con internet, ciberdelitos, ciberdelincuencia organizada y ciberdelincuentes;

- Reformar al Código Nacional de Procedimientos Penales a fin de incluir fallas en la ciberseguridad como elemento de convicción para fincar responsabilidad penal a las personas jurídicas. Se debe considerar que la responsabilidad penal para las empresas sólo existe en la medida en la que no cuenten con un programa de cumplimiento o "compliance" en materia de ciberseguridad; por ello, deben establecerse reglas de cumplimiento elementales que den claridad sobre los límites de responsabilidad penal de las personas jurídicas (morales y físicas).

b) En materia de cooperación internacional

- Incluir dentro de la **ENCI** un pilar de cooperación internacional, básico para su efectividad, dado el carácter transnacional de los delitos cibernéticos;

- Fortalecer de manera especial, dentro del pilar de cooperación internacional de **ENCI**, la colaboración entre Estados Unidos, Canadá y México, en el marco del TMEC, con un mapa de ruta específico que incluya autoridades involucradas, mecanismos de colaboración interinstitucional, e indicadores de seguimiento;

- Acogerse, en la medida de lo posible, al Convenio de Budapest sobre la ciberdelincuencia del Consejo de Europa, ya que estos delitos no reconocen fronteras y se requiere la cooperación internacional.

c) En materia de impartición de justicia

- Asignar autoridades competentes y específicas que gobiernen, procuren justicia y juzguen el ámbito cibernético, incluidos juicios a través de internet; mediante las plataformas de **TIC** de comunicación disponibles, garantizando su disponibilidad, integridad y confidencialidad;

- Capacitar a los jueces que conocerán de los casos relacionados con ciberseguridad, ciberdelincuencia, ciberdelitos, y funcionamiento de las **TIC** para que los juzgadores tengan una perspectiva clara y a la vanguardia sobre los casos que les sean presentados por los fiscales especializados.

d) Sector financiero

- Reformar la normatividad en materia de: a) Instituciones de crédito y sus órganos reguladores –SHCP y CNBV-; b) Protección de los usuarios de servicios financieros; c) Protección a los consumidores, a fin de adecuarlas a la realidad y evolución de las TIC, brindar seguridad jurídica a los usuarios y mejorar procedimientos administrativos en materia de ciberataques, observando reglas en materia de ciberseguridad;

- Contemplar, en dicha normatividad, que sea requisito para todas las instituciones financieras, públicas y privada, la designación de un oficial de ciberseguridad que sea enlace en la materia frente a la Secretaría de Hacienda y Crédito Público (SHyCP) y Comisión Nacional Bancaria y de Valores (CNByV);

- Seguir un enfoque sectorial dado que en el sistema financiero, hay múltiples actores con diferentes modelos de operación, a fin de que las reglas que apliquen a cada uno de ellos en materia de ciberseguridad, corresponda a sus características propias.

e) En materia educativa y cultural

- Implementar programas académicos con reconocimiento de validez oficial, que generen más profesionales de la ciberseguridad;

- Incluir en la currícula de la educación básica y media superior, programas sobre el ciberespacio y ciberseguridad;

- Impulsar acciones de difusión pública (espacios del Estado) para fortalecer la cultura de ciberseguridad entre la población, incluyendo la cultura de denuncia de delitos de esta índole.

Notas

1) De conformidad con el artículo 3, fracción XXXII, de la Ley Federal de Telecomunicaciones y Radiodifusión, jurídicamente por internet se entiende: "Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única".

2) De acuerdo a la Resolución A/RES/53/70 del 4 de enero de 1999, consultable en https://undocs.org/sp/A/RES/53/70, se advierte que Naciones Unidas pidió a los Estados Miembros que promovieran el examen multilateral de los peligros actuales y posibles en el ámbito de la seguridad de la información, asimismo, invitó a los Estados Miembros a que se pronunciaran sobre: a) Evaluación general de los problemas de la seguridad de la información; b) Determinación de criterios básicos relacionados con la seguridad de la información, en particular la injerencia no autorizada o la utilización ilícita de los sistemas de información y de telecomunicaciones y de los recursos de información; c) Conveniencia de elaborar principios internacionales que aumenten la seguridad de los sistemas de información y de telecomunicaciones mundiales y ayuden a luchar contra el terrorismo y la delincuencia en la esfera de la información. Lo cual fue reiterado en la Resolución A/RES/54/49 del 23 de diciembre de 1999, consultable en https://undocs.org/sp/A/RES/54/49 y en la resolución A/RES/55/28 del 20 de diciembre de 2000, consultable en https://undocs.org/sp/A/RES/55/28.

3) De acuerdo a la Resolución A/74/120, de fecha 24 de junio de 2019, "Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional", de Naciones Unidas, consultable en https://undocs.org/pdf?symbol=es/A/74/120, "Las tecnologías de la información y las comunicaciones (TIC) brindan oportunidades inéditas para el progreso económico, social, cultural, científico y político, y el avance de dichas tecnologías se encuentra inexorablemente ligado a mayores niveles de desarrollo y bienestar. El ciberespacio se ha convertido en un elemento fundamental en la vida de las personas y las organizaciones, y cada vez más servicios esenciales dependen de las redes informáticas".

4) Obtenida de https://www.bcmpedia.org/wiki/Cyber_Security.

5) De acuerdo al Informe Ciberseguridad 2016 ¿Estamos preparados en América Latina y el Caribe?, emitido por el Banco Interamericano de Desarrollo, consultable en https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/. el cibercrimen le cuesta al mundo hasta US$575.000 millones al año, lo que representa 0,5% del PIB global, eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90.000 millones al año. De acuerdo al informe Tendencias de seguridad cibernética en américa latina y el caribe de 2014, emitido por la Organización de los Estados Americanos, en 2013 los delitos cibernéticos generaron daños por lo menos en USD 113.000 millones. En México su costo alcanzó los USD 3.000 millones.

6) De conformidad con el párrafo tercero del artículo 6 de la Constitución Federal: "El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios". Lo que se robustece por lo señalado en el artículo 191, fracción VI, de la Ley Federal de Telecomunicaciones y Radiodifusión en donde se reconoce como derecho de los usuarios "la libre elección y no discriminación en el acceso a los servicios de internet".

7) Artículo 1, párrafo tercero, de la Constitución Política de los Estados Unidos Mexicanos: "Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley".

8) En 2017 se diseñó una primera Estrategia, visible en https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

9) Por ejemplo, en el ACUERDO que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, publicado en el Diario Oficial de la Federación el 9 de diciembre de 2005, encontramos que el Gobierno Electrónico comprende "las políticas, acciones y criterios para el uso y aprovechamiento de las tecnologías de información y comunicaciones, con la finalidad de mejorar la entrega de servicios al ciudadano; la interacción del gobierno con la industria; facilitar el acceso del ciudadano a la información de éste, así como hacer más eficiente la gestión gubernamental para un mejor gobierno y facilitar la interoperabilidad entre las Dependencias y Entidades.

10) Dentro del artículo 5 de la Ley de Seguridad Nacional, que describe cuales son las amenazas a la Seguridad Nacional, la ciberseguridad o ataques en el ciberespacio no están considerados de forma alguna.

11) De conformidad al informe de 2015 del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, consultable en https://undocs.org/es/A/70/174, "4. Varios Estados están desarrollando capacidad en materia de TIC con fines militares y aumentando las probabilidades de que los futuros conflictos entre Estados entrañen el uso de esas tecnologías. 5. Entre los ataques más perjudiciales en los que se utilizan las TIC se encuentran los dirigidos contra la infraestructura fundamental y los sistemas de información conexos de un Estado. El riesgo de ataques dañinos de esta naturaleza contra infraestructura fundamental es a la vez real y grave. 6. La utilización de las TIC con fines de terrorismo, más allá del reclutamiento, la financiación, la capacitación y la incitación, e incluso la comisión de atentados terroristas contra las TIC o infraestructuras dependientes de estas tecnologías, es una posibilidad creciente que, si no se aborda, podría amenazar la paz y la seguridad internacionales".

12) Por ejemplo, de acuerdo a "Ciberseguridad marco NIST" emitido por la Organización de los Estados Americanos, consultable en https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf, "EEUU identifica 16 sectores de infraestructuras críticas, estos son: químico; instalaciones comerciales; comunicaciones; fabricación crítica; presas/represas; base industrial de defensa; servicios de emergencia; energía; servicios financieros; comida y agricultura; instalaciones gubernamentales; salud y salud pública; tecnología de información; reactores nucleares, materiales y residuos; sistemas de transporte; sistemas de agua y aguas residuales".

13) Claro ejemplo de ello lo tenemos considerando la actual pandemia que vive la humanidad por la enfermedad COVID-19, en donde una noticia falsa puede causar alarma o riesgo en la vida y salud de las personas, consultar "'Fake news', la otra pandemia que arrasa el planeta" en https://cincodias.elpais.com/cincodias/2020/04/07/fortunas/1586287641_973226.html.

14) Por ejemplo, la pandemia generada por el virus SARS-COV2 causante de la enfermedad COVID 19 que atraviesa actualmente la humanidad, en donde se torna indispensable la ciberseguridad en el uso de los servicios de internet, en donde al reducirse notablemente el contacto físico y cercano entre las personas, las TIC que generan y transmiten audio y video, así como información o datos e información oficial al respecto, se vuelven indispensables.

15) Consultable en https://www.gob.mx/cms/uploads/attachment/file/534997/INEGI_SCT_IFT_ENDUTIH_2019.pdf.

16) Pasaron de 62.4 millones en 2015 a 80.6 millones en 2019.

17) Las operaciones bancarias en línea pasaron del 15.4% al 16.8%

18) Cumbre Virtual de Líderes del G20 en youtube https://www.youtube.com/watch?v=rVghqd9UOMU.

19) Consultable en https://www.milenio.com/internacional/europa/ministros-salud-g20-analizan-impacto-covid-19-sector.

20) Sesión remota del Pleno de la SCJN 27 Abril 2020 visible en youtube https://www.youtube.com/watch?v=hUIeH4u6xtk.

21) Hacker no implica ser delincuente, generalmente es un término mal empleado, ya que específicamente ese tipo de hackers (malos) son conocidos como Black Hat Hackers, y los especialistas en contrainteligencia a estos últimos son los White Hat Hackers quienes son los expertos en seguridad informática ayudando a prevenir ataques.

22) Consultable en https://www.inegi.org.mx/contenidos/programas/enif/2018/doc/enif_20

23) Consultable en https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf.

24) Consultables en https://www.nist.gov/.

25) Como ejemplo de propuesta de delitos federales tenemos la Iniciativa de la Senadora Jesús Lucía Trasviña Waldenrath con proyecto de decreto por el que se reforman y derogan diversas disposiciones del Título Noveno, Libro Segundo del Código Penal Federal y se expide la Ley de Seguridad Informática consultable en https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2019-03-27-1/assets/documentos/Inic_MORENA_Seguridad_Informatica.pdf.

26) https://www.cidob.org/es/content/download/62758/1952061/version/5/file/35-56_CLAUDIA%20JIMENEZ.pdf, podemos consultar información sobre el crimen organizado en la Unión Europea.

27) Como ejemplo, a nivel federal tenemos la estrategia digital nacional cuya página web es https://www.gob.mx/mexicodigital, asimismo, se utilizarían portales web para la realización de trámites como el establecido por la Ciudad de México consultable en https://www.gobiernodigital.cdmx.gob.mx/home/index.