ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

Análisis de la Iniciativa
DE LA LEY FEDERAL DE CIBERSEGURIDAD.

MESA 5 CIBERSEGURIDAD

Introducción

El pasado 25 de abril del 2023 se publicó en la Gaceta Parlamentaria de la LXV Legislatura de la Cámara de Diputados la iniciativa de Ley Federal de Ciberseguridad, a cargo del diputado Javier Joaquín López Casarín, del grupo parlamentario del Partido Verde Ecologista de México. La iniciativa reforma, adiciona y deroga diversos Artículos de las Leyes Orgánicas de la Administración Pública Federal.

Dentro de las consideraciones, la iniciativa menciona que "*La Ciberseguridad es la piedra angular para evitar ataques en contra de la confidencialidad, integridad y disponibilidad de la información al permitir dotar a los equipos técnicos y humanos de las capacidades y legislación necesaria para combatir eficazmente los riesgos cibernéticos*."- y añade que- "…debe existir *un marco legislativo robusto en la materia que apoye y dé certidumbre a todas las entidades que participan en las tareas asignadas, es por esto y ante las condiciones actuales, que es importante materializar los esfuerzos encaminados hacia el fortalecimiento de la ciberseguridad en México.*".

Así mismo, establece que "*se requiere de un organismo que coordine los diferentes esfuerzos a nivel nacional y que se encargue de generar estrategias y políticas públicas a seguir. Para tal efecto se considera pertinente crear una Agencia Nacional de Ciberseguridad.".* – así como- *"…establecer las bases de colaboración del gobierno con la iniciativa privada a través de las diferentes cámaras industriales, empresas y la población, para combatir delitos cibernéticos en especial aquellos que puedan poner en riesgo el suministro de servicios básicos a la población y protección de infraestructuras críticas de información."*

Como resultado de lo anteriormente citado, así como de otras consideraciones relacionadas con la comisión de delitos cibernéticos en México, la gestión de riesgos y la necesidad de una profesionalización de los recursos humanos involucrados, la iniciativa considera *"indispensable emitir una Ley Federal de Ciberseguridad, para lograr un entendimiento común entre todos los sectores interesados, impulsar la profesionalización del poder judicial, establecer a una Agencia de Ciberseguridad que sea el responsable en la materia, así como constituir la base para la generación de estrategias, y políticas públicas desarrolladas con la participación de los tres órdenes de gobierno, sector privado y sociedad en general.".*

Ciberseguridad. Contribuciones y propuestas.

Por otro lado, y como parte de las actividades realizadas por la Mesa 5 Ciberseguridad del Comité Técnico en Materia de despliegue de 5G en México, el año pasado se puso a consideración de los miembros de este Comité el documento **Marco Nacional de Ciberseguridad. Recomendaciones**, que presentó algunas consideraciones y aspectos que una regulación sobre Ciberseguridad debiera cumplir. Este documento fue

aprobado el pasado 2 de diciembre del 2022. Como seguimiento de esta primera contribución y a la luz de la Iniciativa de Ley Federal de Ciberseguridad a la que se ha hecho referencia en este documento, se presentan comentarios y sugerencias a la iniciativa presentada.

Los integrantes del Comité coinciden en el hecho de que las agencias nacionales de ciberseguridad desempeñan diversas funciones en el ámbito de la protección de la información y la seguridad cibernética. Así mismo y de acuerdo con la experiencia internacional en cuanto a la creación de estas agencias, sus funciones específicas pueden variar en cada país, siendo las más usuales las siguientes:

- **Coordinación y asesoría a los grupos interesados**. Las agencias de ciberseguridad suelen actuar como organismos de coordinación de las actividades de las dependencias gubernamentales en la materia, así como brindar apoyo y asesoría para la adopción de buenas prácticas en ciberseguridad, en organismos gubernamentales, empresas y otros usuarios de las Tecnologías de la Información y las Comunicaciones (TIC).
- **Categorización, supervisión y detección de amenazas**. Las agencias asumen la responsabilidad de monitorear las amenazas cibernéticas y detectar posibles ciberataques. Trabajan con otros organismos gubernamentales e intercambian información con los usuarios para identificar y clasificar las amenazas. Haciendo uso de estrategias de Gestión de Riesgos, diseñan y aplican sistemas de detección y análisis de eventos para reconocer patrones de los ciberataques a fin de anticiparlos y contrarrestarlos. Coordinan esfuerzos para la detección de actividades sospechosas en las redes y sistemas informáticos.
- **Respuesta a incidentes.** Las agencias son responsables de coordinar y dirigir la respuesta a incidentes de seguridad cibernética a nivel nacional. Esto implica coordinar la gestión, el desarrollo de herramientas y coordinación de esfuerzos para la mitigación de incidentes, la recopilación de pruebas digitales, el apoyo a las organizaciones afectadas y la colaboración con otros actores relevantes, como otras agencias gubernamentales y proveedores de servicios de internet.
- **Inteligencia de amenazas**. Las agencias recopilan y analizan información sobre amenazas y tendencias en seguridad cibernética a nivel global. Esto les permite entender mejor las tácticas y técnicas utilizadas por ciberdelincuentes para poder ofrecer advertencias y recomendaciones oportunas a los grupos interesados.
- **Protección de infraestructuras críticas.** Es usual que las agencias asuman, al menos en forma compartida con otras dependencias gubernamentales, la responsabilidad de identificar y proteger las infraestructuras críticas contra posibles ataques cibernéticos.
- **Sensibilización, capacitación y educación.** Las agencias realizan múltiples actividades para aumentar la conciencia sobre la importancia de la seguridad cibernética a través de campañas de sensibilización, capacitación y programas educativos. Para tal efecto, promueven la formación en seguridad cibernética en instituciones educativas de todos los niveles, capacitan personal de otras dependencias gubernamentales y empresas, y ofrecen recursos y materiales informativos para ayudar a las personas y organizaciones a protegerse de las amenazas en línea.
- **Investigación, desarrollo e innovación.** Algunas agencias participan

activamente, en colaboración con otras dependencias gubernamentales, universidades y empresas proveedoras de servicios de TIC, en programas de investigación enfocados en desarrollo de mejores metodologías y herramientas de protección.

Como seguimiento de la primera Contribución aprobada por el Comité con relación a la regulación de la Ciberseguridad, se exponen algunos comentarios, consideraciones y sugerencias a la iniciativa presentada. Cabe mencionar que los comentarios aquí presentados provienen de expertos y profesionales de los sectores académico, de investigación, de empresas tecnológicas, de entidades federales, de diversas cámaras y agrupaciones de empresas del medio, así como de la sociedad civil que integran el Comité. Lo anterior en un ánimo de colaborar y contribuir a la integración de un marco normativo robusto.

Si bien el documento presentado es producto del trabajo y contribuciones de todos los integrantes de la Mesa 5 del Comité, se destaca la colaboración para la integración de este documento de los siguientes integrantes del Comité:

- Javier Altamirano Magaña - Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información
- Manuel Díaz Franco - Huawei Technologies de México, S.A. de C.V.
- Ileana Gisela San Juan Rivera
- José Luis Solleiro Rebolledo
- José Luis Ponce González - Micronet de México, S.A. de C.V.
- Ricardo Martínez Salazar - Instituto Federal de Telecomunicaciones
- Sayuri Adriana Koike Quintanar - Instituto Federal de Telecomunicaciones
- Julia Urbina-Pineda- Ciberseguridad Móvil e Inalámbrica, S.A.S. de C.V.

Comentarios en lo particular a las disposiciones de la INICIATIVA DE LEY FEDERAL DE CIBERSEGURIDAD

Disposición de la Iniciativa:	**Observaciones**	**Sugerencias:**
TÍTULO PRIMERO DISPOSICIONES GENERALES		
ARTÍCULO 1		
Se sugiere armonizar la previsión de este Artículo con lo que establecen las leyes que norman tanto a la Administración Pública Federal (APF) como a Organismos Constitucionales Autónomos.		
Fracción I		Se recomienda definir los principios y lineamientos generales a los que debe sujetarse la Política Nacional en la materia. Se sugiere la siguiente redacción: *Definir las instituciones responsables de la Ciberseguridad, así como los*

		principios y lineamientos generales a los que debe sujetarse la Política Nacional en la materia, sin perjuicio de lo establecido en la ley de Seguridad Nacional y Seguridad Pública;
Fracción II	Se sugiere armonizar con las leyes en materia de seguridad, y en su caso, del Código Penal Federal.	Se sugiere incluir a los titulares, administradores etc., de Infraestructuras Críticas. Se sugiere considerar la siguiente redacción: *Establecer las bases de coordinación entre la Administración Pública Federal, así como con las Entidades Federativas y Organismos Constitucionales Autónomos, de conformidad con su marco jurídico vigente;*
Fracción III		Se sugiere utilizar el término "Ciberresiliencia" y adicionar su definición conforme a lo establecido en el Glosario de Términos SEDENA-MARINA en Materia de Seguridad en el Ciberespacio: https://www.gob.mx/cms/uploads/attachment/file/661790/Glosario_de_Terminos_SD-SM_compressed.pdf Se sugiere considerar la siguiente redacción: *Fomentar la colaboración con la Academia e instancias del Sector privado del país;*
Fracción VI		Se sugiere complementar con la siguiente redacción: Fomentar la colaboración con la Academia e instancias del Sector privado del país;
Fracción IX	Es de considerar que la potestad sancionadora del Estado por la comisión de delitos está establecida en los Códigos Penales. Se recomienda revisar para evitar duplicidad y/o competencia.	
ARTÍCULO 3		
Se recomienda homologar las definiciones del glosario presentado en este Artículo con el Glosario de Términos de SEDENA-MARINA (https://www.gob.mx/cms/uploads/attachment/file/661790/Glosario_de_Terminos_SD-SM_compressed.pdf).		
Fracción III		Se sugiere valorar las definiciones presentadas en el NIST relativas a aplicación https://csrc.nist.gov/glossary/term/application La fracción establece textualmente: "Aplicaciones. Programa o conjunto de

		programas informáticos que realizan el procesamiento de registros para una función específica, diseñado para el beneficio del usuario final.” Se sugiere que diga: “Aplicaciones. Programa o conjunto de programas informáticos que realizan el procesamiento de registros, datos, o información contextualizada que forme parte o no de un registro, para una función específica, diseñado para el beneficio del usuario final.”
Fracción IV	Dado que la autenticación es un proceso, mientras que los factores de autenticación están relacionados con los conceptos de componentes de conocimiento, pertenencia y/o características, se sugiere que estas definiciones sean tomadas en cuenta en la fracción.	Se sugiere valorar la permanencia de este texto, de conformidad con lo establecido en el NIST https://csrc.nist.gov/glossary/term/authenticate
Fracción V		Se sugiere el cambio de definición hacia: "Autenticidad. La propiedad de ser genuino y poder ser verificado y confiable; confianza en la validez de una transmisión, un mensaje o el emisor del mensaje", debido a que adicionalmente la comprobación y confirmación están relacionados con la fiabilidad.
Fracción VI		Dice: “Base de datos. Recopilación de datos estructurados almacenados de manera digital.” Se sugiere que diga: “Base de Datos. La recopilación, colección o compilación de datos estructurados y no estructurados almacenados de manera digital.” Ya que existen bases de datos para ambos tipos de información. Se sugiere armonizar la definición de Bases de Datos con lo establecido en la Ley Federal de Derechos de Autor. Art.107 : Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Esa protección no se extenderá a los datos y materiales en sí mismos.
Fracción VIII		Se sugiere complementar la definición conforme lo definido por el *European*

		Telecommunications Standards Institute (ETSI) y por el *National Instituto of Standards and Technology* (NIST) de Estados Unidos de América. https://portal.etsi.org/webapp/ewp/copy_file.asp?wki_id=63989 https://csrc.nist.gov/glossary/term/Cyber_Threat
Fracción X		En la fracción XXIX de este mismo Artículo de hace referencia a un *Estado-Nación*. Se sugiere validar si la referencia a *Estado* usado en esta fracción es la misma.
Fracción XIV		Se sugiere lo siguiente: Dice: "Confidencialidad. Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información." Se sugiere que diga: "Confidencialidad. Es la facultad de restringir el acceso a cierta información ejercida por su titular en contra de terceros o de permitir el acceso a la misma con los Requisitos de preservación señalados por dicho titular."
Fracción XV	Es de resaltarse que los datos no solo se encuentran en formato electrónico y su transmisión puede ser a través de señales eléctricas, haces de luz, señales electromagnéticas. Para el almacenamiento no solo se realiza en medios magnéticos, ópticos y mecánicos, sino que existen tecnologías como electrónicos, biotecnologías y otros. Cabe mencionar que los datos informáticos no solo se recuperan o transmiten, sino que también se procesan por lo que la definición debe tomar en consideración los datos que se están procesando en tiempo real. Adicionalmente, se sugiere tomaren consideración los activos que procesan información en el cómputo cuántico.	Se sugiere lo siguiente: Dice: "Datos Informáticos. información en formato electrónico que permite su recuperación o transmisión, incluyendo cantidades, caracteres o símbolos, en forma de señales eléctricas o grabación en medios magnéticos, ópticos o mecánicos." Se propone: "Datos Informáticos. Información o datos en cualquier tipo de formato electrónico que permite su recuperación, transmisión o procesamiento, incluyendo cantidades, caracteres o símbolos, en forma de señales eléctricas, haces de luz, señales electromagnéticas o grabación en medios magnéticos, ópticos o mecánicos."
Fracción XVI		Si se prevé la firma del Convenio sobre Ciberdelincuencia (Convenio de Budapest), se sugiere considerar incluir también el ámbito internacional. Por ejemplo, la definición de este término incluida en el Glosario de

		Términos SEDENA-MARINA en Materia de Seguridad en el Ciberespacio señala lo siguiente: "Delitos Cibernéticos (Ciberdelitos): acciones ilícitas que se encuentran en la legislación nacional y/o internacional vigentes…" https://www.gob.mx/cms/uploads/attachment/file/661790/Glosario_de_Terminos_SD-_SM_compressed.pdf Se sugiere referir que el combate es para todo tipo de delito en el contexto del empleo de las TIC, para no limitarlo a un solo tipo de delitos
Fracción XVII	Se sugiere considerar que la disponibilidad es un principio de la seguridad de la información para que los activos de información puedan ser utilizados para los fines establecidos en el momento en el que se requieren. Se recomienda revisar la definición en los términos mencionados.	
Fracción XVIII	Se sugiere tomar en consideración las tecnologías basadas en señales biotecnológicas, cuánticas, lumínicas. Se recomienda complementar la definición considerando lo mencionado.	Se sugiere lo siguiente: Dice: "Dispositivo. Combinación de diversos elementos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas para cumplir un propósito específico." Se propone: "Combinación de diversos elementos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas, biotecnológicas, cuánticas, lumínicas, entre otras, para cumplir un propósito específico."
Fracción XX		Se sugiere hacer referencia al documento emitido en 2017 https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
Fracción XXI	Se sugiere considerar que una evidencia es algo que ya se encuentra en una investigación, para que no se confunda el concepto con un indicio.	Se recomienda revisar la definición de evidencia para diferenciarla de la definición de indicio.
Fracción XXII		Se sugiere ahondar en la referencia hecha a "una probabilidad significativa", definiendo de manera cuantitativa su valor y el mecanismo para obtenerlo. Se recomienda complementar la definición de Incidente de

		Ciberseguridad, basado en las mejores prácticas internacionales.
Fracción XXIII		Se recomienda que se especifiquen cuáles son los servicios o infraestructuras que serán considerados como Infraestructuras Críticas de Información, con el objeto de dar claridad a si se incluye al prestador final de servicio o también a las cadenas de suministro. Se sugiere se incluya la definición de "Servicios esenciales".
Fracción XXX		Se sugiere complementar la definición en los siguientes términos: "Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado, considerando: (i) los impactos adversos que surgirían si la circunstancia o evento ocurriera; y (ii) la probabilidad de ocurrencia".
Fracción XXXII		Se sugiere complementar esta definición con la especificación de lo que es el ciclo de vida de la información y/o datos.
Fracción XXXV	Se sugiere acotar la definición de Tecnología para Intervención de Comunicaciones toda vez que es muy amplia y pudiera referirse, no sólo a la intervención de los servicios de comunicación, sino también a cualquier tipo de servicio tecnológico. Si no se especifica, podría referirse a cualquier otro servicio basado en tecnologías de la información.	Se sugiere acotar la definición, con el objeto de que se armonice con el objeto de la Ley.
Fracción XXXVII		Se sugiere considerar en la definición que un usuario, en el marco del derecho penal, sería el sujeto activo en la comisión de delitos, se aprecia relevante considerar que la investigación y proceso penal se siguen respecto de las personas (físicas o morales), no así por los conceptos de entidad o proceso.
ARTÍCULO 4		
		Supletoriedad de la Ley Federal de Ciberseguridad: Se sugiere adicionar al Artículo 4° como ley supletoria el Código Nacional

		de Procedimientos Penales, toda vez que dicha ley regula actos y técnicas de investigación de los delitos en materia de ciberseguridad. Toda vez que, si regula delitos, investigación y partes del procedimiento penal, será necesario que el Código Nacional sea supletorio en dicha parte. Se sugiere que se integren de forma supletoria: Ley Federal de Derechos de Autor. Ley Federal de Protección al Consumidor. Código Fiscal de la Federación. Código de Comercio, de acuerdo con la Ley Federal de Protección a la Propiedad Industrial.
TÍTULO SEGUNDO: DE LA POLÍTICA NACIONAL DE CIBERSEGURIDAD		
ARTÍCULO 5		
		Se sugiere incorporar al listado de los objetos de protección a las "Infraestructuras Críticas de Información".
ARTÍCULO 6		
		Se recomienda utilizar las definiciones de NIST (https://csrc.nist.gov/glossary/term/asset), y ENISA (https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary), y ISO (https://www.iso.org/glossary.html), y ETSI (https://www.etsi.org) y UIT (www.itu.int). Se sugiere especificar los incidentes que se mencionan como Cibernéticos.
ARTÍCULO 8		
Fracción I		La definición de ciberseguridad en el Artículo 3 se centra en los aspectos técnicos por lo que, para hablar de un "derecho a la ciberseguridad", se sugiere especificar lo que implica el derecho a la ciberseguridad, si refiere a la protección de la privacidad, seguridad de la información, protección contra delitos informáticos y acceso seguro a servicios digitales.
Fracción III		Se sugiere se incluya el monitoreo de las amenazas.
Fracción IV		Se recomienda armonizar lo mencionado en esta fracción con la legislación existente, ya que el acceso a internet se encuentra previsto en la Ley Federal de Telecomunicaciones y

		Radiodifusión así como en los Lineamientos para la gestión de tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet, publicados por el IFT y disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5622965&fecha=05/07/2021#gsc.tab=0
Fracción VI		Toda vez que el combate a la delincuencia organizada y la trata de personas es facultad de otras dependencias, así como otros tipos de crímenes específicos que igualmente se cometen en el ciberespacio, se sugiere agregar a esta fracción que el combate a la delincuencia y trata se realizarán de conformidad con las leyes aplicables.
Fracción VII	Al ser un modelo de seguridad compartida se sugiere no instar a una de las partes a ser responsable único.	Se recomienda que se establezca que para cada caso en particular se identificará la responsabilidad y corresponsabilidad de la información e infraestructura tecnológica desde un punto de vista de un modelo de seguridad compartida, incluyendo a los que ofrecen, administran, operan, colectan, almacenan información, así como la que transita por cualquier medio.
Fracción VIII		Se sugiere que se utilice la palabra *controles* en lugar de *medidas*, ya que, en el argot de la ciberseguridad, los controles permiten administrar el riesgo y con ello mitigar, evitar, transferir, compartir o aceptar el riesgo con base en el análisis de los activos de información.
CAPÍTULO I DE LA COMISIÓN INTERSECRETARIAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, Y DE LA SEGURIDAD DE LA INFORMACIÓN		
ARTÍCULO 9		
		El inciso (c) menciona la CFE, repitiendo el numeral XXIX del inciso (b). Se sugiere eliminar uno de los dos.
ARTÍCULO 10		
		Debido al rol que las telecomunicaciones juegan en el ciberespacio, se considera necesario que el Instituto Federal de

		Telecomunicaciones, como regulador sectorial en la materia, forme parte de la Comisión desde un principio y no esté sujeta su presencia a la invitación de los integrantes de esta.
Artículo 11		
FRACCIÓN IV		Se sugiere se incorpore un Artículo transitorio para esta actividad.
FRACCIÓN IX		Se sugiere se incorpore un Artículo transitorio para esta actividad.
CAPÍTULO II **DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD**		
ARTÍCULO 13		
• Se sugiere proveer una mayor claridad respecto a la naturaleza jurídica de la Agencia Nacional de Ciberseguridad.		Se sugiere clarificar la naturaleza jurídica de la Agencia Nacional de Ciberseguridad y dotarla de autonomía de gestión y presupuesto, así como establecer con certeza su adscripción. Se sugiere que el precepto sea específico y expreso en cuanto a que la Agencia sea la autoridad que exija, a quienes ofrezcan servicios en el ciberespacio o detenten información del público en general, el cumplimiento de los estándares internacionales en materia de ciberseguridad y la consecuencia de su incumplimiento.
FRACCIÓN I		Si bien el Artículo 14 señala que le corresponderá a la Agencia formular la Estrategia Nacional de Ciberseguridad, se sugiere establecerlo como una atribución en el Artículo 13.
FRACCIÓN IV	Se sugiere definir las restricciones de difusión y las normas de intercambio de información para permitir este nivel de coordinación e intercambio de información.	Se recomienda armonizar con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados al abordar el tratamiento y transferencia de los datos personales y en la Ley General de Transparencia y Acceso a la Información Pública y en la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Se recomienda que se utilicen los mecanismos establecidos de forma internacional Se sugiere intercambiar la palabra "esquemas" por "protocolos", así mismo, se sugiere considera lo establecido en el Protocolo Nacional-Homologado de Gestión de Incidentes Cibernéticos https://www.gob.mx/gncertmx/documentos/94081

FRACCIÓN V		Se sugiere que la fracción tome como base lo estipulado por el Convenio de Budapest al respecto.
FRACCIÓN VI		Se recomienda revisar si el organismo cuenta con mecanismos de segregación de funciones con estas atribuciones.
FRACCIÓN IX	Resulta importante señalar que de conformidad con la Ley Federal de Telecomunicaciones y Radiodifusión que establece entre otros, lo siguiente: "Artículo 15. Para el ejercicio de sus atribuciones corresponde al Instituto: I. Expedir disposiciones administrativas de carácter general, planes técnicos fundamentales, lineamientos, modelos de costos, procedimientos de evaluación de la conformidad, procedimientos de homologación y certificación y ordenamientos técnicos en materia de telecomunicaciones y radiodifusión; así como demás disposiciones para el cumplimiento de lo dispuesto en esta Ley;…" Dichas disposiciones administrativas resultan aplicable a productos, equipos, dispositivos o aparatos destinados a telecomunicaciones o radiodifusión que puede ser conectado a una red de telecomunicaciones y/o hacer uso del espectro radioeléctrico.	Se sugiere especificar a qué clase de certificación se refiere, ya que se puede referir a productos, personas, servicios o incluso la certificación de sistemas de gestión de la seguridad aplicables a empresas como el ISO 27001, de modo que se evite duplicidad con la legislación actual.
FRACCIÓN X		Se sugiere valorar que en esta fracción se añada a las Entidades Federativas, Organismos Constitucionales Autónomos, Academia e instancias del Sector privado del país.
FRACCIÓN XII		Se sugiere enlistar los beneficios de informar con oportunidad de los incidentes cibernéticos que se presenten.
FRACCIÓN XVII		Se sugiere adherirse a prácticas internacionales reconocidas tales como Common Criteria o ISO 15408. Se sugiere definir qué comprenden los "mecanismos de seguridad tecnológica". Se sugiere que la fracción diga: "Definir los mecanismos de seguridad tecnológica o la adopción de normas o estándares de organismos

		internacionales con los que deberán cumplir los dispositivos electrónicos que se comercialicen en México". Lo anterior en el entendido que, en la definición de dichos mecanismos, la Agencia deberá atender los estándares internacionales y las mejores prácticas de mercado;
FRACCIÓN XIX		Toda vez que se cuenta con un antecedente de catálogo nacional de Infraestructuras Críticas, Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información, se sugiere que se realice la actualización. Se sugiere valorar el incluir, en su caso, los servicios esenciales y replicar en donde se considere necesario.
FRACCIÓN XX	Las normas y estándares internacionales consideran incluir la promoción de la cooperación internacional, pues la ciberseguridad es un desafío global que requiere aprovechar el intercambio de buenas prácticas con todos los países. Se sugiere consultar el documento de posicionamiento elaborado por la Mesa 5 en el 2022: "Marco Nacional de Regulación sobre Ciberseguridad. Recomendaciones". Comité Técnico en materia de despliegue de 5G en México. Mesa 5. Ciberseguridad" como referencia. Disponible en la liga: https://comite5g.ift.org.mx/vendor/descarga_archivo.php?id_archivo=22632	Se propone incorporar a las autoridades competentes, para lo cual se presenta la propuesta siguiente: Definir controles estandarizados, o adoptar normas o estándares de organismos internacionales de seguridad de las Infraestructuras Críticas de Información, en coordinación con las autoridades competentes. Dentro de estas autoridades competentes pudieran estar la Comisión Nacional de Hidrocarburos, la Comisión Reguladora de Energía, el Instituto Federal de Telecomunicaciones, entre otras.
FRACCIÓN XXIII		Las actividades de inteligencia están designadas para organismos como CNI, SEMAR, SEDENA, GN, por lo que se sugiere delimitar las atribuciones de esta Agencia.
FRACCIÓN XXV		Se recomienda considerar el modelo de ISAOCs (*Information Sharing and Analysis Organization or Center*) para ampliar los mecanismos de comunicación entre distintos sectores de la industria. En la redacción, se sugiere sustituir *permanentes* por *estandarizados*.
FRACCIÓN XXVII		En cuanto al mapa de riesgos, se sugiere especificar que la facultad de la Agencia sería la de consolidar o

		coordinar, ya que la elaboración le corresponde al organismo que gestiona su infraestructura.
FRACCIÓN XXVIII	Se recomienda ahondar en la composición de este Consejo Consultivo y sus funciones. Se recomienda que este Consejo no dependa de la Agencia para que tenga suficiente autonomía para emitir sus recomendaciones.	Se sugiere complementar el texto de la fracción, de acuerdo con lo siguiente: Promover la creación de un Consejo Consultivo Ciudadano de Ciberseguridad para generar un entorno de comunicación multisectorial abierto entre el organismo regulador y las empresas del sector privado, que estimule la colaboración y que debe consultar a operadores y proveedores para establecer y fortalecer la ciberseguridad. A través de este Consejo Consultivo, los operadores y proveedores podrán participar con experiencias, propuestas, y posturas en el marco de una responsabilidad compartida. Los integrantes deberán ser especialistas de reconocido prestigio en las materias gestión de riesgos y ciberseguridad, serán personas con una trayectoria reconocida, capacidades acreditadas y con vasta experiencia. Con base en los principios de independencia, igualdad, pluralidad y representatividad, entre otros.
FRACCIÓN XXIX		• Se sugiere sustituir la palabra *evidencias* por la palabra *indicios*.
FRACCIÓN XXX	• Se recomienda definir el término "conducta ilícita".	Se recomienda establecer mecanismos para monitorear y evaluar la efectividad de estas medidas en la lucha contra las conductas ilícitas en línea. Esto permitirá ajustar y mejorar las políticas y prácticas a medida que sea necesario y garantizar que se aborden de manera efectiva los desafíos de ciberseguridad. Se sugiere que se acredite además de la dirección IP el puerto de conexión origen. Se sugiere detallar los mecanismos bajo los cuales se "darán de baja" los elementos listados en esta fracción, adicionando que esto se llevará a cabo con apego al debido proceso. Adicionalmente, se sugiere incluir una definición para "dominios". Se sugiere que, para proceder a la solicitud de baja, se establezca un proceso junto con la Secretaría de

		Seguridad y Protección Ciudadana, la Policía Cibernética, el CERT-MX, y el resto de las autoridades involucradas. Se recomienda definir "conducta ilícita". Se sugiere que la facultad establecida pase por control judicial.
FRACCIÓN XXXI		Se sugiere que la Agencia tenga atribuciones para celebrar acuerdos y convenios en materia de Ciberseguridad con cualquier parte interesada, como legisladores, reguladores, academia, privados, con el fin de cumplir con sus atribuciones como la señalada en el Artículo 19, referente al Registro.
CAPÍTULO III **DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD**		
ARTÍCULO 14		
	Se sugiere establecer las capacidades y recursos necesarios para implementar la estrategia de ciberseguridad. Esto implica el desarrollo de infraestructura tecnológica, la formación de expertos en ciberseguridad y la asignación de recursos financieros suficientes para respaldar las iniciativas de seguridad de la Agencia Nacional y otras dependencias de la administración pública. Se recomienda definir el marco normativo complementario a la ley que establezca reglamentos, normas y lineamientos que faciliten la distribución de competencias, responsabilidades y obligaciones para los actores relevantes. Los marcos para la certificación de procesos y prácticas son puntos importantes por atender. Se sugiere que la estrategia aborde aspectos de Innovación y desarrollo tecnológico, lo cual implica la promoción de la investigación y el desarrollo en seguridad cibernética, adopción de tecnologías emergentes como inteligencia artificial y blockchain para fortalecer la protección de infraestructuras, sistemas e información. Se sugiere que la estrategia defina una estrategia de gestión de riesgos que contemple la evaluación de	Se sugiere revisar la armonización de la Ley con la legislación existente en los EE.UU., Latinoamérica, Europa, Asia y Medio Oriente, en particular por lo que se refiere a la gestión de riesgos, controles de seguridad, evaluación de seguridad, respuesta a incidentes y referencia a mejores prácticas. En el año de 2017 se emitió la Estrategia Nacional de Ciberseguridad de México (https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf) por lo que se sugiere la actualización a dicha estrategia. Se sugiere definir o precisar a qué se refiere el "Sistema Nacional de Planeación".

	amenazas y vulnerabilidades cibernéticas, desarrollo de herramientas para su prevención y manejo y mecanismos de comunicación sobre esos riesgos. Se sugiere que la estrategia incluya la promoción de la cooperación internacional. Toda vez que la ciberseguridad se fortalece con el intercambio de buenas prácticas con otros países.	
FRACCIÓN V		Se sugiere contemplar la firma del Convenio sobre la Ciberdelincuencia (Convenio de Budapest) al corresponder a un instrumento internacional vigente en materia de ciberdelito.
FRACCIÓN VI		Se sugiere considerar que el desarrollo de una industria de este tipo pudiera escapar al objetivo de la ciberseguridad.
CAPÍTULO IV DEL REGISTRO NACIONAL DE INCIDENTES DE CIBERSEGURIDAD		
ARTÍCULO 16		
		Se sugiere ampliar la gama de Incidentes de Ciberseguridad que se definen, así como ahondar y precisar la frase *interrupción o degradación importante o relevante* a fin de que la notificación temprana de incidentes cibernéticos sea eficaz.
ARTÍCULO 18		
FRACCIÓN V	Para el cumplimiento de esta fracción se recomienda detallar el proceso de notificación y determinación/definición de riesgos. Se recomienda acotar y determinar un catálogo de amenazas y alcances de la propia notificación.	Se recomienda una definición más específica de lo que es una Infraestructura Crítica de Información. Se recomienda revisar el NFC Risk Management Framework de la CISA y de ETSI (https://www.etsi.org/technologies/cyber-security) y de ENISA y de ITU. Se sugiere especificar el tipo de riesgo relacionado con las Infraestructuras Críticas.
TÍTULO TERCERO: DE LA DISTRIBUCIÓN DE COMPETENCIAS CAPÍTULO I DE LA SEGURIDAD NACIONAL		
ARTÍCULO 20		
Se recomienda adicionar al glosario de términos la definición de *Amenazas a la Seguridad Nacional* en el sentido de la presente iniciativa de Ley.		
FRACCIÓN III	Se sugiere armonizar con lo establecido y definido, respecto a las amenazas a la seguridad nacional, en la Ley de Seguridad Nacional,	

	"Artículo 5 fracción XII. Actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos".	
Artículo 22		
		Se sugiere identificar el proceso e instancia responsable de los mecanismos de mitigación o reparación de los daños.
CAPÍTULO II DE LA SEGURIDAD PÚBLICA		
ARTÍCULO 27		
	Se sugiere armonizar con el marco jurídico actual, ya que el Poder Judicial Federal cuenta con jueces de control para emitir las medidas cautelares necesarias en los procedimientos penales. (Artículo 16 Constitucional)	Se propone el establecimiento de un mecanismo de actualización de los jueces penales del Poder Judicial Federal en materia de ciberseguridad.
CAPÍTULO III DE LA CIBERDEFENSA		
ARTÍCULO 28		
FRACCIÓN I		Se sugiere detallar y especificar cómo se deben realizar los monitoreos mencionados y cuál es el alcance de los mismos, a efecto de evitar posibles injerencias que atenten contra los derechos a la privacidad, así como a la inviolabilidad de las comunicaciones privadas.
FRACCIÓN III		Se recomienda impulsar la firma del Convenio sobre la Ciberdelincuencia (Convenio de Budapest).
FRACCIÓN VI	Se recomienda delimitar y especificar atribuciones y facultades de las fuerzas armadas en las operaciones militares que se mencionan en esta y otras secciones, para garantizar los derechos fundamentales de privacidad, datos personales o información en perjuicio de terceros.	
FRACCIÓN VII		Toda vez que el tema de la Seguridad Nacional que se aborda en el presente Artículo ya se encuentra previsto por la Ley de Seguridad Nacional, en cuyo Artículo 3º, fracción V, se establece la defensa legítima del Estado respecto de otros Estados, se recomienda revisar para evitar duplicidad de funciones.
FRACCIÓN VIII		Se sugiere delimitar alcances, con el

		objeto de que no se presente un traslape de atribuciones con el Instituto Federal de Telecomunicaciones, ya que de conformidad con la Ley Federal de Telecomunicaciones y Radiodifusión: "Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán: … XI. En los términos que defina el Instituto en coordinación con las instituciones y autoridades competentes, dar prioridad a las comunicaciones con relación a situaciones de emergencia, y …" Motivo por el cual los Lineamientos de Colaboración en Materia de Seguridad y Justicia establecen lo siguiente: "CUADRAGÉSIMO NOVENO.- El Instituto coadyuvará con las autoridades competentes, en el establecimiento de un protocolo común para alertar por riesgos o Situaciones de Emergencia en materia de protección civil, el cual incluirá un formato electrónico general para el intercambio de alertas de emergencia y advertencias públicas que puedan ser difundidas simultáneamente en diversas plataformas de telecomunicaciones y radiodifusión, en los términos que éste establezca conforme a la normatividad aplicable de protección civil.". "Derivando finalmente esto, en los Lineamientos que establecen el Protocolo de Alerta Común conforme al lineamiento cuadragésimo noveno de los Lineamientos de Colaboración en Materia de Seguridad y Justicia".
Con base a las observaciones realizadas previamente, se sugiere complementar el Artículo en los siguientes términos: "Artículo 28. Corresponderá a la Secretaría de la Defensa Nacional y la Secretaría de Marina en el ámbito de sus competencias y a través de las unidades administrativas que determinen sus titulares, la atención, única y exclusivamente, de los incidentes cibernéticos que provengan o sean promovidos por otros Estados sujetos de derecho internacional, para lo cual, previa publicación de los lineamientos correspondientes por parte de dichas Secretarías y en cumplimiento de la Ley de Seguridad Nacional, contarán con las atribuciones siguientes:"		
CAPÍTULO IV **DE LA CIBERSEGURIDAD EN LA ADMINISTRACIÓN PÚBLICA FEDERAL**		
Se sugiere establecer un Artículo en el que se indique que debe destinarse presupuesto suficiente para desplegar la infraestructura necesaria y mantenerla en funcionamiento, así como		

el presupuesto necesario para la formación de recursos humanos necesarios. Asimismo, se recomienda establecer la facultad del responsable de la Seguridad de la Información de notificar incumplimientos u omisiones.		
ARTÍCULO 30		
	Se recomienda que se especifiquen los criterios y estándares mínimos que garantizan la seguridad de las organizaciones y las instituciones, mencionados en el Artículo.	Se recomienda incluir estándares mínimos en los siguientes aspectos: - Políticas y procedimientos de seguridad: Desarrollar y mantener políticas y procedimientos de seguridad de la información actualizados y alineados con las regulaciones y estándares aplicables. - Evaluación de riesgos: Realizar evaluaciones periódicas de riesgos de seguridad de la información para identificar y mitigar posibles vulnerabilidades y amenazas. - Capacitación y concientización: Ofrecer capacitación y concientización en ciberseguridad a empleados y personal para garantizar que entiendan sus responsabilidades y las amenazas a las que se enfrentan. - Control de acceso: Implementar controles de acceso sólidos y basados en roles para garantizar que solo las personas autorizadas tengan acceso a sistemas y datos sensibles. - Seguridad física: Asegurar la protección física de las instalaciones y activos de TI mediante medidas de seguridad adecuadas, como sistemas de vigilancia y acceso restringido. - Protección de datos y privacidad: Implementar mecanismos para proteger los datos personales y sensibles almacenados y procesados por las dependencias y entidades, cumpliendo con las leyes y regulaciones de privacidad aplicables. - Seguridad de redes y comunicaciones: Establecer controles de seguridad de red, como firewalls, sistemas de detección y prevención de intrusiones, para proteger las redes y las comunicaciones de amenazas externas e internas.

		- Gestión y respuesta a incidentes: Desarrollar y mantener un plan de respuesta a incidentes de seguridad de la información, incluyendo la creación de un equipo de respuesta a incidentes que pueda actuar de manera rápida y eficaz en caso de un incidente de seguridad. - Monitoreo y auditoría: Implementar sistemas de monitoreo y auditoría para identificar posibles incidentes de seguridad y garantizar el cumplimiento de las políticas y procedimientos de seguridad de la información. - Continuidad del negocio y recuperación ante desastres: Desarrollar y mantener planes de continuidad del negocio y recuperación ante desastres para garantizar la capacidad de las dependencias y entidades de mantener y restaurar sus operaciones en caso de un evento adverso.
ARTÍCULO 32		
		Se sugiere incluir un Artículo transitorio que indique el tiempo en el que serán implementados los Protocolos de Seguridad de la Información referidos.
CAPÍTULO V **DE LAS INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN**		
ARTÍCULO 36		
		Se sugiere incluir un Artículo transitorio que indique el tiempo en el que será implementado.
ARTÍCULO 37		
	Se recomienda partir de una definición de infraestructura crítica.	
ARTÍCULO 38		
		En aras de impulsar la colaboración, se sugiere que el Artículo complemente su redacción como se indica: "Artículo 38. La Agencia Nacional de Ciberseguridad, con el apoyo de las autoridades de la federación, entidades federativas, órganos constitucionales autónomos y los particulares, deberá determinar si las infraestructuras de estos cumplen con los criterios

		establecidos para ser consideradas como Infraestructuras Críticas de Información, en cuyo caso la Agencia deberá inscribir dicha infraestructura en el catálogo correspondiente.”
ARTÍCULO 40		
FRACCIÓN III		Se sugiere acotar la definición de Incidente de Ciberseguridad, basado en las mejores prácticas internacionales.
FRACCIÓN VI	Se recomienda delimitar y especificar qué elementos del sistema estarían sujetos a las revisiones, ejercicios, simulacros y análisis, así como la descripción de cada uno de los aspectos listados.	
Artículo 43		
		Se propone definir los criterios para asegurar la privacidad de la información a la que accedan los servidores públicos. Se sugiere sustituir la palabra “promesa” por Acuerdo o convenio de confidencialidad.
TÍTULO CUARTO: PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES CAPÍTULO I DE LOS DERECHOS Y OBLIGACIONES		
Se recomienda que los Capítulos, Artículos y fracciones definidas en este Título se armonicen con el marco legal actual en México.		
ARTÍCULO 44		
	Se propone complementar la redacción de acuerdo con lo siguiente: Artículo 44. Conforme a lo establecido en la Constitución Política de los Estados Unidos Mexicanos, todas las personas tendrán los siguientes derechos digitales:	
FRACCIÓN IV		Se sugiere complementar qué Leyes son aplicables; por ejemplo: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Artículo 45		
FRACCIÓN II Y III		Se sugiere adicionar la definición de lo que se entiende por fin lícito.
FRACCIÓN IV		Se sugiere definir a lo que se refiere un acceso legal.
CAPÍTULO II DE LA PROTECCIÓN DE DATOS PERSONALES		
ARTÍCULO 46		
	Con el fin de evitar duplicidades se	Se recomienda no limitar a datos

	recomienda armonizar lo contenido en este Artículo con lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.	personales e involucrar al INAI. Se sugiere incorporar que dichas autoridades deben desarrollar procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales, en los cuales se incluyan los periodos de conservación de los mismos.
ARTÍCULO 47		
	Se sugiere alinear lo establecido en este Artículo con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO), que en México se aplica a entidades gubernamentales y organismos autónomos en todos los niveles del gobierno, incluyendo federal, estatal y municipal.	
ARTÍCULO 49		
	Se recomienda analizar lo relativo a la competencia, ya que la protección de los datos personales es competencia del INAI. Se recomienda armonizar con la legislación actual relacionada con la notificación de violación de la seguridad, ya que de acuerdo con la LFPDPPP (Ley Federal de Protección de Datos Personales en Posesión de Particulares), en caso de una violación de la seguridad de datos personales que afecte de forma significativa los derechos patrimoniales o morales de los titulares, el responsable (la empresa que maneja los datos personales) debe informar a los titulares de los datos sobre la violación.	Notificación a la Agencia Nacional de Ciberseguridad: se recomienda definir el contenido y términos de la notificación, en armonía con el marco legal actual, conforme al cual la comunicación debe incluir, al menos: ○ La naturaleza del incidente. ○ Los datos personales comprometidos. ○ Las recomendaciones para que el titular pueda proteger sus intereses. ○ Las acciones correctivas inmediatas que se hayan implementado. ○ Los medios para obtener más información sobre el incidente.
ARTÍCULO 50		
	Se recomienda definir con precisión el término "alto riesgo para los derechos y libertades de las personas físicas".	Se sugiere que en este Artículo se incluya que la Agencia Nacional de Ciberseguridad deberá implementar mecanismos/procesos de anonimización de la información. De esta forma puede generar información compartible sin afectar a los involucrados.
ARTÍCULO 52		
		Se sugiere definir si el término "Información Reservada" se debe interpretar como lo indica el Artículo 110 de la Ley Federal de

		Transparencia: "aquella que pueda comprometer la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable".
TÍTULO QUINTO DE LA PRESTACIÓN DE SERVICIOS, USO DE INFRAESTRUCTURA DIGITAL Y TELECOMUNICACIONES		
ARTÍCULO 53		
	Se recomienda armonizar la disposición con tratados y acuerdos internacionales en la materia.	Se recomienda revisar y armonizar con lo establecido en el Art. 20.89 del T-MEC, y demás Artículos relacionados en el mismo tratado.
	En términos generales se considera que el almacenamiento de datos en territorio nacional no resulta en mayor seguridad de la información. En contraste, almacenar la información en la nube puede estar en condiciones de brindar una mayor seguridad, dado que la información se encuentra resguardada en múltiples sitios y no en un solo lugar físico, como ocurre cuando se cuenta con infraestructura propia, independientemente del lugar donde ésta se encuentre. En ese sentido, para efectos de seguridad de la información, la inversión en la infraestructura y su mantenimiento es, por mucho, más crítica que el lugar donde se encuentre esta almacenada. Adicionalmente, se sugiere considerar que el almacenamiento de datos en territorio nacional no se vincula con el acceso a la información en el marco de alguna investigación judicial.	Se recomienda revisar lo previsto en la Ley Federal de Telecomunicaciones y Radiodifusión en el Artículo 189. Se considera necesario crear reglas para los servicios de infraestructura digital o como lo define la Ley Federal de Telecomunicaciones y Radiodifusión, como "proveedores de servicios de aplicaciones y contenidos". Se sugiere agregar definiciones para cada uno de los siguientes elementos: plataformas de redes sociales, comunidades de videojuegos en línea, streaming y plataformas de entretenimiento en línea. Se sugiere complementar la redacción del Artículo en el siguiente sentido: Los proveedores de servicios de infraestructura digital, plataformas de redes sociales, plataformas comerciales para juegos en línea, streaming, plataformas de entretenimiento en línea y telecomunicaciones que operen en territorio nacional están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezca la Constitución Política de los Estados Unidos Mexicanos y demás leyes. Para lo cual estarán sujetos a las siguientes obligaciones específicas: …
FRACCIÓN III	Se recomienda especificar los términos y condiciones del registro ante la Agencia.	Se recomienda homologar con lo establecido en el Art. 190 de la Ley Federal de Telecomunicaciones y Radiodifusión.
FRACCIÓN VI		Se sugiere considerar las siguientes recomendaciones para el reporte de incidentes:

		○ Reportar incidentes confirmados y significativos a la infraestructura crítica, es decir, que el incidente lleve a la pérdida de confidencialidad, integridad, o disponibilidad de la información, y que tenga impacto en la seguridad y resiliencia de los sistemas operativos. ○ Un esquema de reportes sencillo, confidencial y confiable incentiva un ambiente colaborativo.
FRACCIÓN VIII	Se recomienda armonizar esta disposición con el Capítulo 19 del T-MEC Ya que, en línea con las disposiciones 19.11 y 19.12 del Capítulo 19 del TMEC, las organizaciones de todos los tamaños y en todos los sectores deben poder mover datos de forma segura a través de las fronteras para competir de manera efectiva. Los requisitos para localizar datos pueden constituir una barrera para ingresar a un mercado, lo que socava la competitividad y eleva los costos. Por ello, se sugiere la inclusión de disposiciones que protejan el movimiento de datos a través de las fronteras. De la misma manera, las disposiciones 19.8 y 19.15 del TMEC exigen a las Partes que adopten marcos legales para proteger la información personal y promover las mejores prácticas de la industria, estándares internacionales y otros mecanismos de cooperación para fortalecer la privacidad y la protección de datos. Paralelamente, promueven el fortalecimiento de las capacidades de seguridad cibernética a través de la cooperación internacional y la adopción de enfoques basados en el riesgo para la regulación de la seguridad cibernética.	Se sugiere procurar la compatibilidad de las fracciones VII y VIII del presente Artículo, con las obligaciones de México conforme a los Artículos 15.6 y 19.12 del T-MEC, en virtud de que no puede exigirse un requisito de presencia local a prestadores de servicios transfronterizos, que operan desde el territorio de EE. UU. o Canadá.
FRACCIONES VIII Y IX	Se sugiere considerar que los datos almacenados localmente no están libres de ciberataques. Las transferencias transfronterizas de datos son una herramienta importante para la ciberseguridad:	Se recomienda establecer una definición precisa de vulneración a la seguridad nacional.

	crean redundancia, resiliencia y reducen la latencia. Se puede así monitorear patrones de tráfico, anomalías y desviar amenazas.	
FRACCIÓN XIII	Se recomienda considerar que la constitución establece que será autorizada exclusivamente por la autoridad judicial federal a petición de la autoridad administrativa federal competente o de la Procuraduría General de la República.	Se sugiere modificar la redacción en los siguientes términos: "XIII. Dar de baja direcciones IP, aplicaciones, dominios y sitios de internet dentro de un plazo oportuno posterior a la notificación que le realicen la Agencia, la Fiscalía General de la República, CERT-MX y autoridades judiciales competentes para su inhabilitación, debiendo cumplir con cualesquiera recursos legales que pudiera obtener el afectado que suspendan o desechen la notificación correspondiente". Se sugiere establecer el proceso para poder llevar a cabo las bajas mencionadas.
FRACCIÓN XIV		Se recomienda armonizar las funciones con la legislación actual para evitar duplicidad. Respecto a la conservación de direcciones IP. La Le Federal de Telecomunicaciones y Radiodifusión prevé un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos: a) Nombre, denominación o razón social y domicilio del suscriptor; b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados); c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas

		de prepago; d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia; Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio; e) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor; f) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y g) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación. Asimismo, se sugiere considerar que no se establece la obligación de conservar direcciones IP a los concesionarios de telecomunicaciones y, en su caso, a los autorizados de los servicios móviles.
ARTÍCULO 54		
		Se sugiere que lo relativo a la cooperación internacional sea considerado a través de la adopción del convenio de Budapest. Toda vez que estos servicios se refieren a los servicios Over the Top los cuales pueden definirse como aquellos servicios de video, audio, voz o datos que se transmiten sobre las plataformas de internet fijo o móvil y que generalmente no son provistos por los operadores tradicionales de telecomunicaciones. Este tipo de servicios incluye la distribución de audio y video asociado (como YouTube), videoconferencias (como Skype o Facetime), contenidos audiovisuales bajo demanda (Netflix,

		Claro TV, etc.), servicios de mensajería (WhatsApp, Line, etc.) y comunicación a través de redes sociales (como Facebook, Twitter, LinkedIn, Waze), se sugiere considerar el alcance de la Ley Federal de Telecomunicaciones y Radiodifusión. En ese sentido, con fines de precisión, se sugiere la siguiente adición al segundo párrafo del referido Artículo para quedar como sigue: Para efectos del párrafo anterior, los proveedores antes citados, deberán sujetarse, en lo que les resulte aplicable, a lo dispuesto en el Título Octavo "De la Colaboración con la Justicia", de la Ley Federal de Telecomunicaciones y Radiodifusión."
ARTÍCULO 56		
		Se sugiere considerar que las autoridades facultadas y designadas deberán observar lo previsto en la Ley Federal de Telecomunicaciones y Radiodifusión, así como en los Lineamientos de Colaboración en materia de Seguridad y Justicia respecto a la solicitud de la intervención de comunicaciones privadas; los referidos instrumentos prevén que las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. En función de lo anterior, se sugiere agregar o modificar este Artículo a efecto de señalar lo anterior. Se sugiere retomar lo señalado en el Artículo 16 párrafos 12 y 13 de la Constitución Política de los Estados Unidos Mexicanos, así como lo señalado en el último párrafo del Artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión.
ARTÍCULO 58		
	Se sugiere revisar si lo establecido en este Artículo contraviene el principio de publicidad de la información contenido en el Artículo 6o.	Se sugiere omitir la reserva previa establecida en el Artículo respecto de la información contenida en el Registro Nacional de Proveedores de Tecnología

	constitucional y criterios de la Suprema Corte que establecen que las reservas previas violan el derecho a la información.	para Intervención de Comunicaciones.
ARTÍCULO 59	Se sugiere precisar la definición de "tecnología para intervención de comunicaciones"; y considerar que la prohibición del uso privado de spyware hace sentido, al mismo tiempo que sea posible y permitido utilizar herramientas legítimas de ciberseguridad para proteger las redes.	
TÍTULO SEXTO: DE LA CULTURA Y EDUCACIÓN		
ARTÍCULO 60		
FRACCIÓN V		Se proponen las siguientes consideraciones que permitan una nueva redacción o la integración de las fracciones que fueran oportunas: Promover acciones con la Secretaría de Educación y la Secretaría del Trabajo y Previsión Social, para desarrollar los programas de ciberseguridad a través de la diversificación de los planes de estudios de los Institutos de Educación Superior (IES) en términos de contenido, niveles y lenguaje. Promover mecanismos de concesión de becas, especialmente en las áreas de educación media y en investigación tecnológica para promover la ciberseguridad como un campo diverso. Desarrollar un enfoque unificado en el gobierno, la industria y las instituciones de educación superior a través de la educación pública y privada. Implementar mediciones de los resultados de los programas (incluidos los resultados y las lecciones aprendidas) de las instituciones de educación superior. Elaborar el análisis de las necesidades y tendencias del mercado de ciberseguridad a través de métricas que muestran la extensión del problema y posibles medidas de control. Monitorear las tendencias en cuanto al número de graduados en ciberseguridad, así como las vacantes en el sector público y privado en

		materia de ciberseguridad.
TÍTULO SÉPTIMO: DE LAS INFRACCIONES Y SANCIONES		
ARTÍCULO 63 Se recomienda incluir dentro de los criterios la velocidad de recuperación.		
FRACCIÓN I		Se sugiere considerar si el infractor adoptó las medidas necesarias apegado a las mejores prácticas internacionales para resguardar la seguridad informática de las operaciones.
TÍTULO OCTAVO: DE LOS DELITOS CIBERNÉTICOS **CAPÍTULO I DE LOS DELITOS CONTRA LA CIBERSEGURIDAD** **SECCIÓN PRIMERA: DE LOS DELITOS CONTRA LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD**		
ARTÍCULO 65		
	Se recomienda revisar, para evitar duplicidad con los delitos tipificados en los Artículos 211 bis 1 al 211 bis 7 del Código Penal Federal (Acceso ilícito a sistemas y equipos de informática). Toda vez que se describen varias conductas con una sola penalización, se sugiere diferenciar unas de otras para la determinación de la pena. Sirva de ejemplo que el simple acceso merece la pena menor, mientras que copiar y extraer información es más lesivo requiere otra sanción más alta; pero aún más grave es que modifique, altere, destruya o elimine.	Se sugiere adicionar la transferencia de información.
ARTÍCULO 66		
	Se sugiere revisar la referencia al Artículo 61 de esta propuesta de Ley, pudiendo ser al Artículo al 65.	Se sugiere que al utilizar conceptos técnicos (cifre, exflitre) estos sean definidos con precisión, ya que al momento del proceso penal sería motivo de dificultades, en aras de evitar un tipo penal en blanco o de apreciación subjetiva.
ARTÍCULO 67		
	Se sugiere revisar la referencia a los Artículos 61 y 62 de esta propuesta de Ley, ya que podrían referirse a los Artículos 65 y 66.	
SECCIÓN SEGUNDA: DEL ATAQUE A LA INTEGRIDAD DE UN SISTEMA INFORMÁTICO		
ARTÍCULO 68		
	Se recomienda diferenciar las conductas referidas (p. ej.: al que sin autorización o excediendo de la autorización), ya que podrían significar una pena distinta o	

	agravada para cada una de estas.	
SECCIÓN TERCERA DE LA INTERCEPCIÓN DE DATOS		
ARTÍCULO 70		
		Se recomienda incluir una definición para el término "Tecnologías para intervención de comunicaciones", que permita limitar su posible uso. Se recomienda adicionar cuales son las facultades legales que se mencionan, así como adicionar especificaciones como uso y posesión de este tipo de tecnología.
SECCIÓN QUINTA. DEL ABUSO DE DISPOSITIVOS TECNOLÓGICOS		
Se sugiere alinear esta sección con lo establecido en el Artículo 6, relacionado con el uso indebido de dispositivos de la Convención de Budapest.		
ARTÍCULO 73		
	El Artículo refiere Artículos que no tienen que ver con delitos. Se sugiere revisar. Se sugiere revisar si lo planteado es en sí una tipología aislada o una agravante de los delitos anteriores.	Se sugiere especificar el origen de la autorización para pruebas y los mecanismos para obtenerla.
SECCIÓN SEXTA. DEL FRAUDE POR MEDIO INFORMÁTICO		
ARTÍCULO 74		
	Se recomienda revisar lo establecido para evitar duplicidad con el delito de fraude tipificado en el Código Penal Federal, sólo que para su comisión se utilizan las TIC.	Se sugiere agregar a la agravante establecida en el segundo párrafo, no sólo cuando se suplante la identidad de una Entidad de Gobierno, sino además cuando se suplante la identidad de una Entidad Privada que administre Infraestructuras Críticas de Información. En este caso se propondría una reforma al Código Penal como agravante o agregarlos en la lista de tipos específico de fraude que están el Artículo 387 del mismo código. Se sugiere incluir la obtención de cualquier beneficio por terceros particulares o afectar a terceras partes.
SECCIÓN SÉPTIMA. DE LOS DELITOS CONTRA LA INTEGRIDAD Y LIBERTAD DE LAS PERSONAS		
ARTÍCULO 78		
	Se sugiere considerar que las palabras "odio nacional", "hostilidad" o "instigación" no están definidas en la legislación mexicana; lo que podría generar incertidumbre para las personas o empresas que utilizan tecnologías digitales, y podría	Se recomienda adicionar como conducta punible al autor del material digital con el propósito de ser exhibido mediante sistemas informáticos, toda vez que solo se contempla al que describa, diseñe o grabe.

	requerir moderación de contenidos y dar paso a actos arbitrarios por parte de las autoridades. Se recomienda evitar su uso. Se recomienda especificar que la definición del delito va dirigido a las personas que describen, diseñan o graban dichos materiales, y no a la plataforma en la que circula el contenido. Se recomienda que lo establecido respete el derecho a la información y a la libre expresión Se recomienda evitar el uso de términos como "desinformar" y "manipular". Así mismo, se sugiere analizar que lo establecido no contravenga los derechos de libertad de expresión y el derecho al libre acceso a la información y a buscar, recibir y difundir información e ideas, contenidos en el artículo 6o constitucional.	
ARTÍCULO 80		
	En el Artículo se establece que para la "connotación sexual" se requiere del acreditamiento de una finalidad de gratificación o placer sexual, sin embargo, se sugiere considerar que el delito puede realizarse sin dicha finalidad.	Se sugiere omitir el último párrafo del Artículo en comento.
CAPÍTULO II DE LAS TÉCNICAS ESPECIALES DE INVESTIGACIÓN		
ARTÍCULO 90		
		Se sugiere establecer que toda actuación del ministerio público que, durante la investigación de los delitos previstos en la Ley Federal de Ciberseguridad, pudiera ocasionar una afectación (actos de molestia y/o privación) en los derechos de la persona investigada, requerirán en todo momento de previa autorización del juez de control. Se sugiere delimitar el alcance de los agentes encubiertos pues no pueden estar exentos de responsabilidad alguna por aquellos delitos que llegarás incurrir, respondiendo por los daños ocasionados, al igual que aquellos que por su naturaleza obtuviera beneficios extraordinarios.
TRANSITORIOS		

Se sugiera la adición de transitorios que consideren lo siguiente: La Agencia Nacional de Ciberseguridad es un órgano de la Administración Pública Federal, con funciones operativas, asignación presupuestaria y de decisión, encargado de promover y difundir el ejercicio de la estrategia de ciberseguridad. El Presupuesto de Egresos de la Federación para cada Ejercicio Fiscal anual considerará partidas suficientes para el adecuado funcionamiento de la Agencia Nacional de Ciberseguridad en las materias de esta Ley.

ift INSTITUTO FEDERAL DE TELECOMUNICACIONES