**La Iniciativa de Ley Federal de Ciberseguridad pone en riesgo derechos humanos e incumple obligaciones internacionales en la materia**

Los organismos empresariales que suscribimos el presente documento, estamos comprometidos con la construcción de marcos legales que garanticen el Estado de Derecho, la certidumbre jurídica y la protección de los derechos humanos. Impulsamos el desarrollo del entorno global, brindando servicios de alta calidad para la ciudadanía y a todos los sectores productivos de México, incluyendo gobierno y academia; promoviendo la seguridad digital, la innovación, el respeto irrestricto a los derechos humanos como la privacidad, la protección de datos personales, la promoción de la libertad de expresión, así como la libre asociación, por mencionar algunos.

- Manifestamos nuestro compromiso por cuidar la seguridad de todas y todos, por lo que hacemos un llamado a no poner en riesgo los derechos humanos fundamentales.
- La Iniciativa de Ley Federal de Ciberseguridad pone en riesgo derechos como la libertad de expresión, la privacidad, el incumplimiento por parte del Estado a la protección de datos personales reconocidos internacional y nacionalmente los cuales son fundamentales en cualquier entorno digital.
- Como sectores esenciales afectados por esta propuesta de regulación, abogamos por respetar los compromisos internacionales en materia de derechos humanos de los que México es parte, así como garantizar los ya mencionados.
- El respeto a las obligaciones asumidas en los tratados internacionales son la base para el impulso y la promoción de inversiones económicas.

La discusión de una ley federal de ciberseguridad debe realizarse de manera colaborativa entre el sector público, academia, sociedad civil e iniciativa privada cuando nos une el objetivo de un México Hiper-Conectado, reduciendo la brecha digital en todo el país, incrementando la competitividad y productividad; mejorando la calidad de vida y las condiciones de bienestar de los mexicanos sin ser ajenos a las obligaciones asumidas en los tratados internacionales, como base para el impulso y promoción de inversión económica La Ley que actualmente se discute en el Congreso, pone en riesgo la libertad de expresión, la privacidad y el incumplimiento por parte del Estado a la protección de datos personales reconocidos internacional y nacionalmente, los cuales son fundamentales en cualquier entorno digital. Es por lo que, identificamos las principales preocupaciones que tenemos empresas y asociaciones en torno a la Iniciativa de Ley Federal de Ciberseguridad.

## La exposición de México a los ciberataques va en aumento

- El país se mantiene en el primer lugar de intentos en ciberataques en Latinoamérica, con 187,000 millones de intentos en 2022, un crecimiento del 20% según datos de Fortinet[1].
- De acuerdo con el Índice de Ciberseguridad Global (Global Cybersecurity Index) México se encuentra en el lugar 52 y en la región ha caído hasta la posición 4, después de Estados Unidos, Canadá y Brasil.
- El Banco Mundial establece que, México se encuentra en el puesto 15 de las mejores economías en el mundo en relación con la generación del PIB, para el INEGI, las PyMEs generan el 52% del PIB y 72% del empleo en el país, sin embargo, las PyMEs que sufren un ciberataque pueden llegar a pagar hasta dos millones de pesos por un rescate, aumentado los factores por los cuales las PyMEs pueden desaparecer y afectar la economía del país[2].

## Reconocemos que la Iniciativa de Ley Federal de Ciberseguridad tiene aspectos positivos y recupera diversos planteamientos del sector privado

- Celebramos que la Iniciativa considere la creación de una política, una estrategia y una Agencia nacionales de Ciberseguridad, con la participación de un Consejo Consultivo Ciudadano. Se fomenta así una cultura de ciberseguridad entre la población, contribuyendo a la seguridad de los usuarios digitales, sin embargo, es importante enfatizar la importancia de la prevención como herramienta de mitigación frente a los posibles riesgos asociados al uso de la tecnología en la que la voz de los expertos de la industria pueda formar parte.

[1] https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-registro-137-mil-millones-de-intentos-de-ciberataques-e
[2] Worldbank.ong

- Se resalta en la exposición de motivos el establecer bases de colaboración entre el gobierno y la iniciativa privada a través de las diferentes cámaras industriales, empresas y la población, aspecto fundamental para combatir los delitos cibernéticos.
- Si bien la Agencia Nacional tendría un rol relevante en la ejecución de acciones relacionadas con la ciberseguridad, el Transitorio Tercero establece de facto que la Coordinación de Estrategia Digital Nacional adscrita a la Oficina de la Presidencia, tendría igualmente facultades otorgadas de manera discrecional al Titular del Ejecutivo (de manera temporal hasta por 36 meses posteriores a la entrada en vigor del decreto).
- Reconocer el derecho a la intimidad, en sus diversas manifestaciones, ha ampliado su ámbito de protección, donde además de rechazar invasiones en el ámbito privado, ahora supone el uso y control sobre los datos concernientes a cada individuo; por lo cual debe serle reconocido como un derecho fundamental protegido y garantizado.

## Mejorar el fundamento legal de la Iniciativa

- Es necesario definir el fundamento constitucional conforme al cual el Congreso de la Unión pueda legislar en materia de ciberseguridad, lo cual idealmente debe realizarse a través de la reforma constitucional que le confiera la facultad exclusiva para legislar en la materia; o, si el Congreso decide que existan facultades concurrentes, se señale que tendrá facultad para expedir la Ley General correspondiente.
- La redacción es confusa para delimitar atribuciones relacionadas con asuntos vinculados a la seguridad pública y a la seguridad nacional. Es necesario distinguir la ciberseguridad a nivel civil y proteger la seguridad pública de las fuerzas del orden y las actividades relacionadas con la ciberdefensa, las cuales, deben ser debidamente acotadas conforme a las facultades de los diferentes cuerpos de seguridad involucrados en la atención de estos casos, considerando sus áreas de responsabilidad.

## Definir claramente los aspectos relacionados con la ciberseguridad, garantizar los derechos humanos y los derechos digitales

Las restricciones a los derechos humanos, en particular los de privacidad, libertad de expresión y protección de datos personales, deben ser sometidas a un escrutinio estricto y pasar por la prueba de proporcionalidad. Presentamos los señalamientos específicos siguientes al texto de la Iniciativa:

**Limitaciones a la libertad de expresión**

- El artículo 78 castiga con una pena de tres a seis años de prisión y una multa de quinientas a mil unidades de medida y actualización “al que describa, diseñe o grabe cualquier tipo de material digital, auditivo, fotográfico o video gráfico con el propósito de que sea exhibido, publicado o compartido a través de redes de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean producto de la evolución tecnológica mediante los cuales se incite, facilite, induzca u obligue a personas a ocasionar un daño físico, psicológico o material, a sí mismas o a terceros”.
- Si bien el propio artículo señala que no se sancionarán expresiones que se realicen en apego a la libertad de expresión, la amplitud de conductas que pueden estar incluidas en la definición ocasionarán graves problemas en su aplicación práctica. En este mismo tenor, el artículo tiene concepciones que pueden resultar subjetivas al momento de su valoración.
- Cualquier iniciativa y/o lineamientos en materia de ciberseguridad, deben contener y detallar sólidas salvaguardas procesales y de derechos humanos, además de cumplir estándares y prácticas internacionales como son legalidad, necesidad y proporcionalidad.
- El derecho a la privacidad y la seguridad de la información en el entorno digital debe ser garantizado por todos los agentes de la cadena de valor en la prestación de los servicios; estableciendo y delimitando claramente las responsabilidades de cada agente que participa. El artículo 13 en su fracción V no establece una limitante que garantice que la colaboración con autoridades extranjeras preserve la privacidad de los ciudadanos mexicanos.
- Las intromisiones a los derechos humanos en los términos planteados por la Iniciativa no son aceptables. En particular, las restricciones a los derechos de privacidad y protección de datos personales al ordenar la entrega de información personal a un catálogo indefinido de autoridades competentes, mismas que no resultan necesarias ni son proporcionales puesto que ya existen disposiciones legales para atender requerimientos de autoridades con fines de investigación y persecución de delitos. Toda restricción a los derechos humanos debe ser mínima y limitada, máxime cuando en la práctica ya existen figuras jurídicas similares para cumplir propósitos similares (artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión; y artículos 301 y 303 del Código Nacional de Procedimientos Penales).

- Reconocemos el interés de contar con un control sobre los eventos que se consideren como un delito cibernético, analizando información y asegurando procesos a través de controles y su implementación; sin embargo, una eficaz estrategia de ciberseguridad a través de la integración de un Registro Nacional de Incidentes, como se propone, requiere de esfuerzos que deberían enfocarse únicamente cuando se comprometa infraestructura con información esencial o estratégica para la provisión de bienes o la prestación de servicios públicos básicos; y, por ende, pudiera afectarse o ponerse en riesgo la Seguridad Pública o la Seguridad Nacional.
- En suma, obtener información de una forma desproporcionada y excesiva bajo el argumento de un incidente cibernético, término que resulta sumamente genérico al no definir qué se entiende o qué parámetros se emplearán para así determinarlo, resulta violatorio de los derechos de las personas a la libertad y a la privacidad. Por lo anterior, un Registro como el propuesto llevará a un control excesivo del Estado en detrimento de estos derechos fundamentales.

**Invasión a la privacidad y protección de datos personales a través de un "monitoreo" de las Secretarías de la Defensa Nacional y de la Marina**

- Consideramos que existen elementos que conllevan al riesgo de que las fuerzas armadas profundicen las tareas de vigilancia, espionaje e intervención de comunicaciones privadas de la población, sin autorización expresa del titular y sin controles judiciales pertinentes.
- El artículo 28 de la Iniciativa considera que ambas dependencias "en el ámbito de sus competencias y a través de las unidades administrativas que determinen sus titulares" podrán "monitorear el ciberespacio para prevenir, identificar y neutralizar las ciberamenazas y ciberataques".
- Asimismo, se faculta a la "Agencia Nacional de Ciberseguridad" para solicitar a los particulares la entrega de cualquier información que le sea requerida, sin definir con claridad los procedimientos, requisitos y salvaguardas (Artículo 13, fracción XII).
- La tutela de los derechos de privacidad y protección de datos personales es fundamental para la garantía efectiva de los derechos humanos en México. Que la Iniciativa de Ley habilite a diversas autoridades y en concreto a la Agencia Nacional de Ciberseguridad, representa por sí misma una injerencia indebida e injustificada en los derechos humanos de privacidad y protección de datos personales.
- La entrega de información a autoridades en los términos de la Iniciativa es contraria a lo previsto en la Constitución y la normatividad de protección de datos personales, ya que aquélla no plantea los estándares de seguridad de la información que los sujetos obligados (autoridades) habrán de observar a fin de garantizar la integridad, disponibilidad y confidencialidad; situación que puede conducir a violaciones irreparables en los derechos de privacidad y protección de datos personales.
  En caso de sufrir un incidente de ciberseguridad las organizaciones estarían obligadas a entregar la información al Registro Nacional de Incidente, sin embargo, el acceso a la información debería ser limitado a autoridades con plenas competencias, y no otorgar un acceso generalizado.

**Derechos digitales**

- La Iniciativa establece un catálogo amplio y genérico de derechos digitales (incluso derechos no previstos en la normatividad de protección de datos aplicable y sin definición estandarizada) que las organizaciones deberán tramitar y considerar, una Iniciativa de esta naturaleza no es el medio idóneo para establecer dicho catálogo, máxime cuando diversas organizaciones nacionales e internacionales trabajan en la definición de derechos digitales con amplia participación de la industria y de la sociedad en general. Ejemplos son la Carta de Derechos de la Persona Digital, de la Comisión de Datos Personales del Sistema Nacional de Transparencia; y la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales. No es recomendable establecer nuevos derechos de forma genérica y amplia, mejor dicho, deben referirse a derechos existentes que ya se encuentran regulados en las leyes vigentes. De otra forma, resulta imposible cumplir con la observancia de derechos de este tipo en que no se aporta la definición.

- La Iniciativa debiera alinearse a la gestión de riesgos que contempla el "NIST Framework"[3] identificando las siguientes funciones: i) identificar, ii) proteger, iii) detectar, iv) responder y v) recuperar con el objetivo de determinar aquellos riesgos de mayor impacto. Sin embargo, en la Iniciativa no son atendidos los puntos relativos a la detección, contención, mitigación y reacción conjunta de la sociedad para lograr ciberseguridad ante ciberataques.
- El lenguaje de la Iniciativa se centra, en la exposición de motivos, en el daño o en la protección del daño a los sistemas informáticos, cuando la principal protección debería enfocarse en las personas físicas y morales; ya sea que se causen daños económicos, o de carácter estético, psicológico, reputacional, ambiental, colectivo, emergente, de seguridad nacional, entre otros; según reconozcan las distintas jurisdicciones de cada país que, a través del uso de las tecnologías, se le puedan ocasionar por parte de terceros y de manera intencional para afectarles o cometer delitos en su contra.

## Considerar las obligaciones asumidas en el T-MEC y ser coherente con los compromisos internacionales

El acuerdo comercial entre México, Estados Unidos y Canadá (T-MEC) entró en vigor en junio 2020. El documento compromete a nuestro país (entre otras cosas) a construir capacidades de respuesta ante incidentes cibernéticos, fortalecer la colaboración, proteger a la ciudadanía, y garantizar la privacidad de datos en el corto plazo. Cualquier legislación en la materia debe estar homologada a los compromisos adquiridos para adoptar mejores prácticas, pues la ciberseguridad afecta de forma transversal a todos los usuarios desde individuos hasta países y organizaciones.

**Información crítica**

- En la Iniciativa, un incidente cibernético se refiere a uno o varios eventos no deseados o inesperados que tienen una "probabilidad significativa de comprometer o comprometan las operaciones organizacionales y amenazar la seguridad de la información." Es una definición sumamente genérica ya que no establece qué se entiende o qué parámetros se emplearán para determinar la "probabilidad significativa de comprometer las operaciones organizacionales y amenazar la seguridad de la información."
- Se requiere aclarar el ámbito y alcance del concepto, así como establecer los estándares mínimos de ciberseguridad, pues es necesario cumplir con los compromisos internacionales ya señalados como el T-MEC, entre otros.

**Enfoque basado en riesgos**

- Dada la naturaleza cambiante y constante de las amenazas, cualquier ley y estrategia de ciberseguridad debe utilizar el enfoque basado en prevención y detección de riesgos como lo prevé el T-MEC en su artículo 19.15. Ciberseguridad. Por ello, se recomienda que la Iniciativa utilice un modelo legislativo alternativo a la regulación prescriptiva, que enfatiza conductas prohibidas y sanciones. Con el enfoque de riesgos se establecen disposiciones que esencialmente replican mecanismos de gestión conforme a estándares internacionales.
- En la formulación de la estrategia nacional de ciberseguridad en el Artículo 14, fracción V de la Iniciativa, se privilegia que las empresas usen los enfoques basados en riesgos para tratar las amenazas. Del mismo modo, se recomienda que, en el Título Sexto, de la Cultura y Educación, específicamente en la fracción II, del Artículo 60, los Poderes de la Unión desarrollen y difundan una cultura de ciberseguridad con el objetivo de promover el uso de enfoques basados en riesgos y se desincentive la regulación prescriptiva para tratar las amenazas.
- En relación a la obligación para los proveedores de servicios de infraestructura digital, plataformas de redes sociales, comunidades de videojuegos en línea, streaming, plataformas de entretenimiento en línea, y telecomunicaciones que operen en territorio nacional (artículo 53 del Título Quinto, de la Prestación de servicios, de la Iniciativa); que establece privilegiar que la información de los usuarios se encuentre almacenada en territorio nacional, se contravienen obligaciones comerciales internacionales de México en los tratados internacionales; en específico, el artículo 19.12 del T-MEC de la Ubicación de las instalaciones informáticas, que dice: "ninguna Parte podrá exigir a una persona cubierta usar o ubicar las instalaciones informáticas en el territorio de esa Parte, como condición para la realización de negocios en ese territorio.".

[3] El Instituto Nacional de Normas y Tecnología (NIST), agencia perteneciente al Departamento de Comercio de los Estados Unidos, desarrolló este marco voluntario de manera coherente con su misión de promover la innovación y la competitividad en el país. El Cybersecurity Framework de NIST utiliza un lenguaje común para guiar a las compañías de todos los tamaños a gestionar y reducir los riesgos de ciberseguridad y proteger su información. https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

**Baja de contenidos**

- Desde nuestros sectores, estamos comprometidos a garantizar el derecho irrestricto a la libertad de expresión de las personas; prohibiciones que afecten este derecho únicamente deben ejecutarse cuando el Estado lo determine en casos excepcionales, como la incitación al terrorismo, actos de apología al odio, instigación al genocidio, trata de personas o pornografía infantil. El dar de baja direcciones IP, aplicaciones, dominios y sitios de internet, solo procede cuando hay una sólida justificación de las autoridades, respetando lo establecido en la Declaración Universal de los Derechos Humanos, así como la Convención Americana Sobre Derechos Humanos. De otra forma, se vulneran distintos preceptos que se encuentran contemplados en los artículos 8 (Garantías Judiciales), 13 (Libertad de Pensamiento y de Expresión), y 25 (Protección Judicial); la Iniciativa establece facultades de "monitoreo" y de realización de "operaciones militares en el ciberespacio" a las fuerzas armadas (artículo 18, 21, 26, 40 de la presente Ley). Sugerimos respetar y adoptar el principio de inviolabilidad de las comunicaciones contemplado en los artículos 16 de la CPEUM, el artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, la Ley de Seguridad Nacional, el Código Nacional de Procedimientos Penales, y la Ley de la Guardia Nacional en donde se exige siempre que las solicitudes de información de los usuarios estén acompañadas o sustentadas por una Orden Judicial.
- A fin de promover la transparencia, toda orden de restricción de servicio del gobierno debería ser emitida solo por escrito a los operadores, citar los fundamentos legales y establecer un claro mecanismo de auditoría que indique quién es la persona que autoriza dicha orden. También se debería informar a los ciudadanos que es el gobierno quien ordena la restricción del servicio y que fue aprobada por una autoridad judicial o cualquier otra que tenga competencia, de conformidad con los procedimientos administrativos establecidos por ley[4].
- Es fundamental atender a lo dispuesto en el T-MEC, específicamente el Capítulo 19 "Comercio Digital", el cual busca eliminar obstáculos injustificados al comercio realizado por medios electrónicos; otorgar certeza jurídica a los inversionistas y empresas; y garantizar un entorno en línea seguro para la ciudadanía. En el artículo 19.8: "protección de la información personal" se estipula que las partes adoptarán un marco legal que disponga la protección de la información personal de los usuarios del comercio digital; para ello, el propio organismo mexicano encargado de tutelar el cuidado y protección de los datos personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), ha reiterado que es primordial adoptar instrumentos de cooperación innovadores y fortalecer mecanismos que protejan a los usuarios y al flujo transfronterizo de datos a nivel global; lo que obliga a las plataformas de comercio electrónico a implementar mecanismos de seguridad y a la protección de datos personales.
- En 2020 se reformó la Ley Federal del Derecho de Autor para dar cumplimiento a la normativa acordada en el T-MEC. En el Capítulo V "De las medidas tecnológicas de protección, la información sobre la gestión de derechos y los proveedores de servicios de internet", particularmente el artículo 114 Octies, se considera un mecanismo similar sobre la baja de contenidos digitales, refiriendo que los proveedores de servicios de Internet no serán responsables por los daños y perjuicios ocasionados a los titulares de derechos de autor, derechos conexos y demás titulares de algún derecho de propiedad intelectual.

**Censura**

- La Iniciativa contempla la obligación para los proveedores de servicios de "**dar de baja direcciones IP**, aplicaciones, dominios y sitios de internet dentro de las 72 horas posteriores a la notificación que le realicen la Agencia, la Fiscalía General de la República, CERT-MX y autoridades judiciales competentes para su inhabilitación" (Artículo 53, fracción XIII).
- No se establecen contrapesos, y al otorgarles ser juez y parte se corre el riesgo de que se efectúen decisiones de manera discrecional.
- Lo anterior atenta contra la Constitución, tratados internacionales suscritos por México, y criterios de la Suprema Corte en el sentido de que toda restricción, sanción o limitación a la libertad de expresión debe ser interpretada en forma restrictiva y el Estado, a través del Poder Judicial, es el único legitimado para limitarla en los casos excepcionales que establece el derecho internacional, arriba descritos.

[4] Seguridad y privacidad a lo largo del ecosistema móvil, GSMA en https://www.gsma.com/latinamerica/wp-content/uploads/2023/01/CyberSecurityReport_Spanish_Web_Singles-2.pdf

**La ciberseguridad trasciende fronteras, por ello es urgente que México ratifique el Convenio de Budapest.**

- Se recomienda que México se integre al Convenio de Budapest, siendo un acuerdo internacional con el objetivo de proteger a la sociedad frente a los delitos informáticos y en Internet mediante la elaboración de leyes adecuadas; la mejora de las técnicas de investigación; y el aumento de la cooperación y la transparencia internacional. Este Convenio permite que los requerimientos formulados por los operadores jurídicos a nivel nacional sean remitidos de manera célere a los Estados Parte del Convenio, entre los cuales figuran: Estados Unidos de América, Italia, España, Japón, Canadá, Israel, Argentina, Chile, Costa Rica, Paraguay, República Dominicana, Panamá y Colombia, entre otros.
- El Convenio representa un referente en los esfuerzos para fortalecer al Estado de derecho en el ciberespacio. No obstante, en caso de que el Senado de la República ratifique la adhesión del Estado Mexicano al Convenio de Budapest, y la Iniciativa ya hubiere sido aprobada por el Congreso, esta última deberá ser modificada para armonizar su contenido con las disposiciones en el Convenio. Es recomendable ratificarlo primero, y luego homologar cualquier legislación en la materia.

**Ciberdelitos**

- México no ha sido omiso a las preocupaciones sobre ciberdelitos, y cuenta con regulaciones definidas en el Código Penal Federal que dentro del Título Noveno "Revelación de secretos y acceso ilícito a sistemas y equipos de informática", tipifica delitos como la modificación, destrucción o pérdida intencional de información contenida en sistemas informáticos; la revelación, divulgación o utilización indebida o en perjuicio de otro, de información o imágenes obtenidas en una intervención de comunicación privada. Toda normativa posterior debiera basarse en estos conceptos, homologarlos o, en su caso, actualizarlos.
- En general, el Título Octavo de la Iniciativa relativo a los delitos cibernéticos carece de claridad en aspectos fundamentales relacionados con la ciberseguridad y disposiciones penales, violando el principio de legalidad que exige que dichas disposiciones sean accesibles al público, claras y precisas en su alcance; de modo que las personas puedan determinar razonablemente qué conductas están prohibidas y ajustar su comportamiento. Las definiciones poco precisas dejan lugar a interpretaciones arbitrarias y corren el riesgo de infringir los derechos humanos.
- Los cibercrímenes pueden afectar de manera directa la confidencialidad, integridad y disponibilidad de la información, propiedad intelectual, sistemas informáticos, redes de telecomunicaciones, entre otros, por lo cual no solo corresponde al Estado la capacidad de ciberdefensa, pues involucra a toda la comunidad del ecosistema digital. Deben por tanto mantenerse los mecanismos de colaboración con el sector privado, y establecer de manera clara que los proveedores de servicio de internet solo aportan conectividad y no son responsables de su uso para fines delictivos.
- Cualesquiera tipos penales que se creen, no deben duplicar los que ya están tipificados en otros cuerpos legales como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares que señala diversas infracciones relacionadas con la inobservancia de los deberes de confidencialidad y seguridad, así como delitos particulares relacionados con el indebido tratamiento de datos personales.
- La Iniciativa debe abstenerse de incluir mecanismos punitivos que resulten en una doble vía de sanción de acuerdo con la normatividad vigente, en la que ya se considera que los incidentes de seguridad de datos personales pueden dar lugar a la imposición de sanciones a los sujetos de derecho público y privado.
- Se debe establecer un plazo de prescripción para la persecución de delitos que se describen en la Iniciativa.
- Las sanciones previstas en la Iniciativa son desproporcionadas; y una organización que adoptó medidas para una debida diligencia y cuidado en la protección de la información bajo su poder, no debería ser sujeta a sanción ya que en la práctica se entiende que ha establecido los medios y mecanismos necesarios para cumplir con el deber de seguridad.

**Enriquecer el proyecto reconociendo principios, buenas prácticas y recomendaciones de organismos y asociaciones con aval internacional.**

- Bajo esa premisa, vemos positivamente las propuestas, por ejemplo, de la Guardia Nacional puesto que contempla recomendaciones/lineamientos de adopción voluntaria por parte de la industria, las micro, pequeñas y medianas empresas y los principales agentes que participan del ecosistema móvil y digital para propiciar la seguridad desde el diseño e incentivar la innovación tecnológica.

- Es importante tener en cuenta en la Iniciativa y en la eventual Ley la legislación en socios comerciales como los EE. UU.[5], y Europa[6], así como de otras regiones de Latinoamérica y Asia, 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.
- Otro ejemplo es la Organización para la Cooperación y el Desarrollo Económicos (OCDE), para definiciones de conceptos.

**Coordinación entre el gobierno, el sector privado, academia y la sociedad civil.**

- Se recomienda incluir la opinión de sociedad civil, academia y sector privado para definir: (1) la adopción de estándares internacionales de ciberseguridad; (2) el reconocimiento mutuo/ equivalencia de certificaciones; y, (3) la promoción de la educación y la industria de la ciberseguridad en atención a referencias internacionales como ISO[7], UIT[8], ETSI[9], NIST[10], ENISA[11], 3GPP[12], GSMA[13], entre otros.
- Intercambio de información: se deben definir esquemas y lineamientos, así como establecer Centros de Respuestas a Incidentes para promover (1) una mayor transparencia en torno a los ataques de ciberseguridad; y, (2) la utilidad de los datos relativos al estado actual de los ataques.
- La redacción de la Iniciativa se enfoca principalmente a los órganos de Gobierno, por lo que es necesario que la Ley no sólo se refiera a la actuación de las autoridades sino incluir la actuación y participación que la iniciativa privada y la sociedad tienen para fortalecer la ciberseguridad.

**De la investigación, desarrollo e innovación.**

- Se recomienda incrementar el financiamiento e incentivos a la investigación, desarrollo, innovación para los investigadores en gobierno, industria y academia, así como promover el talento altamente especializado, capacitado y certificado en materia de ciberseguridad; e impulsar la inclusión de ramas o materias de ciberseguridad desde la educación básica hasta la superior.

**"Pentesting" o ataque malicioso simulado contra los sistemas informáticos que se usa para encontrar y verificar posibles vulnerabilidades**

- La Iniciativa omite el tratamiento que se va a dar a las empresas o personas que realizan "pentesting" y análisis de vulnerabilidades, mismos que ayudan a las empresas a mejorar sus defensas ante ataques, y a prevenirlos. Se puede afectar a dichas empresas al caer en un vacío legal, cuando sus actividades sientan las bases para fomentar el desarrollo e innovación en la investigación para prevenir ciberataques.
- Reconocer este tipo de "hacking" permisivo, legal y ético cuenta con el consentimiento pleno de los dueños de los equipos en los que se va a trabajar la prueba. Además, permite identificar los problemas, se obtiene conocimiento suficiente para determinar cuáles son las defensas del sistema, las posibilidades de éxito de un ciberataque y la capacidad de respuesta por parte de la organización.

**De la cultura y Educación**

- Considerando que México busca la transformación digital en ámbitos públicos y privados al igual que en instituciones de educación, la Iniciativa debería considerar el uso responsable de internet en materia de seguridad de la información como parte de los programas de educación básica, media y superior en apego a la norma NMX-I-319-NYCE-2018 "Escuelas Responsables en el Uso de Internet" que ayude a robustecer la formación de sus ciudadanos y ayude como medida de prevención de riesgos de delitos informáticos.

[5] https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist
[6] https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-policies
[7] https://www.ccn-cert.cni.es/gl/gestion-de-incidentes/lucia/23-noticias/297-publicada-isoiec-27013.html#:~:text=M%C3%A1s%20concretamente%2C%20ISO%2FIEC%2027032,personas%20en%20todo%20el%20mundo.
[8] https://www.itu.int/itu-d/sites/cybersecurity/es/
[9] https://www.telesemana.com/blog/2021/11/25/el-etsi-aprueba-nuevas-normas-para-elevar-la-seguridad-de-los-dispositivos/
[10] https://www.nist.gov/cyberframework
[11] https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-policies
[12] https://www.bnamericas.com/es/noticias/informe-de-5g-americas-delinea-evolucion-de-lte-y-5g
[13] https://www.gsma.com/latinamerica/es/resources/seguridad-y-privacidad-a-lo-largo-del-ecosistema-movil/

## De las técnicas específicas de investigación.

**Alcances de la figura de "agentes encubiertos"**

- El artículo 90 de la Iniciativa señala que el Ministerio Público, atendiendo a la urgencia del caso, puede solicitar al juez de control la actuación de agentes encubiertos a efecto de realizar las investigaciones. El agente podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener imágenes y grabaciones de referidas comunicaciones.
- Al habilitar a los Agentes Encubiertos para operar de forma libre, está en sus manos evitar violaciones a derechos fundamentales; en caso extremo, al no haber supervisión adecuada pudiera alguno de ellos convertirse en el principal punto de distribución de, por ejemplo, material pornográfico infantil; o al intervenir comunicaciones privadas, facilitar acciones del cibercrimen organizado en distintas modalidades. Urge por tanto la reglamentación precisa y supervisión a las funciones de estos agentes, dentro de las estrategias y políticas públicas en materia de ciberseguridad.

## Cargas Regulatorias gravosas y de imposible cumplimiento.

- La Iniciativa no distingue entre los diversos tipos de proveedores de servicios de telecomunicaciones, cuya oferta e infraestructura puede variar considerablemente; algunos proveen servicios de conectividad (algunos accesos a Internet), más no contenido; otros, como las plataformas sociales o los prestadores de servicios de streaming, dotan de contenido a sus usuarios. En este sentido, las obligaciones impuestas no solo resultan en su conjunto una carga excesiva para los operadores, quienes ya son regulados en la Ley Federal de Telecomunicaciones y Radiodifusión, sino que muchas de las nuevas obligaciones son de imposible cumplimiento o de la competencia de la propia autoridad.
- Por ejemplo, la obligación de atender y dar respuesta a los incidentes de ciberseguridad, la cual debiera ser una responsabilidad de la autoridad y no de los operadores, quienes no cuentan con la facultad, capacidad e infraestructura para realizar dicha labor.
- Las obligaciones referentes al manejo, uso, disponibilidad, confidencialidad, entre otros, de la "información de los usuarios" no pueden ser aplicables a los prestadores de servicios de telecomunicaciones, en tanto que los mismos no tienen acceso a dicha información; es, en su caso, obligación de los proveedores con acceso a dicha información comunicar a los usuarios lo que corresponda, e implementar las medidas requeridas en términos de la Iniciativa que sean razonables.
- Los protocolos de preservación de evidencia digital establecidos en el artículo 13 de la propuesta, así como la normativa en cuanto a evidencia digital, pueden abrir la puerta a una sobrerregulación y costos adicionales de almacenamiento de información por parte de las empresas, ya que no se define quiénes serían los responsables.
- Es prudente señalar que, a partir de la definición de incidente cibernético, las obligaciones, infracciones y sanciones previstas en la Iniciativa se establece una doble vía de sanción para las organizaciones del sector privado pues, en la práctica, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ya puede sancionar a las organizaciones del sector privado con motivo de una vulneración de seguridad de datos personales; la Iniciativa pretende que una organización sea sancionada también al actualizar la definición de incidente cibernético prevista en la ley, dando lugar a la violación del principio *non bis in ídem*.
- No es idóneo ni adecuado que esta ley regule medidas de resarcimiento en los términos planteados ya que esto solo supondrá una carga sumamente onerosa para las organizaciones, sin que pueda demostrarse un efectivo cumplimiento de las resoluciones. Debe privilegiarse el uso de vías legales idóneas como la vía civil para reclamar daños y perjuicios o bien, los medios previstos en la normatividad de datos personales.

## Sostener reuniones de trabajo con las comisiones dictaminadoras.

- Actualmente la Iniciativa está en estudio de las comisiones de Seguridad Ciudadana, así como Ciencia, Tecnología e Innovación, y para opinión de las de Defensa Nacional y de Presupuesto y Cuenta Pública de la Cámara de Diputados del Congreso de la Unión. Es por ello por lo que se solicita respetuosamente a los presidentes de dichas comisiones se lleven a cabo reuniones de trabajo con las cámaras, asociaciones y organismos firmantes donde puedan expresarse las preocupaciones y propuestas de todos los sectores.