INICIATIVA QUE EXPIDE LA LEY NACIONAL DE SEGURIDAD EN EL CIBERESPACIO, A CARGO DEL DIPUTADO JAVIER SALINAS NARVÁEZ, DEL GRUPO PARLAMENTARIO DE MORENA

El suscrito, diputado Javier Salinas Narváez, integrante del Grupo Parlamentario de Morena en la LXIV Legislatura del Congreso de la Unión, con fundamento en lo dispuesto en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos y 6, numeral 1, fracción I; 77 y 78 del Reglamento de la Cámara de Diputados, somete a consideración del pleno de la honorable Cámara de Diputados iniciativa con proyecto de decreto que expide la Ley Nacional de Seguridad en el Ciberespacio, con base en la siguiente

Exposición de Motivos

El empleo y desarrollo de las tecnologías de la información y la comunicación (TIC), indiscutiblemente ha generado un aumento de la productividad para los seres humanos; a los gobiernos y empresas les ha permitido desarrollar una comunicación instantánea con los ciudadanos a través de "internet", quienes a su vez fácilmente acceden a esta red para obtener información, comunicarse y comunicar a gran distancia, de forma que a la par del mundo físico se ha venido consolidando el "Ciberespacio",[1] el cual se ha convertido en un factor clave para el desarrollo de los países, pues a través de éste se canaliza prácticamente toda la información que se genera y transmite en todos los sectores de la sociedad.

Sin embargo, todas estas ventajas y beneficios del empleo de las TIC, conlleva riesgos derivados de la propia naturaleza insegura de este entorno virtual de información, dado que es ideal para el anonimato y de fácil acceso por las amenazas tradicionales y emergentes; esto ha quedado demostrado a través de un sinfín de "ciberincidentes" y "ciberataques" a nivel mundial, de los cuales no se tiene una estadística completa y son cada vez más numerosos, lo que ha afectado a la seguridad pública y a la seguridad nacional.

Los esfuerzos de los organismos internacionales por incrementar la seguridad en el Ciberespacio para hacerlo un entorno confiable, estable, abierto y accesible, han contribuido a que los países adopten políticas públicas que permitan reducir su vulnerabilidad cibernética de los estados, siendo factores clave la coordinación y cooperación a nivel interinstitucional, nacional e internacional; los esfuerzos más significativos son los siguientes:

Organización de Naciones Unidas (ONU): Desde 1998, la ONU promueve resoluciones a través del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, y a través del Grupo de Expertos Gubernamentales (GEG),[2] promoviendo el derecho internacional y particularmente la Carta de Naciones Unidas en el Ciberespacio para mantener la paz y seguridad internacional; asimismo, a través de cumbres y foros internacionales donde se aborda la seguridad en el Ciberespacio como un fenómeno multifactorial que es pieza clave para el desarrollo sostenible de los estados; actualmente México recientemente ha iniciado su participación en esta materia a través de la Secretaría de Relaciones Exteriores.

Estados miembros del Consejo de Europa: En 2001 se adoptó el "Convenio sobre la Ciberdelincuencia"[3] (más conocido como Convenio de Budapest por el lugar donde se signó), en el cual se establecen términos, medidas, principios de cooperación y disposiciones para proteger a la sociedad frente a la delincuencia en el ciberespacio, instando a todos los países a formar parte de este mecanismo de cooperación internacional mediante una armonización legislativa. En marzo de 2014 México hizo público su interés por adherirse a este convenio; sin embargo, a pesar de los trabajos efectuados en ese entonces, el Senado no ratificó dicho compromiso, por lo que actualmente, debido a la falta de legislación en materia de seguridad en el Ciberespacio, México no forma parte del convenio a pesar de ser altamente vulnerable de cibercrimen como los demás países de la región.

Organización para la Cooperación y Desarrollo Económicos (OCDE): Durante la Reunión Ministerial de Economía Digital de 2016,[4] los países participantes se comprometieron a colaborar para aprovechar el potencial de la economía digital. En cuanto a Ciberespacio, México junto con otros 40 países, suscribió 3 factores, (1) Promover la gestión del riesgo de seguridad digital y la protección de la privacidad al más alto nivel decisorio, (2) Contribuir a mantener el carácter esencialmente abierto de internet, alcanzando simultáneamente ciertos objetivos de política pública, y (3) Establecer estrategias de privacidad y protección de datos al máximo nivel de gobierno que incorporen una perspectiva de la sociedad en su conjunto.

Unión Internacional de Telecomunicaciones (UIT): Desarrolló el Índice Global de Ciberseguridad 2018,[5] encuesta que mide el compromiso de los países mediante cinco categorías, (1) medidas legales, (2) medidas técnicas, (3) medidas organizacionales, (4) Creación de capacidades y (5) medidas de cooperación. México, al igual que otros 76 países, se identifica en la etapa inicial de "maduración", en tanto que sólo 21 países son ubicados en etapa "líder"; lejos de ello, conforme al informe previo presentado el 27 de marzo de 2019, del lugar 28 en el cual se encontraba entre 2017 y 2018, pasó al lugar 63 de los 175 países evaluados al obtener un índice de 0.629, con lo cual a nivel de América Latina fue desplazado por Uruguay al quedar en cuarto lugar.

Organización de Estados Americanos (OEA): En conjunto con el Banco Interamericano de Desarrollo (BID) y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford, se publicó el documento *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?* ,[6] donde México se ubica en un escaso nivel de implementación en los componentes de política y estrategia, y tecnologías. Adicionalmente, el programa de seguridad cibernética del Comité Interamericano contra el Terrorismo (CICTE), lidera la plataforma hemisférica de cooperación internacional y asistencia técnica en ciberseguridad para los estados miembros. Además, creó el Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio, para alinear avances internacionales con necesidades e intereses regionales.

Alianza del Pacífico: En 2016 se aprobó la Agenda Digita[7] con el precepto de "potenciar la cooperación en materia de seguridad digital y fomento de la confianza en el uso de las TIC". Dicha agenda posee una hoja de ruta con cuatro ejes, (1) economía digital, (2) conectividad digital, (3) gobierno digital y (4) ecosistema digital, siendo en este último donde se abordan los compromisos de neutralidad de la red, seguridad digital, protección de datos personales y coordinación entre centros de información de red regionales.

Para hacer frente a los riesgos y amenazas en el Ciberespacio, a fin de asegurar una gestión pública gubernamental transparente y segura, así como la provisión de bienes y servicios a la sociedad y la propia seguridad de los ciudadanos en este entorno, de manera general los estados a nivel mundial han desarrollado tres capacidades:

Seguridad de la Información: Los estados han creado agencias de gobierno que colaboran con sus proveedores de internet y de TIC, generando normatividad que es aplicable al interior de las instituciones del estado y a los proveedores de bienes y servicios; se enfoca a la seguridad en las personas, los procesos y las TIC. En México no se tiene una agencia de este tipo; el esfuerzo se hace a través del Comité Especializado en Seguridad de la Información (CESI) integrado por las instancias de seguridad nacional; a través del cual se inició el desarrolló la Estrategia Nacional de Ciberseguridad 2017, el MAAGTICSI, entre otros trabajos a nivel federal, no siendo suficiente para el enorme reto que se tiene de desarrollar una política pública acorde, primero a los acuerdos, convenios y tratados internacionales; y segundo para la coordinación y la cooperación entre el sector público y privado para hacer frente al enorme reto de la gobernanza en el Ciberespacio.

Ciberseguridad: Los estados han creado centros nacionales de respuesta a incidentes en cómputo, atendiendo los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, falsificación y fraude informático, pornografía infantil a través del Ciberespacio, entre otros que afectan a la ciudadanía, al sector privado, académico, dependencias de gobierno, y en general abarcando a todo el Estado en beneficio de la

sociedad. En México se tiene el Centro Especializado en Respuesta Tecnológica-México (CERT-MX) de la actual División Científica de la Policía Federal, el cual es reconocido internacionalmente por estándares de calidad para la atención de incidentes cibernéticos; en este sentido el reto es enorme, ya que de acuerdo a estadísticas de la propia dependencia,[8] el número de incidentes cibernéticos identificados, se ha triplicado de 2013 a 2016, pasando de 20 mil incidentes a más de 60 mil; mientras que la presencia de sitios web apócrifos con fines de fraude, se incrementó 11 por ciento entre 2015 y 2016, llegando a casi cinco mil; la propagación de virus informáticos con afectaciones en México creció 57 por ciento de 2015 a 2016, llegando casi a 40 mil eventos.

Por su parte, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) señala que durante el primer trimestre de 2011 el fraude cibernético pasó de 7 por ciento a 42 por ciento en 2017; el monto reclamado en el primer trimestre de 2017 ascendió a mil 167 millones de pesos, del cual se abonó 53 por ciento del total; y 90 por ciento de los asuntos se resolvieron a favor del usuario; el canal por donde más se presenta el fraude cibernético es por comercio electrónico con 91 por ciento; asimismo, en 2017 el promedio mensual de fraudes cibernéticos en comercio electrónico fue de 193 mil casos respecto a 131 mil de 2016; por último, en cuanto a fraudes cibernéticos en banca móvil, en marzo de 2017 se presentó una cifra histórica con tres mil 682 casos. Además, de acuerdo con la "Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2018"[9] del Instituto Nacional de Estadística y Geografía (Inegi), en México hay 74.3 millones de usuarios de internet de seis años o más, que representan 65.8 por ciento de la población en ese rango de edad, observándose un crecimiento de 4.2 puntos porcentuales respecto a 2017; asimismo, de acuerdo al estudio informativo *Perspectiva de ciberseguridad en México 2018* [10] desarrollado por McKinsey&Company y el Consejo Mexicano de Asuntos Internacionales, fueron 33 millones de mexicanos víctimas del cibercrimen (uno de cada cuatro mexicanos), con un daño patrimonial calculado en 7.7 mil millones de dólares. Con esta información estadística; por un lado, se deja evidencia de la gravedad de la situación nacional para reforzar los mecanismos de prevención e investigación de delitos cometidos a través del empleo de las TIC; y por otro, permite apoyar en la toma de decisiones en materia legislativa y de política pública.

Ciberdefensa: Los estados, a través de sus Fuerzas Armadas, están realizando operaciones de seguridad en el ciberespacio para proteger sus propias redes y para defender los intereses nacionales, principalmente orientadas a proteger la infraestructura crítica de sus países, dado que los ciberataques se ubican en el número cinco en términos de probabilidad y el siete en términos de impacto; a su vez, el robo masivo de datos reveló nuevas debilidades de *hardware* y el ingenio de ciberataques más sofisticados a través del uso de la inteligencia artificial; razón por la cual se deben fortalecer las capacidades de los estados por motivos de seguridad nacional. En México, la Secretaría de la Defensa Nacional recientemente creó el Centro de Operaciones en el Ciberespacio y la Secretaría de Marina el Centro de Ciberdefensa y Ciberseguridad, integrando el Ciberespacio a las operaciones de mar, aire y tierra para coadyuvar en la protección de las instalaciones estratégicas del país, pero no es suficiente el actual marco legal para dar sustento a las acciones de defensa en la protección y aseguramiento de la provisión de bienes y servicios a la sociedad mexicana.

Es bien sabido que al adquirir tecnología en todos los sectores de la sociedad, se busca en primer lugar que sea cada vez más funcional, que resuelva fácilmente los problemas de comunicación, que tenga gran capacidad de creación y almacenamiento de datos, que los programas sean amigables con el usuario, etcétera, no considerando o dejando en segundo término la seguridad en el Ciberespacio, siendo esto aprovechado por las amenazas tradicionales y emergentes para atentar contra la intimidad de las personas, la economía, la política, la democracia y la seguridad nacional de los países; a raíz de esta dependencia tecnológica y facilidad en la transmisión de datos, los "ciberataques van en aumento exponencial, aunado a las propias fallas en las TIC o las provocadas por desconocimiento de los propios usuarios.

Ha quedado claro que la seguridad en el Ciberespacio es todo un proceso de protección de los sistemas, redes, aplicaciones, procesos y usuarios, y es por ello que debe abordarse holísticamente, para abordar los tres aspectos en que el Estado mexicano tiene la necesidad de legislar:

A. Para que las instancias del gobierno de México tengan un mismo nivel de capacidades en **seguridad de la información** que permitan mantener una gestión pública gubernamental transparente, asegurando la confidencialidad, integridad y disponibilidad de la información que se gestiona dentro de sus procesos críticos.

B. Para que las instancias de seguridad del Estado mexicano incrementen las capacidades de **Ciberseguridad** que permitan robustecer los mecanismos de prevención y coordinación para la persecución de delitos cometidos a través del Ciberespacio, a fin de proteger a los ciudadanos en materia de seguridad pública.

C. Para que las instancias de seguridad nacional protejan las infraestructuras críticas del país en el ámbito de sus atribuciones a través de la **Ciberdefensa** , a fin de asegurar la provisión de bienes y servicios a la sociedad mexicana.

Es imperante la necesidad de una misma legislación estableciendo obligaciones específicas para incrementar la seguridad en el Ciberespacio a través de los siguientes organismos:

A la **Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIGDE):** Para coordinar y vigilar que las dependencias y organismos desconcentrados del gobierno federal apliquen las normas oficiales mexicanas que éste determine, a fin de mantener un nivel óptimo de ciberseguridad y resiliencia en el ciberespacio, siendo enlace de coordinación con el sector privado y académico para garantizar la seguridad en la provisión y desarrollo de las TIC respectivamente.

A la **División Científica de la Policía Federal (Guardia Nacional):** Para perseguir e investigar delitos cometidos a través del Ciberespacio debidamente tipificados en la legislación, coordinando las acciones con la Fiscalía General de la Republica y los diferentes centros de respuesta a incidentes en cómputo en los tres niveles de gobierno; asimismo, ser enlace de coordinación con las diferentes instancias y organismos nacionales e internacionales para el cumplimiento de los acuerdos y tratados internacionales de los que el Estado mexicano es y forme parte en materia de Ciberseguridad.

A las **Instancias de Seguridad Nacional:** Para dar sustento legal en las acciones y coordinaciones que realizan para la seguridad en el Ciberespacio, a fin de proteger las infraestructuras críticas de información del Estado mexicano, asegurando la provisión de bienes y servicios a la sociedad mexicana.

Decreto

Artículo Único. Se expide la **Ley Nacional de Seguridad en el Ciberespacio**

Ley Nacional de Seguridad en el Ciberespacio

Título Primero
De la Seguridad en el Ciberespacio

Capítulo I
Disposiciones Generales

Artículo 1. La aplicación e interpretación de esta Ley se hará acorde a la Constitución Política de los Estados Unidos Mexicanos y los tratados internacionales de los que México sea parte, privilegiando el respeto irrestricto a los derechos humanos en el Ciberespacio y favoreciendo en todo tiempo la protección más amplia a las personas y el interés público.

Artículo 2. La presente Ley es de orden público e interés social, de observancia general en toda la República y reglamentaria del artículo 73, fracción XVII de la Constitución Política de los Estados Unidos Mexicanos; tiene por objeto garantizar la protección de la sociedad mexicana en el Ciberespacio y la correcta operación de las Infraestructuras de Información Esenciales (IIE) e Infraestructuras Criticas de Información (ICI) que generan, procesan y/o almacenan información de los sujetos obligados, por lo que se deberán emplear capacidades de seguridad en el Ciberespacio en el respectivo ámbito de las atribuciones y competencias para identificar, proteger, detectar, responder y recuperarse ante los riesgos y amenazas que atentan contra la seguridad en el ciberespacio y que afectan o puedan afectar a la sociedad mexicana; todo ello bajo los principios previstos en el artículo 73, fracción XXIX-M de la Constitución Federal.

Artículo 3. Son objetivos específicos de esta Ley:

I. Proteger a la sociedad mexicana en el uso del ciberespacio a través del CERT-MX, coordinando con las instancias de seguridad y justicia en los tres niveles de gobierno para la prevención e investigación de ciberdelitos.

II. Proteger la información que generan, procesan y/o almacenan los sujetos obligados para garantizar la confidencialidad, integridad y disponibilidad de la información, tanto de los datos personales de la sociedad mexicana como de la información que procesan las IIE e ICI del Estado Mexicano, mediante:

A. La publicación de Normas Oficiales Mexicanas en materia de Seguridad de la Información.

B. La implementación de estrategias, mecanismos de prevención y gestión de riesgos cibernéticos que aseguren los Activos de TIC y de Información de los sujetos obligados.

C. La coordinación de esfuerzos de las Instancias de Seguridad Nacional para asegurar la provisión de bienes y prestación de servicios públicos esenciales para la sociedad mexicana en el Ciberespacio.

Artículo 4. Son sujetos obligados al cumplimiento de lo dispuesto en esta Ley, cualquier autoridad, entidad, órgano, organismo de los Poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos, fondos públicos, así como de cualquier personas física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la federación, las entidades federativas y los municipios; así como cualquier ente privado que tenga acceso a la información reservada y confidencial a que refiere la Ley General de Protección de datos personales en posesión de Sujetos Obligados, Ley Federal contra la Delincuencia Organizada, Ley Federal de Protección de datos personales en posesión de los Particulares, Ley General de Transparencia y acceso a la Información Pública y la Ley Federal de Transparencia y acceso a la Información Pública, o se encuentren en los supuestos del artículo 29 de la presente Ley.

Artículo 5. La Federación, las entidades federativas, los municipios y las demarcaciones territoriales de la Ciudad de México y los entes privados a que se refiere esta ley, ejercen sus atribuciones y obligaciones en materia de Seguridad en el Ciberespacio, de conformidad con la distribución de competencias prevista en esta Ley y en otros ordenamientos legales.

Artículo 6. Para los efectos de esta Ley se estará a las siguientes definiciones, así como aquellas previstas en los tratados internacionales de los que México sea Parte y que se encuentren directamente relacionadas con la Seguridad en el Ciberespacio.

Se entiende por:

I. Activo de información: Toda aquella información y medio que la contiene, que, por su importancia para el sujeto obligado, debe ser protegido para mantener su confidencialidad, integridad y disponibilidad, acorde al nivel de protección que se le haya otorgado.

II. Activo de TIC: El hardware y/o software de cómputo, soluciones o servicios tecnológicos, sistemas o aplicativos, sus componentes y bases de datos, archivos digitales o electrónicos y la información contenida en éstos y que pueden o no formar parte de una red informática.

III. Capacidades de Seguridad en el Ciberespacio: Son las capacidades del Estado Mexicano para garantizar la correcta operación de los Activos de Información y de TIC de las Infraestructuras de Información esenciales (IIE) e Infraestructuras Criticas de Información (ICI); entendidas como Seguridad de la Información, Ciberseguridad y Ciberdefensa en su respectivo ámbito de atribuciones y competencias.

IV. Centro Especializado en Respuesta Tecnológica de México (CERT-MX). Organismo del Estado Mexicano encargado de prevenir y proteger a la sociedad mexicana en el ciberespacio, así como investigar los ciberincidentes y/o ciberataques que pueden constituir ciberdelitos, coordinando para ello con los diferentes organismos en el ámbito nacional e internacional.

V. Centros de Ciberdefensa: Son los Centros de Operaciones en el Ciberespacio de la Secretaría de la Defensa Nacional y de la Secretaría de Marina para proporcionar Seguridad en el Ciberespacio en materia de Seguridad Nacional.

VI. Ciberamenaza. Amenaza emergente con capacidad de provocar un efecto adverso en o desde el ciberespacio, y está relacionado a las vulnerabilidades de las personas, los procesos críticos y las TIC de los sujetos obligados.

VII. Ciberataque. Acción voluntaria ofensiva o maliciosa en o desde el ciberespacio con la intención de causar un efecto adverso a las Tecnologías de Operación (TO) de las Infraestructuras Críticas de Información e infraestructuras de información esenciales, así como cualquier situación que ponga en peligro inminente a la Seguridad Nacional a través del Ciberespacio.

VIII. Ciberdefensa. Capacidad del Estado Mexicano traducida en acciones, recursos y mecanismos de seguridad y defensa nacional en el Ciberespacio, gestionada a través de las Instancias de Seguridad Nacional.

IX. Ciberdelito. Conductas delictivas perpetradas en o desde el ciberespacio utilizando las TIC como medio o fin y que se encuentran tipificados en la legislación nacional y/o legislación internacional aplicable.

X. Ciberespacio. Ámbito digital intangible de naturaleza global soportado por las TIC, en el que se comunican e interactúan las entidades públicas, privadas y la sociedad en general, permitiendo el ejercicio de los derechos y libertades como en el mundo físico.

XI. Ciberincidente o Incidente de Ciberseguridad: Interrupción, acceso no autorizado, cualquier falla o incidente que no sea un ciberataque y que provoque o pueda provocar afectación a los activos de TIC de las

Infraestructuras Críticas de Información e Infraestructuras de Información Esencial de los sujetos obligados, pudiendo concretarse o no una acción de ciberdelito.

XII. Ciberoperaciones: Empleo de las capacidades del Estado Mexicano a través de las Instancias de Seguridad Nacional para llevar a cabo acciones defensivas, ofensivas o de inteligencia en el ciberespacio.

XIII. Ciberresilencia. Capacidad de un proceso, negocio, organización o nación para anticipar, resistir, recuperarse y evolucionar a fin de mejorar las capacidades de Seguridad en el Ciberespacio frente a condiciones adversas, cibereincidentes o ciberataques a las IIE e ICI que requieren para funcionar.

XIV. Ciberriesgo. La posibilidad de que una amenaza aproveche una vulnerabilidad y cause una pérdida o daño a la ciudadanía o a los activos de TIC y/o TO de las IIE e ICI.

XV. Ciberseguridad. Capacidad del Estado Mexicano para implementar políticas, normas, procedimientos, medidas y controles asociados con la protección de activos de información y de TIC de la sociedad, gobierno, economía y Seguridad Nacional en el ciberespacio.

XVI. Comisión Investigadora de Ciberdelitos: Es encabezada por la Fiscalía General de la Republica en coordinación con el CERT-MX y con otras instancias u organismos del sector afectado.

XVII. Información: Conjunto de datos organizados en cualquier soporte en que estos se encuentren, así como el personal y material que puede ser observado y procesados como tal, y que puedan ser comunicados o transmitidos por cualquier medio o forma.

XVIII. Infraestructura(s) Crítica(s) de Información (ICI): Las infraestructuras de información esenciales consideradas estratégicas por estar relacionadas con la provisión de bienes y de prestación de servicios públicos esenciales y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la ley de la materia.

XIX. Infraestructura(s) de Información Esencial(es) (IIE): Las redes, servicios, equipos e instalaciones asociados o vinculados con Activos de TIC y/o TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de los sujetos obligados.

XX. Normas Oficiales Mexicanas (NOM): Para los efectos e interpretación de la presente Ley, se remitirá a la definición de Norma Oficial Mexicana contenida en la Ley Federal sobre Metrología y Normalización; las cuales en lo particular establecerán las medidas y controles de Seguridad de la Información, Ciberseguridad y Ciberdefensa.

XXI. Plataforma Nacional de Ciberseguridad: Es la tecnología a través de la cual se intercomunican los sujetos obligados con el CERT-MX y con los Centros de Ciberdefensa de las Fuerzas Armadas a efectos de coordinar las acciones para disminuir la vulnerabilidad cibernética nacional.

XXII. Responsables de Red de Internet Nacional: Son, el Instituto Federal de Telecomunicaciones y proveedores de servicio de internet en México.

XXIII. Seguridad de la Información: Capacidad del Estado Mexicano para preservar la confidencialidad, integridad y disponibilidad de la información a través de la gestión de riesgos, así como su autenticidad, auditabilidad, trazabilidad, protección a la duplicación, no repudio y legalidad.

XXIV. TIC o Tecnologías de Información y Comunicaciones: Hardware y/o software que son empleadas por sí solas o dentro de una red para almacenar, procesar, imprimir, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

XXV. TO o Tecnologías de Operación: Hardware y/o software de TIC que detecta o genera un cambio a través del control y/o monitoreo de dispositivos físicos, procesos y eventos en las Infraestructuras Criticas de Información o Infraestructuras de Información Esenciales.

Artículo 7. La Comisión Intersecretarial para el Desarrollo de Gobierno Electrónico será responsable de mantener actualizada y dar seguimiento a la implementación de la Estrategia Nacional de Seguridad en el Ciberespacio del Gobierno Federal y a la presente Ley en coordinación con las Instancias de Seguridad Nacional y todos los sectores de la sociedad.

Artículo 8. En materia de Seguridad Nacional; el Ejecutivo, a través de las Instancias descritas en el Artículo 6. de la ley en la materia, implementará una Política Interinstitucional para el Ciberespacio a fin de proteger las ICI de carácter estratégico del país, que de vulnerarse o afectarse su TO, Activos de TIC y/o de Información, se pondría en grave peligro el bienestar nacional, la provisión de bienes y servicios y los medios de vida de las personas o el interés público y con ello la Seguridad Nacional. Así mismo, desde este ámbito se coadyuvará en la protección de las IIE de los sujetos obligados.

Artículo 9. Serán aplicables de manera supletoria, en lo conducente, las disposiciones contenidas en la Ley de Seguridad Nacional, Código Penal Federal, Ley Federal contra la Delincuencia Organizada, Ley General de Responsabilidades Administrativas, Ley General de Transparencia y Acceso a la Información, Ley General de Datos Personales en posesión de los Sujetos Obligados y la Ley Federal de transparencia y Acceso a la Información Pública.

Artículo 10. Para los efectos del artículo 8 de la presente ley, las ICI e IIE a que se refiere, se encontrarán encuadradas de manera enunciativa mas no limitativa en los siguientes sectores: Gobierno, Energía, Financiero, Industrial, Comercial, Servicios de Emergencia, Alimentación, Telecomunicaciones, Suministro de Agua, Salud Publica, Fuerzas de Seguridad, Fuerzas Armadas, entre otras que puedan afectar la provisión de bienes y la prestación de servicios a la sociedad.

Capítulo II
De la Prevención e Investigación de Ciberdelitos

Sección Primera
De la Protección de la Sociedad Mexicana en el Ciberespacio

Artículo 11. A efecto de proteger a la sociedad mexicana en el ciberespacio de las ciberamenazas, los sujetos obligados deberán proteger los datos personales y datos personales sensibles conforme a las leyes en la materia, basándose en las Normas Oficiales Mexicanas a que se refiere esta Ley.

Artículo 12. A efectos de proteger a la sociedad mexicana en el ciberespacio de las amenazas y riesgos a los que se enfrentan cuando se encuentran conectados a internet, el CERT-MX será responsable de la prevención y apoyo directo en investigación de Ciberdelitos, coordinando a nivel nacional e internacional con diferentes instancias y organismos para su persecución y sanción de los mismos; y que estarán tipificados en la legislación nacional y otros ordenamientos del Derecho Internacional que resulten aplicables.

Artículo 13: Los Ciberdelitos además de aquellos comprendidos en la Legislación Nacional, serán entre otros:

I. Aquellos que atenten contra la confidencialidad, integridad y la disponibilidad de los datos y los sistemas informáticos; entre otros: acceso ilícito, interceptación ilícita, ciberataque a la integridad de los datos, ciberataque a la integridad de los sistemas y abuso de los dispositivos.

II. Aquellos que puedan clasificarse como: Falsificación informática y/o fraude informático.

III. Aquellos relacionados con el contenido que ofrezcan o promuevan pornografía infantil y/o la trata de personas, entre otras.

IV. Aquellos relacionados con infracciones de la propiedad intelectual y los derechos afines y otras formas de responsabilidad sancionables.

Artículo 14. Para incrementar la Seguridad en el Ciberespacio para proteger a la sociedad mexicana en este entorno, se promoverá la asociación público – privada en el ámbito nacional e internacional para sumar los esfuerzos de coordinación entre la academia, la industria, el comercio, la sociedad civil, los organismos de investigación y desarrollo del Estado Mexicano y los sujetos obligados, para fortalecer la identificación, protección, detección, respuesta y recuperación ante los riesgos y amenazas que atentan contra la Seguridad Publica y la Seguridad Nacional.

Artículo 15. En materia de prevención de Ciberdelitos, la federación, las entidades federativas y los municipios promoverán a través de los medios de comunicación la publicidad para todos los sectores de la sociedad a fin de generar una cultura de Seguridad en el Ciberespacio, con las limitaciones establecidas en la legislación nacional en materia electoral.

Sección Segunda
De la Protección de las Infraestructuras de Información Esencial y Críticas de Información

Artículo 16. Cuando se detecten o perciban conductas presuntamente constitutivas de un Ciberdelito derivado de un Ciberincidente en las IIE o ICI del país, los sujetos obligados deben informar inmediatamente al CERT-MX, para efectos de que se conforme una Comisión Investigadora de Ciberdelitos para desarrollar la investigación prevista en el Código Nacional de Procedimientos Penales, proporcionándose toda aquella información relacionada con el ciberincidente, así como con el o los probables responsables, siempre que se determine que existe información en este sentido.

Artículo 17. Cuando se aprecie que el Ciberincidente tiene las características de un ciberataque que afecte a la Seguridad Nacional y/o pudiera constituir una conducta encaminada a un conflicto internacional, la Comisión Investigadora de Ciberdelitos coadyuvará desde el ámbito de su competencia para la debida diligencia con las Instancias de Seguridad Nacional a efectos de proceder en los términos del artículo 59 de la presente Ley.

Título Segundo
De la Seguridad de la Información

Capítulo I
De las Normas y Planes de Seguridad en el Ciberespacio

Sección Primera
De la Aplicación de Normas Oficiales Mexicanas

Artículo 18. A efecto de garantizar la confidencialidad, integridad y disponibilidad de la información que generan, procesan y/o almacenan de los sujetos obligados, la Comisión Intersecretarial para el Desarrollo de Gobierno Electrónico gestionará con diferentes organismos nacionales e internacionales para promover y emitir Normas Oficiales Mexicanas (NOM) en materia de Seguridad de la Información y Ciberseguridad, las cuales establecerán las medidas y controles que permitirán disminuir los riesgos a que se enfrenta la Sociedad Mexicana, las IIE e ICI del Estado Mexicano en el ciberespacio.

Los ciudadanos, organizaciones sociales y/o empresariales interesadas, podrán presentar a la Comisión Intersecretarial las propuestas de NOM a las que hace referencia el presente artículo; y tanto su expedición como sus modificaciones estarán sujetas al procedimiento establecido en la Ley Federal sobre Metrología y Normalización. Estas Normas se actualizarán al menos cada cinco años y se podrán emitir adendas o normas de emergencia, o actualización cuando por una situación no prevista o relevante sean necesario adecuarlas.

Artículo 19. Las NOM a que se refiere el artículo anterior considerarán al menos lo siguiente:

I. Establecer los requisitos, especificaciones, condiciones, procedimientos, metas y parámetros para la industria y proveedores de los Activos de TIC a través de los cuales los sujetos obligados crean, transmiten y/o almacenan información de datos personales de la Sociedad Mexicana;

II. Establecer los requisitos, especificaciones, condiciones, procedimientos, metas y parámetros para la industria y proveedores de los Activos de TIC a través de los cuales los sujetos obligados crean, transmiten y almacenan información respecto a sus Infraestructuras de Información Esenciales e Infraestructuras Criticas de Información;

III. Incluir las mejores prácticas y normas nacionales e internacionales, para disminuir los riesgos de seguridad de la información; así como las condiciones necesarias para su implementación.

En su formulación se deberá considerar que el cumplimiento de sus previsiones, se realice de conformidad con las características de cada proceso productivo o actividad sujeta a regulación, sin que ello implique el uso obligatorio de marcas o proveedores específicos.

Artículo 20. Las NOM deberán considerar que los sujetos obligados puedan certificarse en materia Seguridad de la Información y Ciberseguridad, siendo deber de la Comisión Intersecretarial para el Desarrollo de Gobierno Electrónico alentarlos a llevarlas a cabo para la correcta operación de las TIC y TO.

Artículo 21. Por lo menos una vez al año, los sujetos obligados responsables de IIE e ICI realizarán una inspección de Seguridad de la Información y Ciberseguridad, que podrá ser efectuada por una Institución externa o por una empresa o auditor particular; y en función de ello, se deberán implementar las medidas y controles de seguridad que sean necesarias conforme a las NOM y bajo normas estrictas de confidencialidad.

Sección Segunda
De los Planes de Seguridad en el Ciberespacio de los Sujetos Obligados

Artículo 22. Los sujetos obligados elaborarán un Plan Anual de Seguridad en el Ciberespacio que adopte las Normas que prevé la presente Ley, remitiéndolo para su aprobación a la Comisión Intersecretarial para el Desarrollo de Gobierno Electrónico en el mes de octubre de cada año, a fin de que sea implementado en el año inmediato siguiente.

Artículo 23. Los requisitos mínimos del Plan Anual de Seguridad en el Ciberespacio que los sujetos obligados de carácter público elaborarán en términos de la presente Ley, contienen al menos:

I. Objetivo general y específicos en materia de Seguridad en el Ciberespacio;

II. Alienación estratégica o compatibilidad con el Plan Nacional de Desarrollo y los planes o programas sectoriales que se deriven de este, según el caso;

III. Relación de las ICI e IIE con que cuenta cada sujeto obligado;

VI. Medidas y Controles de Seguridad a implementar adoptando las NOM a que se refiere la presente Ley.

Artículo 24. Los sujetos obligados de carácter público que cuenten con recursos en el Presupuesto de Egresos para TIC, incluirán en sus Programas Anuales la parte correspondiente a la renovación y fortalecimiento de la Seguridad en el Ciberespacio.

Artículo 25. Las dos Cámaras del Congreso de la Unión, el Poder Judicial de la Federación, así como los Órganos a los que la Constitución Política de los Estados Unidos Mexicanos les otorga autonomía, deben prever en su Reglamento Interior u ordenamiento equivalente, el mecanismo para la elaboración, aprobación y registro de sus Planes Anuales, de conformidad con lo establecido en el presente Capítulo. Los Poderes Legislativos y Judiciales de las Entidades Federativas, así como los organismos constitucionales autónomos locales deberán prever en su Reglamento Interior u ordenamiento equivalente, el mecanismo para la elaboración, aprobación y registro de sus Programas Anuales, de conformidad con lo establecido en el presente Capítulo.

Artículo 26. En el caso de las Instancias de Seguridad Nacional, a través del Comité Especializado en Seguridad de la Información dependiente del Consejo de Seguridad Nacional, materializarán la Política Interinstitucional a que se refiere el artículo 8 de la presente ley, implementando un Plan Rector para el Ciberespacio en materia de Seguridad Nacional a efectos de generar capacidades de Seguridad de la Información, Ciberseguridad y Ciberdefensa para el Estado Mexicano, trabajando coordinadamente con la Comisión Intersecretarial para el Desarrollo de Gobierno Electrónico a efectos de asesorar y coadyuvar en las funciones que desarrolla esa comisión en la materia.

Artículo 27. Los sujetos obligados responsables de la operación y mantenimiento de IIE e ICI, además del Plan Anual de Seguridad en el Ciberespacio, realizarán las siguientes tareas:

I. Realizar verificación de antecedentes de las personas que ocupan cargos y/o responsabilidades estratégicas en la materia;

II. Capacitar a los empleados en habilidades técnicas y operacionales en materia de Seguridad de la Información y Ciberseguridad;

III. De acuerdo a cada IIE e ICI se deberán crear cargos de Oficiales de Seguridad de la Información para gestionar los riesgos y mantener un enlace permanente con el CERT-MX;

IV. En el caso de las ICI deberán crear, además, Áreas Especializadas de Ciberseguridad para proteger y salvaguardar sus ICI, manteniendo enlace permanente con el CERT-MX y los Centros de Ciberdefensa Nacional;

V. Desarrollar un Plan de Continuidad de Operaciones que contemple la Ciberresiliencia en caso de desastres, fallas, Ciberincidentes y/o Ciberataques; practicando simulacros o ciberejercicios periódicamente.

Capítulo II
De los Sujetos Obligados de carácter Público y Privado

Sección Primera
Deberes y Responsabilidades de lossujetos obligados de carácter Público

Artículo 28. Los Sujetos Obligados en cualquiera de los niveles de gobierno, en el ámbito de sus competencias deberán de forma permanente:

I. Incluir en sus organigramas Oficiales de Seguridad de la Información y Área Especializada de Ciberseguridad en el caso de ICI, con las obligaciones específicas marcadas por esta ley.

II. Alimentar trimestralmente la Plataforma Nacional de Seguridad en el Ciberespacio de acuerdo a las bases de coordinación con el CERT-MX.

III. Compartir información a través de la Plataforma Nacional de Seguridad en el Ciberespacio respecto a Ciberincidentes, metodologías y bases de conocimiento para que este sea replicado.

IV. Crear y someter a evaluación y aprobación del CIDGE, el Plan Anual de Seguridad en el Ciberespacio, acorde con sus funciones y presupuesto.

V. Firmar los convenios de cooperación que estimen necesarios, con la finalidad de implementar las mejores prácticas en la materia, así como para coadyuvar con otros organismos interesados o sujetos obligados en la capacitación del personal, informando a través de la Plataforma de los mismos.

VI. Iniciar procedimientos de responsabilidad conforme a la legislación que le sea aplicable a quienes incumplan la presente norma, así como a quienes se encuentren involucrados en la comisión de algún Ciberdelito.

Sección Segunda
Deberes y Responsabilidades de los Sujetos Obligados de Carácter Privado

Artículo 29. Están obligados al cumplimiento de la presente ley, las personas físicas o morales de carácter privado a que se refiere el artículo 4, que con motivo de su actividad se encuentren en los siguientes supuestos:

I. Posean bases de datos con información de datos personales y/o datos personales sensible de los habitantes del territorio nacional.

II. De forma ocasional o permanente realicen actividades para los entes de la administración pública u órganos dotados de autonomía o similares de cualquiera de los niveles de gobierno, por virtud de la cual obtengan información de los habitantes del territorio nacional catalogada así por la Ley Federal de Transparencia y Acceso a la Información Pública.

III. Creen u operen Aplicativos de Computo, por virtud de las cuales obtengan información de datos personales de los usuarios.

IV. Sean proveedores de TO o de Activos de TIC para los entes públicos con independencia del nivel de gobierno al que pertenezcan.

Artículo 30. Son obligaciones específicas de los sujetos señalados en el artículo anterior, además de las que se deriven del texto de la presente ley:

I. Inscribirse en la Plataforma Nacional de Seguridad en el Ciberespacio;

II. Cumplir con las medidas mínimas de seguridad en sus TO y Activos de TIC que se describen en la presente ley;

III. Abstenerse de almacenar información gubernamental confidencial en términos de lo establecido por el artículo 6 de la Ley de Seguridad Nacional en servidores fuera del territorio nacional.

IV. Dar aviso inmediato a través de la Plataforma de cualquier ciberincidente o ciberataque de que tenga conocimiento, se haya o no consumado; informando las medidas tomadas y los daños ocasionados, y en caso de que se haya evitado compartir la información para que esta pueda llegar a todos los sujetos obligados y se evite de la misma forma el daño.

Capítulo III
De las TIC y TO de los Sujetos Obligados y la Seguridad en el Ciberespacio

Sección Primera
De las Compras, Contrataciones, Renovaciones y/o Desarrollo de TIC y/o TO

Artículo 31. Para la adquisición o arrendamiento de TO y/o Activos de TIC, las convocatorias para licitación, cartas invitación o requisitos de adjudicación directa, deben incluirse estrictamente todos los requisitos previstos en esta ley y en las NOM, salvo que ya se cuente con los programas de seguridad para ser instalados en los equipos a arrendar o adquirir, debiendo hacer constar esta circunstancia.

La omisión en el cumplimiento de lo dispuesto es causa de responsabilidad para los servidores públicos involucrados en la contratación, así como los particulares que provean sin las especificaciones técnicas mínimas de los bienes o servicios a adquirir, con el fin de fortalecer y hacer eficientes los procesos de Seguridad de la Información, Ciberseguridad y Ciberdefensa establecidas en las Normas, en los términos de la Ley General de Responsabilidades Administrativas de los Servidores Públicos si el caso lo amerita.

Artículo 32. En el caso de las IIE e ICI, se deberá considerar la firma de Promesas de Confidencialidad con los proveedores según el caso, aclarando los deberes y las responsabilidades de Reserva y Confidencialidad de la Información cuando los sujetos obligados compren, contraten, renueven y/o desarrollen TO y/o Activos de TIC.

Sección Segunda
De la Provisión de Activos de TIC y Servicios de Internet o Soluciones Tecnológicas

Artículo 33. Los proveedores de TO y Activos de TIC no deben contener hardware y/o software malicioso; y hará todo lo que es posible para descubrir fallas o vulnerabilidades de seguridad en sus productos y servicios antes de ofertarlos, y en el último de los casos, es responsabilidad del proveedor, informar de inmediato a los sujetos obligados que adquirieron el bien o servicio para adoptar medidas correctivas, quienes lo informarán inmediatamente a través de la Plataforma Nacional para que los sujetos obligados adopten las medidas de seguridad de la información y ciberseguridad correspondientes.

Los proveedores de bienes y servicios deberán garantizar el mantenimiento de seguridad correspondiente para todos sus productos durante todo el período de tiempo establecido por contrato. Asimismo, cuando se recopile información de datos personales de usuarios e información gubernamental confidencial, sus proveedores garantizarán la implementación de medidas legales, administrativas y técnicas a que se refiere la Legislación en la materia.

Artículo 34. El equipo de red crítica y los productos de seguridad de red especializados deben cumplir con las normas nacionales, internacionales y las mejores prácticas internacionales, y deberán estar certificados por una empresa calificada o cumplir con los requisitos de una inspección de seguridad. La Comisión debe formular y publicar un catálogo de equipos de red críticos y productos especializados de seguridad de la red, y promover el reconocimiento de las certificaciones de seguridad y los resultados de la inspección de seguridad para evitar certificaciones e inspecciones duplicadas.

Artículo 35. En los casos de ciberamenaza y/o ciberataque en o a través del Ciberespacio que ponga en peligro actual e inminente a la soberanía, los intereses nacionales y la infraestructura crítica de las instalaciones estratégicas del País, cualquier proveedor de servicio de telefonía y/o internet sea nacional o extranjero, siempre y cuando tenga operaciones en territorio nacional, estará obligado a cooperar de forma inmediata y oportuna en la investigación y persecución de estos supuestos, en los términos de los Lineamientos de Colaboración en materia de Seguridad y Justicia vigentes.

Artículo 36. Los proveedores de servicio de telefonía y/o internet a través de sus Planes de Respuesta a Incidentes de Seguridad en el Ciberespacio y Planes de Continuidad de Operaciones, y a fin disminuir los impactos a los sectores de IIE e ICI, estos deberán proporcionar alertas y reportes de Ciberseguridad al CERT-MX para la investigación de ciberdelitos y a los Centros de Ciberdefensa Nacional en materia de Seguridad Nacional.

Artículo 37. Los proveedores de Activos de Información, TIC y/o TO deberán llevar a cabo certificaciones de seguridad de la información y/o ciberseguridad observando las Normas a que se refiere la presente ley y la legislación vigente en relación con la protección de información confidencial y reservada a que se refiere la legislación en materia de transparencia y acceso a la información, protección de Datos Personales y la Ley de Seguridad Nacional.

Título Tercero
De la Ciberseguridad

Capítulo I
De la Plataforma Nacional de Ciberseguridad

Artículo 38. La Plataforma Nacional de Ciberseguridad consiste en un sistema electrónico de ecosistema cerrado que permite la distribución del contenido en línea bajo ciertos lineamientos y características de seguridad, en la cual se contiene la información textual, visual y/o sonora. Además, funge como canal de comunicación y distribución de contenido de valor para los sujetos obligados, a la cual solo pueden acceder estos a través de los mecanismos de seguridad establecidos. El CERT-MX administrará y operará citada plataforma.

Artículo 39. Para la integración y funcionamiento de la Plataforma Nacional de Ciberseguridad, los Oficiales de Seguridad de la Información y Áreas Especializadas de Ciberseguridad de los sujetos obligados deben establecer de forma periódica las bases de coordinación con el CERT-MX, de forma tal que se facilite el flujo de información en tiempo real de cualquier ciberincidente y/o ciberataque que sufran y exponga las debilidades del sistema, repercuta o no en otros sujetos obligados.

Artículo 40. Son objetivos de la Plataforma Nacional de Seguridad en el Ciberespacio:

I. Ser el enlace de comunicación y coordinación entre el CERT-MX y las Áreas Especializadas de Ciberseguridad de los Sujetos Obligados.

II. Contener la información recibida de los sujetos obligados con carácter Reservado.

III. Recibir de los sujetos obligados:

a. La información relacionada con su Plan Anual de Seguridad en el Ciberespacio y cualquier otra información que pueda ser de interés para todos los sujetos obligados.

b. Los avisos de ciberincidentes o ciberataques ocurridos o que pudieran llegar a ocurrir, a efectos de implementar acciones pertinentes ante los riesgos y amenazas que atentan contra la seguridad en el ciberespacio.

IV. Recibir del CERT-MX:

a. La información de alertas de ciberincidentes y/o ciberataques para que los sujetos obligados adopten las acciones para identificar, proteger, detectar, responder y recuperarse.

b. Las experiencias de la base de conocimiento que se genere derivado de los convenios de cooperación e implementación de estrategias en la materia.

c. Las estadísticas anuales de incidentes y/o ciberataques que genere el CERT-MX a efectos de que los sujetos obligados consideren esta información para la gestión de riesgos en el ciberespacio en apoyo a la toma de decisiones.

Capítulo II
De los Oficiales de Seguridad de la Información y Áreas Especializadas de Ciberseguridad de los sujetos obligados

Sección Primera
De las funciones de las Áreas Especializadas de Ciberseguridad

Artículo 41. Dependiendo del tamaño y tipo de organización, es deber de todos los sujetos obligados contar con al menos un Oficial de Seguridad de la Información y en el caso de las ICI se deberá contar además con un Área Especializada en Ciberseguridad, responsables de analizar, diseñar, desarrollar, implantar, probar y mejorar los mecanismos y controles de ciberseguridad que se requieran para proteger los activos de TIC y TO, acorde con la presente ley y los requerimientos propios de cada sujeto de acuerdo con su actividad.

Artículo 42. El Oficial de Seguridad de la Información y/o responsable del Área Especializada en Ciberseguridad, tendrá la responsabilidad de mantener una seguridad efectiva, realizando permanentemente revisiones para asegurar la mejora continua; así como de alimentar la Plataforma Nacional de Seguridad Informática, dar y recibir los avisos de ciberincidentes y/o ciberataques para llevar a cabo las medidas de prevención, reacción y corrección que procedan en tiempo real. Por lo que, de manera general mas no limitativa, tendrá las siguientes funciones:

I. Ser el responsable de los medios de autenticación que se le otorgue para acceder a la Plataforma Nacional en Ciberseguridad.

II. Implementar Planes de Continuidad de Operaciones para ser resilientes en el ciberespacio.

III. Reportar mensualmente a la Plataforma Nacional de Ciberseguridad de los ciberincidentes o ciberataques que sufra o que haya detectado como amenaza, así como de los resultados derivados de las pruebas de penetración que se lleven a cabo.

IV. Ser responsable directo del cumplimiento de todas las medidas de prevención que se desglosan en la presente ley, así como del seguimiento de las medidas correctivas que deban implementarse.

V. Diseñar el plan anual de trabajo en materia de seguridad en el Ciberespacio del sujeto obligado, subirlo a la plataforma, atender las recomendaciones e implementarlo una vez aprobado, reportando el resultado a la Plataforma en forma anual.

VI. Implementar las medidas y controles de seguridad de la información y ciberseguridad correspondientes de acuerdo al sector y a las NOM a que se refiere esta Ley.

VII. Desarrollar análisis de riesgos cibernéticos para implementar las medidas y controles de seguridad que se determinen.

VIII. Ser el responsable del control de acceso de sus usuarios a la información.

IX. Formular sistemas internos de gestión de seguridad y reglas operativas, designar a las personas responsables de la seguridad de la red e implementar la responsabilidad de la protección de la seguridad de la red.

X. Adoptar medidas tecnológicas para prevenir malware, virus informáticos, ataques a la red, intrusiones en la red y otras acciones que pongan en peligro la ciberseguridad;

XI. Adoptar medidas tecnológicas para monitorear y registrar el estado de la red y los ciberincidentes ocurridos, almacenando los registros durante al menos doce meses.

XII. Adoptar medidas como la clasificación de datos, el respaldo de datos al menos una vez por semana y el cifrado de los mismos.

XIII. Organizar periódicamente ejercicios de respuesta a incidentes de ciberseguridad para incrementar los niveles de seguridad y de coordinación.

XIV. Promover el intercambio de información a través de la Plataforma Nacional de Ciberseguridad.

Artículo 43. Atendiendo a que los Oficiales de Seguridad de la Información y Áreas Especializadas de Ciberseguridad de los sujetos obligados, constituyen el eje invaluable para el cumplimiento de la presente Ley, dicha responsabilidad deberá recaer en quien reúna al menos las siguientes condiciones.

I. Perfil profesional mínimo, grado de licenciatura con título y cedula profesional en materias afines a la Seguridad de la Información y/o la Ciberseguridad.

II. Contar con experiencia mínima de tres años antes del día de su designación.

III. Acreditar que cuenta con capacitación mínima, actualización y/o certificación en materias afines a la Seguridad de la Información y/o la Ciberseguridad.

IV. A través de la plataforma, acreditar de forma anual la actualización de las habilidades y/o conocimientos técnicos que requiere el perfil.

Sección Segunda
De los Controles de Ciberseguridad a Implementar

Artículo 44. Para llevar a cabo una correcta implementación de controles de seguridad en los Activos de Información y de TIC, los sujetos obligados deberán generar capacidades de seguridad de la información para una adecuada gestión de riesgos de sus ICI e IIE según el caso.

Artículo 45. Los Activos de información y de TIC de las ICI e IIE, que se destinen a la creación, resguardo, operación, transmisión de información de cualquier clase, y en cualquier nivel, además de aquellos que se establezcan en las NOM a que se refiere esta ley, deberán tener instalados al menos antivirus, antimalware y realizar respaldos mensuales.

Artículo 46. Para proteger los activos de información, de TIC y TO, todas las Áreas Especializadas de Ciberseguridad de los sujetos obligados tendrán Sistemas de Seguridad Perimetral, además de aquellos que establezcan las NOM a que se refiere esta Ley, y deberán contar al menos con parches, actualizaciones, hardening, antiphising, antihaking, antimalware, antiransonware, además de realizar pruebas documentadas de penetración y tener un Plan de Recuperación de Desastres.

Capítulo III
De las Alertas de Ciberincidentes y/o Ciberataques y las Medidas de Verificación

Sección Primera
De las Alertas de Ciberincidente y/o Ciberataques

Artículo 47. Todos los sujetos obligados a través de las Áreas Especializadas de Ciberseguridad, darán alerta inmediata al CERT-MX a través de la Plataforma Nacional, de cualquier Ciberincidente o Ciberataque detectado, para que este a su vez de aviso a las demás Áreas Especializadas de Ciberseguridad en los sujetos obligados.

Artículo 48. Las Áreas Especializadas de Ciberseguridad de los sujetos obligados que reciban alertas de ciberincidentes o ciberataques, deberán reportar las acciones tomadas y los hallazgos encontrados a través de la plataforma, así como las posibles soluciones.

Artículo 49. Dependiendo de la naturaleza del ciberincidente o ciberataque, el CERT-MX informará a los sujetos obligados que deban de conocer de la situación, elaborará un detallado análisis junto con las medidas de prevención, reacción o corrección, las cuales no serán limitativas para los sujetos obligados, quienes ante todo velarán por la seguridad de sus Activos de Información, Activos de TIC y TO.

Artículo 50. Tratándose de ciberamenazas o ciberataques a las ICI correspondiente a las Instalaciones Estratégicas del País, el CERT-MX además, dará aviso a los Centros de Ciberdefensa para sumar esfuerzos en la identificación, protección, detección, respuesta y recuperación ante los riesgos y amenazas que atentan contra la seguridad en el ciberespacio y que afectan a la sociedad mexicana, informando al Consejo de Seguridad Nacional a efectos de coordinar los esfuerzos de las Instancias conforme al Título Cuatro de la presente Ley.

Sección Segunda
De las Medidas de Verificación por Ciberincidente o Ciberataque

Artículo 51. Los sujetos obligados, luego de dar aviso a través de la Plataforma Nacional de Ciberseguridad respecto de un ciberincidente y/o ciberataque según el caso, deberán de permitir al CERT-MX realizar una verificación de la Ciberseguridad, otorgando las facilidades que se requieran, estando desde luego presente personal del Área Especializada de Ciberseguridad del sujeto obligado a efecto de que conste la verificación y los hallazgos.

Artículo 52. En el procedimiento de verificación tendrá acceso a todos los equipos y medios de autenticación que considere necesarios; para ello el CERT-MX dispondrá de un Equipo de Respuesta a Incidentes obligado a guardar confidencialidad de la información y sobre los hallazgos hasta en tanto sean valorados y se genere la presunción de responsabilidad o bien se detecte el tipo de falla que permitió el ciberincidente y/o ciberataque.

Artículo 53. El Equipo de Respuesta a Incidentes del CERT-MX en conjunto con personal del Área Especializada de Ciberseguridad del sujeto obligado afectado, analizarán las condiciones que permitieron o bien evitaron que se consumará el ciberincidente a efectos de establecer las medidas y controles de ciberseguridad o en su caso emitir las normas que se requieran para todos los sujetos obligados.

Artículo 54. El Equipo de Respuesta a Incidentes del CERT-MX tendrá las siguientes tareas de acuerdo a la presente Ley:

I. Ser el primer respondiente en materia de Ciberincidentes, evaluando y emitiendo la opinión técnica correspondiente.

II. En caso de que el Ciberincidente tenga características de Ciberdelito, el CERT-MX notificara a la Comisión Investigadora de Ciberdelitos de acuerdo con el sector afectado para que procedan en consecuencia.

III. En caso de que el incidente tenga características de ciberataque a las ICI, el CERT-MX además de la notificación establecida en la fracción anterior, notificará a la Comisión Investigadora de Ciberdelitos de acuerdo con el sector afectado y además informará a los Centros de Ciberdefensa de las Fuerzas Armadas y a las Instancias de Seguridad Nacional.

IV. En cualquiera de los casos, el CERT-MX activará los protocolos de alerta de Ciberseguridad o Ciberdefensa según corresponda.

Título Cuarto De la Ciberdefensa

Capítulo I
De las Fuerzas Armadas en el Ciberespacio

Artículo 55. Toda ciberamenaza y/o ciberataque en o a través del Ciberespacio que ponga en peligro actual e inminente a la soberanía, los intereses nacionales, la infraestructura crítica de información militar y las correspondientes a las instalaciones estratégicas del País, dará lugar al ejercicio de la Fuerza Armada el derecho de legítima defensa, conforme lo establece el artículo 51 de la Carta de las Naciones Unidas, las normas de Derecho Internacional de los Derechos Humanos y el Derecho Internacional Humanitario, así como por el artículo 15 fracción IV, del Código Penal Federal.

Artículo 56. Los Centros de Ciberdefensa Nacionales de las Fuerzas Armadas Mexicanas llevarán a cabo ciberoperaciones militares y navales en el ciberespacio por sí solas o en apoyo a las operaciones de tierra, aire y/o mar, a fin de disminuir los riesgos plasmados en la Agenda a que se refiere la Ley de Seguridad Nacional; para ello destinarán y reorganizarán los recursos humanos, tecnológicos y financieros para el eficiente y eficaz empleo de las

capacidades de ciberdefensa, de acuerdo a las atribuciones establecidas por ley y en el ámbito de sus respectivas competencias, y estarán sujetas a los principios de oportunidad, proporcionalidad, racionalidad y legalidad aplicables al uso de la fuerza conforme a la legislación nacional e internacional vigente en la materia.

Artículo 57. En el supuesto de que las capacidades del Área Especializada de Ciberseguridad de una ICI afectada hayan sido sobrepasadas, con el fin de mantener las capacidades nacionales en el ámbito de la seguridad nacional, los Centros de Ciberdefensa Nacionales de la Secretaría de la Defensa Nacional y de la Secretaría de Marina apoyarán para reestablecer la provisión de bienes y servicios a la sociedad mexicana en o través del Ciberespacio. Para ello, las Fuerzas Armadas Mexicanas implementarán una Estrategia de Ciberdefensa para el país.

Artículo 58. En todo momento los miembros de las Fuerzas Armadas Mexicanas, privilegiarán el respeto irrestricto a los derechos humanos y favorecerán en todo tiempo la protección más amplia a las personas y el interés público; esto es, deberán conducirse con los sujetos obligados y los servidores públicos o privados bajo estos principios; cumpliendo y haciendo cumplir la legislación vigente en materia de seguridad nacional, protección de datos personales, archivo, transparencia y acceso a la información.

Capítulo II
De los Ciberataques y/o Ciberamenazas a la Seguridad Nacional

Artículo 59. Cuando un ciberataque ocurra contra la Infraestructura Crítica de Información correspondiente a las Instalaciones Estratégicas del País, y sea de tal magnitud que la Comisión Investigadora de Ciberdelitos determine que se puede derivar en una crisis de Seguridad Nacional, o que pueda causar una afectación significativa en o desde el Ciberespacio en el ámbito político, económico, social o militar; dará aviso inmediato al CERT-MX y a los Centros de Ciberdefensa Nacional y estos a su vez a las Instancias del Consejo de Seguridad Nacional para que se tomen las acciones necesarias en todos los niveles.

Artículo 60. En los términos establecidos en el artículo anterior, los Centros de Ciberdefensa Nacional y el CERT-MX conformarán un Equipo de Misión Nacional para la coordinación de acciones en materia de Seguridad Nacional en todos los niveles, a través de protocolos aprobados por el Consejo de Seguridad Nacional, y que como consecuencia de algún ciberataque que habiendo sido prevenido o no, tenga como consecuencia la exposición de las debilidades de cualquiera de los activos de información y de TIC de uno o más entes públicos y/o privados obligados.

Artículo 61. Cuando los Centros de Ciberdefensa Nacional y/o el CERT-MX con motivo de las actividades de exploración del Ciberespacio, detecten uno o varios ciberataques de las magnitudes que refiere el artículo 59 de esta Ley, de igual forma se informará al Consejo de Seguridad Nacional, para coordinar con los sujetos obligados a efectos de identificar, proteger, detectar, responder y recuperarse de un ciberataque contra la Infraestructura Crítica de Información correspondiente a las Instalaciones Estratégicas del País.

Artículo 62. Al tratarse de Ciberataques que pongan en peligro o afecten la Seguridad Nacional, será deber de todos los sujetos obligados aportar sus conocimientos para la solución de vulnerabilidades que se adviertan, independientemente de que se encuentren o no involucrados con el mismo.

Título Quinto
De las Infracciones y Sanciones

Capítulo I
De los Servidores públicos como Usuarios de Activos de TIC

Artículo 63. A través de los equipos móviles institucionales o personales de los empleados o funcionarios de los sujetos obligados que hacen uso de las redes públicas, no se debe transmitir información reservada o confidencial de forma directa o desde las aplicaciones instaladas dentro de los dispositivos móviles.

Artículo 64. Como usuarios de los activos de TIC, previo análisis técnico basado en los criterios y prioridades establecidos en la presente Ley y con apego a las NOM que se deban ir actualizando, se instalarán bajo estricto resguardo del usuario que deba operarlos quien rendirá un informe semestral al área de informática de uso, fallas, así como debilidades si llegaré a detectarlas.

El desconocimiento de manejo de tecnologías de la información no será obstáculo para la emisión del informe, a efecto de que el área encargada de cada dependencia conozca de las posibles anomalías, fallos detectados o situaciones irregulares.

La omisión en la elaboración y entrega de dicho informe, es causa de responsabilidad por incumplimiento, con independencia de que para el caso de que por su negligencia se facilite un ciberataque, tenga o no consecuencias.

Capítulo II
De las Infracciones a esta Ley y sus Sanciones

Artículo 65. Constituyen infracciones a la presente Ley por parte de los sujetos obligados de carácter público, según sea el caso:

I. No implementar las medidas y controles de Seguridad de la Información y Ciberseguridad descritas en esta ley y en las Normas que emite la Comisión.

II. No gestionar la Plataforma Nacional o adoptar las medidas reactivas y correctivas que se determinen por esta vía, tratándose de ciberincidentes, ciberataques o ciberdelitos.

III. No dar aviso inmediato de los ciberincidentes y/o ciberataques a través de la Plataforma Nacional.

IV. No cumplir con los requisitos previstos para la adquisición de Activos de TIC y TO respecto a las obligaciones específicas con proveedores externos descritos en esta ley.

V. Transmitir información Reservada o Confidencial a través de activos de TIC no autorizados.

La falta de expedición de las normas referidas, no representa impedimento ni exime a los sujetos obligados de adoptar a partir de la entrada en vigor de la presente ley, las medidas de prevención para incrementar la seguridad de sus Activos de Información y de TIC.

Artículo 66. Constituyen infracciones a la presente Ley por los sujetos obligados de carácter privado, según sea el caso:

I. Incumplir acuerdos como proveedores de Activos de TIC, respecto de las condiciones de seguridad que deben prevalecer para preservar la Confidencialidad, Integridad y Disponibilidad de la Información.

II. Instalar hardware o software malicioso por cualquier razón que fuere.

III. Hacer pública la información de la red después de haber efectuado evaluaciones de Seguridad de la Información y Ciberseguridad.

IV. No darse de alta en la Plataforma Nacional de Seguridad Informática, cuando se encuentren en el supuesto y no dar aviso de ciberincidentes o ciberataques.

V. No permitir la verificación de seguridad cuando sean requeridos por la autoridad investigadora de delitos.

VI. Incumplir cualquiera de las obligaciones que se les imponen en términos del artículo 29 y 30 de la presente ley.

Artículo 67. Las sanciones por incumplimiento de parte de los sujetos obligados, serán impuestas en términos de la Ley General de Responsabilidades Administrativas, las cuales son independientes de las responsabilidades penales o civiles que resulten por el incumplimiento.

Artículo 68. Cuando las autoridades federales, estatales o municipales cometan alguna infracción prevista en esta Ley, se dará vista al superior jerárquico y, en su caso, presentará la queja ante la autoridad competente por hechos que pudieran constituir responsabilidades administrativas o las denuncias o querellas ante el agente del Ministerio Público que deba conocer de ellas, a fin de que se proceda en los términos de las leyes aplicables.

Artículo 69. La contravención a lo dispuesto por la presente Ley, será motivo de responsabilidad administrativa, patrimonial, civil y penal de los involucrados en términos de la legislación aplicable.

Transitorios

Primero. La presente ley entrará en vigor a partir de su publicación en el Diario Oficial de la Federación.

Segundo. El gobierno federal tendrá un año para adecuar el marco legal correspondiente.

Tercero. Los gobiernos estatales contarán con dos años para adecuar el marco legal correspondiente.

Cuarto . Los gobiernos municipales contarán con tres años para adecuar el marco legal correspondiente.

Quinto. Los sujetos obligados deberán asignar presupuesto de renovación y/o contratación de tecnología para dar cumplimiento a las obligaciones a lo establecido en la presente ley.

Sexto. Las modificaciones a las legislaciones de responsabilidades y penales para incluir las infracciones y los tipos penales relacionados con la presente ley se deberán presentar en un lapso máximo de dos años.

Séptimo. La expedición del reglamento correspondiente a la presente ley deberá presentarse en un lapso no mayor a dos años y estará a cargo del Ejecutivo federal.

Octavo. Se establece el plazo de dos años para inicio de operaciones de la plataforma.

Noveno. Las atribuciones de la CERT-MX, señaladas en la presente ley, serán absorbidas por la Guardia Nacional a través de la misma CERT-MX una vez que ésta sea integrada a dicha institución.

Notas

1 Ciberespacio: Es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico, Estrategia Nacional de Ciberseguridad, 2017.

2 https://www.un.org/disarmament/es/los-avances-en-la-informatizacion-y-l as-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/

3 https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

4 https://www.oecd.org/centrodemexico/medios/declaracion-ministerial-sbor e-la-economia-digital.htm

5 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-i ndex.aspx

6 https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean

7 https://alianzapacifico.net/wp-content/uploads/Hoja-de-Ruta-SGAD2016-20 17.pdf

8 https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

9 https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2019/OtrTemE con/ENDUTIH_2018.pdf

10 https://consejomexicano.org/multimedia/1528987628-817.pdf

Palacio Legislativo de San Lázaro, a 19 de octubre de 2020.

Diputado Javier Salinas Narváez (rúbrica)