INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD

La suscrita **Juanita Guerra Mena** Diputada Federal integrante del Grupo Parlamentario de MORENA en la LXV Legislatura, con fundamento en los artículos 71 fracción II y 73 fracción XXIII de la Constitución Política de los Estados Unidos Mexicanos; 6º numeral 1, fracción I, 77 numeral 1 y 78 del Reglamento de la Cámara de Diputados, someto a la consideración de esta Honorable Cámara de Diputados la **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD,** al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

Hablar de ciberseguridad es hablar de nuevas modalidades de regulación de la conducta pero al mismo tiempo, del mayor reto al que se enfrenta la ciencia del derecho penal.

La ordenación de nuevos tipos penales a partir de la implementación de todo un ecosistema tecnológico que involucra prácticamente todas las esferas de nuestra vida, se ha convertido en uno de los mayores retos para la ciencia del derecho en el Siglo XXI.

Ello, debido a que, si el derecho es un regulador de la conducta de la persona en colectividad, éste siempre responde a las dinámicas existentes, al devenir imperante en un momento y realidad determinados, por lo que es preciso reconocer que la ciencia jurídica siempre va a la retaguardia de las circunstancias sociales ya que su principal característica ha sido, la de regular hechos concretos, materializables y tangibles.

Si para el derecho es complejo regular conductas ya dadas, cuando éstas se presentan en el universo informático, la situación se torna sumamente compleja; regular las conductas de la persona desde una perspectiva virtual, no solo obliga a incorporar al lenguaje normativo conceptos como *internet, web, host, malware, fireware, hackeo* y en general, una compleja nomenclatura que para efectos jurídicos deberá tener su correspondiente equivalencia.

Legislar sobre ciberseguridad implica un reto que se intensifica con barreras como la idea -mas o menos válida- de que el universo informático corresponde más a la intimidad y libertad de la persona y que pretender regular la vida virtual es el equivalente a una intromisión en donde el Estado no debe participar.

Por estas razones, legislar sobre delitos que involucran el uso de la tecnología no es un problema exclusivo de nuestro país, la necesidad de establecer comunes denominadores a un lenguaje tan global como lo es el cibernético, es una preocupación multinacional que derivó en la suscripción de instrumentos internacionales como el Convenio de Budapest, mejor conocido como Convenio sobre Ciberdelincuencia, el cual, surge de la preocupación por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes.

El Convenio de Budapest, reconoce la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información.

Sobre todo, bajo el argumento de que la lucha efectiva contra la ciberdelincuencia implica entender que ésta no distingue ámbitos territoriales de validez normativa por lo que se requiere de una cooperación internacional reforzada, rápida y eficaz en materia penal.

En Budapest, los Estados parte manifiestan que es necesaria una regulación armonizada y uniforme para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el combate al abuso de dichos sistemas, redes y datos, garantizando con una tipificación global como delito la no ocurrencia de dichos actos, y la lucha eficaz contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable.

Para ello, se requiere que implementemos dentro de nuestras legislaciones nacionales las siguientes cuestiones: criminalizar ciertas conductas como delitos de orden nacional y dotar a las autoridades en materia de procuración de justicia penal de las facultades y herramientas procedimentales necesarias para investigar la comisión de estos delitos, incluyendo expandir capacidades de inteligencia y vigilancia, es decir, hacer de la tecnología el mejor aliado de la seguridad.

Desde el año 2017, México presentó su estrategia de seguridad cibernética, teniendo como objetivo principal el de indentificar y establecer las acciones de seguridad cibernética aplicables a todas las áreas que le permita a la población en

general y a las organizaciones públicas y privadas el uso de las TIC de manera responsable.

Sin embargo, México no cuenta con una ley dedicada a los delitos cibernéticos, únicamente el Código Penal Federal cuenta con un Titulo dedicado a la revelación de secretos y acceso ilícito a sistemas y equipos informáticos. No obstante, estas disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen.

Se estima que México es el noveno país más afectado por el crimen cibernético. En América Latina solo es superado por Brasil.

De acuerdo con datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) en 2017, cada hora se cometían 463 fraudes cibernéticos en operaciones por comercio electrónico y banca móvil. En 2018, las pérdidas por este delito sumaron cuatro mil 412 millones de pesos.

Por su parte el Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA) revelan que se pierden alrededor de 9 mil millones de dólares anuales por delitos cibernéticos. Incluso, los propios sitios del Gobierno Federal como Pemex; las secretarías de Economía, Hacienda y del Trabajo y Previsión Social han sufrido ataques.

Entre enero y junio de 2020 se han registrado 3.1 millones de intentos de ciberataque. De acuerdo con la Dirección General Científica de la Guardia Nacional hubo una disminución del 12% en la actividad maliciosa en internet durante el periodo de diciembre de 2019 a febrero de 2020. Sin embargo, esta cifra incrementó un 14% durante los meses de marzo y abril, periodo correspondiente a la emergencia sanitaria. En cuanto a la pornografía infantil, la Guardia Nacional calculó un incremento del 73% durante el mismo periodo. Casi el 80 por ciento fueron relacionados con la red social Facebook.

La realidad es, que los delitos cibernéticos o ciberdelitos, son conductas que realizan las personas en las que se violenta la seguridad en el entorno informático; a pesar de ser conductas que se realizan por lo menos hace una década, la gran mayoría de los Códigos Penales de los Estados son omisos en la regulación de este tipo de delitos y por ende, poco o nada se puede hacer para sancionarlos.

Los delitos de carácter cibernético son conductas dolosas que comprometen el uso y manejo de información de millones de personas, afectan la esfera privada de quien accede a la red informática y, aprovechándose del anonimato y los mecanismos remotos por los que se comete, un delincuente cibernético hace uso de los avances de la tecnología para la comisión de delitos.

Hay conductas delictivas que se dan por el uso de redes sociales y eso es una realidad. También lo es, el hecho de que, cada que surge una nueva iniciativa para sancionar las conductas delictivas realizadas por medio de las redes -como el caso de los retos o la inducción al suicidio- surgen voces que a priori y sin fundamento acusan de pretender establecer “leyes mordaza” o “limitar las libertades” en una discursiva que pareciera diseñada por los propios delincuentes cibernéticos y cuya falta de empatía con las víctimas de este tipo de delitos es abrumadoramente preocupante.

Son muchas y cada vez más agresivas las conductas delictivas que se dan desde el mundo cibernético.

La relación entre países a nivel mundial a través del uso de tecnologías de la información y las comunicaciones, incluido el Internet (TIC), hacen indispensable el establecimiento de reglas jurídicas de la convivencia. Tema por demás complicado, porque los ámbitos de regulación no están delimitados por espacios y fronteras territoriales como países, Entidades Federativas y Municipios y sus respectivas competencias.

En este ámbito de relación, en el caso de la legislación mexicana y en específico de la legislación de la Ciudad de México, en la presente Iniciativa se trata de establecer reglas en una realidad virtual (ciberespacio), cuya jurisdicción establece criterios de competencia donde dicha realidad no está debidamente regulada para efectos de determinar las conductas adecuadas y cuales no lo son; ni mucho menos, una regulación normativa que establezca conductas constitutivas de delitos, a partir de la consideración de bienes jurídicamente protegidos (ciberdelitos).

Si bien las TIC y particularmente el Internet, es un bien de la humanidad, no debe estar exento de ser regulado ya que su uso involucra siempre a seres humanos que pueden utilizarlo adecuadamente, pero también pueden usarlo para hacer daño a los bienes más preciados. Al respecto habrá quienes digan que resulta obvio que esos bienes son los derechos humanos establecidos en la Carta Magna y en los Instrumentos Internacionales ratificados por México. Pero no hay que perder de vista que cuando se trata de delimitar responsabilidades y obligaciones de las autoridades involucradas y de personas en materia del Derecho Penal, es una garantía de certeza jurídica el que se identifiquen con toda precisión, todos los elementos del tipo delictivo, así como el bien jurídico que se pretende proteger con la sanción prevista para quien atentó o quienes atentaron contra ese bien jurídico.

La Unión Internacional de Telecomunicaciones, organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas, encargado de regular las telecomunicaciones a nivel internacional entre las distintas

administraciones y empresas operadoras, aporta una definición de la Ciberseguridad, que engloba los componentes de la misma:

> ***"****La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:*
>
> - *disponibilidad;*
> - *integridad, que puede incluir la autenticidad y el no repudio;*
> - *confidencialidad"*[1]

En la actualidad, las comunicaciones tanto públicas como privadas y el progreso de las sociedades a nivel mundial, no se conciben sin las TIC. Su rápida evolución y la multiplicación de medios de interconexión a través del ciberespacio evidencian la necesidad de ocuparse de la Ciberseguridad, para atender los riesgos y amenazas que han ido surgiendo.

En sus inicios, la Ciberseguridad se centró en la protección de la información de forma reactiva, así fue evolucionando a una posición proactiva que identifica y gestiona los referidos riesgos y amenazas al ciberespacio.

En el ámbito internacional, en la Resolución 70/125 de la Asamblea General de la Organización de las Naciones Unidas, en los siguientes numerales hace referencia a los derechos humanos en la sociedad de la información:[2]

---

[1] La Conferencia aprobó una definición de ciberseguridad tal como se expresa en la Recomendación UIT–T X.1205. https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

[2] Resolución 70/125. Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información. 79ª sesión plenaria, 16 de diciembre de 2015. Páginas 10,11,12 y 13. https://unctad.org/es/system/files/official-document/ares70d125_es.pdf

- Reafirma el compromiso enunciado en la Declaración de Principios de Ginebra y el Compromiso de Túnez con la universalidad, indivisibilidad, interdependencia e interrelación de todos los derechos humanos y las libertades fundamentales, incluido el derecho al desarrollo consagrado en la Declaración de Viena y el Programa de Acción de la Conferencia Mundial de Derechos Humanos. (numeral 41)

- Que los derechos humanos han sido parte esencial de la visión de la Cumbre Mundial sobre la Sociedad de la Información y que las tecnologías de la información y las comunicaciones han demostrado su potencial para fortalecer el ejercicio de los derechos humanos, facilitando el acceso a la información, la libertad de expresión y la de reunión y asociación. (numeral 42)

- En esta resolución se afirma que los mismos derechos que tienen las personas fuera de la red, deben estar protegidos también en línea. (numeral 43)

- Se acogen con beneplácito los esfuerzos emprendidos por los gobiernos, el sector privado, la sociedad civil, la comunidad técnica y las instituciones académicas para crear confianza y seguridad en la utilización de las TIC. (numeral 49)

- Se reconoce la función de liderazgo de los gobiernos en las cuestiones de ciberseguridad relativas a la seguridad nacional. Y se reafirma que la creación de confianza y seguridad en la utilización de las tecnologías de la información y las comunicaciones debe ser compatible con los derechos humanos. (numeral 50)

- Se reconoce que la gestión de Internet como un recurso mundial que incluye procesos multilaterales, transparentes, democráticos y de múltiples interesados, con la plena participación de los gobiernos, sector privado, sociedad civil, organizaciones internacionales, comunidades técnica y académica y todas las demás partes interesadas, de conformidad con sus respectivas funciones y responsabilidades. (numeral 57)

- Se reitera la definición de trabajo de la gobernanza de Internet como el "*desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivas funciones, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y la utilización de Internet*". (numeral 58)

La Ciberseguridad: Una vertiente de la Seguridad Pública

Para efectos de una legislación como la que se propone en la presente Iniciativa de Ley de Ciberseguridad que regula la prevención, investigación y persecución de vulnerabilidades, amenazas y ataques a cargo de ciberdelincuentes que cometen ciberdelitos, así como las estrategias, políticas públicas y acciones que se construyan, no pueden ser regulados de manera aislada y ajena a las disposiciones jurídicas relacionadas y aplicables de la legislación del país, correspondientes a los órdenes de gobierno, sectores y niveles de la sociedad de que se trata. En el caso de México y sus Entidades Federativas, debe construirse una legislación en esta materia, orientada en diversos contenidos de la legislación del Sistema Nacional de Seguridad Pública.

Por tanto, en la presente Iniciativa de Ley de Ciberseguridad se tiene presente que:

1. Con fundamento en el artículo 21 de la Carta Magna, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social, de conformidad con lo previsto en la Constitución Federal y las leyes en la materia, se deben regular sus contenidos, con una visión moderna de sistema articulado, coordinado y comunicado en la actuación de las diversas autoridades que tienen atribuciones en la seguridad pública o seguridad ciudadana.

2. Los contenidos se deben regular atendiendo a una política criminológica integral, que comprende la prevención, investigación y persecución de los delitos, así como la sanción de las infracciones administrativas, en los términos de la ley, en las respectivas competencias que la Constitución Federal señala.

3. La actuación de las autoridades e instituciones que tengan competencia, responsabilidades y obligaciones en materia de Ciberseguridad se regirán por los principios de legalidad, objetividad, eficiencia, profesionalismo,

honradez y respeto a los derechos humanos reconocidos en la Constitución Federal.

4. Prever la valiosa participación ciudadana y de los sectores privado, social y educativo, tanto en la prevención de ciberamenazas y ciberataques, así como en la formación de una cultura de la Ciberseguridad.

Por lo anteriormente expuesto sometemos a consideración de esta H. Cámara de Diputados la siguiente Iniciativa con:

PROYECTO DE DECRETO

ÚNICO. Se **EXPIDE** la **LEY GENERAL DE CIBERSEGURIDAD,** para quedar como sigue:

LEY GENERAL DE CIBERSEGURIDAD

TÍTULO PRIMERO

DISPOSICIONES GENERALES

Capítulo Único

Disposiciones Generales

Artículo 1. Las disposiciones de la presente Ley son de orden público, interés social y observancia general en todo el territorio del país.

Artículo 2. La presente Ley tiene por objeto:

I. Establecer los ámbitos de competencia de las autoridades en materia de prevención y atención de riesgos y amenazas en materia de Ciberseguridad como un componente de la Seguridad Pública;

II. Determinar las bases para la generación de estrategias, políticas públicas y acciones de Seguridad Pública en su vertiente de Ciberseguridad y Seguridad Cibernética; y

III. Establecer el marco normativo para la coordinación de acciones entre particulares y autoridades para la prevención, investigación y persecución de los ciberdelitos.

Artículo 3. Son de aplicación supletoria de la presente Ley, la Ley del Sistema Nacional de Seguridad Pública, la Ley Nacional Sobre el Uso de la Fuerza y la Ley de la Guardia Nacional, así como la Ley de Seguridad Nacional.

Artículo 4. Para garantizar la protección de los derechos humanos de los cibernautas, las autoridades deberán atender los siguientes principios:

I. Las políticas de Ciberseguridad son un componente de la Seguridad Pública y deben respetar en todo momento las libertades de los gobernados, contenidas en la Constitución federal, y demás legislación relacionada y aplicable;

II. Se deben garantizar los principios de transparencia y rendición de cuentas;

III. En la construcción, implementación y evaluación de políticas de Ciberseguridad deben involucrarse mecanismos de participación de las personas, comunidades, industria, sociedad civil, academia y comunidad técnica;

IV. La protección del derecho a la privacidad para garantizar la seguridad personal, autonomía y dignidad humana;

V. La vigilancia e intervención de comunicaciones privadas, deben estar fundadas en la legislación aplicable, atendiendo a los principios de necesidad y proporcionalidad, utilizando mecanismos de control, transparencia y rendición de cuentas;

VI. Deberán promover el mejoramiento y adopción del cifrado como medida para mitigar riesgos y fortalecer la Ciberseguridad;

VII. Las políticas de Ciberseguridad diseñadas e implementadas por las autoridades deben contribuir a la progresividad de la reducción de vulnerabilidades;

VIII. Se abstendrán en lo posible de establecer la obligación de recolección y almacenamiento de datos;

IX. Abstenerse de adoptar políticas que suspendan o interrumpan la disponibilidad del servicio de acceso a Internet;

X. Las políticas de Ciberseguridad deben sustentarse en la disponibilidad continua de la conectividad, y

XI. La regulación de la vigilancia y monitoreo de la red y de la investigación y persecución de los ciberdelitos, se hará con absoluto respeto a los derechos humanos y garantías individuales.

Artículo 5. Para los efectos de la presente Ley, se entiende por:

I. Ciberamenaza.- Al riesgo potencial relacionado con las vulnerabilidades de los sistemas informáticos e infraestructura física y pasiva de las redes públicas de telecomunicaciones, de permitir causar daño a los procesos y continuidad de las infraestructuras críticas de información, las infraestructuras de información esenciales, así como la seguridad de las personas;

II. Ciberataque.- A la acción realizada a través de las redes de telecomunicaciones con el objetivo de dañar las infraestructuras críticas de información, las infraestructuras de información esenciales, así como la seguridad de las personas;

III. Ciberdefensa.- Al conjunto de acciones, recursos y mecanismos implementados por el Gobierno Federal en materia de ciberseguridad, para prevenir, identificar y neutralizar toda ciberamenaza o ciberataque.

IV. Ciberdelincuencia.- A las actividades que llevan a cabo una o más personas, o una o más empresas, y que utilizan como medio o como fin a las tecnologías de la información y comunicaciones en la comisión de delitos;

V. Ciberdelincuente.- Persona que realiza una actividad ilegal mediante el uso de la Tecnología De la información y las comunicaciones.

VI. Ciberseguridad.- Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La Ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad;

VII. 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;

VIII. Cibernauta.- Persona que utiliza servicios informáticos del ciberespacio;

IX. Ciberresiliencia o Resistencia Cibernética.- Capacidad de un sistema para recuperarse de un fallo y mantener la confiabilidad en el servicio.

X. Ciberriesgo.- La posibilidad de que una amenaza aproveche una vulnerabilidad y cause pérdida o daño sobre los activos de las tecnologías de información y comunicaciones;

XII. Consejo.- Al Consejo Nacional de Seguridad Pública;

XIII. Constitución federal.- Constitución Política de los Estados Unidos Mexicanos;

XV. Datos personales.- Cualquier información concerniente a una persona física identificada o identificable, en términos de las leyes aplicables;

XVI. Delitos cibernéticos o Ciberdelitos.- Acciones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicaciones y que se encuentran tipificados en el Código Penal para el Distrito Federal;

XVII. Fiscalía Especializada.- Fiscalía Especializada en Delitos Cibernéticos;

XVIII. Fiscalía General.- Fiscalía General de Justicia;

XIX. Hiperconectividad.- Conexión a los sistemas de información a través de diferentes dispositivos;

XX. Internet.- Conjunto de redes de telecomunicaciones que a través de la red pública de telecomunicaciones ofertan servicios y comunicaciones digitales;

XXI. Ley.- La Ley General de Ciberseguridad;

XXII. Pharming.- Técnica de ciberdelincuencia consistente en redirigir el tráfico de la red a un sitio web fraudulento para robar la información que se introduzca en este;

XXIII. Phishing.- Técnica de ciberdelincuencia consistente en un engaño, haciéndose pasar por una persona o institución de confianza para manipular a un tercero;

XXIV. Secretaría.- La Secretaría de Seguridad y Protección Ciudadana;

XXV. Sistema Informático.- Cualquier sistema compuesto por una parte física (Hardware) y una parte intangible (Software) que permita almacenar y procesar información;

XXVI. Smishing.- Técnica de ciberdelincuencia derivada del phishing, en la que el engaño se logra a través de llamadas o mensajes telefónicos;

XXVII. TIC.- Tecnologías de Información y Comunicaciones, que comprende los equipos de cómputo, programas de computación, servicios y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video;

XXVIII. Virtual.- Todo lo que tiene lugar en los medios digitales, y

XXIX. Vulnerabilidades.- Debilidades identificadas en la ciberseguridad dentro de las dependencias o entidades públicas, los órganos constitucionales autónomos, los Gobiernos de los tres órdenes de gobierno, los particulares que potencialmente permiten que una amenaza afecte a las TIC, a la infraestructura de información esencial.

TÍTULO SEGUNDO

DE LOS ÁMBITOS DE COMPETENCIA EN CIBERSEGURIDAD

Capítulo I

Distribución de competencias

Artículo 6. La función de Ciberseguridad es una vertiente de la Seguridad Pública y es responsabilidad del Gobierno Federal, en colaboración con las Entidades Federativas, los Municipios y las Alcaldías de la Ciudad de México y sus habitantes para la prevención, investigación y persecución de los ciberdelitos, la reinserción social, el acceso a una vida libre de violencia y la protección de las personas frente a ciberriesgos, ciberamenazas y ciberataques que atenten contra los derechos, libertades, integridad personal, bienes y entorno. En los términos y competencias establecidos en la Constitución federal, las Leyes Generales, Leyes Federales, Ley del Sistema Nacional de Seguridad Pública y demás legislación aplicable.

Artículo 7. Las autoridades en materia de Ciberseguridad son:

I. El Presidente de la República;

II. El Consejo Nacional de Seguridad Pública;

III. La o el Secretario de Seguridad y Protección Ciudadana;

IV. La o el Fiscal General, y

V. Las demás que con ese carácter determinen la presente Ley y otras disposiciones legales aplicables.

Artículo 8. Son atribuciones que el Presidente de la República delega en el Secretario de Seguridad y Protección Ciudadana, el dirigir las Instituciones de Seguridad Ciudadana en materia de Ciberseguridad a fin de que diseñe e implemente el proyecto de estrategia nacional en materia de Ciberseguridad, mismo que deberá ser sometido al análisis y aprobación del Consejo.

Artículo 9. Las Entidades Federativas son colaboradoras con el gobierno federal en la prevención del ciberdelito y en la formación de una cultura de la Ciberseguridad en las comunidades de sus respectivos Municipios y Alcaldías, en los términos previstos en la Constitución federal, esta ley y demás legislación local aplicable.

Artículo 10. Son auxiliares en materia de Ciberseguridad, cuando sean requeridos por algunas de las autoridades en el cumplimiento de sus atribuciones, los siguientes:

I. Las dependencias, organismos y entidades de la administración pública y de las Entidades Federativas, en el ámbito de sus competencias;

II. Las empresas de Ciberseguridad;

III. Las autoridades, empresas, grupos o personas especializadas en materia de protección civil, prevención y mitigación de riesgos;

IV. Las asociaciones civiles, instituciones educativas, empresas, cámaras empresariales, colegios de profesionistas, instituciones de asistencia privada, grupos voluntarios, asociaciones de vecinos, y

V. Las demás que dispongan los ordenamientos legales aplicables, cuando su colaboración resulte necesaria para el cumplimiento de los fines de esta Ley.

Capítulo II

Del Consejo Nacional de Seguridad Pública respecto de la Ciberseguridad

Artículo 11. Además de las atribuciones establecidas en la Ley General del Sistema Nacional de Seguridad Pública, el Consejo, como instancia de coordinación y seguimiento del Sistema, en materia de Ciberseguridad, se encargará de:

I. Proponer y coadyuvar en el diseño de políticas públicas, estrategias e instrumentos en materia de Ciberseguridad para los tres órdenes de gobierno;

II. Crear los lineamientos relativos al manejo de datos de incidencia delictiva;

III. Dar seguimiento a sus los acuerdos, lineamientos y políticas en materia de Ciberseguridad;

IV. Promover la efectiva coordinación de las instancias que tienen atribuciones y responsabilidades en materia de Ciberseguridad y dar seguimiento a las acciones que para tal efecto se establezcan;

V. Promover la celebración de acuerdos, programas y convenios en materia de Ciberseguridad, con estricto apego a la legislación federal y local aplicables;

VI. Establecer programas o acuerdos para que la sociedad participe en los procesos de evaluación de las políticas públicas en la materia, así como de las instituciones de Ciberseguridad, y

VII. Promover políticas de coordinación y colaboración con el Poder Judicial de la Federación y organismos autónomos.

Capítulo III

De la Secretaría de Seguridad y Protección Ciudadana

Artículo 12. Además de las facultades que la Ley del Sistema Nacional de Seguridad Pública, corresponde a la o el Secretario de Seguridad y Protección Ciudadana:

I. Preparar el proyecto de estrategia en materia de Ciberseguridad, mismo que deberá ser sometido al análisis y aprobación del Consejo;

II. Ejercer las atribuciones en materia de Ciberseguridad por sí o por conducto de la Dirección General de Investigación Cibernética y Operaciones Tecnológicas y de la Policía Cibernética;

III. Coordinar el Centro de Comando y Control en Ciberseguridad, y

IV. Elaborar los Lineamientos del Centro de Comando y Control en Ciberseguridad**.**

Artículo 13. El Centro de Comando y Control en Ciberseguridad es la instancia que contribuye a prevenir y atender posibles incidentes y ataques provocados por la actividad delictiva o maliciosa en el ciberespacio, con la finalidad de detectarlos, analizarlos de manera efectiva y ayudar a la toma de acciones para evitarlos, controlarlos, o documentarlos para su posible investigación, persecución y en su caso, castigo.

Estará a cargo de la Secretaría, en los términos que establece la presente Ley.

Artículo 14. La operación del Centro de Comando y Control en Ciberseguridad estará a cargo de profesionales especializados y calificados en materia de Ciberseguridad y análisis de datos. Su perfil incluirá disciplinas como las matemáticas e ingenierías en telecomunicaciones o informática.

Artículo 15. El Centro de Comando y Control en Ciberseguridad tendrá las siguientes funciones:

I. Realizar el monitoreo de la red y sistemas en busca de amenazas, respetando en todo momento los derechos humanos;

II. Averiguar si los sistemas o datos se han visto comprometidos y proponer acciones pertinentes para contrarrestar los ataques;

III. Resolver incidentes de Ciberseguridad;

IV. Prevenir ataques, mediante labores de detección oportuna;

V. Obtener información para mejorar las medidas de defensa ante ataques similares y detectar vulnerabilidades o errores que están facilitando ese tipo de ataques;

VI. La clasificación y análisis de las alertas, de forma posterior a la resolución de un ataque o incidencia de Ciberseguridad, y

VII. Recuperar datos que puedan ser robados o dañados, después de recibir un ataque externo.

Sección Primera

De la Dirección General de Investigación Cibernética y Operaciones Tecnológicas

Artículo 16. Son atribuciones de la Dirección General de Investigación Cibernética y Operaciones Tecnológicas, en materia de Ciberseguridad:

I. Implementar políticas y procedimientos para la difusión de acciones preventivas respecto a la identificación y denuncia de los delitos cibernéticos;

II. Monitorear la red pública de Internet con el fin de prevenir conductas delictivas;

III. Coordinar y autorizar los métodos de análisis y monitoreo en medios electrónicos u otras plataformas tecnológicas que pudieran ser utilizadas para cometer un hecho probablemente constitutivo de delito;

IV. Detectar rutas de acceso que puedan poner en riesgo los sistemas informáticos, programas, datos o archivos que circulan por la red pública de Internet;

V. Auxiliar a las autoridades competentes en el rastreo y análisis de correos electrónicos relacionados en la investigación y prevención de delitos;

VI. Promover y gestionar ante las instancias correspondientes la atención de las denuncias para la prevención y combate de los delitos que se cometen utilizando medios electrónicos y tecnológicos, así como aquellos hechos ilícitos en cuya comisión se hayan utilizado dichos medios;

VII. Realizar el análisis de sistemas y equipos informáticos y de telecomunicaciones que hayan sido utilizados para reproducir, sustraer, destruir, modificar o perder información contenida en los mismos, con la finalidad de obtener evidencia sobre el delito cometido y, en su caso, hacerlo del conocimiento de las autoridades competentes;

VIII. Analizar los sistemas y equipos informáticos, electrónicos y tecnológicos, vinculados con cualquier hecho ilícito, a efecto de prevenir su comisión o investigarlo de conformidad con las disposiciones aplicables;

IX. Evaluar y documentar la operación técnica de amenazas electrónicas relacionadas con delitos que se cometen utilizando medios electrónicos o tecnológicos, así como aquellos hechos ilícitos en cuya comisión se hayan utilizado dichos medios;

X. Solicitar la baja de información, sitios o páginas electrónicas que representen un riesgo, amenaza o peligro para la seguridad ciudadana, conforme a las disposiciones aplicables;

XI. Promover la cultura de la prevención de los delitos en los que se utilizan medios electrónicos para su comisión, así como la difusión del marco legal que sanciona los mismos;

XII. Generar alertas preventivas en relación con los modos de operación de personas y grupos que utilizan los medios electrónicos u otras plataformas tecnológicas para cometer hechos probablemente constitutivos de delitos;

XIII. Elaborar proyectos y estudios relacionados con la adquisición de equipo táctico, de acuerdo con las necesidades de la Secretaría;

XIV. Establecer procesos que permitan, en forma sistemática, hacer la evaluación confiable del equipamiento táctico para las tareas de prevención y combate del delito;

XV. Generar fichas y registros delictivos con todos aquellos datos que permitan identificar y desarticular organizaciones delictivas;

XVI. Implementar y operar una base de datos conformada con información sustantiva para generar inteligencia operacional que permita identificar a personas, grupos, organizaciones, antecedentes, evolución criminal y modos de operación con el fin de prevenir su comisión;

XVII. Consultar las bases de datos que contenga la Plataforma de Seguridad Ciudadana, para los efectos del ámbito de su competencia;

XVIII. Apoyar los operativos de revisión en puntos estratégicos con la utilización de tecnologías móviles que permitan detectar probables hechos delictivos en el ámbito de su competencia;

XIX. Colaborar con las diferentes áreas de la Secretaría en el desarrollo de operativos de prevención y, en el ámbito de su competencia, combate del delito mediante la obtención de información gráfica y video gráfica, con tecnologías de vanguardia;

XX. Generar información gráfica derivada del monitoreo en puntos estratégicos que se realice con los diferentes equipos tecnológicos de punta, a solicitud de autoridades competentes;

XXI. Administrar la información gráfica y videográfica generada en los distintos operativos de la Institución que den cuenta del desarrollo de éstos, con respeto a los derechos humanos;

XXII. Asegurar el funcionamiento del equipo de captación y procesamiento de información gráfica;

XXIII. Desarrollar mecanismos para la instalación de equipo tecnológico para vigilancias en puntos fijos y móviles;

XXIV. Elaborar los contenidos de capacitación de la Red de colaboradores comunitarios en Ciberseguridad;

XXV. Coordinar el funcionamiento de la Red de colaboradores comunitarios en Ciberseguridad, y

XXVI. Las demás que le atribuya la normatividad vigente.

Sección Segunda

De la Policía Cibernética

Artículo 17. La Policía Cibernética tiene la finalidad de prevenir, por medio del monitoreo y patrullaje en la red pública, cualquier situación constitutiva de un delito que pudiera poner en riesgo la integridad física y/o patrimonial de los habitantes.

Busca, con estrategias de prevención inculcar entre los cibernautas una cultura de respeto y civismo digital, estableciendo un estrecho vínculo con la ciudadanía, promoviendo la denuncia, acciones de alertas preventivas, noticia criminal, pláticas informativas y acopio y análisis de información.

Capítulo IV

De la Fiscalía General de Justicia

Artículo 18. La Fiscalía Especializada en Delitos Cibernéticos, adscrita a la Fiscalía General de Justicia, tiene las facultades de investigar y perseguir delitos cibernéticos en el ámbito local, interviniendo en todas las etapas del procedimiento penal y realizando todas las actuaciones procesales aplicables.

Artículo 19. Es delito cibernético o ciberdelito, toda acción u omisión que comete una persona, que cause perjuicio a otra persona o personas, tipificado por la ley, que se realiza en el entorno informático y que está sancionado con una pena.

Artículo 20. La Persona Titular de la Fiscalía Especializada deberá ser Agente del Ministerio Público, quien contará con conocimientos y experiencia en materia de Ciberseguridad.

El personal a su cargo deberá ser profesional, especializado y calificado en materia de Ciberseguridad y análisis de datos.

El nombramiento de la Persona Titular de la Fiscalía Especializada recaerá en el Secretario de Seguridad y Protección Ciudadana.

Capítulo V

De los Juzgados Federales Especializados en materia Cibernética

Artículo 21. Los Juzgados Federales Especializados en materia Cibernética, conocerán:

I. De los procedimientos en materia Cibernética, que deriven de la presente Ley y demás legislación relacionada y aplicable en la materia;

II. De las medidas cautelares en materia Cibernética;

III. De la diligenciación de los exhortos, rogatorias, suplicatorias, requisitorias y despachos, en la materia; y

IV. De las demás diligencias, acuerdos y actividades que les encomiende la legislación relacionada y aplicable.

Artículo 22. Para ser Juez o Jueza en materia Cibernética, además de cumplir con los requisitos establecidos en la Ley Orgánica del Poder Judicial de la Federación, se requiere tener práctica profesional relacionada con la materia penal mínima de cinco años, contados a partir de la obtención del título profesional, así como conocimientos especializados en materia de TIC.

TÍTULO TERCERO

DE LA COOORDINACIÓN DE ACCIONES EN CIBERSEGURIDAD

Capítulo I

De la coordinación entre autoridades competentes en Ciberseguridad

Artículo 23. La Secretaría podrá suscribir convenios de coordinación y colaboración con las autoridades e instituciones públicas de los distintos órdenes de gobierno en la respuesta a incidentes, protegiendo datos de usuarios y víctimas.

Artículo 24. La Secretaría coordinará la elaboración de estadísticas oficiales, concentrando datos de instituciones públicas y privadas, de los tipos de riesgos en Ciberseguridad, que aporten lugares, periodicidad, incidencia, modos de operar y perfiles criminológicos.

Artículo 25. La Secretaría coordinará la práctica de simulacros en Ciberseguridad en ámbitos públicos, invitando a instituciones del sector privado y académico, conducidos por expertos en la materia.

Artículo 26. La Secretaría coordinará la capacitación y acciones de sensibilización a dependencias de gobierno local y la impartición de cursos y talleres para el personal, sobre la atención de posibles delitos en el entorno digital.

Asimismo, podrá orientar en la implementación de pláticas y materiales sobre el uso de medios digitales enfocados a la prevención, al personal que labora en dichas dependencias de gobierno y que con motivo de sus funciones utiliza las TIC.

Capítulo II

De la coordinación de las autoridades con los sectores de la sociedad

Artículo 27. La Secretaría podrá suscribir convenios de colaboración con empresas privadas, para la prevención, gestión y respuesta de incidentes de Ciberseguridad.

Artículo 28. La Secretaría podrá suscribir convenios de colaboración con las micro, pequeñas y medianas empresas, para impartirles cursos de Ciberseguridad.

Capítulo III

De la coordinación con las Entidades Federativas

Artículo 29. Las Entidades Federativas podrán celebrar convenios de colaboración con la Secretaría, para la impartición de cursos sobre medidas preventivas en Ciberseguridad, en la formación de una cultura en la materia a vecinos,

comunidades, grupos y organizaciones de los sectores educativo, empresarial, económico y laboral, entre otros, residentes o que desempeñen actividades en la correspondiente demarcación territorial.

También, para la coordinación y organización de la Red de colaboradores comunitarios en Ciberseguridad, conforme a lo que establece el Capítulo II, del Título Séptimo de esta Ley.

Artículo 30. En la instrumentación del plan de prevención social de las violencias y del delito, con la participación de la ciudadanía, a que hace referencia la Ley del Sistema Nacional de Seguridad Pública, las Entidades Federativas incorporarán mecanismos y acciones de prevención de ciberdelitos y de la formación de una cultura de Ciberseguridad, atendiendo a los convenios de coordinación con la Secretaría, relacionados con el diseño de acciones y tareas, de organización, contenidos de capacitación y de articulación de acciones establecidas en esta Ley, estrategias, políticas públicas, lineamientos a cargo de la Secretaría, así como a las facultades de las Entidades Federativas previstas en los demás ordenamientos relacionados y aplicables.

TÍTULO CUARTO

DE LAS ESTRATEGIAS FOCALIZADAS DE CIBERSEGURIDAD

Capítulo I

De las Estrategias

Artículo 31. Las estrategias son las políticas públicas, mecanismos y acciones contenidos en los diversos instrumentos que, de conformidad con esta Ley, elabore la Secretaría, y apruebe el Consejo.

Artículo 32. Las estrategias invariablemente deberán contener y precisar lineamientos básicos para la prevención de ciberriegos, ciberamenazas y vulnerabilidades de los sistemas informáticos tanto públicos como privados.

Artículo 33. En las estrategias se privilegiarán las acciones o medidas tendientes al fomento de la cultura de la Ciberseguridad, para lo cual deberán prever en su

implementación un amplio esquema de información y participación ciudadana, así como el acercamiento de las autoridades responsables en materia de Ciberseguridad con la población.

Capítulo II

De los mecanismos de vinculación con autoridades del Sistema Educativo Nacional

Artículo 34. La Secretaría, en coordinación con la Secretaría de Educación Pública, deberá establecer los mecanismos de colaboración a fin de que se diseñe, implemente y evalúe, un Programa Nacional de Prevención Escolar contra la Ciberdelincuencia.

Artículo 35. El Programa Nacional de Prevención Escolar contra la Ciberdelincuencia, es el instrumento de política pública, por el que se establecen las bases de coordinación entre la Secretaría y las autoridades del sistema educativo nacional y deberá considerar, de manera enunciativa, mas no limitativa:

I. Las acciones de prevención desde las escuelas;

II. La participación de la comunidad escolar;

III. El grado de intervención y colaboración de las autoridades, siempre con pleno respeto a los Derechos Humanos de los educandos; y

IV. Las acciones de carácter transversal.

Artículo 36. Las escuelas y en general, la comunidad escolar, deberán diseñar y proponer ante las autoridades educativas de cada plantel, los mecanismos coadyuvantes a fin de generar acciones específicas de prevención y de información a los alumnos de nivel básico y medio básico.

Capítulo III

De las políticas públicas, mecanismos y acciones

Artículo 37. Las políticas públicas, mecanismos y acciones que, para la Ciberseguridad de los particulares emita el Consejo, deberán:

I. Tener la mayor difusión posible como elemento de generación de una cultura de prevención de ciberriesgos, ciberamenazas y vulnerabilidades;

II. Difundirse en un lenguaje que pueda ser comprendido por la mayoría de los habitantes;

III. Establecer actividades concretas para la prevención de los ciberriesgos a los que están expuestos niñas, niños y adolescentes como grupo especialmente vulnerable;

IV. Contener acciones específicas para prevenir la comisión de Ciberdelitos que afecten el patrimonio de los usuarios de servicios de banca en línea, compra en línea o cualquier otro similar, y

V. Establecer mecanismos ágiles de coordinación para el alertamiento cuando se detecte o manifieste la existencia de ciberrisegos o ciberamenazas, tanto a particulares como a las instituciones y organismos públicos.

Artículo 38. Las políticas públicas, mecanismos y acciones que forman parte de las estrategias deberán ser revisadas y evaluadas anualmente por el Consejo.

Artículo 39. Para la medición y evaluación de las políticas públicas, mecanismos y acciones, el Consejo deberá establecer indicadores de gestión gubernamental.

Capítulo III

De las garantías de Ciberseguridad a cargo de los proveedores de servicios

Artículo 40. En el país podrán establecerse y operar particulares y empresas proveedoras de servicios de Ciberseguridad.

Para su funcionamiento deberán estar debidamente registradas en el padrón nacional de proveedores de Ciberseguridad y contar con el certificado, que para tal efecto expida la Dirección General de Investigación Cibernética y Operaciones Tecnológicas.

Artículo 41. Los proveedores de servicios de Ciberseguridad deberán cumplir con los lineamientos que para el desarrollo de su actividad emita el Consejo, mismos que atenderán los existentes, así como las normas técnicas establecidas a nivel nacional.

TÍTULO QUINTO

DE LAS AMENAZAS, VULNERABILIDADES Y RIESGOS POR EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN.

Capítulo I

Del uso de sistemas informáticos

Artículo 42. Queda prohibida a la Secretaría, la colocación de equipos y sistemas tecnológicos al interior de los domicilios particulares, así como su instalación en cualquier lugar, con el objeto de obtener información personal o familiar, violando la privacidad de los particulares y poniendo en riesgo su Ciberseguridad.

Artículo 43. Los equipos y sistemas tecnológicos utilizados por las áreas de la administración pública del gobierno federal con atribuciones en materia de Ciberseguridad, deberán incorporarse al Registro de Equipos y Sistemas Tecnológicos para la Seguridad Pública, en los términos de la legislación aplicable así como de los lineamientos que para tales efectos emita el Consejo.

Artículo 44. Con la finalidad de contribuir al fortalecimiento de la Ciberseguridad, el Gobierno Federal, a través de la Secretaría realizará las siguientes acciones:

I. Diseñar políticas para la adquisición, utilización e implementación de equipos y sistemas tecnológicos por la Secretaría y la Fiscalía General;

II. Atender las consultas que, en materia de Ciberseguridad, soliciten las Entidades Federativas, Municipios y Alcaldías de la Ciudad de México;

III. Emitir opinión sobre los procesos, equipos y sistemas tecnológicos para una segura, eficiente, debida y sustentable destrucción de la información; y

IV. Las demás que señale el Reglamento de la presente Ley.

Capítulo II
De los Perfiles del ciberdelincuente y la cibervíctima

Artículo 45. Con el fin de ayudar a la prevención de los ciberdelitos, la Secretaría deberá elaborar, actualizar y difundir a la población de manera periódica la descripción de los perfiles de las potenciales cibervíctimas y ciberdelincuentes, tomando como referencia las denuncias y carpetas de investigación de los ciberdelitos.

La descripción a que hace referencia el párrafo anterior deberá contener cuando menos:

I. Edad y género más frecuentes de la cibervíctima y el ciberdelincuente por tipo delictivo;

II. Perfil psicológico del ciberdelincuente;

III. Modus operandi del ciberdelincuente;

IV. Técnicas utilizadas para realizar los ataques, y

V. Zonas y entornos donde se cometen el mayor número de ciberdelitos por cada tipo delictivo.

TÍTULO SEXTO

DE LA PREVENCIÓN Y ATENCIÓN A LOS DELITOS CIBERNÉTICOS

Capítulo Único

Del Procedimiento

Artículo 46. La Dirección General de Investigación Cibernética y Operaciones Tecnológicas y la Policía Cibernética serán responsables de la creación de un semáforo de ciberdelitos en el que se cataloguen los que se cometan con mayor frecuencia, para generar alertas preventivas con las que las personas y los sectores público, privado y social puedan adoptar medidas de protección, para evitar ser víctimas de estas conductas.

Artículo 47. La Dirección General de Investigación Cibernética y Operaciones Tecnológicas y la Policía Cibernética crearán un Atlas Ciberdelictivo de carácter Nacional en el que se destaquen los índices delictivos, las conductas ilícitas de alto impacto y su incidencia delictiva, las zonas más vulnerables por cada tipo de conducta ilícita y los índices de percepción de seguridad, así como cualquier otro instrumento de análisis que se considere necesario.

Artículo 48. Para la elaboración de los instrumentos a que hacen referencia los dos artículos anteriores, se tomarán en cuenta los datos que se recaben de la tarea constante de vigilancia, identificación, monitoreo y rastreo de las redes públicas de Internet para prevenir y detectar conductas delictivas, así como los datos extraídos de denuncias y carpetas de investigación acerca de zonas y entornos donde se cometen, y las conductas más recurrentes.

Artículo 49. La Secretaría de Seguridad y Protección Ciudadana podrá celebrar convenios de coordinación con las autoridades responsables de Ciberseguridad en las Entidades Federativas, Municipios y Alcaldías de la Ciudad de México, para prevenir la comisión de ciberdelitos de mayor recurrencia que tengan lugar en las entidades federativas.

TÍTULO SÉPTIMO

DE LA PROMOCIÓN Y FORMACIÓN DE UNA CULTURA DE CIBERSEGURIDAD

Artículo 50. La cultura de Ciberseguridad es el conjunto de valores, principios y acciones en materia de concientización, educación y formación, que se llevan a cabo por la sociedad, academia, sectores público y privado que inciden en la forma de interactuar en el ciberespacio de forma armónica, confiable y como factor de desarrollo sostenible.

Artículo 51. La cultura de Ciberseguridad tendrá como objetivos:

I. Contribuir a la promoción, cumplimiento y protección de los derechos de personas y organizaciones públicas y privadas, con énfasis en la protección de niñas, niños y adolescentes en el ciberespacio y sus derechos;

II. Favorecer el máximo aprovechamiento y uso responsable de las TIC, la convivencia armónica y el desarrollo de actividades en el ciberespacio;

III. Incentivar la innovación y la economía para el desarrollo sostenible;

IV. Fortalecer la prevención de ciberriesgos y conductas ciberdelictivas que afectan a personas, organizaciones privadas y públicas;

V. Incrementar la confianza y continuidad de los servicios y trámites digitales públicos y privados, y

VI. Contribuir a la prevención de ciberriesgos que pudieran afectar a las infraestructuras críticas de información y operación.

Capítulo I

De la participación ciudadana

Artículo 52. Las autoridades en materia de Ciberseguridad establecerán mecanismos idóneos para estimular la participación de las personas, familias, comunidades, empresas y sector académico, así como de las organizaciones de la sociedad civil, en la formación de una cultura de Ciberseguridad, en los términos de esta Ley y demás ordenamientos aplicables.

Artículo 53. Las Entidades Federativas, Municipios y Alcaldías de la Ciudad de México podrán participar en los ámbitos de su respectiva competencia, en la formación de una cultura de Ciberseguridad, para lo cual suscribirán convenios de colaboración con la Secretaría.

Capítulo II

De la Red de Colaboradores Comunitarios en Ciberseguridad

Artículo 54. La Red de colaboradores comunitarios en Ciberseguridad es una estructura organizada y formada por voluntarios con conocimiento en las TIC, que contribuyen con las autoridades de la Secretaría a impartir pláticas dirigidas a las personas, familias, comunidad vecinal, educativa, empresarial y laboral, en la orientación de conductas de prevención de ciberriesgos, ciberamenazas y ciberataques por el uso de las TIC, que contribuyan a la reducción de vulnerabilidades y con ello a la protección de la integridad física, la libertad, patrimonio y entornos de convivencia.

Artículo 55. Para formar parte de la Red de colaboradores comunitarios en Ciberseguridad, las y los solicitantes deberán cumplir los siguientes requisitos:

I. Tener conocimiento de las TIC;

II. Acreditar el curso de capacitación que imparta la Secretaría, y

III. Registrarse en la Red de colaboradores comunitarios en Ciberseguridad.

Artículo 56. La Dirección General de Investigación Cibernética y Operaciones Tecnológicas, en materia de Ciberseguridad de la Secretaría, elaborará los contenidos de la correspondiente capacitación, mismos que serán sometidos a la aprobación del Secretario. Asimismo, coordinará el funcionamiento de la Red de colaboradores comunitarios en Ciberseguridad.

Artículo 57. Las Entidades Federativas, Municipios y Alcaldías de la Ciudad de México podrán participar en los ámbitos de su respectiva competencia, en el funcionamiento de la Red de colaboradores comunitarios en Ciberseguridad, pudiendo constituir Redes de colaboradores comunitarios en Ciberseguridad. Para tal efecto, se deberán suscribir convenios de colaboración con la Secretaría.

TÍTULO OCTAVO

DE LOS CONVENIOS CON ENTIDADES FEDERATIVAS

Artículo 58. El Gobierno Federal, a través de la Secretaría de Seguridad y Protección Ciudadana, podrá celebrar convenios con las Entidades Federativas, Municipios y Alcaldías de la Ciudad de México, en materia de prevención para la Ciberseguridad.

Artículo 59. Los convenios que se suscriban tendrán por objeto:

I. Difundir las acciones y medidas que se estén implementado para la Ciberseguridad;

II. Informar sobre ciberamenazas a la Ciberseguridad, que involucren a personas, empresas o al territorio de específico de cada Entidad Federativa, y

III. Intercambiar información que pueda resultar de utilidad para prevenir ciberamenazas a la Ciberseguridad.

TRANSITORIOS

PRIMERO. El presente Decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

SEGUNDO. Se derogan todas aquellas disposiciones que se opongan al presente Decreto.

TERCERO. El Reglamento de la presente Ley, deberá expedirse dentro de los seis meses siguientes a la entrada en vigor de esta.

CUARTO. La aprobación de la estrategia en materia de Ciberseguridad por el Consejo Nacional de Seguridad Pública deberá ser aprobada dentro de los seis meses, contados a partir de la entrada en vigor del presente Decreto.

QUINTO. El protocolo para compartir información de ataques cibernéticos deberá ser aprobado dentro de los ciento ochenta días siguientes a la entrada en vigor de la estrategia de Ciberseguridad; y en el mismo plazo de ciento ochenta días siguientes a la entrada en vigor de la mencionada estrategia, deberán ser aprobados los Lineamientos del Centro de Comando y Control en Ciberseguridad.

SEXTO. El Centro de Comando y Control en Ciberseguridad deberá estar funcionando, dentro de los noventa días siguientes a la aprobación de los Lineamientos del mismo.

SÉPTIMO. La Red de Colaboradores Comunitarios en Ciberseguridad deberá estar en funcionamiento dentro de los seis meses siguientes a la entrada en vigor del presente Decreto.

OCTAVO. La Fiscalía Especializada en Delitos Cibernéticos deberá estar en funcionamiento dentro de los seis meses siguientes a la entrada en vigor del presente Decreto.

NOVENO. Los Juzgados Federales Especializados en materia Cibernética deberán estar en funcionamiento dentro de los seis meses siguientes a la entrada en vigor del presente Decreto.

Dado en el Salón de Sesiones del Palacio Legislativo de San Lázaro a los 03 días del mes de octubre del 2022.

Suscribe