CÁMARA DE DIPUTADOS
LXV LEGISLATURA

Gaceta Parlamentaria

Año XXVI | Palacio Legislativo de San Lázaro, martes 25 de abril de 2023 | Número 6262-II-2

CONTENIDO

Anexo II-2

Martes 25 de abril

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

Quien suscribe, **Diputado Javier Joaquín López Casarín**, integrante del Grupo Parlamentario del Partido Verde Ecologista de México, de la LXV Legislatura del honorable Congreso de la Unión, con fundamento en lo dispuesto por los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, así como 6, numeral 1, fracción I, 77 y 78 del Reglamento de la Cámara de Diputados, somete a la consideración de esta asamblea la presente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE DE LEY FEDERAL DE CIBERSEGURIDAD**, al tenor de la siguiente:

Exposición de Motivos

En los últimos años, el uso de las tecnologías de información y telecomunicaciones (TIC), se han desarrollado de manera acelerada.

Hoy en día, los sectores productivos de los países, los servicios en los ámbitos social, político, económico, cultural y de seguridad, se llevan a cabo por medio de infraestructuras tecnológicas que almacenan, procesan y transmiten información.

En esta era digital, el uso de las tecnologías ha transformado la forma en que las personas interactúan, en el trabajo, estudio, en su vida familiar y en cómo se comunican con su entorno, el cual, por medio del internet no se reduce al físico inmediato sino al ciberespacio que por tanto genera acceso a una conexión global.

A nivel mundial, este ciberespacio, se ha constituido por tanto, en un entorno virtual de desarrollo, integrado por redes de computadoras y telecomunicaciones, tecnologías de operación (TO) usadas en la industria, pero también, por cualquier dispositivo por pequeño que sea, capaz de almacenar, procesar o transmitir información, incluidos los dispositivos de Internet de las Cosas (Internet of Things o IoT) que son dispositivos de uso común y de la vida diaria como bocinas, cámaras, puertas, refrigeradores, automóviles, etc, con capacidades de comunicarse y conectarse con redes de computadoras, principalmente Internet.

Cada vez más, los servicios vitales para la sociedad están siendo dependientes de las infraestructuras tecnológicas, a tal grado, que fallas en ellas, pueden causar enormes daños humanos y financieros, e inclusive riesgos a la seguridad nacional.

De acuerdo a la Unión Internacional de Telecomunicaciones (UIT), se estima que, en el 2021, cerca de 4.9 billones de personas en todo el mundo tienen acceso a internet, lo que representa aproximadamente el 60% de la población mundial.

La Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) realizada por el INEGI, estimó que en México en 2021 había 88.6 millones de personas usuarias de internet, lo que representa el 75.6 %

de la población de seis años o más, siendo esta cifra 4.1 puntos porcentuales mayor respecto a la de 2020. (71.5 %)[1]

En el resguardo e intercambio de datos e información en la red, a través de los distintos protocolos utilizados, existen riesgos de intrusión, robo, suplantación, manipulación, entre otros; para proteger a los sistemas informáticos de cualquiera de estos ataques, se aplican un conjunto de procesos, prácticas y tecnologías diseñadas para salvaguardar la confidencialidad, integridad y disponibilidad de los datos y sistemas de información, a estas medidas se le denomina ciberseguridad.

La ciberseguridad implica el uso de herramientas de seguridad informática, como firewalls, software antivirus, autenticación, cifrado de datos, con el fin de resguardar, prevenir, detectar y responder a amenazas cibernéticas.

La implementación de políticas y procedimientos de seguridad cibernética, la capacitación de los usuarios sobre buenas prácticas de seguridad en línea y la realización de evaluaciones y pruebas de seguridad para identificar y mitigar vulnerabilidades son elementos imprescindibles en un entorno adecuado de ciberseguridad, lo anterior derivado de la creciente cantidad de información que se maneja en línea, incluyendo información confidencial de empresas, de los propios

[1] https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/OtrTemEcon/ENDUTIH_21.pdf

usuarios, y de las entidades de gobierno, pudiendo algunas de ellas en caso de ser afectadas representar riesgos de seguridad nacional.

Para la UIT, 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 usuarios en el ciberentorno”[2].

Para el Estado mexicano, la importancia de la seguridad informática, radica en que, a través del llamado ciberespacio, fluye la información prácticamente de forma instantánea, lo que conlleva grandes beneficios, pero al mismo tiempo se convierte en un reto, si no se consideran los riesgos de seguridad que implican los medios digitales.

El uso natural de dispositivos electrónicos para la vida diaria como lo son teléfonos, tabletas, relojes y bocinas inteligentes, sólo por mencionar algunos, hace que perdamos de vista que todo el tiempo se genera y recopila información a través de ellos.

Es importante considerar que muchos datos tales como información personal, financiera, de salud, y del trabajo que viven en los dispositivos electrónicos pueden

[2] Unión Internacional de Telecomunicaciones (UIT). https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

vulnerar al dueño de la información, en caso de que las condiciones de seguridad no sean las adecuadas.

En este sentido la ciberseguridad se ha convertido en una prioridad para los gobiernos y sociedades de todo el mundo; la cual radica en integrar los diferentes esfuerzos legislativos, técnicos y humanos a fin de mitigar posibles riesgos y amenazas que están presentes en la red.

Actualmente, el objetivo principal de muchos grupos de hackers y otros antagonistas son las infraestructuras críticas y los servicios esenciales a la población.

Durante 2022 ha sido evidente el incremento de la actividad por parte de grupos APT (Amenaza Persistente Avanzada, por sus siglas en inglés Advanced Persistent Threat), cuyos ataques han afectado incluso a la estabilidad de algunos Estados Nación, el ejemplo más claro es la actual guerra entre Rusia y Ucrania, que ha puesto de manifiesto el potencial dañino de los ciberataques.

La Ciberseguridad es la piedra angular para evitar ataques en contra de la confidencialidad, integridad y disponibilidad de la información al permitir dotar a los equipos técnicos y humanos de las capacidades y legislación necesaria para combatir eficazmente los riesgos cibernéticos.

Por lo que debe existir un marco legislativo robusto en la materia que apoye y dé certidumbre a todas las entidades que participan en las tareas asignadas, es por esto y ante las condiciones actuales, que es importante materializar los esfuerzos encaminados hacia el fortalecimiento de la ciberseguridad en México.

La pandemia COVID-19 acrecentó la dependencia de los sistemas digitales, acelerando el trabajo remoto y con ello la adopción de plataformas y dispositivos que permiten que los datos confidenciales sean compartidos por terceros, mediante intermediarios relacionados con tecnología como servicios en la nube, aplicaciones, interfaces de programación (API), entre otras.

Un problema importante que tiene México, para organizar y establecer la ciberseguridad en el país y para combatir y sancionar las actividades irregulares o lesivas en el internet consiste en establecer una adecuada definición de los delitos cometidos mediante el uso de las tecnologías de la información, también llamados ciberdelitos ya que no hay una legislación específica.

Adicionalmente, la definición de delitos cibernéticos no guarda homogeneidad con los conceptos establecidos en otros países, lo que dificulta también que el país se integre a iniciativas legales internacionales, lo que permitiría sancionar a los cibercriminales independientemente de la nación en la que se encuentren. Como señala el Wilson Center's Mexico Institute, "si las leyes no se crean y fortalecen México puede ser un objetivo vulnerable para las amenazas de los agentes criminales"[3].

Entre las necesidades que se buscan cubrir a través del proyecto de Ley Federal de Ciberseguridad, se encuentra la definición de un modelo de operación de la Ciberseguridad en México, el cual abarca un amplio espectro de temáticas por

[3] Parragez Kobek, L. (2017). The State of Cybersecurity in Mexico: An Overview. México: Wilson Center's Mexico Institute.

resolver que van desde la seguridad individual de las personas, hasta la seguridad y defensa nacional del Estado, por lo que es necesario delimitar atribuciones, competencias y responsabilidades que permitan a cada uno de los actores involucrados tener una visión clara de los objetivos que tienen que cumplir para fortalecerla.

En ese sentido, se requiere de un organismo que coordine los diferentes esfuerzos a nivel nacional y que se encargue de generar estrategias y políticas públicas a seguir. Para tal efecto se considera pertinente crear una Agencia Nacional de Ciberseguridad.

Es necesario establecer convenios de colaboración que permitan al Estado mexicano, afrontar los delitos cibernéticos en todo el territorio nacional, buscando la homologación de estructuras, de criterios y de preparación de los impartidores de justicia.

Se requiere establecer las bases de colaboración del gobierno con la iniciativa privada a través de las diferentes cámaras industriales, empresas y la población, para combatir delitos cibernéticos en especial aquellos que puedan poner en riesgo el suministro de servicios básicos a la población y protección de infraestructuras críticas de información.

Actualmente no existe la obligación de reportar o denunciar incidentes que permita determinar de forma precisa el estado que guarda la ciberseguridad en nuestro país

por lo que es necesario contar con datos y estadísticas oficiales sobre incidentes y ciberdelitos ocurridos en México.

En la mayoría de los casos los organismos y personas que sufren incidentes omiten reportar este tipo de información ya sea por miedo a que afecte su reputación o prestigio, desconocimiento de los medios o simplemente consideran que, aunque lo reporten no será resuelto.

Es indispensable determinar un organismo encargado de concentrar la información sobre incidentes, ciberataques y delitos cibernéticos suscitados en organizaciones públicas y privadas, con lo cual se podrá constituir un parámetro para determinar el nivel de ciberseguridad del país y con ello tener un indicador para mejorarla día con día.

Para atender delitos cibernéticos trasnacionales o supranacionales que afecten al país u otros países de la comunidad internacional, es importante que México se adhiera a tratados internacionales, que posibiliten el castigo de los responsables.

Se requiere una regulación que obligue a los proveedores de servicios de comunicaciones y contenido de Internet, para que, con pleno respeto a los derechos humanos, brinden información relacionada con la investigación de delitos cibernéticos.

En ese mismo sentido, es necesario que las empresas extranjeras que brinden servicios en México, cuenten con representación jurídica en nuestro país, quien

deberá servir como punto de contacto y colaborar con las autoridades mexicanas, siempre que exista un ordenamiento legal de por medio.

Diferentes organizaciones civiles y periodistas, han manifestado que han visto afectada su esfera jurídica por intervenciones a sus comunicaciones, asimismo cada vez es más posible acceder a equipos y tecnología que tenga este tipo de capacidades tanto por grupos de delincuencia organizada como por actores que no tienen la facultad legal para utilizarla.

En ese sentido, es necesario regular la venta de tecnología para intervención de comunicaciones para dar certeza jurídica a los ciudadanos mexicanos; sin vulnerar las capacidades y facultades de las dependencias que tiene la posibilidad legal de utilizarlos, con pleno apego a los derechos humanos.

Si bien existen diferentes instrumentos jurídicos a nivel federal y local que regulan algunas conductas relacionadas con delitos informáticos; estos se encuentran desagregados y no son homogéneos.

Lo anterior, dificulta la procuración de justicia quedando impunes la mayor parte de las conductas ilícitas cometidas a través del ciberespacio; lo cual se agrava por la falta de profesionalización por parte de jueces, ministerios públicos y ausencia de una cultura de ciberseguridad entre la ciudadanía que desconoce los mecanismos legales existentes.

Bajo este contexto resulta indispensable emitir una Ley Federal de Ciberseguridad, para lograr un entendimiento común entre todos los sectores interesados, impulsar

la profesionalización del poder judicial, establecer a una Agencia de Ciberseguridad que sea el responsable en la materia, así como constituir la bases para la generación de estrategias, y políticas públicas desarrolladas con la participación de los tres órdenes de gobierno, sector privado y sociedad en general.

Durante el primer semestre de 2022, México sufrió 85 mil millones de intentos de ciberataques, lo que representó un incremento del 40%, con relación al mismo periodo en 2021; con lo cual se considera que fue el país más atacado en América Latina, seguido por Brasil con 31.5 mil millones de ciberataques durante el mismo periodo de tiempo y Colombia en tercer lugar con 6.3 mil millones.[4]

De acuerdo con el informe de la Junta Internacional de Fiscalización de estupefacientes 2021, perteneciente a la ONU, el uso de criptomonedas y el ciberespacio es cada vez más frecuente entre las organizaciones criminales en México, que se disputan el control de los enormes mercados delictivos de drogas, armas, sexo y personas, “lavan” aproximadamente 25,000 millones de dólares al año, utilizando monedas electrónicas y el ciberespacio para su compunción y ejecución de actividades ligadas con estos ilícitos.[5]

De acuerdo al Informe “El Estado del Ransomware 2022” de Sophos, 74% de las empresas mexicanas fueron víctimas de este tipo de ataque, quienes realizaron un pago promedio de $482,446 dólares para restaurar el acceso a sus datos.[6]

[4] https://www.idc.com/getdoc.jsp?containerId=prLA49766122

[5] https://www.incb.org/documents/Publications/AnnualReports/AR2021/Annual_Report/E_INCB_2021_1_spa.pdf

[6] https://assets.sophos.com/X24WTUEQ/at/npk6g4rwkmqc4s5j7hcrvfpn/sophos-state-of-ransomware-2022-wpes.pdf

La CONDUSEF registró un total de 24,215 fraudes bancarios y 76,000 denuncias por presuntos fraudes en 2021; en lo que va de la pandemia se totalizan 252,170 denuncias.[7]

Conforme al Censo Nacional de Seguridad Pública Federal 2021 (INEGI)[8], la Guardia Nacional atendió los siguientes incidentes:

1. Tentativa de extorsión telefónica (48,099);
2. Delitos en Internet (4,996);
3. Investigaciones cibernéticas (1,104);
4. Sitios web desactivados (5,920);
5. Reportes de Incidentes electrónicos (21,290)
6. Incidentes de seguridad informática (133,469).

Por otra parte, los problemas asociados a la falta de ciberseguridad ocupan el 8º riesgo a nivel mundial de acuerdo al Reporte de Riesgos Global 2023 del Foro Económico Mundial.[9]

Contar con una Ley Federal de Ciberseguridad es imprescindible para dar atribuciones jurídicas a la entidad encargada de la ciberseguridad en el país y certidumbre jurídica a ciudadanos y autoridades para la atención de los delitos cibernéticos.

[7] https://www.condusef.gob.mx/documentos/comercio/FraudesCiber-1erTrim2021.pdf

[8] https://www.inegi.org.mx/contenidos/programas/cnspf/2021/doc/cnspf_2021_resultados.pdf

[9] https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf?_gl=1*i5iw4z*_up*MQ..&gclid=EAIaIQobChMIoPW3hs-W_gIVuQznCh1_qA7GEAAYASAAEgJJifD_BwE

Las principales afectaciones por grupos de Amenazas Persistentes Avanzadas (APT) en México en los últimos años han sido por orden cronológico:

1. Ataque al sistema de interconexión de bancos comerciales al sistema financiero de pagos electrónicos interbancarios (SPEI) en donde hubo un robo de 300 millones de pesos. (mayo 2018)
2. Petróleos Mexicanos fue víctima de ransomware (Doppel Paymer) afectando al 5% de sus computadoras y vulnerando 60 áreas. (noviembre 2019)
3. La Secretaría de Economía sufrió un ataque cibernético en algunos servidores, sin embargo, la información sensible de sus usuarios no se vio comprometida. (febrero 2020)
4. La Secretaría del Trabajo y Previsión Social informó que parte de su infraestructura de cómputo fue afectada lo que provocó que algunos servidores dejaran de operar correctamente. (marzo 2020)
5. El Instituto Nacional de Migración sufrió un ciberataque sin que la secrecía de la información relacionada con trámites migratorios fuera vulnerada. (abril 2020)
6. Ciberataque a la Comisión Nacional para la Protección y Defensa de los Usuario de Servicios Financieros por parte del grupo Anonymous. (julio 2020)
7. El Banco de México fue objeto de un intento de ataque cibernético, lo cual provocó fallas e intermitencias en sus sistemas. (julio 2020)
8. Hackeo a la Lotería Nacional por el grupo ruso Avaddon. (junio 2021)
9. Afectación de 12 empresas del sector industrial y manufacturero por parte del grupo BlackCat. (abril 2022)

10. Afectación de empresas en CDMX, Veracruz, Hidalgo, Sinaloa, Querétaro y Nuevo León por el grupo LAPSUS$. (junio 2022)
11. Afectación a la fábrica Foxconn México por el grupo ruso Lockbit (junio 2022)
12. Robo de información del Buró de Crédito del historial crediticio de decenas de miles de personas del año 2016 (febrero 2023).

Derivado de todo lo anteriormente expuesto, podemos concluir que México al igual que todos los países de la comunidad internacional ha experimentado un desarrollo económico y social gracias a las TIC y TO, de tal forma que varias de sus actividades vitales están soportadas por estas tecnologías, lo que ahora constituyen infraestructuras críticas de información (ICI), y cuyo daño provoca impactos negativos para el funcionamiento de los servicios básicos de la sociedad y del gobierno, poniendo en riesgo la estabilidad, integridad y permanencia del Estado mexicano.

Es de suma importancia destacar que en la actualidad la mayoría de incidentes o ciberdelitos no se reportan o se denuncian, lo que significa que las estadísticas pueden subestimar la magnitud real del problema.

De igual forma, el Internet de las cosas (IoT o Internet of Things), que se refiere a la interconexión de objetos cotidianos a Internet, representará nuevas vías para delinquir y mayores riesgos, por lo que se requerirá aún más la consolidación de iniciativas integrales de ciberseguridad para la coordinación en la atención de ciberdelitos que atenten contra la seguridad nacional.

La Iniciativa de Ley Federal de Ciberseguridad tiene como parte de su objeto, el aumentar la seguridad cibernética bajo un esquema de corresponsabilidad, prevención, combate y persecución de los delitos cibernéticos o ciberdelitos, a su vez la protección de datos personales y el respeto a los derechos humanos.

Por lo aquí expuesto, someto a la consideración de esta asamblea el siguiente:

PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE CIBERSEGURIDAD

Artículo Único. Se expide la Ley Federal de Ciberseguridad, para quedar como sigue:

LEY FEDERAL DE CIBERSEGURIDAD
TÍTULO PRIMERO
DISPOSICIONES GENERALES

Artículo 1. Las disposiciones de la presente Ley son de orden público y observancia general en todo el territorio nacional en materia de Ciberseguridad y tienen por objeto:

I. Definir las instituciones responsables de la Ciberseguridad, así como los principios y lineamientos generales a los que debe sujetarse la Política Nacional en la materia;

II. Establecer las facultades, atribuciones, competencias y coordinación entre las dependencias y entidades de la Administración Pública Federal, así como sentar las bases de colaboración con Entidades Federativas, Organismos Constitucionales Autónomos, Academia e instancias del Sector privado del país;

III. Establecer las bases para la prevención y persecución de los delitos cibernéticos, así como el marco regulatorio que fortalezca el ciclo de gestión de incidentes cibernéticos y resiliencia cibernética;

IV. Establecer y coordinar el marco regulatorio de prevención, vigilancia y control sobre infraestructuras críticas de información;

V. Establecer los derechos y obligaciones de los usuarios en el Ciberespacio;

VI. Establecer las bases para el fomento de una cultura de Ciberseguridad;

VII. Definir las facultades, atribuciones y funciones de las autoridades dentro de su ámbito de competencia y los derechos y obligaciones de las personas y las entidades privadas responsables que cuenten, posean o administren tecnologías de la información y comunicación;

VIII. Impulsar la organización, capacidad operativa, integralidad, transversalidad y profesionalización de las instituciones de la Administración Pública Federal, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e instancias del Sector privado del país;

IX. Establecer las bases para sancionar conductas ilícitas en materia de Ciberseguridad; y

X. Penalizar actividades cibernéticas ilegales y otorgar atribuciones a las autoridades encargadas de perseguirlas, con respeto a las garantías procesales, el derecho a la intimidad, las libertades civiles y los derechos humanos.

Artículo 2. Las acciones en materia de Ciberseguridad que regula la presente Ley se rigen por los principios de legalidad, objetividad, profesionalismo, eficiencia, honradez y respeto a los Derechos Humanos.

Artículo 3. Para los efectos de esta Ley, se entenderá por:

I. **Activo**: Una persona, estructura, instalación, información y registros, sistemas y recursos de tecnología de la información, material, proceso, relaciones o reputación que tiene valor para quien lo posee, utiliza o administra.

II. **Agencia:** Agencia Nacional de Ciberseguridad.

III. **Aplicaciones**: Programa o conjunto de programas informáticos que realizan el procesamiento de registros para una función específica, diseñado para el beneficio del usuario final.

IV. **Autenticación**: Procedimiento para comprobar fehacientemente la identidad de un usuario para acceder a un dispositivo, aplicación, sistema, plataforma o servicio en línea, mediante conocimiento, basado en: información que solo conoce el usuario, pertenencia, basado en algo que posee el usuario, o característica, basada en alguna característica del usuario como datos biométricos.

V. **Autenticidad**: característica de la seguridad informática que se refiere a la comprobación y confirmación de la identidad real de los activos.

VI. **Base de Datos**: Recopilación de datos estructurados almacenados de manera digital.

VII. **CERT-MX:** Centro Nacional de Respuesta a Incidentes Cibernéticos de la Guardia Nacional.

VIII. **Ciberamenaza:** fuente potencial interna o externa a través del Ciberespacio, con capacidad de provocar un funcionamiento incorrecto, pérdida de valor o efecto adverso en los activos.

IX. **Ciberataque**: intento deliberado de obtener acceso a un sistema informático sin autorización o provocar su mal funcionamiento, sirviéndose de técnicas y vulnerabilidades para realizar actividades con fines maliciosos

X. **Ciberdefensa**: capacidad de un Estado sujeto de derecho internacional traducida en acciones, recursos y mecanismos en materia de Seguridad y Defensa nacionales en el ciberespacio, para prevenir, identificar y neutralizar Ciberamenazas o Ciberataques, incluidos los que atentan contra Infraestructuras Críticas de Información nacionales.

XI. **Ciberespacio**: entorno o ámbito intangible de naturaleza global, soportado por las Tecnologías de la Información y Comunicaciones, en el que se comunican e interactúan las entidades públicas, privadas y la sociedad en general, haciendo uso del ejercicio de sus derechos y libertades.

XII. **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 cualquier organización y usuarios en el ciberespacio.

XIII. **Comisión o CITICSI:** Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información.

XIV. **Confidencialidad**: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

XV. **Datos Informáticos**: información en formato electrónico que permite su recuperación o transmisión, incluyendo cantidades, caracteres o símbolos, en forma de señales eléctricas o grabación en medios magnéticos, ópticos o mecánicos

XVI. **Delitos cibernéticos o ciberdelitos**: Acciones u omisiones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicación y que se encuentran tipificados en algún código penal u otro ordenamiento nacional.

XVII. **Disponibilidad**: Capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

XVIII. **Dispositivo**: Combinación de diversos elementos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas para cumplir un propósito específico

XIX. **Entorno Digital**: Conjunto de canales, plataformas y herramientas que dispone cualquier individuo, marcas o negocios para tener presencia en Internet.

XX. **Estrategia Nacional de Ciberseguridad**: Documento que establece la visión, principios y objetivos del Estado Mexicano alineados a las prioridades en materia de Ciberseguridad.

XXI. **Evidencia Digital**: Información almacenada de forma binaria que puede ser utilizada en una investigación o procedimiento legal.

XXII. **Incidentes de Ciberseguridad o incidentes cibernéticos**: uno o varios eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer o comprometan las operaciones organizacionales y amenazar la seguridad de la información.

XXIII. **Infraestructuras Críticas de Información**: Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de Tecnologías de Información y Comunicaciones, y de Tecnologías de Operación TO, cuya afectación, interrupción o destrucción, tendría un impacto en la provisión de bienes y prestación de servicios públicos o privados esenciales que pudieran comprometer la Seguridad Nacional en términos de las leyes en la materia.

XXIV. **Integridad**: propiedad de la información, por la que se garantiza la exactitud de los datos transmitidos o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.

XXV. **Instancias de Seguridad Nacional**: instituciones o autoridades que en función de sus atribuciones participan directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional.

XXVI. **Ley**: Ley Federal de Ciberseguridad.

XXVII. **Medio de almacenamiento informático**: Dispositivo que escribe y lee datos digitales en un soporte de forma temporal o permanente, siendo su funcionamiento de tipo mecánico o electrónico.

XXVIII. **No repudio**: La garantía de que una parte no puede negar posteriormente los datos de origen; provisión de prueba de la integridad y el origen de los datos y que puede ser verificada por un tercero.

XXIX. **Operaciones militares en el Ciberespacio**: Actividades que realiza el Estado-Nación en o a través del ciberespacio, para proporcionar seguridad a la sociedad. Para las fuerzas armadas son consideradas como operaciones militares en el ciberespacio en el cumplimiento de las misiones encomendadas.

XXX. **Riesgo**: La posibilidad de que una amenaza aproveche una vulnerabilidad y cause un determinado impacto, pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información.

XXXI. **Seguridad de la Información**: La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, trazabilidad y no repudio de la misma.

XXXII. **Sistema de Información o Sistema Informático**: Conjunto de aplicaciones, servicios, activos de tecnologías de información u otros componentes para el manejo de información.

XXXIII. **Sistema o medio Telemático**: Sistema que combina los sistemas de telecomunicaciones e informáticos como método para transmitir la información.

XXXIV. **TIC o Tecnologías de la Información y Comunicación**: Conjunto diverso de herramientas y recursos tecnológicos utilizados para transmitir, almacenar, crear, compartir o intercambiar información o datos.

XXXV. **Tecnología para Intervención de comunicaciones:** Todo equipo, medio, dispositivo, o software resultado de la evolución tecnológica que, permita el intercambio de datos, información, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real.

XXXVI. **Telecomunicaciones**: Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión.

XXXVII. **Usuario**: Persona, entidad, o proceso autorizado para acceder a un sistema de información.

XXXVIII. **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Artículo 4. En lo no previsto por la presente Ley, se aplicarán, conforme a su naturaleza y de forma supletoria, las disposiciones contenidas en:

I. La Ley General del Sistema Nacional de Seguridad Pública;

II. La Ley de Seguridad Nacional;

III. La Ley de la Guardia Nacional;

IV. La Ley Federal de Telecomunicaciones y Radiodifusión;

V. La Ley Federal de Transparencia y Acceso a la Información Pública;

VI. La Ley General de Transparencia y Acceso a la Información Pública;

VII. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; y

VIII. La Ley Federal de Protección de Datos Personales en Posesión de Particulares.

TÍTULO SEGUNDO
DE LA POLÍTICA NACIONAL DE CIBERSEGURIDAD

Artículo 5. El Estado establecerá una Política Nacional de Ciberseguridad que contendrá las acciones necesarias para reducir riesgos cibernéticos, proteger la información, los bienes, los derechos de las personas y su seguridad.

Artículo 6. El objetivo de la Política Nacional de Ciberseguridad es establecer un sistema de responsabilidad compartida entre los actores públicos, privados y sociales que permita reducir los incidentes y la posible comisión de delitos, a través de la coordinación y atención de los riesgos cibernéticos.

Artículo 7. En el desarrollo de la Política Nacional de Ciberseguridad se deberán considerar como ejes rectores, el cumplimiento normativo, gestión del riesgo, educación, capacitación, fortalecimiento de la cultura, economía, industria, salud, mejora continua, el respeto y protección a los derechos humanos.

Artículo 8. La Política Nacional de Ciberseguridad promoverá:

I. Que todas las personas tienen derecho a la Ciberseguridad y el respeto irrestricto de sus derechos humanos relacionados con las comunicaciones que transmitan y reciban a través de Internet, y en cualquier otro medio o tecnología de información digital y de telecomunicaciones;

II. Que todos los sectores participen en el desarrollo de una Estrategia Nacional de Ciberseguridad incluyente, de acuerdo con el Sistema de Planeación Nacional;

III. Que se contribuya al diseño de mecanismos encaminados a la reducción de vulnerabilidades en las infraestructuras tecnológicas;

IV. El acceso a Internet y disponibilidad de servicios de telecomunicaciones;

V. El respeto a los derechos humanos durante la investigación y persecución de Ciberdelitos;

VI. El combate a la delincuencia organizada y la trata de personas;

VII. Que la seguridad de la información e infraestructura tecnológica sea responsabilidad de aquel que la ofrece, administra u opera, con independencia de la naturaleza pública o privada del organismo;

VIII. Que los responsables de Infraestructura Crítica de Información actúen diligentemente y adopten medidas necesarias para mitigar incidentes de Ciberseguridad o de ciberataques y su posible propagación a otros sistemas informáticos;

IX. Que los responsables de Infraestructura Crítica de Información públicos y privados tengan la obligación de cooperar con la autoridad para resolver los incidentes de Ciberseguridad y cooperar entre diversos sectores, en caso de ser necesario, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.

CAPÍTULO I
DE LA COMISIÓN INTERSECRETARIAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, Y DE LA SEGURIDAD DE LA INFORMACIÓN

Artículo 9. La Comisión, es un órgano gubernamental consultivo en la materia, y estará conformada por:

a) Titular de la Coordinación de Estrategia Digital Nacional, quien la presidirá.

b) Titulares de las Unidades de Tecnologías de la Información y Comunicación, y Seguridad de la Información o equivalentes de la unidad administrativa y dependencias siguientes:

I. Oficina de la Presidencia de la República;

II. Secretaría de Gobernación;

III. Secretaría de Relaciones Exteriores;

IV. Secretaría de la Defensa Nacional;

V. Secretaría de Marina;

VI. Secretaría de Seguridad y Protección Ciudadana;

VII. Secretaría de Hacienda y Crédito Público;

VIII. Secretaría de Bienestar;

IX. Secretaría de Medio Ambiente y Recursos Naturales;

X. Secretaría de Energía;

XI. Secretaría de Economía;

XII. Secretaría de Agricultura y Desarrollo Rural;

XIII. Secretaría de Infraestructura, Comunicaciones y Transportes;

XIV. Secretaría de la Función Pública;

XV. Secretaría de Educación Pública;

XVI. Secretaría de Salud;

XVII. Secretaría del Trabajo y Previsión Social;

XVIII. Secretaría de Desarrollo Agrario, Territorial y Urbano;

XIX. Secretaría de Cultura;

XX. Secretaría de Turismo;

XXI. Consejería Jurídica del Ejecutivo Federal;

XXII. Centro Nacional de Inteligencia;

XXIII. Agencia Nacional de Ciberseguridad;

XXIV. Servicio de Administración Tributaria;

XXV. Consejo Nacional de Ciencia y Tecnología;

XXVI. Instituto Mexicano del Seguro Social;

XXVII. Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado;

XXVIII. Petróleos Mexicanos; y

XXIX. Comisión Federal de Electricidad.

c) Titulares de:

I. La empresa productiva subsidiaria de la Comisión Federal de Electricidad, CFE Telecomunicaciones e Internet para Todos, y

II. La Comisión Nacional de Mejora Regulatoria.

Las personas integrantes de la Comisión tendrán derecho a voz y voto.

En sus ausencias temporales por causas justificadas, podrán ser suplidos por la persona servidora pública con nivel inmediato inferior a quien designen como suplente.

Artículo 10. La Comisión podrá invitar a sus sesiones, a propuesta de cualquiera de sus integrantes, a:

I. Titulares de Tecnologías de Información y Comunicaciones, y Seguridad de la Información o equivalentes de otras entidades de la Administración Pública Federal;

II. Representantes de los órganos constitucionales autónomos;

III. Autoridades de los gobiernos de las entidades federativas y de los municipios o demarcaciones territoriales de la Ciudad de México;

IV. Integrantes del Poder Judicial de la Federación y de las Comisiones Legislativas del Honorable Congreso de la Unión, y

V. Representantes de los sectores académico, social y privado.

VI. Dichas representaciones participarán con derecho a voz, pero sin voto.

Artículo 11. En materia de Ciberseguridad, la CITICSI tendrá las siguientes atribuciones:

I. Fungir como instancia de coordinación entre las autoridades responsables de la implementación y desarrollo de acciones en materia de tecnologías de la información y comunicación, así como de la seguridad de la información, en la Administración Pública Federal;

II. Participar en la implementación de estrategias y acciones interinstitucionales para el uso de las tecnologías de la información y comunicación, y de la seguridad de la información;

III. Impulsar y coordinar con los sectores público, privado, académico y social el desarrollo de estudios y actividades relacionadas con el aprovechamiento de las tecnologías de la información y comunicación, y de la seguridad de la información;

IV. Emitir los lineamientos para su organización y funcionamiento;

V. Crear las subcomisiones y grupos de trabajo que estime necesarios para el cumplimiento de sus funciones;

VI. Emitir los manuales o, en su caso, los lineamientos o políticas de organización y funcionamiento de las subcomisiones y grupos de trabajo que sean creados por la Comisión;

VII. Solicitar a las subcomisiones y grupos de trabajo que para tal efecto instaure, la elaboración de documentos, estudios, proyectos, y lineamientos necesarios para mejorar las tecnologías de la información y comunicación, y de la seguridad de la información en la Administración Pública Federal;

VIII. Recibir y analizar los informes de actividades y, en su caso, aprobar los acuerdos, informes y documentación que les sean presentados por las subcomisiones y grupos de trabajo creados por la Comisión;

IX. Participar en la elaboración de la Política Nacional de Ciberseguridad;

X. Coadyuvar con la Agencia en la definición, implementación y evaluación de la Estrategia Nacional de Ciberseguridad;

XI. Colaborar con la Agencia para el desarrollo de mecanismos estandarizados de Ciberseguridad, programas de capacitación, concientización, investigación y desarrollo, así como para la armonización del orden jurídico interno;

XII. Promover la colaboración y participación en los temas de Ciberseguridad de autoridades de las entidades federativas, los municipios y las demarcaciones territoriales de la Ciudad de México; y

XIII. Las demás que sean necesarias para el cumplimiento de su objeto.

Artículo 12. Los miembros de la CITICSI, así como de los grupos o Subcomisiones que al efecto se conformen, deberán adoptar las medidas necesarias para garantizar la reserva de la información a la que tengan acceso durante el desempeño de las tareas a su cargo, en cumplimiento de las disposiciones de la presente Ley y demás disposiciones aplicables.

CAPÍTULO II
DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD

Artículo 13. La Agencia Nacional de Ciberseguridad, dependerá directamente del Titular del Ejecutivo Federal.

La Agencia contará con las siguientes atribuciones:

I. Coordinar el desarrollo, implementación, evaluación, actualización y mejora continua de la Estrategia Nacional de Ciberseguridad;

II. Solicitar a los participantes de la CITICSI, aportaciones en el ámbito de sus respectivas atribuciones, para la integración de la Estrategia Nacional de Ciberseguridad;

III. Generar un Registro de Centros de Respuesta a Incidentes Cibernéticos Públicos y Privados.

IV. Establecer los esquemas de coordinación e intercambio de información entre los Centros de Respuesta a Incidentes Cibernéticos Públicos y Privados, establecidos en el país;

V. Establecer esquemas de cooperación con organismos internacionales y autoridades extranjeras en materia de Ciberseguridad;

VI. Desarrollar, implementar, evaluar y actualizar las disposiciones de seguridad de la información, estándares y guías en materia de Ciberseguridad;

VII. Diseñar criterios técnicos para la detección, monitoreo, pronóstico y medición de riesgos en las tecnologías de la información y comunicaciones;

VIII. Analizar y proponer la armonización legal en materia de Ciberseguridad;

IX. Promover mecanismos de certificación en materia de Ciberseguridad;

X. Promover entre las instituciones y entidades de la Administración Pública Federal el desarrollo de programas de capacitación de Ciberseguridad;

XI. Operar el Registro Nacional de Incidentes de Ciberseguridad;

XII. Requerir en el marco del Sistema Nacional de Seguridad Pública a las autoridades y particulares, la información sobre incidentes cibernéticos ocurridos dentro de su infraestructura tecnológica para establecer las acciones que correspondan;

XIII. Fungir como órgano de consulta y coordinación de acciones del gobierno federal y de las entidades federativas para convocar, concertar, inducir e integrar las actividades de los diversos participantes e interesados en materia de Ciberseguridad;

XIV. Promover la generación de estadísticas en materia de ciberseguridad e incidentes cibernéticos;

XV. Promover el desarrollo y consolidación de una cultura nacional de Ciberseguridad;

XVI. Promover y facilitar la denuncia ciudadana;

XVII. Definir los mecanismos de seguridad tecnológica con los que deberán cumplir los dispositivos electrónicos que se comercialicen en México;

XVIII. Dar seguimiento a la política de seguridad para las Infraestructuras Críticas de Información;

XIX. Integrar y mantener actualizado un Catálogo Nacional de Infraestructuras Críticas de Información; así como salvaguardar su confidencialidad, integridad y disponibilidad;

XX. Definir medidas estandarizadas de seguridad de las Infraestructuras Críticas de Información;

XXI. Apoyar, en el ámbito de sus atribuciones, a las autoridades competentes en el análisis de riesgos de las Infraestructuras Críticas de Información;

XXII. Promover mecanismos de prevención, atención y respuesta frente a ataques cibernéticos contra las Infraestructuras Críticas de Información, en coordinación con las instancias competentes;

XXIII. Fortalecer las actividades de inteligencia en materia de Ciberseguridad;

XXIV. Promover campañas nacionales de prevención de delitos cibernéticos;

XXV. Establecer mecanismos permanentes de comunicación con los operadores de las Infraestructuras Críticas de Información para, en su caso, promover la emisión de alertas tempranas;

XXVI. Colaborar con las instancias de seguridad nacional y administradores de las Infraestructuras Críticas de Información, en la atención de incidentes cibernéticos, así como promover ejercicios y simulacros para su protección;

XXVII. Elaborar el mapa de riesgos de las Infraestructuras Críticas de Información;

XXVIII. Promover la creación de un Consejo Consultivo Ciudadano de Ciberseguridad, que estimule la participación de todos los sectores de la sociedad;

XXIX. Establecer los Protocolos y mecanismos ágiles que garanticen la preservación de la Evidencia Digital por los propietarios de infraestructura, plataformas y servicios y contenidos en Internet, en términos de la legislación aplicable;

XXX. Solicitar la baja inmediata a proveedores de servicio o administradores, de direcciones IP, aplicaciones, dominios y sitios de internet a través de los cuales se realicen conductas ilícitas; y

XXXI. Las demás que establezcan otras disposiciones legales y las que sean necesarias para el desarrollo de la Política Nacional de Ciberseguridad.

CAPÍTULO III
DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Artículo 14. Corresponderá a la Agencia Nacional de Ciberseguridad, formular, conducir e impulsar el cumplimiento de una Estrategia Nacional de Ciberseguridad, misma que será actualizada de acuerdo con el Sistema Nacional de Planeación, y contendrá al menos, lo siguiente:

I. Un diagnóstico general sobre Ciberseguridad en el país, así como la prospectiva de largo plazo;

II. Objetivos específicos, acciones y autoridades de la Federación responsables de su ejecución;

III. Los indicadores estratégicos que permitan dar seguimiento al logro de los objetivos;

IV. Mecanismos para la generación de esquemas de cooperación nacional e internacional en materia de Ciberseguridad;

V. Promover mecanismos para prevenir y combatir los ciberdelitos;

VI. Desarrollo de una industria de la ciberseguridad;

VII. Acciones de capacitación, asistencia, intercambio de información, tecnología y cualquier otro fin relacionado con el análisis y desarrollo de esquemas estandarizados de Ciberseguridad, así como con el uso y protección de las Tecnologías de la Información y Comunicaciones;

VIII. Acciones para la prevención de riesgos, amenazas y vulnerabilidades de los sistemas informáticos, digitales y de las telecomunicaciones tanto públicas como privadas;

IX. Definir esquemas de información y participación ciudadana, mecanismos de proximidad para atender a la población, así como acciones tendientes al fomento de la cultura de Ciberseguridad que contemplen orientar y concientizar a la población sobre la importancia de la ciberseguridad, impulsar el desarrollo y aplicación de criterios homologados en la materia y promover programas de capacitación para una efectiva adopción y cumplimiento de mecanismos de ciberseguridad; y

X. Las demás que se consideren necesarias.

Artículo 15. Las acciones contempladas en la Estrategia Nacional de Ciberseguridad serán de carácter obligatorio para las dependencias y entidades de la Administración Pública Federal y de carácter indicativo para las entidades federativas, municipios, demarcaciones territoriales de la Ciudad de México y para los tres órdenes de gobierno, órganos constitucionales autónomos y particulares.

CAPÍTULO IV
DEL REGISTRO NACIONAL DE INCIDENTES DE CIBERSEGURIDAD

Artículo 16. El Registro Nacional de Incidentes de Ciberseguridad se integrará con la información de los eventos que representan algún ataque, delito cibernético o evento que haya provocado una interrupción o degradación importante o relevante a la operación dentro de la infraestructura tecnológica de un organismo público o privado.

Artículo 17. El Registro Nacional de Incidentes de Ciberseguridad, será administrado por la Agencia Nacional de Ciberseguridad y tendrá el carácter de reservado, con la finalidad de salvaguardar la confidencialidad de los entes que compartan información.

Artículo 18. Para la conformación del Registro, están obligados a entregar información a la Agencia:

I. La Secretaría de Seguridad y Protección Ciudadana, lo correspondiente al Registro Nacional de Incidentes Cibernéticos;

II. El CERT-MX, todos los incidentes de ciberseguridad que le sean reportados;

III. Las dependencias de la Administración Pública Federal, respecto de sus incidentes de Ciberseguridad;

IV. El Poder Judicial de la Federación todos los incidentes de ciberseguridad que le sean reportados; y

V. Los administradores de Infraestructuras Críticas de Información públicos y privados, todos aquellos incidentes de ciberseguridad que hayan puesto en riesgo su operación o datos personales;

Artículo 19. El Registro estará conformado por los incidentes de Ciberseguridad reportados por los estados de la República, municipios, demarcaciones territoriales de la Ciudad de México y de los poderes legislativo, judicial federales y locales, órganos constitucionales autónomos, con los que la Agencia haya celebrado convenios de colaboración, e instituciones particulares.

TÍTULO TERCERO
DE LA DISTRIBUCIÓN DE COMPETENCIAS

CAPÍTULO I
DE LA SEGURIDAD NACIONAL

Artículo 20. Para efectos de la presente Ley, se consideran amenazas a la Seguridad Nacional en materia de Ciberseguridad, aquellas que:

I. Comprometan la operación y capacidades de las instancias de seguridad nacional;

II. Potencialicen el impacto de amenazas previstas en la Ley de Seguridad Nacional, y

III. Afecten el funcionamiento de algún sistema o Infraestructura Crítica de Información.

Artículo 21. Cuando se investiguen amenazas inminentes y concretas a la seguridad nacional, las entidades públicas y privadas proporcionarán de manera inmediata la información que les sea solicitada, en términos de las disposiciones jurídicas y administrativas aplicables.

Artículo 22. Corresponde a las instancias de seguridad nacional, dentro del ámbito de sus competencias, coordinar las acciones necesarias para prevenir y contener cualquier amenaza cibernética que pudiera constituir un riesgo a la seguridad nacional.

CAPÍTULO II
DE LA SEGURIDAD PÚBLICA

Artículo 23. Las instituciones de seguridad pública de los tres órdenes de gobierno se coordinarán en el marco del Sistema Nacional de Seguridad Pública, para:

I. Suministrar e intercambiar la información obtenida mediante los sistemas e instrumentos tecnológicos respectivos;

II. Generar y difundir campañas orientadas a prevenir y evitar el fenómeno delictivo en materia de Ciberseguridad;

III. Establecer relaciones de colaboración con las autoridades competentes, así como con las organizaciones sociales y privadas con el objetivo de orientar a la sociedad en las medidas que deben adoptar para prevenir los delitos establecidos en esta Ley u otros ordenamientos legales;

IV. Coadyuvar en la generación del Registro Nacional de Incidentes Cibernéticos; y

V. Observar las demás obligaciones establecidas en otros ordenamientos.

Artículo 24. La Fiscalía General de la República contará con una fiscalía especializada cuyas funciones serán investigar y perseguir los delitos cibernéticos, interviniendo en todas las etapas del procedimiento penal y realizando todas las actuaciones procesales aplicables.

Artículo 25. En el marco del Sistema Nacional de Seguridad Pública, se promoverá:

I. La creación de procuradurías o fiscalías estatales especializadas para la investigación de las conductas en materia de Ciberseguridad, promoviendo Ministerios Públicos y policías especializados, recursos humanos, financieros y materiales que requieran para su efectiva operación.

II. La operación de al menos una unidad de policía Cibernética en las entidades federativas, cuyo objetivo será prevenir, por medio del monitoreo y ciber patrullaje en el ciberespacio, cualquier situación constitutiva de un delito que pudiera poner en riesgo la integridad física y/o patrimonial de los habitantes; asimismo, 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, acopio y análisis de información.

Artículo 26. Las Unidades de Policía Cibernética de los Estados formarán parte de una Red que se coordinará con el CERT-MX y con la Agencia, con el fin de compartir información sobre incidentes, alertas, actores, entre otros datos que puedan ser relevantes en un proceso de investigación.

Estos entes, serán los encargados de operar el Modelo Homologado de Unidades de Policía Cibernética.

Artículo 27. El Poder Judicial de la Federación contará con jueces especializados en materia de ciberseguridad, los cuales conocerán de:

I. Los procedimientos que deriven de la presente Ley y demás legislación relacionada y aplicable en la materia;

II. Las medidas cautelares para los ciberdelitos; y

III. Las diligencias en la materia.

CAPÍTULO III
DE LA CIBERDEFENSA

Artículo 28. Corresponderá a la Secretaría de la Defensa Nacional y la Secretaría de Marina en el ámbito de sus competencias y a través de las unidades administrativas que determinen sus titulares, la atención de los incidentes cibernéticos que provengan o sean promovidos por otros Estados sujetos de derecho internacional, para lo cual contarán con las atribuciones siguientes:

I. Monitorear el ciberespacio para prevenir, identificar y neutralizar ciberamenazas y ciberataques;

II. Considerar dentro de su planeación estratégico-militar a las operaciones militares en el ciberespacio;

III. Establecer convenios de colaboración con otros países en materia de ciberdefensa y operaciones militares conjuntas en el ciberespacio;

IV. Desarrollar y ejecutar mecanismos para la ciberdefensa del país;

V. Ejercer el derecho de legítima defensa ante toda ciberamenaza y ciberataque que ponga en riesgo la soberanía, los intereses nacionales, las Infraestructuras Críticas de Información;

VI. Realizar operaciones militares y navales en el ciberespacio, a fin de disminuir los riesgos en materia de Ciberseguridad;

VII. Coadyuvar en coordinación con las entidades y autoridades competentes, en la gestión de riesgos y gestión de incidentes que afecten la seguridad nacional;

VIII. Establecer mecanismos permanentes de comunicación con los operadores de las Infraestructuras Críticas de Información para, en su caso, emitir alertas tempranas y recomendaciones;

IX. Crear unidades para llevar a cabo operaciones militares en el ciberespacio, en cumplimiento de las misiones conferidas en sus Leyes Orgánicas, así como organizar, equipar, mantener dichas unidades y adiestrar continuamente al personal dedicado a estas actividades; y

X. Las demás que le confieran esta ley u otros ordenamientos aplicables.

CAPÍTULO IV
DE LA CIBERSEGURIDAD EN LA ADMINISTRACIÓN PÚBLICA FEDERAL

Artículo 29. La Agencia Nacional de Ciberseguridad emitirá los criterios y las bases generales de seguridad para la protección de la información que generen y administren las dependencias y entidades de la Administración Pública Federal, los cuales serán de observancia obligatoria para éstas.

Artículo 30. Las dependencias y entidades de la Administración Pública Federal deberán cumplir con los requisitos mínimos de seguridad que, al efecto, determine la Agencia Nacional de Ciberseguridad, los cuales deberán considerar:

I. La designación de un responsable de la Seguridad de la Información;

II. El establecimiento de un Marco de Gestión de Seguridad de la Información;

III. El establecimiento de un equipo de respuesta a incidentes.

Artículo 31. El responsable de la Seguridad de la Información, deberá dar aviso inmediato a la Agencia Nacional de Ciberseguridad y al CERT-MX, sobre los incidentes cibernéticos que se presenten y deberá supervisar el cumplimiento del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.

Artículo 32. La Agencia Nacional de Ciberseguridad emitirá los protocolos de Seguridad de la Información que deberán observar las dependencias y entidades de la Administración Pública Federal para la gestión de riesgos y de incidentes.

Artículo 33. La Agencia Nacional de Ciberseguridad promoverá la creación de Centros de Respuesta a Incidentes Cibernéticos, mismos que serán establecidos conforme a los sectores que ésta determine.

CAPÍTULO V
DE LAS INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN

Artículo 34. La protección de las Infraestructuras Críticas de Información estará a cargo de aquellas entidades públicas o privadas que las administren.

Artículo 35. La Agencia Nacional de Ciberseguridad integrará y administrará un Catálogo Nacional de Infraestructuras Críticas de Información en términos de la presente Ley, su Reglamento y demás disposiciones que al efecto se emitan.

Artículo 36. La Agencia Nacional de Ciberseguridad emitirá los lineamientos para la identificación de Infraestructuras Críticas de Información y realizará la evaluación para la integración del Catálogo correspondiente.

Artículo 37. Los lineamientos para la identificación de Infraestructuras Críticas de Información deberán considerar al menos los siguientes aspectos:

I. La relación de sectores considerados críticos;

II. El impacto de una posible interrupción o mal funcionamiento de los componentes de la infraestructura de la información, a partir de la cantidad de usuarios potencialmente afectados y su extensión geográfica;

III. El efecto e impacto en la operación y servicios de sectores regulados cuya afectación es relevante para la población;

IV. La potencial afectación de la vida, integridad física o salud de las personas;

V. Las pérdidas financieras estimadas por fallas o ausencia del servicio a nivel nacional o regional asociada al producto interno bruto;

VI. El grado de afectación y relevancia del funcionamiento del Estado y sus órganos; y,

VII. Impacto en la seguridad nacional y el mantenimiento de la soberanía.

Artículo 38. Las autoridades de la federación, entidades federativas, órganos constitucionales autónomos y los particulares están obligados a evaluar sus infraestructuras e identificar si las mismas cumplen con los criterios establecidos para ser consideradas como Infraestructuras Críticas de Información, en cuyo caso deberán notificarlo a la Agencia, para su evaluación e inscripción en el catálogo correspondiente.

Artículo 39. Las autoridades de la federación, entidades federativas, órganos constitucionales autónomos y los particulares, que tengan a su cargo Infraestructuras Críticas de Información, designarán ante la Agencia Nacional de Ciberseguridad, a un enlace para el desarrollo de acciones de prevención y atención a incidentes cibernéticos.

Artículo 40. Todo aquel responsable de administrar Infraestructuras Críticas de Información que cumpla con los criterios establecidos por la Agencia Nacional de Ciberseguridad para ser identificados como tal, están obligados a:

I. Aplicar permanentemente medidas de seguridad tecnológica, organizacionales, físicas e informativas necesarias para prevenir, reportar y resolver incidentes de Ciberseguridad, así como gestionar riesgos para contener y mitigar el impacto sobre la continuidad operacional;

II. Aplicar medidas para salvaguardar la confidencialidad, integridad y disponibilidad de la información del servicio prestado;

III. Notificar ante la Agencia Nacional aquellos incidentes de Ciberseguridad considerados como relevantes, de acuerdo con los criterios a la que se refiere el artículo 38 de la presente Ley;

IV. Proporcionar información y apoyo a las autoridades para el seguimiento de casos de investigación;

V. Promover una cultura de Ciberseguridad y el desarrollo de normatividad interna que se haga del conocimiento de los empleados, proveedores y usuarios;

VI. Realizar continuamente revisiones, ejercicios, simulacros y análisis, a fin de fortalecer las medidas de protección;

VII. Cumplir con lo establecido en el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos y lo demás establecido en esta Ley o en otros ordenamientos aplicables;

VIII. Designar un encargado de cumplimiento para la atención y respuesta a incidentes cibernéticos;

IX. Establecer un domicilio en territorio nacional, para oír y recibir notificaciones de la autoridad; y

X. Las demás establecidas en la presente Ley, u otros ordenamientos legales.

Artículo 41. La información del Catálogo Nacional de Infraestructuras Críticas de Información será tratada con el carácter de reservada por motivos de Seguridad Nacional, debido a que su revelación indebida podría potenciar una amenaza que ponga en entredicho la integridad, permanencia y estabilidad del Estado mexicano.

Artículo 42. Cuando exista un riesgo a la seguridad nacional, las Secretarías de la Defensa Nacional y de Marina, así como la Guardia Nacional y el Centro Nacional de Inteligencia, en el ámbito de sus competencias, podrán solicitar a la Agencia Nacional de Ciberseguridad el acceso a la información contenida en el Catálogo Nacional de Infraestructuras Críticas de Información.

Artículo 43. Los servidores públicos que tengan acceso al Catálogo Nacional de Infraestructuras Críticas de Información, y a cualquier dato proporcionado por los enlaces responsables de las mismas, deberán abstenerse de difundir la información ahí contenida, y adoptar las medidas necesarias para evitar su publicidad. Además, deberán suscribir una promesa de confidencialidad que se mantendrá vigente en todo tiempo, aún después de que hayan cesado en el cargo en razón del cual se les otorgó el acceso.

TÍTULO CUARTO
PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

CAPÍTULO I
DE LOS DERECHOS Y OBLIGACIONES

Artículo 44. Conforme a los derechos consignados en la Constitución Política de los Estados Unidos Mexicanos, todas las personas tendrán los siguientes derechos digitales:

I. Acceder a servicios de tecnologías de la información y comunicación de calidad, en un entorno de inclusión digital, neutralidad e igualdad en la red, así como libertad para utilizar el sistema y hardware que deseen, siempre y cuando sea lícito;

II. A la no discriminación para el acceso e interacción en medios digitales;

III. A la libertad de expresión en medios digitales y derecho de acceso a la información;

IV. A la protección de sus datos personales en el entorno digital, en términos de lo dispuesto en la Ley aplicable en la materia;

V. A la libertad de conciencia y de religión en el entorno digital;

VI. A la libertad de reunión y asociación en línea;

VII. A la privacidad digital;

VIII. A la protección de la personalidad virtual;

IX. A contar con una identidad digital;

X. A una vida digital libre;

XI. A la defensa de su integridad en medios digitales;

XII. A la protección de sus datos digitales;

XIII. A recibir educación, acceso al conocimiento, cultura y trabajo a través de Internet y otros medios digitales;

XIV. A la reserva de la información que se brinde a la autoridad de aquellos datos sobre incidentes cibernéticos en los que hayan sido víctimas;

XV. A la protección de los derechos de los teletrabajadores en términos de lo dispuesto en la Ley aplicable en la materia;

XVI. A la protección de los derechos de los consumidores en Internet, en términos de lo dispuesto en la Ley aplicable en la materia;

XVII. A que la información recopilada por las empresas que brindan servicios tecnológicos no sea utilizada para fines distintos a los autorizados;

XVIII. Al comercio electrónico legal a través del ciberespacio en términos de lo dispuesto en la Ley aplicable en la materia; y

XIX. Las demás que le confieran esta Ley u otros ordenamientos aplicables.

Artículo 45. Las obligaciones de los usuarios de servicios digitales son:

I. Respetar los derechos de los demás usuarios;

II. Utilizar los servicios digitales con responsabilidad y sólo para fines lícitos;

III. Utilizar la identidad digital sólo para fines lícitos;

IV. Acceder a los servicios de tecnologías de información y comunicaciones, así como cualquier otro servicio digital de manera legal; y

V. Cooperar con las autoridades competentes, ante cualquier investigación en materia de ciberseguridad.

CAPÍTULO II
DE LA PROTECCIÓN DE DATOS PERSONALES

Artículo 46. Las autoridades federales que tengan acceso a información relacionada con datos personales de los usuarios en sus sistemas informáticos, implementarán controles de prevención, detección y corrección que resulten apropiados para salvaguardarlos, incluyendo medidas de atención y respuesta ante incidentes.

Artículo 47. Las empresas que brinden servicios de infraestructura digital y telecomunicaciones dentro del territorio nacional, de redes sociales, aplicaciones o contenido de Internet como correo, blogs, mensajería instantánea, alojamiento web, deberán guardar la confidencialidad de la información de datos personales de los usuarios, y no divulgarla, compartirla o hacer mal uso de ella.

Artículo 48. Los datos personales estarán sujetos a:

I. El uso lícito y transparente en relación con el interesado;

II. Fines determinados, explícitos y legítimos;

III. Las condiciones de operación estrictamente indispensables para el operación u otorgamiento del servicio;

IV. Actualización;

V. Temporalidad; y

VI. Resguardo a través de medidas de seguridad adecuadas, incluyendo métodos de cifrado robustos y la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas apropiadas.

Artículo 49. En caso de violación de la seguridad de los datos personales, el responsable del manejo de los mismos, lo notificará a la Agencia Nacional de Ciberseguridad, a más tardar 72 horas después de que haya tenido conocimiento, a efecto de realizar el análisis de riesgos correspondiente y determinar las acciones que en su caso ameriten.

Artículo 50. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del manejo de los datos, lo comunicará al interesado, a más tardar 72 horas después de que haya tenido constancia de ella.

Artículo 51. Se considerarán reservados, para todos los efectos legales, los antecedentes, datos y registros que obren en poder de la Agencia Nacional de Ciberseguridad, la Red de Policías Cibernéticas y el CERT-MX.

Los servidores públicos, que hubieren tenido conocimiento de este tipo de información, estarán obligados a mantener la confidencialidad de su existencia y contenido aun después del término de sus funciones en sus respectivos servicios, la falta de cumplimiento de este precepto será sancionada de acuerdo al Capítulo correspondiente.

La obligación referida en el párrafo anterior, se extiende a toda persona que, de acuerdo a sus funciones, competencia o prestación de un servicio conozca dicha información.

Artículo 52. Con independencia de la clasificación de información reservada, prevista en otras disposiciones, deberá otorgarse tal carácter a aquella que en materia de ciberseguridad pueda comprometer un servicio o sistema informático, señalando de manera enunciativa, más no limitativa:

I. Las matrices de riesgos de ciberseguridad;

II. Los planes de continuidad operacional y planes de prevención de desastres;

III. Los planes de acción y atención de riesgos de ciberseguridad, y

IV. Los reportes de incidentes de ciberseguridad.

TÍTULO QUINTO
DE LA PRESTACIÓN DE SERVICIOS, USO DE INFRAESTRUCTURA DIGITAL Y TELECOMUNICACIONES

Artículo 53. Los proveedores de servicios de infraestructura digital, plataformas de redes sociales, comunidades de videojuegos en línea, streaming, plataformas de entretenimiento en línea y telecomunicaciones que operen en territorio nacional están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezca la Constitución Política de los

Estados Unidos Mexicanos y demás leyes. Para lo cual estarán sujetos a las siguientes obligaciones específicas:

I. Contar cuando menos con una representación legal con presencia física en el territorio nacional;

II. Contar con una unidad de cumplimiento para la atención y respuesta de incidentes de ciberseguridad;

III. Registrarse ante la Agencia Nacional de Ciberseguridad;

IV. Establecer medidas de autenticación y cifrado para el acceso a servicios donde se ingresen datos personales;

V. Establecer en sus servicios medidas de seguridad tecnológica, que permitan salvaguardar la integridad, confidencialidad y disponibilidad de la información de los usuarios;

VI. Notificar ante el CERT-MX y a la Agencia, cualquier incidente de ciberseguridad en la operación o prestación de su servicio que represente un riesgo relevante de conformidad con los lineamientos a los que hace referencia el artículo 38 de la presente Ley;

VII. Dar aviso a los usuarios, respecto a incidentes cibernéticos que puedan tener impacto en la privacidad o protección de sus datos, o en la continuidad del servicio;

VIII. Privilegiar que la información de los usuarios se encuentre almacenada en territorio nacional;

IX. En caso de que la información contenga datos que pudieran vulnerar la seguridad nacional, deberá almacenarse en territorio nacional;

X. Informar a los usuarios de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de seguridad de la información y permitan, entre otros, la protección frente a códigos maliciosos;

XI. Informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para los menores de edad;

XII. Facilitarán información a los usuarios acerca de las posibles responsabilidades en que puedan incurrir por el uso indebido de sus servicios, en particular, para la comisión de delitos y vulneración de la legislación en materia de propiedad intelectual e industrial;

XIII. Dar de baja direcciones IP, aplicaciones, dominios y sitios de internet dentro de las 72 horas posteriores a la notificación que le realicen la Agencia, la Fiscalía General de la República, CERT-MX y autoridades judiciales competentes para su inhabilitación

XIV. Conservar la información sobre las IP y datos de registro; y

XV. Establecer un acuerdo de corresponsabilidad y confidencialidad en el caso de realizar actos de subcontratación o intermediación sobre el uso o distribución de bases de datos e información digital.

Lo anterior, sin perjuicio en lo dispuesto por la Ley Federal de Telecomunicaciones y Radiodifusión y demás leyes en la materia.

Artículo 54. De conformidad con el principio de cooperación internacional, los proveedores de servicios y plataformas constituidas en el extranjero que tengan y operen plataformas, sistemas de información, productos o servicios digitales a través de Internet o algún otro medio tecnológico que cuenten con usuarios registrados y activos en México, podrán ser requeridos mediante orden judicial, a colaborar con las autoridades mexicanas de procuración de justicia o encargadas de la seguridad pública y nacional, según corresponda en términos de las disposiciones aplicables en la materia.

Para efectos del párrafo anterior, los proveedores antes citados, deberán sujetarse a lo dispuesto en el Título Octavo “De la Colaboración con la Justicia”, de la Ley Federal de Telecomunicaciones y Radiodifusión.

Artículo 55. Los proveedores de servicios bancarios y financieros están obligados a establecer las medidas de Ciberseguridad necesarias para evitar fraudes electrónicos en las plataformas y los servicios que prestan.

Artículo 56. Los proveedores que desarrollen, operen, comercialicen o pretendan comercializar la tecnología a que se refiere el artículo 3 fracción XXXV, dentro del territorio nacional, están obligados a inscribirse en el Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones y, a comercializar dicha tecnología únicamente con las autoridades con competencia legal.

Artículo 57. El Centro Nacional de Inteligencia conformará el Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones, en términos de lo dispuesto en el Reglamento de la presente Ley.

Artículo 58. La información contenida en el Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones será tratada con el carácter de reservada por motivos de Seguridad Nacional, debido a que su revelación indebida podría actualizar o potenciar una amenaza que ponga en riesgo la integridad, permanencia y estabilidad del Estado mexicano.

Artículo 59. El uso de Tecnología para Intervención de Comunicaciones es exclusivo para las Instituciones de seguridad pública o nacional; las autoridades observarán en todo momento el respeto a las formalidades legales, y los derechos humanos, por lo que su venta queda prohibida para fines distintos a los establecidos.

TÍTULO SEXTO
DE LA CULTURA Y EDUCACIÓN

Artículo 60. Los poderes de la Unión, en el ámbito de sus respectivas atribuciones, desarrollarán y difundirán una cultura de ciberseguridad, con el objetivo de:

I. Orientar y concientizar a la población sobre la importancia de la ciberseguridad en los ámbitos público y privado;

II. Promover la adopción de mecanismos de seguridad en los sistemas informáticos de cualquier individuo u organización pública o privada;

III. Impulsar el desarrollo y aplicación de criterios homologados de seguridad para la protección de la información en el ciberespacio~~;~~

IV. Informar qué áreas y procedimientos institucionales existen para denunciar una posible vulnerabilidad o amenaza en materia de ciberseguridad;

V. Promover programas de capacitación para una efectiva adopción y cumplimiento de los mecanismos de ciberseguridad en el ejercicio de sus funciones;

VI. Impulsar el desarrollo científico y tecnológico en la materia; y

VII. Los demás que se identifiquen para consolidar una cultura de ciberseguridad en el país.

Artículo 61. Corresponde a las instituciones públicas y privadas de educación, investigación e innovación:

I. Desarrollar programas educativos y de profesionalización, en todos los niveles de escolaridad, que fomenten una cultura de ciberseguridad;

II. Proporcionar acciones formativas a todo el personal de los centros educativos, en materia de ciberseguridad;

III. Fomentar a través de los Centros de Investigación y demás instituciones educativas públicas y privadas, la cultura en materia de ciberseguridad, y

IV. Participar como asesores para la implementación de políticas públicas en materia de ciberseguridad.

TÍTULO SÉPTIMO
DE LAS INFRACCIONES Y SANCIONES

Artículo 62. Los administradores de Infraestructuras Críticas de Información, los proveedores de servicios e instancias públicas y privadas que incumplan con los dispuesto en los artículos 18, 38, 39, 40, 43, 53, 54, 55 y 56 podrán ser acreedores a multas de mil a veinte mil veces el valor diario de la Unidad de Medida y Actualización, por parte de la Agencia.

Artículo 63. A fin de que la calificación de la sanción sea proporcional a la conducta respectiva, la Agencia tomará en cuenta los siguientes criterios:

I. Si el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones;

II. La probabilidad de ocurrencia del riesgo;

III. La gravedad de los efectos de los ataques;

IV. La reiteración en la infracción dentro del plazo de tres años; y

V. La capacidad económica del infractor.

Artículo 64. Las infracciones cometidas por funcionarios de la Administración Pública Federal y demás autoridades competentes para la imposición de las sanciones se regirán por los procedimientos para el establecimiento de sanciones

respectivos en términos de la normatividad y considerando el fuero que corresponda.

TÍTULO OCTAVO
DE LOS DELITOS CIBERNÉTICOS

CAPÍTULO I
DE LOS DELITOS CONTRA LA CIBERSEGURIDAD

SECCIÓN PRIMERA
De los delitos contra la Confidencialidad, Integridad y Disponibilidad

Artículo 65. Al que por cualquier medio o método, sin autorización o excediendo de la autorización que posea de la persona física o moral que legalmente pueda otorgarlo, dolosamente acceda, copie, extraiga, modifique, altere, destruya o elimine la información provocando la pérdida de la confidencialidad, integridad y disponibilidad de la misma contenida en equipos, sistemas o medios informáticos, electrónicos o telemáticos, que estén protegidos o no por un mecanismo de seguridad, se le impondrán de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

Artículo 66. Al que con motivo de la conducta descrita en el artículo 61, cifre, exfiltre y/o controle o manipule el funcionamiento de cualquier dispositivo electrónico que forme parte interna o externa del sistema informático con la finalidad de obligar a otro de hacer o dejar de hacer, usar o no divulgar información obtenida, o bien para obtener un lucro indebido o cualquier tipo de beneficio para sí o para un tercero, se sancionará con pena de diez a quince años de prisión y multa de quince mil a veinticinco mil unidades de actualización.

Artículo 67. La sanción a las conductas descritas en los artículos 61 y 62 se incrementarán en una mitad, cuando el acceso ilícito y el lucro indebido, beneficio, uso divulgación de información, provengan de personas físicas o morales contratadas para proporcionar servicios de seguridad de la información.

SECCIÓN SEGUNDA
Del ataque a la integridad de un Sistema Informático

Artículo 68. Al que sin autorización o excediendo de la autorización que posea, de la persona física o moral que legalmente pueda otorgarlo, obstaculice o impida mediante la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos, el funcionamiento total o parcial de un sistema informático,

electrónico o telemático, se le impondrá una pena de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

SECCIÓN TERCERA
De la interceptación de datos

Artículo 69. Quien a través de cualquier medio o método, intercepte sin una orden judicial, cualquier tipo de datos informáticos, electrónicos telemáticos, incluidas las emisiones electromagnéticas y radiofrecuencias, originadas y/o provenientes desde otro sistema o equipo o realizadas dentro del mismo, se le impondrá de diez a veinte años de prisión y multa de diez mil a veinte mil unidades de medida de actualización.

Artículo 70. A quien sin tener facultades legales para tal efecto adquiera o arriende Tecnología para Intervención de Comunicaciones, se le impondrán de diez a veinte años de prisión y multa de diez mil a veinte mil unidades de medida de actualización.

Artículo 71. A quien sin estar registrado para tal efecto comercialice Tecnología para Intervención de Comunicaciones en territorio nacional, se le impondrán de diez a veinte años de prisión y multa de diez mil a veinte mil unidades de medida de actualización

SECCIÓN CUARTA
De la falsificación informática

Artículo 72. Quien sin autorización de la persona física o moral que legalmente pueda otorgarlo introduzca, altere, bloqueé, borre o suprima datos informáticos, electrónicos telemáticos previamente almacenados en un sistema o base de datos con la intención de que sean tomados como auténticos o utilizados como auténticos para efectos legales, con independencia de que los datos sean legibles e inteligibles directamente. Se le impondrá de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

SECCIÓN QUINTA
Del abuso de dispositivos tecnológicos.

Artículo 73. El que para la comisión de los delitos descritos en los artículos 61 a 68, produzca, venda, adquiera para su uso, importe, exporte programas informáticos, equipos, o dispositivos se sancionará con la pena de cinco a vente años de prisión y multa de mil a veinte mil unidades de medida de actualización.

Las disposiciones del presente artículo no se aplicarán a los casos cuando la producción, venta, adquisición para uso, importación, exportación u otras formas de

prestación para la utilización de los dispositivos estén relacionados, con una prueba autorizada para la identificación de vulnerabilidades con fines preventivos, capacitación o bien para innovación tecnológica, o cualquier otra actividad comercial lícita.

SECCIÓN SEXTA
Del fraude por medio informático.

Artículo 74. Al que por medio del engaño aprovechándose del error en que otro se halle, mediante cualquier medio método informático, electrónico o telemático obtenga cualquier bien o derecho patrimonial en perjuicio de un tercero o del Estado, será sancionado con pena de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

Esta pena se incrementará hasta en una mitad cuando el medio informático, electrónico o telemático utilizado, suplante la identidad de una Entidad del gobierno federal o estatal.

Artículo 75. A quien mediante el engaño, y a través de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, se haya allegado de información personal, documentos, datos financieros verdaderos o apócrifos con independencia de la autorización del titular, con el fin de vulnerar los mecanismos de gestión y/u obtener un beneficio económico a través del otorgamiento de créditos solicitados ante alguna entidad financiera o crediticia o de empresas de servicios de financiamiento tecnológico emergentes, para cobro a través de depósitos transferencias bancarias nacionales e internacionales de divisas o en su defecto mediante la conversión a algún tipo de moneda digital, se le impondrá una sanción de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

La sanción económica y pena se aumentará en una mitad, en los siguientes supuestos:

I. La conducta ha sido repetida en reiteradas ocasiones ante una misma o en diferentes instancias;

II. Exista el consentimiento de una de las partes involucradas para hacer mal uso de su información o datos;

III. Una de las partes involucradas trabajó o formó parte de algunas de las instancias vulneradas, y aprovechándose de sus conocimientos sobre el proceso de selección y tramites auxilió a vulnerar o facilitar de manera dolosa el otorgamiento de un crédito.

SECCIÓN SÉPTIMA
De los delitos contra la integridad y libertad de las personas

Artículo 76. Al que dolosamente trate datos personales mediante el engaño o aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos. Mediante las tecnologías de la información y comunicación, con la finalidad de obtener un lucro indebido o cualquier tipo de beneficio, se le impondrá de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

Por tratamiento deberá atenderse lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Artículo 77. El que se apropie de un medio de identificación de otra persona con el propósito de realizar cualquier acto ilícito, será sancionado con una pena de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

Para fines de este delito, medio de identificación debe entenderse como cualquier dato o información que pueda ser utilizado por sí o junto con otros para identificar a una persona de manera directa o indirecta en entornos digitales, además de datos biométricos, tales como huellas, grabación de voz, retina, imagen del iris o cualquier representación física particularizada.

Artículo 78. Al que describa, diseñe o grabe cualquier tipo de material digital, auditivo, fotográfico o video gráfico con el propósito de que sea exhibido, publicado o compartido a través de redes de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean producto de la evolución tecnológica mediante los cuales se incite, facilite, induzca u obligue a personas a ocasionar un daño físico, psicológico o material, a sí mismas o a terceros, se sancionará con una pena de tres a seis años de prisión y una multa de quinientas a mil unidades de medida y actualización.

No serán motivo de sanción aquellas expresiones que se realicen en apego a la libertad de expresión, siempre y cuando no inciten o consistan en terrorismo, o realicen la apología del odio nacional, racial, sexual o religioso, o constituya discriminación, hostilidad, instigación o realización de genocidio o de pornografía infantil.

Serán consideradas como incitación o realización de violencia aquellas acciones que de forma sistemática, automatizada e intencional desinformen a la población

provocando la manipulación individual o colectiva de las personas, transgrediendo los límites del derecho a la libertad de expresión.

Lo anterior, sin perjuicio de la responsabilidad civil por daños o perjuicios que se hayan podido generar con motivo de la conducta.

Artículo 79. A quien solicite, procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta, a realizar actos sexuales o de exhibición corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, audio grabarlos, fotografiarlos, filmarlos, transmitirlos, exhibirlos o describirlos, a través de anuncios impresos, sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, se le impondrá de siete a catorce años de prisión y multa de mil a diez mil unidades de medida de actualización, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales mencionados.

Si se hiciere uso de violencia física o moral o psicoemocional, o se aproveche de la ignorancia, extrema pobreza o cualquier otra circunstancia que disminuya o elimine la voluntad de la víctima para resistirse, la pena prevista en el párrafo anterior se aumentará en una mitad.

No constituye pornografía el empleo en los programas preventivos, educativos o informativos que diseñen e impartan las instituciones públicas, privadas o sociales, que tengan por objeto la educación sexual, educación sobre la función reproductiva, prevención de infecciones de transmisión sexual y embarazo de adolescentes.

Se impondrán las mismas sanciones a quien financie, elabore, reproduzca, almacene haciendo uso de algún servicio de alojamiento local o remoto en sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, distribuya, comercialice, arriende, exponga, publicite, difunda, adquiera, intercambie o comparta por cualquier medio el material a que se refieren las conductas anteriores

Artículo 80. A quien haciendo uso de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, contacte, incite, facilite, induzca u obligue a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho o a persona que no tenga capacidad para resistirlo, a realizar transmisión en vivo o video llamadas en tiempo real, o solicite archivos electrónicos de tipo imagen, audio, video, u otros, en los que aparezca la víctima realizando actividades sexuales

explícitas, actos de connotación sexual, actos de exhibición corporal con fines lascivos o sexuales, o le solicite un encuentro con propósitos sexuales, se le impondrá una pena de cinco a doce años de prisión y multa de mil a diez mil unidades de medida de actualización.

Para efectos de esta Ley Federal se entenderá por connotación sexual los actos que tengan como característica o finalidad conseguir una gratificación, o placer sexual para el espectador o escucha e inclusive para el sujeto activo.

Artículo 81. Comete el delito de turismo sexual quien promueva, publique, divulgue, publicite, invite, facilite o gestione haciendo uso de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, a que una o más personas viajen al interior o exterior del territorio nacional con la finalidad de que realice cualquier tipo de actos sexuales reales o simulados con una o varias personas menores de dieciocho años de edad, o con una o varias personas que no tienen capacidad para comprender el significado del hecho o acto o con una o varias personas que no tienen capacidad para resistirlo. A los responsables de este delito se les impondrá una pena de ocho a dieciocho años de prisión y multa de dos mil a quince mil unidades de medida de actualización.

Artículo 82. Cuando exista sentencia firme por cualquier delito comprendido en esta sección, la autoridad competente, ordenará el borrado seguro relacionado con pornografía infantil o en su caso la destrucción del dispositivo que contenga la información que haya motivado la sentencia del imputado y que se encuentre en poder o bajo control del Tribunal de Enjuiciamiento o del Ministerio Público.

SECCIÓN OCTAVA
De la propiedad intelectual

Artículo 83. Cuando las conductas descritas en la Ley Federal de Derechos de Autor y en la Ley de Propiedad Industrial, se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o en cualquiera de sus componentes, se sancionará con prisión de seis a doce años y con multa de dos mil a diez mil unidades de medida de actualización, sin perjuicio de las sanciones penales que sea procedente aplicar conforme a otras leyes, en apego al principio penal de especificidad que sobre conductas ilegales corresponde a esta Ley.

SECCIÓN NOVENA
De los sistemas bancarios, financieros, gubernamentales e infraestructuras críticas de información

Artículo 84. Al que dolosamente ponga en peligro o cause daño, altere u obstaculice por cualquier medio o método el funcionamiento de sistemas o medios informáticos, electrónicos o telemáticos de las instituciones que integran el sistema financiero, infraestructuras críticas de información o sistemas gubernamentales, se le impondrán de seis a veinte años de prisión y multa de cinco mil a veinte mil unidades de medida y actualización.

Artículo 85. A la persona que dolosamente, por cualquier medio o método, modifique, altere, destruya o provoque pérdida parcial o total de información contenida en sistemas o medios informáticos, electrónicos o telemáticos, de las instituciones que integran el sistema financiero, infraestructuras críticas de información o sistemas gubernamentales, se le impondrán de seis a veinte años de prisión y multa de cinco mil a veinte mil unidades de medida y actualización.

Artículo 86. Quien mediante el uso de tecnologías de la información y comunicación copie, extraiga, reproduzca, fabrique u obtenga ilícitamente un beneficio patrimonial, económico o de otra naturaleza para sí o para un tercero, así como por cualquier medio o método ilegalmente obtenga modifique dañe, altere o destruya parcial o totalmente información contenida en sistemas, equipos o medios informáticos, electrónicos o telemáticos, locales o remotos, de las instituciones que integran el sistema financiero, infraestructuras críticas de información o sistemas gubernamentales, se le impondrán de ocho a veinticinco años de prisión y multa de ocho mil a veinte mil unidades de medida y actualización.

Artículo 87. Como regla común y en cuanto a las penas previstas en esta sección se incrementarán las sanciones hasta en una mitad cuando las conductas sean cometidas por empleados o ex empleados de las instituciones que integran el sistema financiero.

Artículo 88. A los empleados o ex empleados de las empresas prestadoras de servicios tecnológicos que tengan o hayan tenido relación comercial o contractual con instituciones públicas, y del sistema financiero o de infraestructuras críticas de información, se les aumentará hasta una mitad de las penas previstas en el presente capítulo.

Artículo 89. Las penas a que se refiere el artículo anterior se incrementarán hasta en una mitad cuando los empleados hayan firmado un acuerdo o carta de confidencialidad.

CAPÍTULO II
DE LAS TÉCNICAS ESPECIALES DE INVESTIGACIÓN

Artículo 90. El Ministerio Público atendiendo a la urgencia del caso particular y con la debida diligencia, puede solicitar al juez de control la actuación de agentes encubiertos a efecto de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa en el ciberespacio o mediante tecnologías de la información y comunicación.

La orden judicial que autorice la realización de este acto de investigación, deberá indicar circunstanciadamente el nombre real, alias o nombre de usuario, dirección física o electrónica del afectado, señalar el tipo y la duración de la misma.

El juez de control competente, podrá prorrogar la duración de este acto de investigación, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en el párrafo anterior.

El agente encubierto en línea podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de referidas comunicaciones.

El agente encubierto estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.

CAPÍTULO III
REPARACIÓN DEL DAÑO

Artículo 91. El responsable de la comisión de un delito cibernético deberá resarcir los daños generados, como se describe a continuación:

I. Gastos generados para restituir el daño de la conducta, incluyendo el pago de cualquier deuda u obligación que haya adquirido, y

II. Gastos correspondientes a servicios médicos, psicológicos, psiquiátricos y todos aquellos que se generen con motivo de una afectación a la salud física o mental.

Artículo 92. Asimismo, la autoridad deberá:

I. Solicitar a las instancias competentes, la corrección de cualquier documento público o privado que contenga información falsa en perjuicio de la víctima;

II. Ordenará la cancelación de créditos que no hayan sido solicitados por la víctima, y

III. Ordenará la destrucción de los dispositivos con los cuales se haya cometido la conducta ilícita incluyendo la información contenida en éstos.

TRANSITORIOS

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

SEGUNDO. El Ejecutivo Federal expedirá y publicará el Reglamento de esta Ley dentro de los seis meses posteriores a la entrada en vigor del presente Decreto.

TERCERO. Se conformará la Agencia Nacional de Ciberseguridad dentro de los treinta y seis meses posteriores a la entrada en vigor del presente Decreto, en tanto sus funciones estarán a cargo de la Coordinación de la Estrategia Digital Nacional (CEDN) de Presidencia.

CUARTO. A la entrada en vigor del presente Decreto, la Fiscalía General de la República, contará con treinta y seis meses para implementar la fiscalía especializada en la materia.

QUINTO. A partir de la emisión de los Lineamientos que contienen los criterios para la clasificación de Infraestructuras Críticas de Información, los particulares contarán con doce meses para notificar ante la instancia competente las infraestructuras a su cargo.

SEXTO. El Centro Nacional de Inteligencia contará con 90 días posteriores a la publicación del presente Decreto para expedir las reglas de operación del Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones.

SÉPTIMO. Los proveedores que desarrollan, operan, proporcionan mantenimiento o comercializan Tecnología para Intervención de Comunicaciones dentro del territorio nacional, contarán con seis meses posteriores a la entrada en vigor del presente Decreto, para darse de Alta en el Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones.

OCTAVO. Las instituciones que previamente tengan Tecnología para Intervención de Comunicaciones, contarán con 60 días hábiles a partir de la entrada en vigor del presente Decreto, para informar al Centro Nacional de Inteligencia el nombre de los proveedores de la misma, así como el tipo y características de la tecnología adquirida.

Dado en el Salón de Sesiones del Palacio Legislativo de San Lázaro, a los 25 días de abril de 2023.

SUSCRIBE

DIPUTADO JAVIER JOAQUÍN LÓPEZ CASARÍN

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN, ADICIONAN Y DEROGAN DIVERSOS ARTÍCULOS DE LA LEY ORGÁNICA DE LA ADMINISTRACIÓN PÚBLICA FEDERAL, DE LA LEY ORGÁNICA DEL EJÉRCITO Y FUERZA AÉREA MEXICANOS, DE LA LEY DE AEROPUERTOS Y DE LA LEY DE AVIACIÓN CIVIL, EN MATERIA DE PROTECCIÓN DEL ESPACIO AÉREO MEXICANO

Quien suscribe, diputado federal del Grupo Parlamentario de MORENA para la LXV Legislatura del H. Congreso de la Unión, con fundamento en lo dispuesto por el artículo 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos así como los artículos 77 y 78 del Reglamento de la Cámara de Diputados, someto a consideración de está Soberanía la **Iniciativa con Proyecto de Decreto por el que se Reforman, Adicionan y Derogan Diversos Artículos de la Ley Orgánica de la Administración Pública Federal, de la Ley Orgánica del Ejército y Fuerza Aérea Mexicanos, de la Ley de Aeropuertos y de la Ley de Aviación Civil, en Materia de Protección del Espacio Aéreo Mexicano,** al tenor de lo siguiente:

EXPOSICIÓN DE MOTIVOS

La presente iniciativa tiene por objeto fortalecer el marco jurídico del Estado mexicano para garantizar el efectivo ejercicio de su soberanía y la integridad de su espacio territorial aéreo, así como la seguridad de la navegación de las aeronaves autorizadas para hacer uso de éste. Para tal propósito, se propone armonizar el marco jurídico administrativo de conformidad con la Ley de Protección del Espacio Aéreo Mexicano, publicada el 1 de marzo de 2023.

El territorio constituye uno de los elementos esenciales para la existencia de los Estados mismos. Se integra, por definición, por las aguas y subsuelos de los mares, la superficie terrestre y el espacio aéreo ubicado por encima de éstos, respecto de los cuales se ejerce jurisdicción soberana. Por este motivo, resulta de suma importancia que el Estado mexicano garantice la protección, vigilancia, seguridad y salvaguarda de su espacio aéreo.

En este sentido, el artículo 42, fracción VI, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) considera como parte del territorio nacional, el espacio situado sobre éste, con la extensión y modalidades que establece el derecho internacional. En consecuencia, y de acuerdo con el artículo 27, párrafo cuarto, de

la CPEUM, corresponde a la Nación el dominio directo sobre este espacio.

Legislación Internacional

En el ámbito internacional, la Carta de Naciones Unidas, en su artículo 1, establece el principio general de libre determinación de los pueblos, principio que reconoce la jurisdicción interna y, por tanto, soberana de cada Estado del orbe.

Por su parte, la Carta de Estados Americanos, en su artículo 13, señala que cada Estado tiene derecho a defender su integridad e independencia, a proveer su conservación y prosperidad y, por consiguiente, a organizarse como mejor lo entendiere, a legislar sobre sus intereses, a administrar sus servicios y determinar su jurisdicción, sin mayores límites que el ejercicio de los derechos de otros Estados. El precepto anterior reconoce la jurisdicción de los Estados para legislar, administrar y proteger su espacio aéreo con plena soberanía.

Por su parte, el Convenio sobre Aviación Civil Internacional[1] estipula que los Estados tienen soberanía plena y exclusiva en el espacio aéreo situado sobre su territorio. Este Convenio define al territorio de un Estado como las áreas terrestres y las aguas territoriales adyacentes a ellas que se encuentran bajo su soberanía, dominio, protección o mandato, incluyendo al espacio aéreo.[2]

La Convención de las Naciones Unidas sobre Derecho del Mar de 1982,[3] en su artículo 34, reconoce soberanía y jurisdicción de los Estados sobre sus aguas marítimas, así como el lecho, subsuelo y espacio aéreo situado sobre éstas. En este sentido, el respeto entre Estados independientes de dicha soberanía territorial constituye uno de los principios básicos para el correcto funcionamiento de las relaciones internacionales.

Este reconocimiento implica, además de la rectoría exclusiva del Estado sobre el espacio aéreo, la obligación de salvaguardar su integridad y emplear todos los recursos a su alcance para garantizar la seguridad en materia de navegación aérea y sancionar su uso con fines ilícitos.

---

[1] También conocido como "Convenio de Chicago", adoptado por la Conferencia de Aviación Civil Internacional el 7 de diciembre de 1944 y firmado por México en tal fecha. Fue publicado en el Diario Oficial de la Federación el 12 de abril de 1946.
[2] *Ibidem*, artículos 2 y 3, respectivamente.
[3] ONU. *Convención de las Naciones Unidas sobre el Derecho del Mar.* Adoptada en Ginebra, Suiza, el 10 de diciembre de 1982. Ratificada por México el 21 de febrero de 1983. Sección 1, Artículo 2, numeral 2.

El reconocimiento de los Estados sobre la necesidad de una reglamentación clara y precisa para prevenir eventuales actos ilícitos y violaciones al espacio aéreo por parte de aeronaves civiles ha dado lugar a la adopción de instrumentos internacionales complementarios bajo el marco de la Organización de Aviación Civil Internacional (OACI), entre ellos el Convenio de Chicago. La OACI reconoce la importancia de la seguridad y el fomento ordenado de la navegación y del transporte aéreo internacional. Este marco jurídico reafirma los intereses de los Estados con el ejercicio de su soberanía en el espacio aéreo, a la vez que atiende las preocupaciones legítimas de la comunidad internacional en materia de seguridad para la aviación civil.

Particularmente, el Convenio de Chicago, instrumento marco en la materia, tiene como uno de sus objetivos principales lograr la seguridad de la aviación civil internacional y que ésta pueda desarrollarse de manera segura y ordenada.[4] En este sentido, el Estado es responsable de prevenir, neutralizar o tomar medidas necesarias por razones de índole militar o de seguridad pública para evitar cualquier amenaza o interferencia ilícita al espacio aéreo bajo su dominio soberano y exclusivo.[5] Para tal propósito, una estrecha coordinación entre las autoridades civiles y militares constituye una necesidad básica frente a cualquier tipo de riesgos o actividades potencialmente peligrosas.[6]

De igual forma, la salvaguarda de la integridad territorial y la seguridad del espacio aéreo son un asunto de interés internacional, en tanto que constituyen aspectos interdependientes no sólo para garantizar el dominio soberano efectivo, sino también para la prevención de intervenciones e influencias externas no autorizadas en éste.

Desde esta perspectiva, cualquier violación a la integridad territorial o a la soberanía de un Estado sobre su espacio aéreo, es incompatible con los principios de la Carta

---

[4] Convenio de Chicago, *op. cit.*, Preámbulo.
[5] Convenio de Chicago, artículo 9. OACI. *Anexo 17 "Seguridad". Protección de la aviación civil internacional contra los actos de interferencia ilícita,* Décima segunda edición, julio de 2022, Capítulo 1. "Definiciones".
[6] *Cfr.* Organización de Aviación Civil Internacional (OACI). *Comunicación del Secretario General de la OACI, Raymond Benjamin, sobre la seguridad y protección de las aeronaves civiles que operan en el espacio aéreo afectado por conflicto,* An 13/4.2-14/59, 24 de julio de 2014, párrs. 2, 3 y 5. Disponible en: https://www.icao.int/Newsroom/NewsDoc2014/059e.pdf. En el mismo sentido: OACI. *Anexo 11 al Convenio sobre Aviación Civil Internacional*, decimocuarta edición, julio de 2016, Norma 2.18 "Coordinación entre las autoridades militares y los servicios de tránsito aéreo", pág. 2-10. Disponible en: https://www.anac.gov.ar/anac/web/uploads/normativa/anexos-oaci/anexo-11.pdf

de la Organización de los Estados Americanos, la Carta de las Naciones Unidas y el Convenio de Chicago de 1944, y constituye un riesgo para la seguridad operacional y la seguridad de la aviación civil internacional.

Legislación nacional

Para regular la administración del espacio aéreo, México emitió el 12 de mayo de 1995, la Ley de Aviación Civil que regula la explotación, uso y aprovechamiento del espacio aéreo situado sobre el territorio nacional, como vía general de comunicación, en relación con la prestación y desarrollo de los servicios de transporte aéreo civil y de Estado.

Dicho ordenamiento confiere a la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT) el carácter de autoridad aeronáutica, entre cuyas atribuciones se encuentra la de expedir y aplicar, en coordinación con las secretarías competentes, las medidas y normas de seguridad e higiene, de seguridad en la aviación civil y en materia ambiental, que se deben observar en los servicios de transporte aéreo, así como verificar su cumplimiento a través de la Agencia Federal de Aviación Civil.[7]

Asimismo, la Ley de Aviación Civil establece que en la prestación de los servicios de transporte aéreo se deben adoptar las medidas necesarias para garantizar las condiciones máximas de seguridad de la aeronave y de su operación, a fin de proteger la integridad física de las personas usuarias, de sus bienes y de terceras personas. Para tal propósito, dicha ley otorga a la SICT la facultad de exigir a las personas concesionarias, permisionarias y operadoras aéreas que cumplan con determinados requisitos, con el fin de mantener los niveles de seguridad señalados.

Adicionalmente, distintos instrumentos normativos complementarios, como el Programa Sectorial de Comunicaciones y Transportes 2020-2024,[8] y el Programa Nacional de Seguridad de la Aviación Civil[9] establecen las políticas de coordinación

---

[7] Ley de Aviación Civil, artículo 6, fracción V, y último párrafo.

[8] *Cfr.* Gobierno de México. Secretaría de Infraestructura, Comunicaciones y Transportes (SICT), *Programa Sectorial de Comunicaciones y Transportes 2020-2024*, publicado en el Diario Oficial de la Federación el 2 de julio de 2020. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/728510/SICT_PS_Avance_y_Resultados_2021.pdf

[9] *Cfr.* SICT. Programa Nacional de Seguridad de la Aviación Civil, publicado en el Diario Oficial de la Federación el 12 de junio de 2019. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5562535&fecha=12/06/2019#gsc.tab=0

entre las dependencias, organismos, empresas, personas concesionarias, permisionarias y prestadoras de servicios para el transporte aéreo nacional y extranjero en territorio nacional y cualquier otro organismo en seguridad de la aviación civil para implementar y cumplir con los estándares, métodos y procedimientos, tanto nacionales como internacionales.[10] Su propósito es fortalecer la efectividad de las acciones tendientes a garantizar la seguridad de la aviación civil, para prevenir y, en caso necesario, atender la comisión de actos de interferencia ilícita, preservando la regularidad y eficiencia del tránsito aéreo nacional e internacional y el ejercicio soberano del Estado mexicano sobre su espacio aéreo.

De acuerdo con la Ley Orgánica del Ejército y Fuerza Aérea Mexicanos (LOEFAM), la persona titular de la Secretaría de la Defensa Nacional (Sedena) es la responsable organizar, equipar, educar, adiestrar, capacitar, administrar y desarrollar al Ejército y Fuerza Aérea nacionales. Sin embargo, dicha normatividad no define las facultades que pueda desarrollar la Sedena en materia de protección al espacio aéreo. Por ello, se busca establecer en la legislación vigente las facultades de la Sedena que, por conducto de la Fuerza Aérea Mexicana, realiza en el ámbito de vigilancia, protección y defensa del espacio aéreo nacional, en coordinación con la SICT, su Agencia Federal de Aviación Civil (AFAC) y las dependencias que correspondan.

El 1 de marzo de 2023, se publicó la Ley de Protección del Espacio Aéreo Mexicano, cuyo objeto fue establecer y regular las medidas, acciones y procedimientos para preservar la seguridad y la soberanía e independencia nacionales de este espacio, por medio de la vigilancia y protección coordinada que realizan las distintas dependencias y entidades de la administración pública federal en el ámbito de sus respectivas competencias.

Con la presente iniciativa, se pretende armonizar el marco normativo con la nueva ley dirigido a adecuar las competencias de las dependencias señaladas para garantizar la seguridad de la aviación civil y el control del espacio aéreo nacional y su interrelación con la legislación vigente, reglamentos, normas oficiales mexicanas, circulares de orientación técnica, circulares de información, y demás disposiciones jurídicas aplicables.

---

[10] Específicamente, el Anexo 17 al Convenio sobre Aviación Civil Internacional de 1946, sobre seguridad y protección de la aviación civil internacional contra los actos de interferencia ilícita. Disponible en: https://www.dgac.gob.bo/wp-content/uploads/2018/05/Anexo_17.pdf

Desafíos en el espacio aéreo internacional

El objetivo principal de la seguridad de la aviación civil internacional consiste en asegurar la protección y la salvaguarda de las y los pasajeros, las tripulaciones, el personal en tierra, el público, las aeronaves y las instalaciones aeroportuarias contra actos de interferencia ilícita perpetrados en tierra o en vuelo. Esto implica el deber de diseñar y aplicar una política integral en materia de seguridad, mediante la articulación de los recursos humanos, logísticos y materiales para la protección del espacio aéreo nacional.

La industria del transporte aéreo desempeña un papel central en el desarrollo económico y social sostenible a nivel mundial. De acuerdo con la Organización de Aviación Civil Internacional, se calcula que en 2018 este sector aportó 2.7 billones de dólares anuales, lo que representó el 3.6% del Producto Interno Bruto mundial, y generó 65.5 millones de empleos. Asimismo, en dicho año la navegación aérea civil transportó 4,300 millones de pasajeros y 58 millones de toneladas de carga.[11] Se prevé que en 2036 este sector empleará a 97.8 millones de personas y generará beneficios económicos por 5.7 billones de dólares. De igual forma, el tránsito de pasajeros a nivel internacional se incrementará a 6,000 millones de personas, mientras que la carga aérea transportada será de 125 millones de toneladas.[12]

Estos datos permiten dimensionar la importancia que tiene la seguridad del espacio aéreo a nivel internacional, regional y nacional, puesto que contribuye a gestionar el crecimiento de manera segura y eficiente de la aviación y resulta fundamental para el progreso y el desarrollo económico. Por tanto, al garantizar la seguridad del espacio aéreo, los Estados reafirman su efectivo control soberano sobre esta porción territorial, contribuyen a generar confianza en el público sobre el sistema de aviación y proporcionan una base sólida para el comercio y el turismo a nivel mundial.[13]

Esta confianza en la seguridad del espacio aéreo resulta vital, toda vez que garantiza un entorno global estable y pacífico. Además, los servicios aéreos seguros

---

[11] *Cfr.* OACI. *Aviation Benefits 2019,* Industry High Level Group (IHLG)'s, pp. 5 a 7 y 9. Disponible en: https://www.icao.int/sustainability/Documents/AVIATION-BENEFITS-2019-web.pdf

[12] Organización de Aviación Civil Internacional (OACI). *Plan global para la seguridad de la aviación,* Doc 10118, 2019, pág. 1-1. Disponible en: https://www.icao.int/Security/Documents/GLOBAL%20AVIATION%20SECURITY%20PLAN%20SP.pdf

[13] *Idem.*

mejoran el transporte, la conectividad, el comercio, así como los vínculos políticos y culturales entre los países. En este contexto, la Organización de las Naciones Unidas (ONU) considera que el carácter mundial de la aviación implica que los Estados dependen de la eficacia recíproca de sus sistemas de seguridad de aviación para la protección de las personas. Por tanto, los Estados deben proporcionar un entorno seguro en materia de aviación como objetivo compartido de la comunidad internacional.[14]

El desarrollo del tránsito aéreo facilita significativamente el progreso económico de los Estados y las regiones a través de la mejora de la infraestructura, los ingresos por concepto de turismo, el acceso a mercados distantes para productores locales y la creación de ciclos de inversiones y nuevas redes de proveedores. No obstante, la expansión global de esta floreciente industria ha superado los avances reglamentarios y la infraestructura necesaria para su protección frente a los riesgos contemporáneos de naturaleza multifactorial de la seguridad del espacio aéreo y de la propia seguridad operacional de la aviación civil.

En la actualidad, los Estados se enfrentan a desafíos emergentes de naturaleza transnacional tales como el terrorismo, el contrabando de bienes y mercancías, la trata de personas y el tráfico de drogas, provenientes del crimen organizado. Se trata de desafíos a las normas y principios democráticos de los Estados, conforme a su marco constitucional.[15] Si bien algunas de estas actividades criminales contra la seguridad de la navegación aérea son perpetradas en territorio nacional, también tienen implicaciones regionales y globales, por lo que, en definitiva, afectan a la comunidad internacional en su conjunto.

De acuerdo con el informe más reciente de la Oficina de las Naciones Unidas para la Droga y el Delito (UNODC, por sus siglas en inglés), durante el 2019, la demanda de sustancias ilícitas se incrementó 22% por encima de la registrada en 2010, lo que representa un mercado actual de 275 millones de consumidores. Para 2030, se estima que la proporción mundial de consumidores se incremente un 11% en todo

---

[14] *Cfr.* ONU. Consejo de Seguridad. Resolución 2309 (2016), aprobada por el Consejo de Seguridad en su 7775ª sesión, celebrada el 22 de septiembre de 2016, S/RES/2309 (2016). Preámbulo. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/295/82/PDF/N1629582.pdf?OpenElement

[15] OEA. *Declaración sobre Seguridad en las Américas,* OEA/Ser.K/XXXVIII CES/doc.14/03, 21 de noviembre de 2003. Documento final de la Conferencia Especial sobre Seguridad, celebrada en la Ciudad de México del 27 al 28 de octubre de 2003, p. 34 y 106. Disponible en: https://www.oas.org/csh/ces/documentos/ce00358s06.doc

el mundo.[16] Para satisfacer esta demanda, a partir de 2021 el crimen organizado aumentó la utilización de rutas terrestres y vías de navegación, aeronaves privadas, transporte de mercancías por vía aérea y paquetes postales, así como métodos sin contacto para la entrega de drogas a consumidores.[17] Un ejemplo de lo anterior se observa en la frontera entre México y los Estados Unidos, donde las organizaciones de narcotraficantes están trasladando más productos a través de túneles transfronterizos y mediante aviones teledirigidos y ultraligeros.[18]

Desafíos en el espacio aéreo mexicano

Este comercio de drogas ilícitas a través del espacio aéreo mexicano constituye un freno para la economía y el desarrollo social, al mismo tiempo que impacta desproporcionadamente a las personas en situación de vulnerabilidad y marginación, lo que constituye una amenaza fundamental para la seguridad y la estabilidad nacional.

Además de actividades vinculadas a la delincuencia organizada, de acuerdo con el Centro Nacional de Vigilancia y Protección del Espacio Aéreo, en México cada 36 horas se reporta una alerta de seguridad por aeronaves relacionadas con el uso de documentación falsa, transporte ilegal de hidrocarburos y actos de corrupción de funcionarios públicos. Esto significa que, de diciembre de 2018 a noviembre de 2021 se emitieron 720 alertamientos para la interceptación y seguimiento de aeronaves por probables actividades ilícitas.[19]

La operación de aeronaves relacionadas con el uso ilícito del espacio aéreo no sólo atenta contra el ejercicio soberano del Estado mexicano sobre esta porción territorial, sino que también representa un riesgo latente a la seguridad operacional de las rutas comerciales de aviación, las personas y las comunidades en tierra. Lo anterior, debido a que, por lo regular, los aterrizajes clandestinos se realizan en caminos rurales, carreteras, calles de poblados y ciudades, por lo cual el peligro de la ocurrencia de una catástrofe es considerablemente alto.

---

[16] UNODC. *World Drug Report 2021. Booklet 2 - Global overview of drug demand and drug supply*, Viena, p. 3. Disponible en: https://www.unodc.org/res/wdr2021/field/WDR21_Booklet_2.pdf
[17] UNODC. *World Drug Report 2021. Booklet 1 - Executive summary / Policy implications,* Viena, p. 5. Disponible en: https://www.unodc.org/res/wdr2021/field/V2104298_Spanish.pdf
[18] UNODC. *COVID-19 y la cadena de suministro de drogas: de la producción y el tráfico al consumo,* Viena, 2020, p. 26 a 27. Disponible en: https://www.unodc.org/documents/data-and-analysis/covid/Covid-19_Suministro_de_Drogas.pdf
[19] Gobierno de México. "Temas de primera plana", 1 de mayo de 2022. Disponible en: https://www.inm.gob.mx/gobmx/word/index.php/temas-de-primera-plana-010522/

En este escenario, el fortalecimiento continuo de las capacidades preventivas, de monitoreo y de reacción del Estado mexicano para la protección soberana de su territorio aéreo exige una constante evolución en proporción a los riesgos que, en sus distintas expresiones, el crimen organizado representa para la paz y la seguridad, así como para la vigencia del Estado de derecho y el respeto a los derechos humanos.

La capacidad del Ejército y Fuerza Aérea Mexicanos para la protección del espacio aéreo

La Fuerza Aérea Mexicana ejerce con profesionalismo, a través de los recursos que la Nación pone bajo su disposición y resguardo, sus funciones de vigilancia permanente del espacio aéreo nacional; de combate a la violencia a través de operaciones aéreas que contribuyen a la paz y seguridad del país; de transporte aéreo de tropas y logístico, tanto nacional como internacional; de auxilio a la población civil en casos de desastres, y de traslado de ayuda humanitaria a países hermanos ante catástrofes.

De conformidad con el artículo 1/o. de la Ley Orgánica del Ejército y Fuerza Aérea Mexicanos, las instituciones armadas permanentes tienen como misiones generales: a) defender la integridad, la independencia y la soberanía de la Nación; b) garantizar la seguridad interior; c) auxiliar a la población civil en casos de necesidades públicas; d) realizar acciones cívicas y obras sociales que tiendan al progreso del país, y e) en caso de desastre, prestar ayuda para el mantenimiento del orden, auxilio de las personas y sus bienes y la reconstrucción de las zonas afectadas.

El Ejército y Fuerza Aérea Mexicanos están hoy en día fortalecidos moralmente, organizados, equipados y adiestrados para confrontar con éxito, en los ámbitos táctico, operacional y estratégico, las amenazas tradicionales o multidimensionales de origen interno o externo provenientes de diversos agentes que constituyan un obstáculo al logro de los objetivos nacionales.

De esta manera, la Fuerza Aérea realiza actividades con vocación de servicio, entrega y lealtad, en coordinación con el Ejército y la Armada, para cumplir estrictamente con el marco constitucional, legal y convencional que rige la vida de las mexicanas y mexicanos, siempre con respeto a los derechos humanos de las personas.

Sin embargo, la Ley Orgánica del Ejército y la Fuerza Aérea Mexicanos no considera las acciones que realiza la Fuerza Aérea, particularmente las relacionadas con la protección del espacio aéreo nacional. De igual forma, no regula las Regiones Aéreas y Bases Aéreas Militares, las cuales fungen como instancias de mando superior operativo de dicha fuerza armada. Con el objetivo de que se reconozcan las funciones de la Fuerza Aérea, se considera necesario precisar en el marco legal su responsabilidad en la preservación de la soberanía del espacio situado sobre el territorio nacional.

Para el cumplimiento de tales propósitos, la Fuerza Aérea tiene como misión defender la integridad, independencia y soberanía de la Nación, así como proteger el espacio aéreo situado sobre el territorio nacional. Actualmente, esta Secretaría cuenta con la infraestructura, así como con los recursos humanos y materiales, para atender la problemática del uso ilícito del espacio aéreo, su vigilancia y protección, apegándose a los principios de legalidad, eficiencia, profesionalismo y honradez, para privilegiar el bien social y la protección irrenunciable de los derechos humanos que deben ser tutelados a través de medidas de seguridad reconocidas por ley.

En ese sentido, entre los recursos que la Secretaría de la Defensa Nacional, a través de la Fuerza Aérea Mexicana, aporta para la seguridad del espacio aéreo nacional, se encuentran:

• Radares en tierra y aerotransportados para la vigilancia y detección de aeronaves que realicen vuelos en violación de la normativa aérea vigente.

• Aeronaves para la vigilancia, interceptación, seguimiento y aseguramiento de aeronaves que realicen vuelos en violación de la normativa aérea vigente.

• Estructura de mandos territoriales del Ejército y Fuerza Aérea, tales como Regiones Militares y Zonas Militares, así como Regiones Aéreas y Bases Aéreas.

• Personal militar desplegado en 63 aeropuertos y 46 aeródromos, cuya función principal es la aplicación de la Ley Federal de Armas de Fuego y Explosivos, mediante la revisión de aeronaves para la detección de carga ilícita transportada vía aérea, que representa un activo en favor de las operaciones coordinadas con las autoridades civiles para garantizar la seguridad de las operaciones de aviación en el territorio nacional.

Lo anterior pone de manifiesto la extensa capacidad técnica con la que cuenta la Sedena para ejercer funciones de vigilancia y protección del espacio aéreo dentro del territorio, y para ejercer la coordinación, en el marco de la nueva Ley de Protección del Espacio Aéreo, de otras autoridades, con el fin de conjuntar sus capacidades, recursos y facultades con la SICT, en relación con aeropuertos y aeródromos civiles, y la Secretaría de Marina, en cuanto al espacio aéreo sobre el mar territorial, zona marítimo terrestre, islas, cayos, arrecifes, zócalos y plataforma continental, así como en aguas interiores, lacustres y ríos en sus partes navegables.

Contenido de la iniciativa

La presente iniciativa de reforma propone que se permita al Estado mexicano disponer de mecanismos para atender de manera eficaz los riesgos emergentes y otros desafíos contemporáneos de la seguridad del espacio aéreo nacional, específicamente los relacionados con el crimen organizado, y contribuir a la consolidación de la paz y la observancia del Estado de derecho y el respeto a la soberanía nacional, así como a la vigencia efectiva de los derechos humanos.

Para efectos de lo anterior, se propone establecer en la legislación aplicable, de manera concurrente con las autoridades aeronáuticas civiles, a partir de un enfoque de seguridad nacional, las facultades necesarias para que la Sedena coordine a las dependencias que participan en garantizar la seguridad del espacio aéreo en nuestro territorio, con el fin de identificar y neutralizar el uso de aeronaves y terminales aeroportuarias que violen la normativa en materia de navegación aérea y prevenir amenazas para la seguridad nacional.

Se plantea que, ante la necesidad de brindar mayor seguridad en el espacio aéreo de nuestro país, se amplíen dentro de la Ley Orgánica de la Administración Pública Federal y la Ley de Aviación Civil, aquellas facultades que permitan a la Sedena coordinar las acciones para garantizar la seguridad del espacio aéreo con el fin de prevenir, inhibir y actuar ante la ocurrencia de actos ilícitos en contra de las operaciones aeronáuticas, que puedan afectar la seguridad nacional, en concurrencia con las autoridades civiles.

Para el cumplimiento de tales propósitos, se realizan en la Ley Orgánica del Ejército y Fuerza Aérea Mexicanos, ajustes orgánicos, jerárquicos y técnicos de la Fuerza Aérea, con el fin de profesionalizar al personal adscrito, así como para garantizar el uso eficiente de recursos y perfiles profesionales.

Esta reforma incluye modificaciones a la Ley de Aeropuertos, a efecto de establecer la coordinación entre autoridades civiles y militares, dentro de la administración, operación y explotación de los aeródromos civiles. El objetivo es conjuntar los recursos de la SICT, de la Secretaría de Marina y de la Sedena, para el mejor funcionamiento de las actividades aéreas dentro del territorio nacional.

La presente reforma permitiría al Estado mexicano disponer de mecanismos para atender de manera eficaz los riesgos emergentes y otros desafíos contemporáneos de la seguridad del espacio aéreo nacional, específicamente los relacionados con el crimen organizado, y contribuir a la consolidación de la paz y la observancia del Estado de derecho y el respeto a la soberanía nacional, así como a la vigencia efectiva de los derechos humanos.

Específicamente, se proponen las siguientes modificaciones:

1. Con el fin de especificar las facultades de la Sedena en materia de protección y vigilancia del espacio aéreo mexicano, se adicionan las fracciones VIII Bis a VIII Quinquies, al artículo 29 de la Ley Orgánica de la Administración Pública.

• Se establece que corresponde a la Sedena, en coordinación con la Semar, salvaguardar la soberanía y la defensa de la integridad del espacio aéreo; garantizar las operaciones aéreas lícitas en el territorio nacional; en concurrencia con la SICT, participar en operaciones de búsqueda y salvamento aéreo; establecer las zonas de vigilancia y protección del espacio aéreo, en coordinación con la SICT y la Semar.

2. En la LOEFAM se proponen modificaciones para establecer las facultades de la Fuerza Aérea Mexicana en la defensa del espacio aéreo; se incorpora el Centro Nacional de Vigilancia y Protección del Espacio Aéreo como órgano integrante del alto mando de la Sedena; la organización de la Fuerza Aérea en Regiones Aéreas Militares y Bases Aéreas Militares; la creación del grado de Piloto Aviador General de División y del Estado Mayor, al mando de la Fuerza Aérea; la creación del servicio de archivo; se regula el Servicio Meteorológico y cambia la denominación de servicios, y se adecuan algunas funciones relacionadas con el control del espacio aéreo, para lo cual se modifican los artículos 21, 23, 32 Bis, 32 Ter, 59 Bis, 60, 34, 35, 36 Bis, 38, 38 Bis, 38 Ter, 43, 59, 61, 62, 63, 63 Bis, 68, 74, 75, 95 Quáter, 95 Quinquies, 96, 93, 98, 99, 100, 101 Bis, 101 Ter, 101 Quáter, 101 Quinquies, 101 Sexties, 101 Septies, 160, 191, 192 y 193 de la Ley Orgánica del Ejército y Fuerza

Aérea Mexicanos:

• Se establecen las acciones que la Sedena deberá realizar para proteger el espacio aéreo nacional, que consistirán en: conducir operaciones de inteligencia aérea; definir la zona de vigilancia y protección del espacio aéreo nacional, controlando las operaciones aéreas en dicha zona y las zonas de identificación de defensa aérea, y realizar operaciones de búsqueda y salvamento para resguardar la vida de las personas en el territorio nacional, sin perjuicio de las atribuciones que correspondan a otras autoridades.

• Se determina que el mando de la Fuerza Aérea recaerá en una persona con el grado de General de División Piloto Aviador, que se denominará comandante de la Fuerza Aérea, quien será responsable de su operación y administración, bajo el mando de la persona titular de la Sedena.

• Se establecen las facultades, mandos y estructura de las Regiones y Bases Aéreas Militares, y con ello se brinda sustento legal a sus funciones en materia de defensa aérea. Se distinguen con claridad las Regiones Aéreas Militares, y su composición a partir de las Bases Aéreas Militares, Estaciones Aéreas y otros organismos de la Fuerza Aérea, bajo el mando de personas comandantes con el grado de General de División. Asimismo, se distingue la jurisdicción de las Zonas Militares y de las Regiones Aéreas Militares. Se prevé que las Regiones Aéreas Militares se integren con las Bases Militares que podrán incluir Unidades de Vuelo, servicios y organismos aéreos.

• Se actualiza la denominación de Estado Mayor Aéreo por el de Estado Mayor de la Fuerza Aérea, el cual es el órgano técnico colaborador inmediato de la persona Comandante de la Fuerza Aérea, que tiene función principal auxiliar en la planeación y coordinación de las Misiones encargadas a dicha Fuerza Aérea.

• Se incorpora a las personas Pilotos Aviadores, como integrantes de la Fuerza Aérea Mexicana con formación, capacitación y entrenamiento para la conducción de organismos aéreos y de las aeronaves con las que se encuentren dotados.

• Se reconoce dentro del Ejército y Fuerza Aérea mexicanos, el servicio de archivo, el cual tendrá a su cargo la organización, administración y conservación de los archivos, museos y bibliotecas de la Sedena. La dirección del servicio de archivo estará a cargo una persona titular que deberá contar con el grado de General

procedente de Arma.

• Se establecen las funciones del Servicio Meteorológico, consistentes en proporcionar información meteorológica a los organismos del Ejército y Fuerza Aérea Mexicanos; elaborar los estudios sobre meteorología que le sean requeridos; coordinar acciones con organismos gubernamentales afines, y mantener en condiciones operativas dicho servicio.

• Se actualiza la denominación del Servicio de Control de Vuelo por la denominación Servicio de Defensa Aérea para constituirse como parte de la infraestructura del sistema de Vigilancia y Protección del Espacio Aéreo Mexicano, en este sentido, se amplían las funciones que realiza este servicio, para que opere el control de tránsito de aeronaves militares y civiles.

• Se modifica la denominación del Servicio de Material Aéreo por la denominación Servicio de Mantenimiento de Material Aéreo. Se amplían las facultades de este servicio a efecto de que además de abastecer y realizar mantenimiento del material de vuelo, pueda elaborar estudios de carácter técnico para la adquisición y reparación de componentes, llevar acabo investigación científica y tecnológica, y formar parte de tripulaciones de vuelo, cuando el servicio así lo requiera.

• Se crea el Servicio de Logística Aérea para proporcionar apoyo logístico a organismos aéreos; elaborar estudios en esta materia; administrar toda clase de abastecimientos de la Fuerza Aérea; realizar investigación científica y tecnológica; así como llevar el registro estadístico de refacciones y partes de aviación.

• Se incorpora el Servicio de Material Aéreo Electrónico, el cual debe proporcionar mantenimiento electrónico preventivo y correctivo de los diversos sistemas instalados en las aeronaves militares; elaborar estudios de carácter técnico en materia de reparación; diseñar, fabricar y recuperar material de vuelo electrónico; realizar investigación científica y tecnológica; así como formar parte de tripulaciones en caso de que el servicio lo requiera.

• Se instituye el Servicio de Material Bélico de Fuerza Aérea, con el fin de profesionalizar al grupo encargado del armamento aéreo. Este servicio tiene a su cargo otorgar apoyo logístico de material bélico; elaborar estudios técnicos en su materia; administrar material bélico; diseñar, fabricar, reconstruir, recuperar y modificar material bélico; realizar investigación científica en la materia; dictaminar y

materializar procedimientos de desactivación y destrucción de material; controlar y operar sistemas de armas antiaéreas, así como formar parte de tripulaciones cuando el servicio así lo requiera.

• Se amplían los estudios que imparte la Escuela Superior de Guerra, bajo la denominación "De Estado Mayor". Con ello se busca mejorar la formación militar correspondiente a armas, servicio y especialidad.

• Se incorpora el Cuerpo Especial de Aerotropas a los escalafones y grados que comprenden las Armas y Cuerpos Especiales del Ejército. El cuerpo especial de Aerotropas fue previsto como unidades especializadas en caso de emergencias, con esta modificación las aerotropas se incorporan dentro de las estructuras regulares del Ejército mexicano, lo que permitirá desarrollo profesional de este cuerpo especial.

• Se integra el Grupo de Pagadores a la estructura del Servicio de Administración. Con esto se permitirá incorporar perfiles existentes de personal que cuentan con estudios de licenciatura y maestría en contaduría o administración de empresas, cuyo perfil de egreso es congruente con las funciones de administrativas requeridas.

3. En la Ley de Aeropuertos, se proponen incorporar los requisitos para la emisión de los de estudios operacionales de trayectorias, las causales de revocación de permisos; las facultades para realizar operaciones de interceptación aérea, y la obligación de apoyar en actividades de búsqueda y salvamento por parte de personas permisionarias y concesionarias, para lo cual se modifican los artículos 18, 27 Bis, 32 y 49 de la Ley de Aeropuertos:

• Se establece que los estudios operacionales de trayectorias (requisito para obtener un permiso de operación de aeródromos y helipuertos) incorporen como punto de referencia las instalaciones de la Fuerza Aérea que se encuentren ubicadas en un perímetro de 10 millas náuticas al lugar donde se pretenda operar el aeródromo o helipuerto en cuestión.

• Se incorpora como causal de revocación de permisos, la omisión de la persona permisionaria en informar a la autoridad aeronáutica cuando el aeródromo sea utilizado por una aeronave sin consentimiento de la persona permisionaria.

• Se establece que las operaciones de interceptación aérea estarán sujetas a la coordinación que se realice con la Secretaría de la Defensa Nacional y la Secretaría

de Marina.

• Se incorpora la obligación de las personas concesionarias y permisionarias operadoras aeródromos civiles, de permitir el uso y prestación de servicios aeroportuarios y complementarios para aquellas aeronaves que se encuentren en actividades de búsqueda y salvamento, así como en casos de desastres.

4. Con el objetivo de establecer las acciones específicas de vigilancia y protección del espacio aéreo mexicano, se propone modificar los artículos 8 Bis, 29, 32, 34, 86, 87, 88 y 90 de la Ley de Aviación Civil, a efecto establecer las siguientes atribuciones:

• Se faculta a la Sedena para que, en coadyuvancia con la SICT, garanticen la protección del espacio aéreo en los siguientes ámbitos: solicitud de documentos que amparen certificados de aeronavegación y licencia establecidos en el estado de la matrícula; verificación de talleres, centros de capacitación y adiestramiento, y fábricas de aeronaves y componentes, así como emisión de medidas y normas de tráfico aéreo.

• Se establece la obligación de autoridades que operen aeropuertos, de informar a la Sedena de aterrizajes de aeronaves extranjeras de servicio privado no comercial que se realicen en aeropuertos internacionales mexicanos.

• Se especifica que la SICT, por sí o a solicitud de Sedena, podrá suspender o cancelar certificados de aeronavegación y de matrícula, en caso de incumplimiento de obligaciones por parte de las personas operadoras de aeronaves.

• La SICT y la Sedena, en su carácter de coordinador del Sistema de Vigilancia y Protección del Espacio Aéreo Mexicano, podrán realizar acciones coordinadas para la interceptación de aeronaves que realicen vuelos clandestinos.

• La Agencia Federal de Aviación Civil podrá aplicar a las personas concesionarias, asignatarias, operadoras aéreas o permisionarias, además de las sanciones vigentes, multas por incumplimiento en obligaciones contenidas en disposiciones técnico-administrativas o normas oficiales mexicanas relacionadas con la fabricación de aeronaves, motores, hélices, estaciones de pilotaje a distancia y sus artículos; por no reportar incapacitaciones, durante el vuelo, del personal técnico-aeronáutico o permitir que realicen sus funciones con afectación médica que ponga en riesgo la seguridad operacional o cuando hubieren obtenido un resultado positivo

en detección de alcohol y sustancias psicoactivas, o posterior a un accidente o incidente aéreo, no cumpla requisitos médicos; por coaccionar a las personas inspectoras verificadoras por medio de violencia, física o moral, para obligarlos a que ejecuten un acto oficial, y por no realizar la notificación de dificultades en servicio.

• Se agregan a las sanciones aplicables a personas concesionarias o permisionarias de servicio al público de transporte aéreo multas por realizar maniobras de vuelo que motiven la activación de alertamiento aéreo, cuando no corresponda a una falla técnica o emergencia. Esta activación también dará lugar a sanción para la persona comandante o piloto de cualquier aeronave civil.

• Se establece como causales de revocación de licencia para las personas comandantes, el uso ilícito de instalaciones destinadas al tránsito aéreo; el aterrizaje o despegue fuera de los aeródromos autorizados y la realización de estas operaciones en aeródromo autorizado fuera de los horarios de operación.

Por las razones anteriormente expuestas, y en ejercicio de la facultad que me confiere el artículo 71, fracción I, de la Constitución Política de los Estados Unidos Mexicanos, se somete a la consideración de esa Soberanía la siguiente Iniciativa con Proyecto de

Iniciativa con Proyecto de Decreto por el que se Reforman, Adicionan y Derogan Diversos Artículos de la Ley Orgánica de la Administración Pública Federal, de la Ley Orgánica del Ejército y Fuerza Aérea Mexicanos, de la Ley de Aeropuertos y de la Ley de Aviación Civil, en Materia de Protección del Espacio Aéreo Mexicano

Artículo Primero.- De la Ley Orgánica de la Administración Pública Federal, se **adiciona** al artículo 29, las fracciones VIII Bis, VIII Ter, VIII Quáter y VIII Quinquies, en los siguientes términos:

Artículo 29.- ...

I. a **VIII.-** ...

VIII Bis.- Salvaguardar la soberanía y defender la integridad del territorio nacional, incluyendo su espacio aéreo, en coordinación con la Secretaría de Marina en lo correspondiente a la protección del espacio situado sobre el mar territorial;

VIII Ter.- Establecer acciones para garantizar que las operaciones aéreas en el

territorio nacional no se realicen con fines ilícitos o atenten contra la seguridad nacional;

VIII Quáter.- Participar, con la Secretaría de Infraestructura, Comunicaciones y Transportes, en las operaciones de búsqueda y salvamento aéreo, en términos de artículo 80 de la Ley de Aviación Civil;

VIII Quinquies.- Establecer, en coordinación con la Secretaría de Infraestructura, Comunicaciones y Transportes, las zonas de vigilancia y protección del espacio aéreo;

IX.- a **XXI.-**...

Artículo Segundo.- De la Ley Orgánica del Ejército y Fuerza Aérea Mexicanos se **reforman** los artículos 21, fracciones III y IV; 23; 34 fracciones I, II, III, IV, V y V;35; 38, párrafo primero; 43; 54 QUATER; 59, fracción II; 60; 61; 62; 63; 68, fracciones XIII y XIV; 74; 75; 96; 98, párrafo primero; 99; 100, párrafo primero y sus fracciones I y II; 101; 160; 191, fracciones VII, párrafo segundo y VIII, párrafo segundo; 192, fracciones II, párrafo segundo y III, párrafo segundo, y 193, fracciones III, apartado B, párrafo segundo, VII, párrafo primero y sus apartados C, párrafo segundo, y D, párrafo segundo, XIII, párrafo primero; XIV, párrafo primero, y XV, párrafo primero y sus incisos A, párrafo primero, B, C, párrafo primero, y D, así como las denominaciones de los apartados Servicio de Control de Vuelo y Servicio del Material Aéreo para del Capítulo IV del Título Cuarto; se adicionan los artículos 21, fracción V; 34, fracción IV Bis; 36 BIS; 38 BIS; 38 TER; 59, fracción III Bis; 59 BIS; 63 BIS; 68, fracciones XI Bis, XV, XVI y XVII; 74, párrafo segundo; 96, fracciones I, II, III y IV; 98, fracciones I, II, III, IV y V; 100, fracciones III, IV y V; 191, fracción IX; 193, fracciones VII, apartado E, XII Bis, XIV, párrafo segundo, recorriéndose el subsecuente, XV, apartados A, segundo párrafo y C, segundo párrafo; XVI, XVII, y XVIII; así como las divisiones, así como la Subsección denominada EL CENTRO NACIONAL DE VIGILANCIA Y PROTECCIÓN DEL ESPACIO AÉREO, que se integra con los artículos 32 BIS y 32 TER a la Sección Segunda del Capítulo III del Título Tercero y los apartados denominados Servicio de Archivo que se integra con los artículos 95 QUÁTER y 95 QUINQUIES; Servicio de Logística Aérea que se integra con los artículos 101 BIS y 101 TER; "Servicio de Material Aéreo Electrónico" que se integra con los artículos 101 QUÁTER y 101 QUINQUIES, y "Servicio de Material Bélico de Fuerza Aérea" que se integra con los artículos 101 SEXIES y 101 SEPTIES al Capítulo IV del Título Cuarto, y se derogan los artículos 192, fracción IV; 193, fracción XV, apartados A, incisos a y b, C, incisos a y b, E y F, para quedar como sigue:

ARTÍCULO 21. ...

I. y **II. ...**

III. Órganos del Fuero de Guerra;

IV. Direcciones Generales de la Secretaría de la Defensa Nacional, y

V. Centro Nacional de Vigilancia y Protección del Espacio Aéreo.

ARTÍCULO 23. El Estado Mayor Conjunto de la Defensa Nacional estará formado por personal de Estado Mayor perteneciente al Ejército y Fuerza Aérea y por aquel otro que sea necesario.

EL CENTRO NACIONAL DE VIGILANCIA Y PROTECCIÓN DEL ESPACIO AÉREO

ARTCULO 32 BIS. El Centro Nacional de Vigilancia y Protección del Espacio Aéreo es un órgano dependiente de la Secretaría de la Defensa Nacional, responsable de la vigilancia y protección del espacio aéreo mexicano.

ARTCULO 32 TER. Para desarrollar sus funciones, el Centro Nacional de Vigilancia y Protección del Espacio Aéreo empleará los medios para la detección, identificación, interceptación y salvamento puestos a su disposición.

ARTICULO 34. ...

I. La persona Comandante del Ejército;

II. La persona Comandante de la Fuerza Aérea;

III. Las personas Comandantes de Regiones Militares o Aéreas;

IV. Las personas Comandantes de Zonas Militares;

IV Bis. Las personas Comandantes de Bases Aéreas Militares;

V. Las personas Comandantes de las Grandes Unidades Terrestres o Aéreas;

VI. Las personas Comandantes de las Unidades conjuntas o combinadas, y

VII. Las personas Comandantes de las Unidades Circunstanciales que el Alto Mando determine implementar.

ARTICULO 35. La persona titular de la Secretaría de la Defensa Nacional ejercerá el Mando de las Fuerzas a través de las personas Comandantes del Ejército, de la Fuerza Aérea, de las Regiones Militares y Aéreas, de las Zonas Militares, de las

Bases Aéreas Militares y de las personas Comandantes de Unidades del Ejército o de la Fuerza Aérea, sin perjuicio de ejercerlo directamente cuando así se requiera por motivos del Servicio.

ARTÍCULO 36 BIS. Las Regiones Aéreas Militares se integran con las Bases Aéreas, Estaciones Aéreas y otros organismos de la Fuerza Aérea que se encuentren dentro de su jurisdicción, atendiendo a necesidades estratégicas, y estarán al mando de una persona Comandante con el grado de General de División Piloto Aviador.

ARTÍCULO 38. Las Zonas Militares se integran con organismos del Ejército que se encuentran dentro de su jurisdicción. Se dividen en Sectores y Subsectores Militares en los que radican Unidades del Ejército, pudiendo encontrarse Comandancias de Guarnición, que en todo caso estarán subordinadas a la persona Comandante de la Zona Militar correspondiente.

...

ARTÍCULO 38 BIS. Las Bases Aéreas Militares se integran con organismos de la Fuerza Aérea que se encuentren dentro de su adscripción, pudiendo incluir unidades de vuelo, de los Servicios y organismos aéreos.

ARTÍCULO 38 TER. La Secretaría de la Defensa Nacional por conducto de las personas Comandantes de la Fuerza Aérea, Región Aérea, Base Aérea Militar o Estación Aérea Militar ejercerá sus funciones en materia defensa aérea.

ARTÍCULO 43. Las personas Comandantes del Ejército, de la Fuerza Aérea, de las Regiones Militares y Aéreas, y las Zonas Militares, Bases Aéreas Militares y Grandes Unidades dispondrán de un Cuartel General, según sus planillas, conforme a su nivel jerárquico. Los Estados Mayores que formen parte de estos Cuarteles Generales estarán subordinados técnicamente a los Estados Mayores de la Defensa Nacional, del Ejército y de la Fuerza Aérea, según corresponda.

ARTÍCULO 54 QUÁTER. El Estado Mayor del Ejército, estará formado por personal de Estado Mayor perteneciente al Ejército, así como de aquel otro personal que le sea necesario.

ARTÍCULO 59. ...

I. ...

II. Estado Mayor de la Fuerza Aérea

III. ...

III Bis. Pilotos Aviadores;

IV. y **V.** ...

ARTÍCULO 59 BIS. La Fuerza Aérea tiene a su cargo las siguientes acciones:

I. La defensa del espacio aéreo nacional;

II. Conducir operaciones de inteligencia aérea;

III. Establecer las zonas de vigilancia y protección del espacio aéreo nacional controlando las operaciones aéreas en dicha zona, así como las zonas de identificación de defensa aérea;

IV. Realizar operaciones de búsqueda y salvamento aéreo para salvaguardar la vida de las personas en el territorio nacional, sin perjuicio de las atribuciones que correspondan a otras dependencias, y

V. Ejercer sus atribuciones en materia de seguridad en el espacio aéreo, en coordinación con las autoridades que correspondan.

ARTÍCULO 60. El mando de la Fuerza Aérea recae en una persona con el grado de General de División Piloto Aviador, que se denominará Comandante de la Fuerza Aérea, quien será responsable de su operación y administración, así como del empleo de sus Unidades, de conformidad con las Directivas, Instrucciones, Órdenes y demás disposiciones de la persona titular de la Secretaría de la Defensa Nacional.

ARTÍCULO 61. El Estado Mayor de la Fuerza Aérea es el órgano técnico colaborador inmediato de la persona Comandante de la Fuerza Aérea, a quien auxilia en la planeación y coordinación de las Misiones que tiene a su cargo y transforma las decisiones en órdenes, directivas e instrucciones verificando su cumplimiento.

ARTÍCULO 62. El Estado Mayor de la Fuerza Aérea estará formado por personal de Estado Mayor, así como de aquél que le sea necesario.

ARTÍCULO 63. Las Unidades de Vuelo son los componentes de la Fuerza Aérea cuya misión principal es el combate Aéreo, así como la ejecución de operaciones aéreas militares en tiempo de paz y de guerra, que actúan en la forma peculiar que les impone la misión y el material de vuelo de que están dotadas.

ARTÍCULO 63 BIS. Las personas Pilotos Aviadores son el componente humano de la Fuerza Aérea formado, capacitado y entrenado para la conducción de los

organismos aéreos y de las aeronaves con que se encuentren dotados.

ARTÍCULO 68. ...

I. a **XI.** ...

XI Bis. Archivo;

XII. ...

XIII. Defensa aérea;

XIV. Mantenimiento de material aéreo;

XV. Logística aérea;

XVI. Material aéreo electrónico, y

XVII. Material bélico de Fuerza Aérea.

ARTÍCULO 74. Los servicios del Ejército podrán organizarse en equipos, escuadras, pelotones, secciones, compañías y batallones, exceptuando al de justicia que adoptará su organización de acuerdo con sus necesidades.

Los servicios de la Fuerza Aérea podrán organizarse en equipos, escuadrillas, escuadrones y grupos, con una denominación igual a las Unidades de Vuelo, pero que no serán equiparables en nivel orgánico debido a la cantidad de los elementos que las constituyen y la función que desempeñan.

ARTÍCULO 75. Las direcciones generales, direcciones, jefaturas y el Centro Nacional de Vigilancia y Protección del Espacio Aéreo, previa autorización de la persona titular de la Secretaría de la Defensa Nacional y de la persona Comandante del Ejército o de la Fuerza Aérea, según corresponda, mantendrán estrecha colaboración con órganos afines, oficiales y particulares, a efecto de obtener los datos necesarios que sirvan de fundamento a sus informes y opiniones de carácter técnico para controlar las obras, instalaciones y organizaciones de la misma naturaleza, cuya importancia lo amerite desde el punto de vista militar y para llevar a cabo investigaciones en los campos científico y tecnológico, relativas a sus respectivos servicios.

Servicio de Archivo

ARTÍCULO 95 QUÁTER.- El servicio de archivo tendrá a su cargo la organización, administración y conservación de los archivos, museos y bibliotecas de la

Secretaría; además realizará las actividades siguientes:

I. Llevar a cabo la administración del personal del Servicio;

II. Promover la aplicación de nuevas tecnologías de la información y comunicaciones, que tiendan a la innovación de la organización, administración y conservación de los archivos, museos y bibliotecas, en coordinación con otras áreas de la Secretaría y de la Administración Pública Federal, así como de la iniciativa privada, tanto nacional como internacional;

III. Elaborar, proponer y aplicar las normas, criterios y lineamientos archivísticos basados en la normatividad aplicable;

IV. Promover la creación, organización, establecimiento y sostenimiento de bibliotecas y museos, impulsando el equipamiento, mantenimiento y actualización permanente de los servicios culturales que a través de ellos se otorguen, y

V. Las demás que le confieran esta Ley y la normatividad aplicable.

ARTÍCULO 95 QUINQUIES.- La persona titular de la Dirección del servicio de archivo deberá contar con el grado de General procedente de Arma.

ARTÍCULO 96. El Servicio Meteorológico tendrá a su cargo:

I. Proporcionar información meteorológica a los organismos del Ejército y Fuerza Aérea Mexicanos;

II. Elaborar los estudios sobre la materia que se requieran;

III. Establecer coordinación en asuntos de su especialidad con organismos gubernamentales y afines, y

IV. Recibir, abastecer, instalar, operar y mantener en condiciones operativas el material del Servicio.

Servicio de Defensa Aérea

ARTÍCULO 98. El Servicio de Defensa Aérea se constituye como parte de la infraestructura del sistema de Vigilancia y Protección del Espacio Aéreo Mexicano. Tendrá a su cargo:

I. Proporcionar control de tránsito aéreo, despacho y coordinación de aeronaves militares y civiles que operen dentro de una base aérea militar, en términos de la normatividad aplicable;

II. Elaborar estudios en materia de defensa aérea que se requieran;

III. Establecer coordinación en asuntos de su especialidad con organismos gubernamentales y afines, en términos de las disposiciones normativas aplicables;

IV. Recibir, operar y mantener en condiciones operativas el material del Servicio, y

V. Formar parte de las tripulaciones de vuelo de la Fuerza Aérea en tareas propias de su especialidad, cuando la misión lo requiera.

ARTÍCULO 99. La persona titular de la Dirección del Servicio de Defensa Aérea deberá contar con el grado de General perteneciente a dicho Servicio.

Servicio de Mantenimiento de Material Aéreo

ARTÍCULO 100. El Servicio de Mantenimiento de Material Aéreo tendrá a su cargo:

I. Proporcionar el mantenimiento preventivo y correctivo de los diversos sistemas instalados en las aeronaves militares, así como el equipo de apoyo en tierra característico de la Fuerza Aérea;

II. Elaborar los estudios de carácter técnico para la adquisición y reparación de componentes de las aeronaves de la Fuerza Aérea;

III. Diseñar, fabricar, reconstruir y recuperar el material de vuelo, así como aquel otro característico de la Fuerza Aérea y el del propio Servicio;

IV. Llevar a cabo la investigación científica y tecnológica en aspectos del Servicio, y

V. Formar parte de las tripulaciones de vuelo de la Fuerza Aérea en tareas propias de su especialidad, cuando la misión lo requiera.

ARTÍCULO 101. La persona titular de la Dirección del Servicio de Mantenimiento de Material Aéreo deberá contar con el grado de General perteneciente a dicho Servicio.

Servicio de Logística Aérea

ARTÍCULO 101 BIS. El Servicio de Logística Aérea tendrá a su cargo:

I. Proporcionar el apoyo logístico a los organismos aéreos en aspectos relacionados con el Servicio;

II. Elaborar los estudios en materia de logística aérea que se requieran;

III. Adquirir, recibir, clasificar, almacenar, mantener, conservar, controlar, distribuir y evacuar toda clase de abastecimientos característicos de la Fuerza Aérea y equipo afín, así como los combustibles y lubricantes de aviación y otros necesarios para su funcionamiento;

IV. Llevar a cabo la investigación científica y tecnológica en aspectos del Servicio, y

V. Llevar el registro estadístico de las refacciones y partes de aviación de la Fuerza Aérea, con el objeto de elaborar los programas presupuestarios y logísticos correspondientes.

ARTÍCULO 101 TER. La persona titular de la Dirección del Servicio de Logística Aérea deberá contar con el grado de General perteneciente a dicho Servicio.

Servicio de Material Aéreo Electrónico

ARTÍCULO 101 QUÁTER. El Servicio de Material Aéreo Electrónico tiene a su cargo:

I. Proporcionar el mantenimiento electrónico preventivo y correctivo de los diversos sistemas instalados en las aeronaves militares, así como el equipo de apoyo en tierra característico de la Fuerza Aérea;

II. Elaborar los estudios de carácter técnico para la reparación y, en su caso, adquisición de componentes electrónicos de las aeronaves de la Fuerza Aérea;

III. Diseñar, fabricar y recuperar el material de vuelo electrónico, así como aquel otro característico de la Fuerza Aérea y el del propio Servicio;

IV. Llevar a cabo la investigación científica y tecnológica en aspectos del Servicio, y

V. Formar parte de las tripulaciones de vuelo de la Fuerza Aérea en tareas propias de su especialidad, cuando la misión lo requiera.

ARTÍCULO 101 QUINQUIES. La persona titular de la Dirección del Servicio de Material Aéreo Electrónico deberá contar con el grado de General perteneciente a dicho Servicio.

Servicio de Material Bélico de Fuerza Aérea

ARTÍCULO 101 SEXIES. El Servicio de Material Bélico de Fuerza Aérea tendrá a su cargo:

I. Otorgar apoyo logístico a los organismos aéreos en aspectos relacionados con el servicio y proponer la adquisición de material bélico;

II. Elaborar los estudios de carácter técnico para la reparación y, en su caso, adquisición de componentes del sistema de armas de las aeronaves;

III. Adquirir, recibir, clasificar, almacenar, mantener, conservar, controlar, distribuir y evacuar el material bélico de la Fuerza Aérea, equipos afines y otros necesarios para su funcionamiento;

IV. Diseñar, fabricar, reconstruir, recuperar y modificar el material bélico de la Fuerza Aérea y equipos complementarios de carga explosiva;

V. Llevar a cabo la investigación científica y tecnológica en aspectos del Servicio;

VI. Dictaminar y materializar los métodos y procedimientos para la desactivación y destrucción de material bélico de la Fuerza Aérea;

VII. Controlar y operar los sistemas de armas antiaéreas, en coordinación con el Servicio de Defensa Aérea, y

VIII. Formar parte de las tripulaciones de vuelo de la Fuerza Aérea en tareas propias de su especialidad cuando la misión lo requiera.

ARTÍCULO 101 SEPTIES. La persona titular de la Dirección del Servicio de Material Bélico de Fuerza Aérea deberá contar con el grado de General perteneciente a dicho Servicio.

ARTÍCULO 160. El personal del Ejército y Fuerza Aérea que apruebe los estudios de Estado Mayor en la Escuela Superior de Guerra recibirá la denominación "De Estado Mayor", precedida de la correspondiente a la de su Arma, Servicio o Especialidad.

ARTÍCULO 191. ...

I. a **VI.** ...

VII. ...

De Soldado a General de Brigada;

VIII. ...

De Soldado a Teniente Coronel, y

IX. Del Cuerpo Especial de Aerotropas.

De Soldado a Sargento Primero.

ARTÍCULO 192. ...

I. ...

II. ...

De Subteniente a General de División, y

III. ...

De Soldado a General de División.

IV. Derogada.

ARTÍCULO 193. ...

I. y **II.** ...

III. ...

A. ...

B. ...

De Soldado a Teniente Coronel.

IV. a **VI.** ...

VII. De Administración, que se divide en cinco grupos:

A. y **B.** ...

C. ...

De Cabo a Teniente Coronel;

D. ...

De Soldado a Teniente Coronel, y

E. Pagadores.

De Capitán Segundo a Coronel.

VIII. a **XII.** ...

XII Bis. Del Servicio de Archivo, que se divide en cinco grupos:

A. Licenciados en Archivonomía.

De Subteniente a Teniente Coronel.

B. Licenciados en Historia.

De Subteniente a Teniente Coronel.

C. Licenciados en Biblioteconomía.

De Subteniente a Teniente Coronel.

D. Archivistas.

De Soldado a Teniente Coronel.

E. Especialistas del Servicio de Archivo.

De Soldado a Teniente Coronel.

XIII. Del Servicio Meteorológico, que se divide en tres grupos:

A. a **C.** ...

XIV. Del Servicio de Defensa Aérea.

Controladores de vuelo.

...

XV. Del Servicio de Mantenimiento de Material Aéreo, que se divide en cuatro

grupos;

A. Ingenieros en Aeronáutica.

De Subteniente a General de Brigada;

a. Derogado.

b. Derogado.

B. Especialistas en mantenimiento de aviación.

De Soldado a General Brigadier;

C. Mantenimiento de Paracaídas.

De Cabo a Mayor, y

a. Derogado.

b. Derogado.

D. Especialistas del Servicio de Mantenimiento Material Aéreo.

De Soldado a Teniente Coronel.

E. Derogado.

F. Derogado.

XVI. Del Servicio de Logística Aérea.

Abastecimiento de Material Aéreo.

De Sargento Segundo a General Brigadier;

XVII. Del Servicio de Material Aéreo Electrónico, que se divide en dos grupos:

A. Ingenieros en Electrónica de Aviación.

De Subteniente a General de Brigada, y

B. Especialistas en Electrónica de Aviación.

De Sargento Segundo a General Brigadier, y

XVIII. Del Servicio de Material Bélico de Fuerza Aérea.

Armamento Aéreo.

De Soldado a General Brigadier.

Artículo Tercero.- De la Ley de Aeropuertos, se reforman los artículos 18, párrafo cuarto; 32, y 49, y se adiciona el artículo 27 Bis, en los siguientes términos:

Artículo 18. ...

...

...

Las personas interesadas en obtener un permiso no requerirán estudio operacional de trayectorias, ni estudio de espacio aéreo, cuando se trate de aeródromos o helipuertos, ambos no controlados y de operación bajo reglas visuales de vuelo, siempre y cuando su punto de referencia de aeródromo o helipuerto esté alejado al menos a una distancia de 10 millas náuticas del punto de referencia del aeropuerto o instalación de la Fuerza Aérea Mexicana más cercana, o dentro del espacio aéreo restringido.

ARTÍCULO 27 Bis. Son causas de revocación de los permisos:

I. No iniciar la administración, operación, explotación o, en su caso, construcción del aeródromo civil, en los plazos que al efecto se establezca en el permiso;

II. No mantener vigentes los seguros a que se refiere esta Ley;

III. Ceder, gravar, transferir o enajenar los permisos, los derechos conferidos o bienes afectos a los aeródromos civiles, en contravención de esta Ley;

IV. Alterar la naturaleza o condiciones del aeródromo civil establecidas en el permiso, sin previa autorización de la Agencia Federal de Aviación Civil;

V. Consentir el uso del aeródromo civil de cualquier aeronave que no cumpla con los requisitos de la Ley de Aviación Civil, no haya sido permitida por quien presta el servicio de navegación aérea o que su acción u omisión dolosa contribuya a la comisión de algún delito;

VI. Incumplir con la obligación prevista en el párrafo segundo del artículo 22 de esta

Ley, referente a la remoción de cargos a personas o de transmisión de títulos accionarios, en los supuestos que se indican en dicho artículo;

VII. Modificar el porcentaje de inversión extranjera en contravención a lo establecido en el artículo 19 de esta Ley;

VIII. Contravenir las disposiciones en materia de seguridad en los aeródromos civiles, establecidas en esta Ley y otros ordenamientos aplicables;

IX. Interrumpir, total o parcialmente, la operación del aeródromo civil o la prestación de los servicios aeroportuarios o complementarios, sin causa justificada;

X. Incumplir con las obligaciones de conservación y mantenimiento del aeródromo civil;

XI. Prestar servicios distintos de los permitidos;

XII. No cubrir las indemnizaciones por daños que se originen con motivo de la prestación de los servicios;

XIII. Aplicar tarifas y precios que excedan a los registrados o, en su caso, sujetos a regulación;

XIV. Ejecutar u omitir actos que impidan o tiendan a impedir la actuación de otras personas prestadoras de servicios que tengan derecho a ello, así como la de autoridades que ejerzan atribuciones dentro del aeródromo civil;

XV. Limitar el número de personas prestadoras de servicios complementarios o negar su operación mediante actos de simulación, por razones distintas de las establecidas en el artículo 57 de esta Ley, y

XVI. Incumplir cualquiera de las obligaciones o condiciones establecidas en esta Ley, sus reglamentos y en el permiso respectivo, siempre que por el incumplimiento se haya impuesto una sanción y ésta haya quedado firme en términos de ley.

XVII. Cuando la persona permisionaria no informe a la autoridad aeronáutica cuando el aeródromo sea utilizado por una aeronave sin su consentimiento.

La Agencia Federal de Aviación Civil, en los supuestos de las fracciones I a VI anteriores, debe revocar los permisos de manera inmediata.

La Agencia Federal de Aviación Civil, en los casos de las fracciones VII a XVI, revocará el permiso cuando previamente se hubiese sancionado al permisionario, por lo menos en dos ocasiones, dentro de un periodo de cinco años.

Artículo 32. La operación de los aeródromos civiles que presten servicio a aeronaves militares, así como las operaciones de interceptación aérea, además de sujetarse a esta Ley, se supeditarán a la coordinación que se establezca con la Secretaría de la Defensa Nacional y la Secretaría de Marina.

Artículo 49. Todas las personas concesionarias y permisionarias de aeródromos civiles están obligadas a permitir su uso y prestar los servicios aeroportuarios y complementarios con que cuenten, en forma prioritaria, a las aeronaves militares; a aquéllas que se encuentren en actividades de búsqueda y salvamento; a aquéllas que apoyen en casos de desastre, y a las que se encuentren en condiciones de emergencia.

Artículo Cuarto.- De la Ley de Aviación Civil, se **reforman** los artículos 29, párrafos primero y último; 32, párrafos primero, segundo, tercero, cuarto y quinto; 86, párrafo primero y sus fracciones I, incisos i) y j), VII y VIII; 87, párrafo primero y sus fracciones V, XI, XII, XIV, XVI y XVII; 88, párrafo primero y sus fracciones II, XI, XIV, XVIII, XIX y XX, y 90, párrafo primero y sus fracciones II y III; se **adicionan** los artículos 8 Bis; 29, segundo párrafo, recorriéndose los subsecuentes; 34, segundo párrafo; 86, fracciones I, inciso K, IX, IX Bis, X, XI y XII; 87, fracciones XVIII y XIX; 88, fracciones XXI, XXII, XXIII, XXIV, XXV y XXVI, y 90, fracción IV, y se **deroga** el artículo 29, los actuales párrafos segundo y tercero, para quedar como sigue:

Artículo 8 Bis. Cuando el empleo de una aeronave amenace la seguridad de la aviación, la Secretaría de la Defensa Nacional coadyuvará con la Secretaría para garantizar la protección del espacio aéreo en lo siguiente:

I. Solicitar a las personas propietarias o la tripulación de una aeronave nacional o extranjera de servicio privado no comercial, los documentos que amparen que la aeronave cuenta con los certificados de aeronavegabilidad y licencia establecidos en el estado de su matrícula;

II. Verificar que los talleres aeronáuticos y centros de capacitación y adiestramiento, y la producción en el caso de fábricas de aeronaves y sus componentes, no se empleen para propósitos incompatibles con la aviación civil, y

III. Emitir opinión en la expedición de medidas y normas respecto del tráfico aéreo que afecte la protección del espacio aéreo.

Artículo 29. Las aeronaves para uso particular extranjeras pueden sobrevolar el espacio aéreo nacional y realizar aterrizajes y despegues en territorio mexicano, siempre que cuenten con la autorización de la Agencia Federal de Aviación Civil.

El primer aterrizaje podrá hacerse en un aeropuerto internacional, en el cual se

deberá tramitar la autorización correspondiente y cumplirse con los requisitos establecidos en las disposiciones técnico-administrativas aplicables. La autoridad a cargo del aeropuerto lo hará del conocimiento de la Secretaría de la Defensa Nacional.

Derogado.

Derogado.

Las personas propietarias o la tripulación de aeronaves para uso particular extranjeras deben acreditar ante la Agencia Federal de Aviación Civil, cuando se solicite, que cumplen con los requisitos técnicos sobre aeronavegabilidad y la licencia establecidos en el Estado de su matrícula.

Artículo 32. Toda aeronave, para realizar vuelos, debe llevar a bordo la información aeronáutica necesaria para sus operaciones, la póliza de seguro, así como los certificados de aeronavegabilidad y de matrícula vigentes o copia certificada de éstos.

La obtención del certificado de aeronavegabilidad está sujeta a que se demuestre que la aeronave cumple con los estándares de aeronavegabilidad aceptados por la Agencia Federal de Aviación Civil, así como a las pruebas, al control técnico y a los requisitos de mantenimiento que establezcan los reglamentos, las normas oficiales mexicanas y demás disposiciones técnico-administrativas.

La vigencia del certificado de aeronavegabilidad es de dos años.

Las aeronaves tienen que llevar a bordo los documentos y equipo que señalen esta Ley, sus reglamentos, las normas oficiales mexicanas, los tratados y demás disposiciones técnico-administrativas.

La Agencia Federal de Aviación Civil, por sí misma o a solicitud de la Secretaría de la Defensa Nacional, puede suspender o cancelar el certificado de aeronavegabilidad por incumplir los requerimientos y especificaciones mencionados en este artículo.

...

Artículo 34. ...

La Secretaría y la Secretaría de la Defensa Nacional, en su carácter de ente coordinador del Sistema de Vigilancia y Protección del Espacio Aéreo Mexicano, coordinarán sus acciones para la interceptación de aeronaves que realicen un vuelo clandestino, de conformidad con las disposiciones jurídicas aplicables.

Artículo 86. Las infracciones a lo dispuesto en la presente Ley cometidas por la persona concesionaria, asignataria, operadora aérea o permisionaria, según se trate, serán sancionadas por la Agencia Federal de Aviación Civil de acuerdo con lo siguiente:

I. ...

a) a **h)** ...

i) Por no llevar a bordo certificado de aeronavegabilidad o de matrícula o copia certificada de este último, con una multa de doscientas a un mil Unidades de Medida y Actualización;

j) Con documentos presentados a la Agencia Federal de Aviación Civil que no sean emitidos por una autoridad competente, con la intención de acreditar el cumplimiento de obligaciones o requisitos contenidos en esta Ley, en el reglamento correspondiente, normas oficiales mexicanas y disposiciones-técnico administrativas, con una multa de dos mil a diez mil Unidades de Medida y Actualización, y

k) Con documentos presentados a la Agencia Federal de Aviación Civil que no sean emitidos por las organizaciones responsables del diseño de tipo o responsables de la fabricación de aeronaves, motores, hélices, estaciones de pilotaje a distancia y sus artículos, con la intención de acreditar el cumplimiento de obligaciones o requisitos contenidos en esta Ley, en el reglamento correspondiente, normas oficiales mexicanas y disposiciones técnico-administrativas, con una multa de dos mil a diez mil Unidades de Medida y Actualización.

II. a **VI.** ...

VII. Negarse a participar en las operaciones de búsqueda y salvamento, salvo causa de fuerza mayor, con multa de un mil a cinco mil Unidades de Medida y Actualización;

VIII. ...

IX. No reportar las incapacitaciones, durante el vuelo, del personal técnico-aeronáutico a la Agencia Federal de Aviación Civil dentro de las 24 horas siguientes al suceso, con una multa de quinientas a mil Unidades de Medida y Actualización;

IX Bis. Cuando la aeronave realice maniobras de vuelo que motiven la activación de un alertamiento aéreo con una multa de diez mil a veinticinco mil Unidades de Medida y Actualización, siempre y cuando no sea por falla técnica o emergencia.

X. Permitir que el personal técnico-aeronáutico realice sus funciones:

a) Con una afectación médica que ponga en riesgo la seguridad operacional, con una multa de mil a cinco mil Unidades de Medida y Actualización;

b) Posterior a obtener un resultado positivo en un examen psicofísico o de detección de alcohol y sustancias psicoactivas, con una multa de doscientas a quinientas Unidades de Medida y Actualización, y

c) Con posterioridad a haberse involucrado en un accidente o incidente aéreo, sin que la Agencia Federal de Aviación Civil haya verificado, constatado e inspeccionado el cumplimiento de los requisitos médicos, a pesar de que el reconocimiento psicofísico haya tenido validez previa al evento, con una multa de un mil a dos mil Unidades de Medida y Actualización;

XI. Coaccionar a las personas inspectoras verificadoras por medio de violencia, física o moral, para obligarlos a que ejecuten un acto oficial, con una multa de dos mil a cinco mil Unidades de Medida y Actualización, y

XII. No realizar la notificación de dificultades en servicio, en los términos establecidos en esta Ley, los reglamentos correspondientes y las disposiciones técnico-administrativas aplicables, con multa de quinientas a dos mil Unidades de Medida y Actualización.

Artículo 87. Se les impondrán a las personas concesionarias, asignatarias, operadoras aéreas y permisionarias de servicio al público de transporte aéreo las siguientes sanciones por:

I. a **IV.** ...

V. No dar aviso a la Agencia Federal de Aviación Civil de las rutas que deje de operar, en los términos del artículo 22 de esta Ley, multa de tres mil a cinco mil Unidades de Medida y Actualización;

VI. a **X.** ...

XI. No proporcionar la información que le solicite la Agencia Federal de Aviación Civil, en los plazos fijados por ésta, multa de trescientas a tres mil Unidades de Medida y Actualización;

XII. No sujetarse a los itinerarios, frecuencias de vuelo y horarios autorizados, multa de quinientas a cinco mil Unidades de Medida y Actualización;

XIII. ...

XIV. No entregar mensualmente a la Agencia Federal de Aviación Civil la información señalada en el párrafo último del artículo 84 de esta Ley, multa de tres mil a cinco mil Unidades de Medida y Actualización;

XV. ...

XVI. Permitir que la aeronave transite sin llevar a bordo la copia certificada del Certificado de Explotador de Servicios Aéreos y la copia simple de las especificaciones de operación, con multa de cinco mil a quince mil Unidades de Medida y Actualización;

XVII. Presentar documentación que no fue emitida por la autoridad competente para realizar la operación de una aeronave, con una multa de dos mil a diez mil Unidades de Medida y Actualización, y la cancelación de la matrícula de la aeronave de que se trate:

XVIII. No cumplir con las disposiciones en materia de medio ambiente establecidas en esta Ley, el reglamento correspondiente, normas oficiales mexicanas y disposiciones técnico-administrativas aplicables en materia aeronáutica, multa de cuatro mil a siete mil Unidades de Medida y Actualización, y

XIX. Cuando la aeronave realice maniobras de vuelo que motiven la activación de un alertamiento aéreo, con una multa de diez mil a veinticinco mil Unidades de Medida y Actualización, siempre y cuando no sea por falla técnica o emergencia.

Artículo 88. Se impondrá sanción a la persona comandante o piloto de cualquier aeronave civil por:

I. ...

II. Transportar mercancías peligrosas, armas o artículos peligrosos, sin la debida autorización, multa de un mil a cinco mil Unidades de Medida y Actualización;

III. a **X.** ...

XI. No informar a la Agencia Federal de Aviación Civil o al comandante del aeropuerto más cercano, en el caso de incidentes o accidentes aéreos, dentro de las cuarenta y ocho horas siguientes a que tengan conocimiento de ellos, multa de trescientas a tres mil Unidades de Medida y Actualización;

XII. y **XIII.** ...

XIV. Volar sobre zonas prohibidas, restringidas o peligrosas, sin autorización de la Agencia Federal de Aviación Civil, multa de doscientas a dos mil Unidades de Medida y Actualización;

XV. a **XVII.** ...

XVIII. Operar la aeronave sin los documentos que deban llevarse a bordo de conformidad con esta Ley, el reglamento correspondiente, las disposiciones técnico-administrativas y demás disposiciones jurídicas aplicables, con una multa de quinientas a cinco mil Unidades de Medida y Actualización;

XIX. Operar la aeronave de manera negligente o fuera de los límites y parámetros establecidos por el fabricante de la misma, sin que medie causa justificada, multa de mil a cinco mil Unidades de Medida y Actualización;

XX. Presentar documentación que no fue emitida por la autoridad competente para realizar la operación de una aeronave, multa de dos mil a diez mil Unidades de Medida y Actualización;

XXI. Presentar documentación que no fue emitida por la autoridad competente relacionados con los certificados de aptitud psicofísica, o cualquier documento médico en los trámites administrativos con la Agencia Federal de Aviación Civil, así como en la realización de la evaluación médica, multa de quinientas a mil Unidades de Medida y Actualización;

XXII. Presentar documentación que no fue emitida por la autoridad competente durante la revalidación de la licencia de piloto, multa de quinientas a tres mil Unidades de Medida y Actualización;

XXIII. Ejercer en estado de ebriedad o bajo los efectos de sustancias psicoactivas las funciones que su licencia le confiere, multa de dos mil a cinco mil Unidades de Medida y Actualización;

XXIV. No reportar las incapacitaciones en vuelo a la Agencia Federal de Aviación Civil dentro de 24 horas, multa de doscientas a quinientas Unidades de Medida y Actualización;

XXV. Omitir o asentar en sus declaraciones de salud datos contrarios a su estado de salud, durante la evaluación médica, multa de quinientas a un mil Unidades de Medida y Actualización, y la denegación de la Evaluación Médica por un año, y

XXVI. Cuando realicen maniobras de vuelo que motiven la activación de un alertamiento aéreo, con una multa de diez mil a veinticinco mil Unidades de Medida y Actualización, siempre y cuando no sea por falla técnica o emergencia.

Artículo 90. Sin perjuicio a las demás sanciones que establece esta Ley y su reglamento, se le revocará la licencia a la persona comandante de la aeronave que incurra en los siguientes supuestos:

I. ...

II. Cuando realice actos u omisiones que tiendan al uso ilícito de instalaciones destinadas al tránsito aéreo, contrabando, contrabando equiparado, tráfico de órganos, ataques a las vías generales de comunicación, sabotaje, tráfico ilegal de personas, drogas y armas. Igual sanción se impondrá a cualquier miembro de la tripulación de vuelo, que se encuentre en los mismos supuestos;

III. Presentar documentación que no fue emitida por la autoridad competente para realizar la operación de una aeronave, y

IV. Cuando, sin causa legítima para ello, despegue o aterrice fuera de un aeródromo, o lo haga en uno sin permiso de operación o cuando haga uso de un aeródromo fuera de sus horarios de operación.

TRANSITORIOS

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

Segundo. Las erogaciones que se generen con motivo de la entrada en vigor del presente Decreto se realizarán con cargo al presupuesto autorizado para la Secretaría de la Defensa Nacional, por lo que no incrementará su presupuesto regularizable, y no se autorizarán recursos adicionales para el ejercicio fiscal de que se trate.

Tercero. Se derogan todas las disposiciones que se opongan a lo establecido en el presente Decreto.

Cuarto. A partir de la entrada en vigor del presente Decreto, las menciones contenidas en otras leyes, reglamentos y en general en cualquier disposición, que se realice al personal "Diplomado de Estado Mayor" y "Diplomado de Estado Mayor Aéreo", se entenderán hechas al personal "De Estado Mayor".

Quinto. A la entrada en vigor del presente decreto, la designación del personal "Diplomado de Estado Mayor" y "Diplomado de Estado Mayor Aéreo", será

reconocida plenamente en igualdad de circunstancias que el "De Estado Mayor".

Sexto. Los documentos expedidos al personal "Diplomado de Estado Mayor" y "Diplomado de Estado Mayor Aéreo", mantendrán su validez y vigencia, por lo que no será necesaria su reexpedición como "De Estado Mayor".

Séptimo. A la entrada en vigor del presente Decreto, las menciones contenidas en otras leyes, reglamentos, decretos, acuerdos y demás disposiciones administrativas respecto del Cuartel General Superior del Ejército y Fuerza Aérea, del Estado Mayor Aéreo, del Servicio de Control de Vuelo y del Servicio de Material Aéreo, se entenderán referidas al Cuartel General Superior Conjunto del Ejército y Fuerza Aérea, al Estado Mayor de la Fuerza Aérea, al Servicio de Defensa Aérea y al Servicio de Mantenimiento de Material Aéreo, respectivamente.

Ciudad de México, a 24 de abril de 2023

DIPUTADO FEDERAL
MARIO MIGUEL CARRILLO CUBILLAS