INSTITUTO FEDERAL DE TELECOMUNICACIONES

PLAN DE ACCIONES EN MATERIA DE CIBERSEGURIDAD

Noviembre 2018

Unidad de Política Regulatoria
Dirección General de Regulación Técnica

Versión	3
Fecha	Noviembre 2018
Elaboración	Unidad de Política Regulatoria Dirección General de Regulación Técnica Coordinación General de Política del Usuario Unidad de Asuntos Jurídicos Dirección General de Consulta Jurídica Unidad de Administración Dirección General de Tecnologías de la Información
Versión	2
Fecha	Junio 2018
Elaboración	Unidad de Política Regulatoria Dirección General de Regulación Técnica Coordinación General de Política del Usuario Unidad de Asuntos Jurídicos Dirección General de Consulta Jurídica Unidad de Administración Dirección General de Tecnologías de la Información
Versión	1
Fecha	Febrero 2018
Elaboración	Unidad de Política Regulatoria Dirección General de Regulación Técnica Coordinación General de Política del Usuario Unidad de Asuntos Jurídicos Dirección General de Consulta Jurídica

Tabla de contenido

01 OBJETIVO GENERAL

CIBERSEGURIDAD

Reconociendo la importancia del uso y aprovechamiento de las Tecnologías de la Información y Comunicación (TIC) de manera responsable, así como el incremento de riesgos, amenazas y ataques cibernéticos, el presente documento establece las acciones del Instituto Federal de Telecomunicaciones (Instituto) en el ámbito de la ciberseguridad basadas en un enfoque de gestión de riesgos. El Plan de Acciones en materia de Ciberseguridad del Instituto busca crear condiciones marco para incrementar la confianza en el entorno digital en México.

La ejecución del Plan de Acciones en materia de Ciberseguridad del Instituto permitirá fortalecer los beneficios derivados de una mayor inclusión social digital y de una mayor competencia en el sector de las telecomunicaciones y, favorecer la innovación y la economía digital.

El Instituto mediante el Plan de Acciones en materia de Ciberseguridad coadyuva, en el ámbito de sus atribuciones, a los diversos esfuerzos e iniciativas realizadas al respecto en México por múltiples partes interesadas.

02 JUSTIFICACIÓN

CIBERSEGURIDAD

Actualmente, los riesgos cibernéticos representan un desafío sistemático y la resiliencia cibernética constituye un bien público. Cada organización (pública o privada) contribuye a la resiliencia no solo de sus usuarios/clientes inmediatos, socios y proveedores, sino también a la del entorno digital en general. A efectos de garantizar la ciberseguridad y la resiliencia, las organizaciones deben realizar las acciones y desarrollar las capacidades que permitan el uso y aprovechamiento de las TIC de manera responsable, así como que garanticen su propia capacidad de recuperación[1]. Lo anterior,

[1] https://www.weforum.org/projects/partnering-for-cyber-resilience

en un marco de concientización, coordinación y cooperación de todas las partes interesadas y con un enfoque basado en gestión de riesgos.[2,3]

En este tenor se destaca que, de acuerdo a la *Encuesta de Delitos Económicos 2018*[4]:

- México es el segundo país más atacado de la región de América Latina, el primer lugar lo ocupa Brasil.
- El 49% de las empresas se han enfocado principalmente en evaluar sus vulnerabilidades y riesgos de ciberataques.
- El 56% de las empresas encuestadas, indicaron haber sido víctimas de ciberataques, causando en la mayoría grandes pérdidas para las organizaciones.

Por otra parte, en el reporte de *Tendencias de Seguridad en América Latina y el Caribe*[5] los costos de los delitos cibernéticos alcanzaron aproximadamente los 3,000 millones de dólares.

La legislación vigente en Telecomunicaciones, ha permitido realizar diferentes cambios para establecer los fundamentos constitucionales y legales para crear una nueva arquitectura jurídica, institucional, regulatoria y de competencia y libre concurrencia en el sector de las telecomunicaciones y de la radiodifusión. Fundamentos basados en principios de efectividad, certidumbre jurídica, promoción de la competencia, regulación eficiente, inclusión social digital, independencia, transparencia y rendición de cuentas.

Dicha inclusión social digital no será posible si no existe confianza en los servicios, dispositivos e infraestructura por parte de la población, por lo que es de suma importancia que el Instituto, en el ámbito de sus atribuciones, establezca y ejecute diversas acciones que fortalezcan la seguridad cibernética y resiliencia del entorno digital en México, incremente la confianza en el uso de internet, así como fomente la innovación y permita una evolución tecnológica segura y confiable.

Considerando las mejores prácticas internacionales, las acciones propuestas reflejan un enfoque basado en la gestión de riesgos; esto es, el riesgo de seguridad vinculado a las actividades basadas en el entorno digital.

El Plan de Acciones en materia de Ciberseguridad busca coadyuvar al cumplimiento de las leyes aplicables, de los compromisos internacionales asumidos por el Estado Mexicano y de los instrumentos programáticos del Ejecutivo Federal, en materia de ciberseguridad. Asimismo, pretende contribuir a un ecosistema digital seguro, impulsar tendencias tecnológicas como el Internet de las

---

[2] "*Los responsables de políticas deben reconocer que el riesgo de seguridad digital es una cuestión económica y social, y no solamente un desafío técnico. También han de tener en cuenta que es imposible crear un entorno digital totalmente protegido y seguro en el que se evite por completo el riesgo, por lo que conviene que potencien un enfoque en el que los dirigentes y los responsables de la toma de decisiones asuman la responsabilidad de gestionar dicho riesgo. Esto implica reducirlo a un nivel aceptable que viene dado tanto por los objetivos económicos y sociales y sus correspondientes beneficios, como por el contexto.*" (Políticas de banda ancha para América Latina y el Caribe. Un manual para la economía digital. OCDE, BID 2016)

3 Recomendación que emite el Consejo Consultivo del Instituto Federal de Telecomunicaciones respecto ciberseguridad, CC/IFT/P/4/2018, 5 de julio de 2018.

[4] Encuesta de delitos económicos 2018, PwC, https://www.pwc.com/mx/es/publicaciones/c2g/2018-04-13-encuesta-delitos-economicos-2018-mexicov4.pdf?utm_source=Website&utm_medium=Consulta%20%20https://pwc.to/2HariCi

[5] Tendencias de seguridad en América Latina y el Caribe, OEA, https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Cosas, Internet de las Cosas Industrial y la Inteligencia Artificial, que repercuten en la seguridad digital de infraestructuras críticas, así como coadyuvar, particularmente, al logro de diversos objetivos de la Estrategia Nacional de Ciberseguridad.

03 ANTECEDENTES

CIBERSEGURIDAD

A continuación, se describe de manera general la Estrategia Nacional de Ciberseguridad (ENC) emitida por el poder Ejecutivo en 2017, donde, el Instituto participó activamente en su creación, los compromisos internacionales asumidos por el Estado Mexicano, así como las acciones que el Instituto ha realizado o se encuentra desarrollando en materia de ciberseguridad.

3.1 ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

CIBERSEGURIDAD

El Poder Ejecutivo, en el marco de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), acordó, por unanimidad, la creación de la Subcomisión de Ciberseguridad en octubre de 2017, la cual está presidida por la Secretaría de Gobernación a través de la entonces denominada Comisión Nacional de Seguridad (CNS). Entre otras tareas, la Subcomisión de Ciberseguridad se encargará de dar seguimiento y coordinar la implementación de la Estrategia Nacional de Ciberseguridad[6] (ENC).

La ENC establece ocho ejes transversales a efecto de fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano. Dichos ejes son:

[6] https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

1. Cultura de ciberseguridad
2. Desarrollo de capacidades
3. Coordinación y colaboración
4. Investigación, desarrollo e innovación en TIC
5. Estándares y criterios técnicos
6. Infraestructuras críticas
7. Marco jurídico y autorregulación
8. Medición y seguimiento

Lo anterior, tomando como principios rectores un enfoque basado en gestión de riesgos, una perspectiva de derechos humanos y la colaboración multidisciplinaria y de múltiples actores.

La ENC establece los siguientes objetivos estratégicos:

1. **Sociedad y derechos.**
   Generar las condiciones para que la población realice sus actividades de manera responsable, libre y confiable en el ciberespacio, con la finalidad de mejorar su calidad de vida mediante el desarrollo digital en un marco de respeto a los derechos humanos como la libertad de expresión, vida privada y protección de datos personales, entre otros.

2. **Economía e innovación.**
   Fortalecer los mecanismos en materia de ciberseguridad para proteger la economía de los diferentes sectores productivos del país y propiciar el desarrollo e innovación tecnológica, así como el impulso de la industria nacional en materia de ciberseguridad, a fin de contribuir al desarrollo económico de individuos, organizaciones privadas, instituciones públicas y sociedad en general.

3. **Instituciones públicas.**
   Proteger la información y los sistemas informáticos de las instituciones públicas del país para el funcionamiento óptimo de éstas y la continuidad en la prestación de servicios y trámites a la población.

4. **Seguridad pública.**
   Incrementar las capacidades para la prevención e investigación de conductas delictivas en el ciberespacio que afectan a las personas y su patrimonio, con la finalidad de mantener el orden y la paz pública.

5. **Seguridad nacional.**
   Desarrollar capacidades para prevenir riesgos y amenazas en el ciberespacio que puedan alterar la independencia, integridad y soberanía nacional, afectando el desarrollo y los intereses nacionales.

3.2 COMPROMISOS INTERNACIONALES

El artículo 14.3 del Protocolo Adicional al Acuerdo Marco de la Alianza del Pacífico prevé que un Estado tome medidas que sean necesarias para garantizar la seguridad y confidencialidad de los mensajes, o para proteger la privacidad de los datos personales de los usuarios finales.

El artículo 19.5 del negociado Acuerdo comercial entre México, Estados Unidos y Canadá (T-MEC) prevé acciones de colaboración para contrarrestar amenazas de ciberseguridad, desarrollo de capacidades, enfoque basado en riesgos y compartición de información y mejores prácticas.

Mientras que, las Recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad[7] publicado por la Organización de Estados Americanos (OEA), en las consideraciones sobre la gestión del riesgo, señala que el Gobierno de México debe abordar la seguridad cibernética mediante un enfoque basado en la gestión de riesgos, lo anterior permitirá seleccionar las medidas de seguridad adecuadas para proteger y fomentar el desarrollo económico, social, así como la detección de amenazas, vulnerabilidades y su impacto potencial.

Asimismo, recomienda incentivar a las empresas a invertir en seguridad cibernética, ya sea a través de regulaciones, subvenciones, políticas u otras medidas como la reducción de impuestos. La modernización de la infraestructura y los servicios en México también crea una gran oportunidad para digitalizar los procesos y aumentar el valor de la misma para los ciudadanos.

Finalmente, recomienda desarrollar y difundir estándares de fuerza laboral y productos de seguridad cibernética, lo anterior a efecto de incluir normas mínimas de seguridad de la información para todos los productos vinculados a internet u otros sistemas digitales. Existen numerosos ejemplos de guías de normas disponibles de otras naciones y de la industria, por lo que se sugiere una asociación entre el gobierno y las partes interesadas e implicadas, donde se puedan determinar las normas para México, o en su caso, que los procesos nacionales se puedan adaptar a algún modelo ya existente como base para establecer un conjunto común de características y requisitos donde las mismas compañías puedan compartir sus propias normas y estándares de desempeño.

3.3 ACCIONES REALIZADAS POR EL IFT EN MATERIA DE CIBERSEGURIDAD

CIBERSEGURIDAD

[7] Recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad, OEA, http://www.oas.org/documents/spa/press/Recomendaciones-para-el-Desarrollo-de-la-Estrategia-Nacional-de-Ciberseguridad.pdf

Consciente de la importancia de contribuir a un ecosistema digital más confiable y seguro, el Instituto, ha llevado a cabo diversas acciones en el ámbito de la ciberseguridad, las cuales se describen en la Tabla 1.

Temática	Acciones IFT
Estrategia Nacional de Ciberseguridad	• Se participó activamente en talleres, mesas de trabajo y foros cuyo objetivo fue la construcción de la Estrategia Nacional de Ciberseguridad. • El Instituto es invitado permanente de la Subcomisión de Ciberseguridad y el encargado de liderar el grupo de trabajo correspondiente al objetivo "Sociedad y derechos" de la ENC en coordinación con el Secretario Ejecutivo del Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes (SIPINNA). En este contexto, se han coordinado mesas de trabajo con la participación de organizaciones públicas, privadas y de la sociedad civil a efecto de: o Identificar áreas de oportunidad y mejores prácticas en materia de ciberseguridad en el uso y aprovechamiento de las TIC para el fortalecimiento de políticas públicas con perspectiva de derechos humanos. o Establecer una estrategia de gestión de riesgos en materia de ciberseguridad que permita identificar las principales amenazas a las que se encuentra expuesta la población, con la finalidad de concientizar e incentivar un uso responsable de las TIC. o Recomendar los mecanismos y ruta crítica para la actualización y armonización del marco jurídico en el ámbito de ciberseguridad con perspectiva de derechos humanos y no discriminación.
Prospectiva regulatoria	• En septiembre de 2017 se organizó, en coordinación con la representación de la Unión Europea en México, un taller de ciberseguridad en el marco del instrumento Technical Assistance and Information Exchange (TAIEX) Expert Mission. En dicho taller se contó con la participación de expertos de Reino Unido, España, Finlandia, el Instituto Europeo de Normas de Telecomunicaciones (ETSI) y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA). Se expusieron y discutieron temas relativos a la seguridad en dispositivos y redes, información a los usuarios y futuras amenazas cibernéticas. • Se encuentra en desarrollo el estudio denominado "Estudio prospectivo regulatorio relativo a la ciberseguridad de equipos terminales móviles, infraestructura del servicio móvil y dispositivos IoT", cuyo objetivo fue el análisis de las tendencias a nivel internacional respecto a las mejores prácticas y regulación (evaluación de la conformidad) relativas a la ciberseguridad de equipos terminales móviles, infraestructura del servicio

	móvil y dispositivos IoT. Lo anterior con el fin de contar con elementos para la toma de decisiones en este ámbito. • Se han llevado a cabo diversas reuniones prospectivas con fabricantes de dispositivos e infraestructura de telecomunicaciones. • Se encuentra en desarrollo un nuevo Procedimiento de Evaluación de la Conformidad que contempla esquemas de certificación para productos TIC.
Colaboración en Materia de Seguridad y Justicia	• En abril de 2017 se publicó en el DOF la "Disposición Técnica IFT-011-2017: Especificaciones de los equipos terminales móviles que puedan hacer uso del espectro radioeléctrico o ser conectados a redes de telecomunicaciones. Parte 1. Código de Identidad de Fabricación del Equipo (IMEI) y funcionalidad de receptor de radiodifusión sonora en Frecuencia Modulada (FM).", cuyo objeto, entre otros, es que la existencia de un IMEI único y válido en un equipo terminal móvil sea un requerimiento para la obtención del certificado de homologación correspondiente. Consecuentemente, dichos equipos podrían ser inequívocamente identificados, pudiéndose efectuar su bloqueo cuando exista reporte de robo o extravío. Asimismo, establece la conformación de la base de datos de IMEI de equipos terminales móviles homologados. • En reuniones del Grupo Técnico[8], se ha solicitado a los concesionarios presentar propuestas de solución relativas a la identificación y almacenamiento de direcciones IP. Lo anterior, derivado de las manifestaciones que las autoridades han realizado respecto a la importancia y necesidad de que dichas direcciones IP se almacenen dada la naturaleza y evolución tecnológica de los delitos electrónicos. En este contexto, diversos concesionarios han expuesto los sistemas/problemáticas para identificar y almacenar direcciones IP a efecto de colaborar con las autoridades competentes. • En este tenor, las autoridades también han manifestado su interés de transitar al protocolo de internet IPv6. • Se coordina el Comité Especializado[9] de estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Lo anterior, a efectos de que los productos generados por este Comité Especializado pudieran ser implementados por las autoridades correspondientes.

[8] Grupo de Trabajo conformado por las Autoridades Facultadas, Autoridades Designadas, el Instituto y los Concesionarios y Autorizados, establecidos en los Lineamientos de Colaboración en Materia de Seguridad y Justicia publicados en el Diario Oficial de la Federación el 2 de diciembre de 2015.

[9] El Comité Especializado de Estudios e Investigaciones en Telecomunicaciones cuyas funciones se establecen en los Lineamientos de Colaboración en Materia de Seguridad y Justicia publicados en el Diario Oficial de la Federación el 2 de diciembre de 2015.

Puntos de Intercambio de tráfico de Internet (IXP)	El 24 de julio de 2017, el IFT publicó en el DOF los "Lineamientos que fijan los términos bajo los cuales el agente económico preponderante en el sector de las telecomunicaciones o con poder sustancial deberá tener presencia física en los puntos de intercambio de tráfico de internet en el territorio nacional y celebrar los convenios que permitan a los proveedores de servicios de internet el intercambio interno de tráfico de manera más eficiente y menos costosa", a través de estos lineamientos se enfatiza la seguridad en la información al fomentar la disminución del intercambio de tráfico nacional (incluyendo el intercambio de tráfico local) en el extranjero.
Transición a IPv6	• Con el fin de detectar retos, oportunidades y factores que retrasen e inhiban la adopción del protocolo de internet IPv6, el IFT aplicó un cuestionario para el diagnóstico tecnológico relativo a la migración de IPv6 en México en marzo de 2017. Cabe destacar que, aunque IPv6 no es en estricto sentido más seguro que IPv4, hace extremadamente difícil que un atacante que utiliza la "fuerza bruta" (barrido de puertos, o "*port scanning*") vulnere un equipo servidor o una aplicación. • En diciembre de 2017, se creó un micrositio relativo a IPv6 que puede ser accedido desde el portal de internet del Instituto, el cual presenta información relevante acerca de este protocolo, así como la visión y acciones del Instituto relativas al proceso de adopción, con el fin de que sirvan como referencia para cualquier otra organización (pública o privada) interesada en México. • Actualmente, el Instituto se encuentra analizando tendencias y recomendaciones internacionales con el fin de publicar una serie de recomendaciones que permitan a las entidades públicas y privadas que utilizan y/u ofrecen servicios a través de internet, transitar a IPv6.
Información al usuario	Se asignó una sección especial dentro del rubro de Usuarios, en la página principal del IFT, con la finalidad de agrupar la información y materiales didácticos generados sobre el tema de ciberseguridad. Como actividad continua, se difunden a través de las redes sociales institucionales diversos materiales informativos que promueven las mejores prácticas relativas a la seguridad y la protección de información en la red, en temáticas como virus Informáticos, robo y pérdida de información, aplicaciones no seguras, Wi-Fi público, consejos para descargar aplicaciones, *phishing* y fraude. Asimismo, se dio inicio a dos campañas de difusión dirigidas a niños y MiPymes, que tienen como objetivo difundir información focalizada a las necesidades de cada grupo en materia de seguridad en la red.

Norma Mexicana de Comercio Electrónico	Participación en la elaboración de la Norma Mexicana de Comercio Electrónico, en la que se han propuesto normas internacionales de seguridad.
Tratados y acuerdos internacionales	Se han realizado aportaciones a diversos tratados y acuerdos, como es el caso del Tratado entre México, Estados Unidos y Canadá (T-MEC), así como a los que forman parte del Foro de Cooperación Económica de Asia Pacífico (APEC), donde se enfatiza la necesidad de enfoques basados en gestión de riesgos y la coordinación y colaboración internacional en el ámbito de la ciberseguridad.

Tabla 1. Acciones llevadas a cabo por el IFT.

04 ÁMBITO COMPETENCIAL DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES

CIBERSEGURIDAD

De conformidad con el artículo 28, párrafo décimo quinto de la Constitución Política de los Estados Unidos Mexicanos (en lo sucesivo, "Constitución"), el Instituto tiene por objeto el desarrollo eficiente de la radiodifusión y las telecomunicaciones, conforme a lo dispuesto en la propia Constitución y en los términos que fijen las leyes.

Para tal efecto, en términos del precepto constitucional invocado, así como de los artículos 1 y 7 de la Ley Federal de Telecomunicaciones y Radiodifusión (en lo sucesivo, "LFTR"), el Instituto tiene a su cargo la regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, los recursos orbitales, los servicios satelitales, las redes públicas de telecomunicaciones y la prestación de los servicios de radiodifusión y de telecomunicaciones, así como del acceso a la infraestructura activa y pasiva y otros insumos esenciales, garantizando lo establecido en los artículos 6o. y 7o. de la Constitución.

A su vez, que el artículo 2° de la LFTR establece que, al ejercer la rectoría en la materia, el Estado protegerá la seguridad y la soberanía de la Nación y garantizará la eficiente prestación de los servicios públicos de interés general de telecomunicaciones y radiodifusión; para tales efectos, establecerá condiciones de competencia efectiva en la prestación de dichos servicios para beneficio de la población y bienestar social.

El vigésimo párrafo de la fracción IV del artículo 28 de la Constitución señala que el Instituto podrá emitir disposiciones administrativas de carácter general exclusivamente para el cumplimiento de su función regulatoria en el sector de su competencia. En ese orden de ideas, el párrafo segundo del artículo 7 de la LFTR prevé que el Instituto tiene a su cargo la regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico; y, el párrafo cuarto del mismo artículo, prevé que el Instituto es autoridad en materia de lineamientos técnicos relativos a la infraestructura y los equipos que se conecten a las redes de telecomunicaciones, así como en materia de homologación y evaluación de la conformidad de dicha infraestructura y equipos.

I. Disposiciones técnicas , evaluación de la conformidad y homologación.

El artículo 15, fracciones I y LVI, de la LFTR señala que el Instituto tiene la atribución de expedir disposiciones administrativas de carácter general, planes técnicos fundamentales, lineamientos, modelos de costos, procedimientos de evaluación de la conformidad, procedimientos de homologación y certificación y ordenamientos técnicos en materia de telecomunicaciones y radiodifusión; así como demás disposiciones para el cumplimiento de lo dispuesto en la LFTR.

Las Disposiciones Técnicas son instrumentos de observancia general expedidos por el Instituto conforme a lo establecido en el artículo 15, fracción I de la LFTR, a través de los cuales se regulan características y operación de productos, dispositivos y servicios de telecomunicaciones y radiodifusión y, en su caso, la instalación de los equipos, sistemas y la infraestructura en general asociada a éstos, así como las especificaciones que se refieran a su cumplimiento o aplicación. En este tenor, el Instituto se encuentra facultado para expedir Disposiciones Técnicas que establezcan especificaciones técnicas relativas a la seguridad de dispositivos e infraestructura de telecomunicaciones.

Asimismo, el artículo 15 fracción XXXVIII de la LFTR faculta al Instituto establecer y operar laboratorios de pruebas o autorizar a terceros a que lo hagan, a fin de fortalecer la autoridad regulatoria técnica en materias de validación de los métodos de prueba de las normas y disposiciones técnicas, aplicación de lineamientos para la homologación de productos destinados a telecomunicaciones y radiodifusión, así como sustento a estudios e investigaciones de prospectiva regulatoria en estas materias y las demás que determine, en el ámbito de su competencia, de conformidad con la disponibilidad presupuestaria autorizada. En este tenor, el Instituto podría establecer laboratorios de prueba para validar, en su caso, los métodos de prueba a ser establecidos en disposiciones técnicas relativas a la seguridad de equipos e infraestructura, así como para la aplicación de pruebas de vulnerabilidades a los mismos. Los resultados de dichas pruebas serían publicitados ampliamente y serían elementos para la toma de decisiones del Instituto en el ámbito de ciberseguridad.

Finalmente, el artículo 289 de la LFTR establece que los productos, equipos, dispositivos o aparatos destinados a telecomunicaciones o radiodifusión que puedan ser conectados a una red de telecomunicaciones o hacer uso del espectro radioeléctrico deberán homologarse conforme a las normas o disposiciones técnicas aplicables, de conformidad con lo establecido en la Ley Federal sobre Metrología y Normalización.

Esto es, el Instituto en términos de lo establecido en el artículo 7, cuarto párrafo, de la LFTR es la autoridad en materia de lineamientos técnicos relativos a la infraestructura y a los equipos que hacen uso del espectro radioeléctrico o que se conectan a redes de telecomunicaciones, así como en materia de homologación y evaluación de la conformidad de dicha infraestructura y equipos.

II. Impacto en el comercio exterior.

Si bien el Instituto está facultado por la Constitución, la LFTR y su Estatuto Orgánico para emitir las disposiciones técnicas relativas a la infraestructura y los equipos que se conecten a las redes de telecomunicaciones y hagan uso del espectro radioeléctrico, así como en materia de evaluación de la conformidad de dicha infraestructura y equipos, también es importante resaltar que la regulación de las telecomunicaciones se encuentra estrechamente vinculada a otros sectores y materias que corresponden a dependencias de la Administración Pública Federal, como es el caso de la importación, comercialización, distribución y consumo de productos en el país.

De ahí que la Secretaría de Economía, en el ámbito de su competencia, emita la Norma Oficial Mexicana (NOM) correspondiente, que regule la importación, comercialización y/o distribución

dentro del territorio de los Estados Unidos Mexicanos de dispositivos cuyas especificaciones se prevean en las Disposiciones Técnicas que emita el Instituto.

En este orden de ideas, en el marco de la coordinación y colaboración entre el Instituto y la Secretaría de Economía que prevén la LFTR y la Ley Federal de Metrología y Normalización (en lo sucesivo, "LFMN"), al emitirse por el Instituto una Disposición Técnica, la Secretaría de Economía realiza los actos jurídicos correspondientes como son, por una parte, la emisión de la norma oficial mexicana que regule la importación, comercialización y/o distribución dentro del territorio de los Estados Unidos Mexicanos de Equipos Terminales Móviles y, por la otra, la actualización del Acuerdo de NOMs.

Derivado de lo anterior, en el punto de entrada a México, las autoridades aduaneras deberán hacer cumplir lo dispuesto por las NOMs correspondientes que regulen la importación, comercialización y/o distribución dentro del territorio de los Estados Unidos Mexicanos de productos de telecomunicaciones y radiodifusión, cuyas especificaciones se prevean en dichas Disposiciones Técnicas.

III. Inclusión digital universal y cobertura universal.

El artículo 15 fracción XXXI de la LFTR indica que el Instituto tiene la atribución de realizar las acciones necesarias para contribuir, en el ámbito de su competencia, al logro de los objetivos de la política de inclusión digital universal y cobertura universal establecida por el Ejecutivo Federal; así como a los objetivos, metas fijadas y los demás instrumentos programáticos relacionados con los sectores de radiodifusión y telecomunicaciones.

IV. Privacidad de los usuarios y seguridad de la red.

El artículo 145 fracción III de la LFTR establece que los concesionarios y autorizados que presten el servicio de acceso a internet deberán sujetarse a los lineamientos de carácter general que, al efecto, expida el Instituto donde se deberá contemplar el preservar la privacidad de los usuarios y la seguridad de la red.

Referente a la privacidad de los usuarios, se menciona que el 26 de enero de 2017 se publicó en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que prevé un capítulo específico sobre la obtención y tratamiento de datos personales en posesión de las instancias de seguridad, procuración y administración de justicia, en el cual se dispone la obligación de establecer medidas de seguridad de nivel alto para garantizar su integridad, disponibilidad, confidencialidad y protección (artículo 80 y siguientes). Lo anterior, aunado a las obligaciones que tienen las referidas instancias de establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales (artículos 23 y 24), así como de establecer y mantener las medidas de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado (artículo 31).

Al respecto, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados dispone que corresponde al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en lo sucesivo, "INAI") garantizar el ejercicio del derecho a la protección de datos personales en posesión de las instancias de seguridad, procuración y

administración de justicia como sujetos obligados, así como vigilar y verificar el cumplimiento de la ley (artículos 89, fracciones I y XIV, 146 y siguientes). También le corresponde al INAI emitir las disposiciones administrativas de carácter general para el debido cumplimiento de los principios, deberes y obligaciones que establece la mencionada ley, así como emitir lineamientos generales para el debido tratamiento de los datos personales (artículo 89, fracciones XIX y XXVII).

Por su parte, la Ley General de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública prevén en sus artículos 70, fracción XLVII, y 69, fracción V, inciso a), respectivamente, la obligación que tienen los sujetos obligados en materia de seguridad pública y procuración de justicia de poner a disposición del público y mantener actualizada, en los respectivos medios electrónicos, para efectos estadísticos, el listado de solicitudes a las empresas concesionarias de telecomunicaciones y proveedores de servicios o aplicaciones de internet para la intervención de comunicaciones privadas, el acceso al registro de comunicaciones y la localización geográfica en tiempo real de equipos de comunicación, que contenga exclusivamente el objeto, el alcance temporal y los fundamentos legales del requerimiento, así como, en su caso, la mención de que cuenta con la autorización judicial correspondiente.

La observancia de lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública corresponde al INAI, que garantiza en el ámbito federal el ejercicio de los derechos de acceso a la información (artículo 17) por lo cual se encuentra atribuida de facultades para determinar la responsabilidad por incumplimiento de la misma, la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables (artículo 21, fracción XIX).

En consistencia con lo anterior, por lo que se refiere a los concesionarios de telecomunicaciones y autorizados, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece que las personas físicas o morales de carácter privado son responsables del tratamiento de datos personales, ya sea de su obtención, uso, divulgación o almacenamiento, por cualquier medio, así como de su cancelación (artículos 2, 3, fracciones XIV y XVIII, y 11). Los responsables del tratamiento de datos personales deben establecer medidas de seguridad administrativas, técnicas y físicas que protejan los datos contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado (artículo 19).

Al respecto, es el INAI el garante de la vigilancia, verificación y de imposición de sanciones relacionadas a la obtención, tratamiento, conservación y supresión de datos personales (artículos 38, 59 y siguientes).

De acuerdo con el análisis anterior, el Instituto se encuentra facultado para emitir lineamientos de carácter general para preservar la seguridad de la red a los que los concesionarios y autorizados que presten el servicio de acceso a internet deberán sujetarse.

V. Colaboración con la Justicia.

Es obligación del Estado Mexicano garantizar la seguridad pública, la seguridad nacional, así como una efectiva procuración de justicia, por lo que en la LFTR se incluyó el Título Octavo "De la Colaboración con la Justicia", que establece en el artículo 189 la obligación de los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y

contenidos de atender todo mandamiento por escrito, fundado y motivado de la autoridad competente, en los términos que establezcan las leyes. En este tenor, el artículo Vigésimo Segundo transitorio de la LFTR mandató que el Instituto emitiera las disposiciones administrativas de carácter general a que se refiere el Título Octavo de la LFTR.

Además, conforme al párrafo tercero del artículo 190, fracción I, de la LFTR, le corresponde al Instituto, escuchando a las instancias de seguridad y procuración de justicia, establecer los lineamientos que los concesionarios de telecomunicaciones y autorizados deben adoptar para que la colaboración con dichas autoridades sea efectiva y oportuna.

Al respecto, los Lineamientos de Colaboración en Materia de Seguridad y Justicia fueron publicados en el DOF el 2 de diciembre de 2015.

05 PLAN DE ACCIONES EN MATERIA DE CIBERSEGURIDAD

CIBERSEGURIDAD

La ejecución del Plan de Acciones en materia de Ciberseguridad permitirá robustecer los beneficios derivados de una mayor inclusión social digital, de una mayor competencia en el sector de las telecomunicaciones, así como fomentar la economía digital.

A efecto de lograr los beneficios planteados y considerando el ámbito competencial del Instituto, el Plan de Acciones en materia de Ciberseguridad plantea los siguientes cinco Objetivos Estratégicos Institucionales:

1. Seguridad en dispositivos e infraestructura
2. Seguridad en redes
3. Colaboración en materia de seguridad y justicia
4. Cultura de ciberseguridad
5. Colaboración en la implementación de la Estrategia Nacional de Ciberseguridad

Figura 1. Objetivos Estratégicos Institucionales.

El presente Plan de Acciones en materia de Ciberseguridad se suma a las acciones y esfuerzos gubernamentales existentes en el ámbito, complementando y creando condiciones marco para un entorno digital seguro.

Los Objetivos Estratégicos Institucionales serán alcanzados mediante acciones derivadas de las siguientes acciones transversales, los cuales son armónicos con los ejes transversales establecidos en la ENC:

I. Investigación, desarrollo e innovación
II. Desarrollo de capacidades
III. Coordinación y colaboración
IV. Medición y seguimiento

5.1 OBJETIVOS ESTRATÉGICOS INSTITUCIONALES

5.1.1 SEGURIDAD EN DISPOSITIVOS E INFRAESTRUCTURA

Se encuentra en desarrollo un marco regulatorio o, en su caso, un marco de referencia de seguridad para dispositivos e infraestructura de telecomunicaciones con un enfoque basado en gestión de riesgos y enfatizando la seguridad por diseño, con el fin de disminuir riesgos cibernéticos y aumentar su resiliencia. Lo anterior, como resultado del desarrollo de análisis prospectivos, colaboración y consultas con los actores interesados. Dichos dispositivos e infraestructura incluyen los equipos terminales móviles, dispositivos IoT, infraestructura del servicio móvil, fijo y de radiodifusión.

El marco regulatorio o de referencia será ágil y flexible para permitir la rápida evolución tecnológica y cambiantes necesidades del sector, así como armónico con las mejores prácticas internacionales[10] a efectos de evitar la creación de obstáculos técnicos al comercio e inhibir la innovación.

De conformidad con la disponibilidad presupuestaria autorizada. se prevé establecer y operar un laboratorio de pruebas a fin de fortalecer la autoridad regulatoria técnica que permitirá evaluar la seguridad cibernética de dispositivos e infraestructura y/o su conformidad con el marco regulatorio/de referencia en dicho ámbito; así como dar sustento a estudios e investigaciones de prospectiva regulatoria en esta materia. Los resultados obtenidos serán ampliamente difundidos a efectos de que los usuarios cuenten con información para su toma de decisiones.

Finalmente, se incluirá un nuevo esquema de certificación para productos IoT en el Procedimiento de Evaluación de la Conformidad en materia de telecomunicaciones y radiodifusión, a efectos de sentar las bases para la homologación ágil y flexible y la posterior vigilancia en el mercado de dichos productos.

10 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/748196/054718_DCMS_IoT_Code_of_Practice_SPANISH_LA.pdf

5.1.2 SEGURIDAD EN REDES

Se establecerá un marco regulatorio o, en su caso, un marco de referencia relativo a la seguridad en las redes que presten el servicio de acceso a Internet basado en un enfoque de gestión de riesgos y mejores prácticas internacionales. Dicho marco será el resultado de desarrollo de estudios prospectivos, colaboración y consultas con todos los actores interesados.

El marco regulatorio/de referencia en comento será ágil y flexible para permitir la rápida evolución tecnológica y necesidades del sector, así como armónico con los enfoques internacionales, tendiente a incentivar la economía digital.

Así mismo, el Instituto, continuará llevando a cabo las acciones pertinentes para coadyuvar a la reducción de llamadas realizadas para cometer delitos utilizando las redes públicas de telecomunicaciones.

5.1.3 COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA

El Instituto continúa, conforme lo establece la LFTR, escuchando a las autoridades y realizando acciones, en el ámbito de sus atribuciones, a efectos de que la colaboración de los concesionarios, autorizados y proveedores de servicios y aplicaciones y contenidos, sea efectiva, oportuna y contemple la evolución tecnológica.

El Instituto se mantiene coordinando a los concesionarios, autorizados y las organizaciones a que se refiere el artículo 190, fracción XII de la LFTR en el Comité Especializado[11] en los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Lo anterior, a efecto de que los productos generados por el Comité Especializado pudieran ser implementados por las autoridades correspondientes.

[11] El Comité Especializado de Estudios e Investigaciones en Telecomunicaciones cuyas funciones se establecen en los Lineamientos de Colaboración en Materia de Seguridad y Justicia publicados en el Diario Oficial de la Federación el 2 de diciembre de 2015.

Paralelamente, se trabaja en los Grupos Ejecutivo y Técnico[12] a efecto de dar seguimiento a la definición e implementación de, en su caso, nuevos requerimientos de información conforme a la evolución tecnológica de las telecomunicaciones.

5.1.4 CULTURA DE CIBERSEGURIDAD

El IFT continuará ejecutando una estrategia de comunicación, que incluye objetivos definidos e identifica a los destinatarios de la información, alineada al eje transversal homólogo establecido en la ENC. Lo anterior, con el objeto de concientizar a los usuarios de internet acerca de los principios y acciones para el uso responsable y seguro del mismo.

Dicha estrategia contempla la elaboración de material informativo tales como infografías y videos temáticos en diferentes aspectos de la ciberseguridad. Asimismo, con la finalidad de establecer métodos prácticos de divulgación de la información, así como mecanismos para crear, impulsar y fomentar la alfabetización digital de los usuarios, se realizarán actividades como webinars, talleres, foros y pláticas por públicos objetivo (niños, adolescentes, adultos y adultos mayores) donde participen expertos de la academia, la industria, la sociedad civil y el gobierno.

Asimismo, se impulsará la comunicación entre los actores de los sectores de las telecomunicaciones y radiodifusión respecto a la respuesta a incidentes cibernéticos.

[12] Grupos de Trabajo conformados por las Autoridades Facultadas, Autoridades Designadas, el Instituto y los Concesionarios y Autorizados, establecidos en los Lineamientos de Colaboración en Materia de Seguridad y Justicia a efecto de definir y adoptar medidas que permitan una colaboración más efectiva y oportuna en materia de seguridad y justicia

5.1.5 COLABORACIÓN EN LA IMPLEMENTACIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

El Instituto continuará participando y apoyando activamente en la implementación de la Estrategia Nacional de Ciberseguridad. En este tenor, los objetivos estratégicos y ejes transversales del Instituto coadyuvarán a la ejecución y fortalecimiento de los ejes transversales de la Estrategia Nacional de Ciberseguridad (Tabla 2).

Eje Transversal ENC	Objetivo estratégico/Acción transversal IFT
Cultura de ciberseguridad	Cultura de ciberseguridad
Coordinación y colaboración	Colaboración en materia de Seguridad y Justicia.
Estándares y criterios técnicos	Seguridad en dispositivos e infraestructura Seguridad en redes
Infraestructuras críticas	Seguridad en dispositivos e infraestructura Seguridad en redes
Medición y seguimiento	Medición y seguimiento

Tabla 2. Ejes trasversales de la ENC y el Plan de Acciones en materia de Ciberseguridad.

5.2 ACCIONES TRANSVERSALES

Las labores derivadas de la implementación de las acciones transversales impactarán el logro de todos los objetivos estratégicos institucionales planteados.

5.2.1 INVESTIGACIÓN, DESARROLLO E INNOVACIÓN

A efecto de contar con información y análisis oportunos y continuos de tecnologías de punta, tendencias y enfoques a nivel mundial en el ámbito de la ciberseguridad, se prevé establecer un monitor de ciberseguridad a efecto de realizar el correspondiente seguimiento y conocer el estado del arte en los ámbitos tecnológico, jurídico y social, con el fin de contar con los elementos necesarios para la correspondiente toma de decisiones informada y basada en evidencia. Lo anterior, de conformidad con la disponibilidad presupuestaria autorizada.

Se continuarán elaborando estudios prospectivos relativos a la ciberseguridad en dispositivos, infraestructura y redes considerando su impacto en diversos ámbitos, tales como la economía digital, la innovación y el Internet de las Cosas. Asimismo, se desarrollarán estudios con enfoques jurídicos y de desarrollo digital, todo lo anterior con el objetivo de contar con un panorama general, así como recomendaciones derivadas del análisis sobre las mejores prácticas, regulación y evaluación de la conformidad a nivel internacional para que la Unidad de Política Regulatoria identifique alternativas, y, en su caso, ejecute las acciones necesarias.

En el laboratorio de pruebas de ciberseguridad se podrán diseñar, desarrollar y/o validar métodos de pruebas, con el objeto de identificar vulnerabilidades de dispositivos e infraestructura

5.2.2 DESARROLLO DE CAPACIDADES

A efecto de estar en condiciones de lograr efectivamente los objetivos estratégicos planteados, se continuará y se extenderá la capacitación del personal involucrado. Adicionalmente, se robustecerán los esfuerzos para el intercambio de experiencias y capacitación a nivel internacional. El desarrollo de capacidades de personal altamente especializado constituirá una actividad permanente.

Asimismo, con el fin de coadyuvar al fortalecimiento institucional, continuará la adopción de las mejores prácticas y marcos de seguridad, armonizado con enfoques internacionales, en materia de ciberseguridad a efecto no sólo de lograr una organización más segura y resiliente, sino también de consolidar al Instituto como referente nacional en la materia.

5.2.3 COORDINACIÓN Y COLABORACIÓN

Se continuará robusteciendo la colaboración interinstitucional y, dentro de las atribuciones del Instituto, se coadyuvará a la ejecución coordinada de los esfuerzos y ejercicios relativos a la ciberseguridad.

Aunado lo anterior y conforme a las mejores prácticas internacionales, se llevarán a cabo mesas de trabajo focalizadas (ej. PyMEs, asociaciones de consumidores) con los múltiples actores interesados, no solo con los actores del sector TIC/telecomunicaciones.

Se participará activamente en organismos internacionales de estandarización, tales como la Unión Internacional de Telecomunicaciones, en esquemas y foros de cooperación internacional, y se fortalecerá la interacción con los diferentes actores de la industria de telecomunicaciones y la radiodifusión, compartiendo experiencias y problemáticas en el ámbito de la ciberseguridad.

De la misma manera, se promoverá la colaboración entre los diferentes actores de la industria de telecomunicaciones y la radiodifusión, con el objetivo de establecer protocolos de comunicación y respuesta a incidentes de ciberseguridad que aumenten la resiliencia de los servicios y el entorno digital.

5.2.4 MEDICIÓN Y SEGUIMIENTO

Se implementará un sistema de medición y seguimiento del avance en el logro de los objetivos estratégicos, basado en los esfuerzos y ejercicios tanto institucionales como nacionales e internacionales existentes, en su caso, adecuados al entorno nacional. Paralelamente, el impacto, así como la efectividad de los marcos regulatorios propuestos, serán medidos a través de los análisis de impacto regulatorio ex ante y ex post correspondientes.

La Tabla 3 muestra un resumen del Plan de Acciones en materia de Ciberseguridad descrito anteriormente:

Objetivo Estratégico	Acciones
Seguridad en dispositivos e infraestructura	• Desarrollo de estudios prospectivos relativos a la seguridad de equipos terminales móviles, dispositivos IoT, infraestructura del servicio móvil y fijo y la nube. • Estudio de planeación relativo al establecimiento gradual de un laboratorio de pruebas de ciberseguridad. • Establecimiento y operación de un laboratorio de pruebas de ciberseguridad. • Nuevo esquema de certificación para productos IoT. • Formación de personal altamente especializado. • Participación activa en la Comisión de Estudio 17 de la UIT y en foros relativos al intercambio de experiencias en el ámbito. • Establecimiento de un marco regulatorio/de referencia para la seguridad de dispositivos e infraestructura. • Conformación de mesas de trabajo de múltiples partes interesadas.
Seguridad en redes	• Desarrollo de estudios prospectivos relativos a la seguridad de las redes. • Formación de personal altamente especializado. • Participación activa en la Comisión de Estudio 17 de la UIT y en foros relativos al intercambio de experiencias en el ámbito. • Conformación de mesas de trabajo de múltiples partes interesadas. • Coordinación para coadyuvar a la reducción de llamadas realizadas para cometer delitos utilizando las redes públicas de telecomunicaciones. • Establecimiento de marcos regulatorios/de referencia relativos a la seguridad de las redes.
Colaboración en materia de seguridad y justicia	• Identificar las necesidades en términos de estudios e investigaciones de las autoridades de seguridad y justicia y, comunicarlo a los integrantes del Comité Especializado a efecto de que sean considerados por los mismos. • Participar en el Grupo Técnico a efecto de dar seguimiento a la definición e implementación, en su caso, de nuevos requerimientos de información conforme a la

	evolución tecnológica de las telecomunicaciones (ej. conservación de direcciones IP y transición a IPv6).
Cultura de ciberseguridad	• Elaboración de material informativo tales como infografías y videos temáticos. • Llevar a cabo diversas actividades de alfabetización digital como webinars, talleres, foros y pláticas por sectores (niños, adolescentes y adultos) donde participen expertos de la academia, la industria, la sociedad civil y el gobierno. • Establecer y/o armonizar protocolos de comunicación y respuesta a incidentes de ciberseguridad entre los diferentes actores de la industria de telecomunicaciones y la radiodifusión.
Colaboración en la implementación de la Estrategia Nacional de Ciberseguridad	• Continuar colaborando como líder del grupo Sociedad y Derechos en la organización de mesas de trabajo para el logro de los objetivos del grupo. • Contribuir a los ejes de Estándares y Criterios Técnicos, Cultura de Ciberseguridad e Infraestructura Crítica.

Tabla 3. Plan de Acciones en materia de Ciberseguridad.

06 CONCLUSIONES

CIBERSEGURIDAD

El Instituto, consciente de que la seguridad cibernética es una tarea transversal y de todos, continuará coadyuvando y, en su caso, fortaleciendo las acciones en materia de ciberseguridad, en el ámbito de sus atribuciones, que permitan a las múltiples partes interesadas el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible de México.

La ejecución del Plan de Acciones en materia de Ciberseguridad del Instituto, basado en un enfoque de gestión de riesgos, permitirá fortalecer los beneficios derivados de una mayor inclusión social digital y de una mayor competencia en el sector de las telecomunicaciones y, favorecer la innovación y la economía digital.

El Plan de Acciones en materia de Ciberseguridad del Instituto complementa los esfuerzos realizados desde diferentes ámbitos, fomentando el debate y la cooperación entre el sector público y el privado, el impulso a la creación de herramientas, el intercambio y, en su caso, adopción de mejores prácticas y la convocatoria a las partes interesadas para tomar decisiones de forma efectiva sobre las responsabilidades de seguridad compartidas.