RECOMENDACIÓN QUE EMITE EL VII CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES EN MATERIA DE APROXIMACIÓN, PROSPECTIVA Y COLABORACIÓN REGULATORIA MULTIDISCIPLINARIA DEL IFT CON OTROS ÓRGANOS REGULADORES

1. INTRODUCCIÓN

La regulación de las telecomunicaciones es una función administrativa y técnica del Estado. La habilitación del derecho de acceso a Internet, los servicios de telecomunicaciones y las Tecnologías de la Información y Comunicación, como un derecho fundamental, es un mandato constitucional.

Artículo 6º de la Constitución Política de los Estados Unidos Mexicanos (Constitución):

"El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet."

Artículo 1° de la Constitución.

"Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad."

La interpretación de estas dos disposiciones constitucionales, supone que el derecho de acceso a Internet habilita, *ipso iure*, dentro del mundo digital, todos los derechos humanos reconocidos en la Constitución.

El derecho de acceso a Internet se transforma en un derecho habilitador de derechos fundamentales en el ejercicio y uso de las telecomunicaciones y las tecnologías digitales. La interpretación literal de esta disposición constituye un mandato para todas las autoridades en sus distintas competencias federales y administrativas, quienes deben promover la más amplia tutela y protección a esta disposición. Para el caso de los órganos garantes y reguladores, los mandatos constitucionales mencionados, generan interpretaciones, acciones y procesos específicos dentro de su esfera de competencia, que viene a enriquecer

la actividad regulatoria del Estado mexicano en su conjunto. Este corpus de interpretaciones, nace disperso, subjetivo y construye convicción jurídica para cada órgano autónomo o regulatorio, por lo que se mantiene independiente, de una aproximación o visión regulatoria integral del Estado.

El Instituto Federal de Telecomunicaciones (IFT) es un órgano autónomo constitucional del Estado mexicano, cuyas competencias y facultades están circunscritas a la Constitución y la Ley Federal de Telecomunicaciones y Radiodifusión. Las facultades del IFT nos permiten identificarlo como un órgano regulador en diversas materias, como competencia económica y acceso a la infraestructura de telecomunicaciones, pero también como un órgano habilitador y garante del derecho de acceso a Internet y los servicios de telecomunicaciones.

El IFT es un órgano dual que regula y se vuelve un órgano garante de derechos fundamentales, a partir de habilitar el derecho de acceso a Internet en todas sus formas y bajo los procesos determinados por la ley.

La función reguladora y la habilitadora de derechos fundamentales en el mundo digital es una función de alta dinámica en su gestión, ejecución procesal, interpretación y prospectiva.

Los organismos garantes son autónomos, especializados, independientes, imparciales y colegiados, con personalidad jurídica y patrimonio propios, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, al igual que los órganos regulatorios.

Sin embargo, derivado del ejercicio de sus competencias, las acciones regulatorias, determinaciones habilitantes de derechos fundamentales en sus distintas expresiones y diversas acciones, comienzan a ser coincidentes, semejantes en grado de confusión o competencial y comienzan a coincidir o converger entre distintos órganos garantes o regulatorios del Estado[1].

[1] Ejemplos de ello se pueden encontrar en:

Con el avance científico y tecnológico, tiene como resultado nueva tecnología, infraestructura de conectividad y se presenta un efecto multiplicador del impacto de la tecnología, creando nuevas conductas o efectos que se expresan de diversas formas, áreas del derecho y órganos garantes o regulatorios del Estado.

Pensar en lo digital es imaginar la realidad jurídica en su conjunto, pero digitalizada, fragmentada; porciones de una misma realidad esparcidas en diversas áreas, materias y realidades. El hecho digital es un objeto fragmentado en múltiples materias, cuya percepción es compleja.

Es fácil vivir en el mundo digital, pero difícil regular, legislar y generar política pública o política regulatoria. Hace falta una aproximación compleja para hablar de lo digital, en suma, de lo que haremos con ella.

Por lo anterior, hay que aproximarnos desde una perspectiva multi e interdisciplinaria a esta realidad.

2. RECOMENDACIONES

I. El Instituto Federal de Telecomunicaciones diseñe una metodología para identificar, observar, analizar, evaluar, generar indicadores, y simular el impacto de las diversas expresiones de la tecnología digital e infraestructura de telecomunicaciones en materia de competencia económica, derechos humanos y diversas disciplinas que, aparentemente, no son competencia del IFT.

- RECOMENDACIÓN QUE EMITE EL CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES (INSTITUTO) RELACIONADA CON EL IMPULSO DE LA CREACIÓN DE UN COMITÉ TÉCNICO DE POLÍTICA PARA EL ENTORNO DIGITAL, IV Consejo Consultivo, 2019
- RECOMENDACIÓN QUE EMITE EL CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES EN MATERIA DE CIBERSEGURIDAD Y CIBER RESILIENCIA EN EL ÁMBITO DE LAS COMPETENCIAS DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES, VII Consejo Consultivo, 2023, y
- OPINIÓN QUE EMITE EL VII CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES SOBRE EL DESPLIEGUE SOSTENIBLE DE LAS TELECOMUNICACIONES Y LA RADIODIFUSIÓN PARA LA EXPLORACIÓN DE GUÍAS DE REGULACIÓN DEL SECTOR DESDE LA PERSPECTIVA DEL IMPACTO AL AMBIENTE, LA SOCIEDAD Y LOS ASPECTOS TÉCNICOS. VII Consejo Consultivo, 2023.

II. La observación regulatoria o prospectiva regulatoria sugerida documentada y presentada a la evaluación de un grupo interdisciplinario convocado expresamente por el IFT.

III. El IFT institucionalice un trabajo de conversaciones de tipo regulatorio, legislativo, de política pública y regulatoria con diversos órganos autónomos y de la administración pública, que sean competentes en alguna dimensión jurídica, con la tecnología digital e infraestructura de telecomunicaciones, con la finalidad de generar un proceso de observación y prospectiva regulatoria que identifique y defina futuros problemas regulatorios, de competencia entre diversos órganos autónomos del Estado y administrativos centralizados, así como la posible colaboración multidisciplinaria e interinstitucional.

Lilia Eurídice Palma Salas
Presidenta del VII Consejo Consultivo

Mtra. Rebeca Escobar Briones
Secretaria del Consejo Consultivo

La Recomendación fue aprobada por el VII Consejo Consultivo del Instituto Federal de Telecomunicaciones por unanimidad de votos de los consejeros: Alejandro Ildefonso Castañeda Sabido, Sara Gabriela Castellanos Pascacio, Ernesto M. Flores-Roux, Mario Germán Fromow Rangel, Gerardo Francisco González Abarca, Misha Leonel Granados Fernández, Ali Bernard Haddou Ruiz, Erik Huesca Morales, Salma Leticia Jalife Villalón, Luis Miguel Martínez Cervantes, Jorge Fernando Negrete Pacheco, Lucía Ojeda Cárdenas, Edgar Olvera Jiménez[2], Eurídice Palma Salas y Cynthia Gabriela Solís Arredondo. Lo anterior, en términos del artículo 17, en la X Sesión Ordinaria celebrada el 28 de septiembre de 2023, mediante Acuerdo CC/VII/IFT/280923/34.

El proyecto de Recomendación fue elaborado por el consejero Jorge Fernando Negrete Pacheco.

[2]El consejero Edgar Olvera Jiménez manifestó su voto a favor de la recomendación por vía WhatsApp del grupo del VII CCIFT. Al respecto, la consejera presidenta Eurídice Palma Salas dio cuenta del voto del consejero Olvera Jiménez en la X Sesión Ordinaria del VII CCIFT.

FIRMADO POR: LILIA EURIDICE PALMA SALAS
FECHA FIRMA: 2023/10/18 5:29 PM
AC: AUTORIDAD CERTIFICADORA
ID: 73110
HASH:
65E5DF8BCCC46E4ADC3985CA25C6973E2BB56269263D1D
B452821504D33C035E

FIRMADO POR: REBECA ESCOBAR BRIONES
FECHA FIRMA: 2023/10/23 10:17 AM
AC: AUTORIDAD CERTIFICADORA
ID: 73110
HASH:
65E5DF8BCCC46E4ADC3985CA25C6973E2BB56269263D1D
B452821504D33C035E

RECOMENDACIÓN QUE EMITE EL CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES EN MATERIA DE CIBERSEGURIDAD Y CIBER RESILIENCIA EN EL ÁMBITO DE LAS COMPETENCIAS DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES

I. INTRODUCCIÓN

En 2022, el Foro Económico Mundial (WEF, por sus siglas en inglés) estimó que la transformación digital, como parte de una cuarta revolución industrial, podría agregar a la economía mundial en 2025 un valor del orden de 100 trillones de dólares estadounidenses, debido a que la pandemia ha acelerado la digitalización de múltiples bienes y servicios.[1] Si bien en ese mismo año las empresas del sector de tecnologías de información registraron fuertes disminuciones en su valor y reducciones de personal laboral, la transformación digital sigue en curso y es una motivación para diseñar, construir y administrar acciones que propicien la ciber resiliencia de las empresas.

El Reporte de Riesgos Globales 2023 del Foro Económico Mundial[2] posiciona a los ciberataques en infraestructuras críticas entre los diez principales riesgos globales que enfrenta el mundo. Además, el registro de noticias mundiales sobre ataques exitosos a organizaciones y sus cadenas de suministro en infraestructuras cibernéticas nos demuestran que no existe un ciberespacio 100% seguro, debido a que el ritmo de crecimiento de los ciberataques es del 15% anual y estos cada vez se vuelven más sofisticados.[3] La revista especializada *Cybersecurity Ventures* reconoce que el volumen de

[1] The *Cyber Resilience Index: Advancing Organizational and Cyber Resilience, World Economic Forum in collaboration with Accenture*, July 2022.

[2] Disponible a través de la liga: https://www.weforum.org/agenda/2023/01/these-are-the-biggest-risks-facing-the-world-global-risks-2023/?DAG=3&gclid=EAIaIQobChMI852q3qHugAMVSBitBh0Gog54EAAYASAAEgI1CvD_BwE. Véase también https://es.weforum.org/agenda/2023/01/riesgos-globales-2023-que-los-expertos-dicen-que-podemos-hacer-al-respecto/.

[3] Para el caso de Estados Unidos, véase por ejemplo *Cybersecurity: Selected Cyberattacks, 2012-2022, Congressional Research Service,* Updated August 9, 2023, disponible a través de la liga: https://crsreports.congress.gov/product/pdf/R/R46974. Para el de México, véase por ejemplo "2020, en 12 hackeos o incidentes de seguridad en México", Rodrigo Riquelme, El Economista, 2 de enero de 2021, disponible a través de la liga: https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html

las transferencias económicas ocasionadas por los ciberataques exitosos ha sido el de mayor impacto monetario en la historia, aunque no sólo ha impactado en los aspectos financieros de las organizaciones; sino que, además, se pierde la productividad, existen daños a la reputación, pueden incurrir en responsabilidades legales o situarse en una discontinuidad de la operación de la organización.

Los principales objetivos de ciberataque habían sido las grandes empresas privadas y algunas infraestructuras críticas gubernamentales[4], tanto en sus infraestructuras físicas y lógicas como en sus cadenas de suministro. No obstante, en 2019 *Accenture* publicó el estudio *Cost of Cyber Crime*[5] donde se indica que el 43% de los ciberataques ya corresponden a pequeñas organizaciones y solamente 14% de las mismas tienen la capacidad de recuperarse. Asimismo, especialistas en ciberseguridad reportan que a julio de 2023 en México se detectaron 43 millones de ataques con *phishing*, 10 veces más que en 2022, y más de 2 millones 311 mil ataques mediante *malware* dirigido a dispositivos móviles, principalmente con sistema operativo Android.[6]

A raíz del crecimiento exponencial de ataques cibernéticos a nivel mundial y la expansión hacia nuevos objetivos como lo son las micro, pequeñas y medianas empresas (mipymes), se incorpora el concepto de ciber resiliencia. En el glosario del Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de los Estados Unidos (NIST) **la ciber resiliencia se define como "la habilidad de anticipar, soportar, recuperarse de y adaptarse a condiciones adversas, tensión, ataques o afectaciones en sistemas que**

[4] El hackeo de SEDENA-*papers* –por parte del grupo "Guacamaya"– filtró un total de 4 millones de correos electrónicos de la Secretaría de Defensa Nacional de México, que supervisa el Ejército y la Fuerza Aérea del país. La eventualidad originó preocupación en la reunión bilateral sobre temas de seguridad entre México y Estados Unidos en Washington D.C., ya que el ataque fue dirigido específicamente a la infraestructura militar mexicana. Además, tras estos sucesos, se reconoció el riesgo de que información sensible, relacionada con las operaciones de campo para el combate al crimen organizado trasnacional, sea expuesta en los foros de la *dark web*. (extraído de https://www.forbes.com.mx/ad-cuatro-ciberataques-grandes-ciberseguridad-uber-sedena-conti-optus/)

[5] Disponible a través de la liga: https://www.accenture.com/us-en

[6] Véase para más detalles "Se disparan los ataques de phishing y troyanos bancarios en México", Antonio Hernández, El Universal, 22/08/2023, disponible a través de la liga: https://www.eluniversal.com.mx/cartera/se-disparan-los-ataques-de-phishing-y-troyanos-bancarios-en-mexico/

utilizan o están habilitados por recursos cibernéticos" y "tiene la intención de habilitar misiones y objetivos de negocios cuyo logro depende de recursos cibernéticos en un ciber ambiente competido".[7] Cabe destacar que la recuperación por lo general se dará bajo condiciones diferentes a las del estado inicial en el que se encontraba dicha organización al haber sufrido dicho incidente. Por lo tanto. la naturaleza de la ciber resiliencia es más de carácter evolutivo y adaptativo; a diferencia de la ciberseguridad, la seguridad de la información y los planes de desastre y recuperación (DRP por sus siglas en inglés), entre otros, que son de carácter preventivo.

Al establecer cadenas de suministro a través de tecnologías de la información e infraestructuras de redes de telecomunicaciones e Internet asociadas a servicios, aplicaciones, equipos y dispositivos que se conectan a estas infraestructuras, tanto las cadenas de suministro como las infraestructuras pueden ser susceptibles de ser vulneradas. Además, existe la posibilidad de que a través de ellas se puedan alcanzar a otros elementos de la cadena de suministro y de otras infraestructuras TIC (proveedores, clientes, cadena de importación, y exportación, entre otros) extendiendo el daño más allá del origen de la perpetración.

Por ejemplo, en el ciber ambiente[8] de algunos de los sectores que suelen adoptar las nuevas tecnologías con mayor rapidez, como lo es el financiero, las instituciones financieras y grandes empresas tecnológicas (*big tech*) ofrecen productos y servicios financieros mediante diversas asociaciones que varían desde la realización de funciones de interfase con usuarios a la provisión conjunta. Si bien la falta de transparencia alrededor de tales asociaciones dificulta identificar si éstas incentivan a una mayor toma de riesgos, lo que sí es claro es que estas asociaciones abren una oportunidad amplia para que sufran ciberataques y otras actividades criminales. Cuando en la cadena de valor de algún bien o servicio participan diferentes empresas, como pueden ser las *big techs* y las de servicios de

[7] Véase, para más detalles, https://csrc.nist.gov/glossary/term/cyber_resiliency
[8] Véase para más detalles El ciber-ambiente como entorno dentro del ciber-espacio. Perspectiva jurídica-ambiental, César Alfredo Contreras Ruiz, Publicaciones e Investigación, ISSN-e 2539-4088, ISSN 1900-6608, Vol. 15, Nº. 1, 2021.

telecomunicaciones, es más difícil identificar quiénes son los responsables de fallas en la protección de los intereses de los usuarios. En este contexto, las fallas en la operación de las empresas proveedoras de servicios de telecomunicaciones pueden tener un impacto negativo en la reputación de las empresas que son sus clientes. En la medida en que la digitalización avance en otras actividades económicas, más empresas pueden enfrentar problemas similares y, actualmente, ya se han registrado casos en que esa afectación se presenta en la seguridad de información de los clientes o de las propias empresas, o en la interrupción del acceso a ciertos servicios almacenados o provistos a través de medios cibernéticos de los clientes o de las propias empresas, afectando su confidencialidad, integridad y disponibilidad (anexo).[9, 10]

El Instituto Federal de Telecomunicaciones (IFT o Instituto), en el Plan de Acciones en materia de Ciberseguridad (Plan) que divulgó para consulta pública en noviembre de 2018[11] reconoce que: "***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***

[9] El Banco de México publica desde 2019 un reporte anual acerca de los principales incidentes cibernéticos ocurridos en el sistema financiero nacional a través de la liga: https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html. En otros países han experimentado ciber ataques redes de hospitales ("Ciberataque afecta hospitales y atención médica en cinco estados de EEUU", Los Angeles Times, 4/ago/2023, disponible a través de la liga https://www.latimes.com/espanol/eeuu/articulo/2023-08-04/ciberataque-afecta-hospitales-y-atencion-medica-en-cinco-estados-de-eeuu) **A**gricultores ("Farmers are being targeted by cyber-criminals", The Economist, 5/ago/2021, disponible a través de la liga: https://www.economist.com/britain/2021/08/05/farmers-are-being-targeted-by-cyber-criminals)

[10] La ciberseguridad es una herramienta que se utiliza dentro de la seguridad de la información para proteger datos almacenados en sistemas de cómputo. Pero la ciberseguridad también es una práctica más amplia de defender los activos de tecnologías de información de ataques, del cual la seguridad de información es un componente. En consecuencia, se puede considerar que ambos campos que se intersectan. Para más detalles, véase "Information security vs. cyber security: The definite guide", Dataguard, UK (disponible a través de la liga https://www.dataguard.co.uk/blog/information security vs cyber security) o "What is information security? Definition, principles, and Jobs", CSO, 17/Jan/2020 (disponible a través de la liga: https//www.csoonline.com/article/568841/what-is-information-security-definition-principles-and-jobs.html)

[11] Para más detalles, el Plan de Acciones en materia de Ciberseguridad del IFT está disponible a través de la liga https://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/upr-planaccionesciberseguridad.pdf

que permitan el uso y aprovechamiento de las TIC de manera responsable, así como que garanticen su propia capacidad de recuperación".

Para lograr los beneficios planteados y considerando el ámbito competencial del Instituto, el Plan señala 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; y

5. Colaboración en la implementación de la Estrategia Nacional de Ciberseguridad.

A su vez, anteriores Consejos Consultivos del IFT han presentado al Instituto recomendaciones en materia de ciberseguridad en 2018[12] y en 2021[13]. Aquellas recomendaciones propusieron que el IFT se involucre de manera activa en este tema mediante la colaboración con otras autoridades, la emisión de lineamientos técnicos, la creación de áreas especializadas de análisis y laboratorios de pruebas, o la negociación de tratados internacionales, entre otras acciones y medidas.

Esta recomendación aborda algunos temas sobre ciber resiliencia que este Consejo Consultivo considera prioritarios. El resto de este documento está organizado en tres secciones. En la sección II se presenta un breve recuento de algunas de las acciones relevantes que ya ha realizado el IFT en materia de ciber resiliencia. En la sección III se

[12] Recomendación que emite el Consejo Consultivo del Instituto Federal de Telecomunicaciones respecto ciberseguridad (disponible a través de la liga https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fconsejoconsultivo.ift.org.mx%2Fdocs%2Frecomendaciones%2F2018%2FRecomendacion-Ciberseguridad.docx&wdOrigin=BROWSELINK)

[13] Recomendación que emite el Consejo Consultivo del Instituto Federal de Telecomunicaciones (Instituto) para promover la economía digital: Impulsar la cultura de la Ciberseguridad en México para incrementar la confianza en la economía digital (disponible a través de la liga https://consejoconsultivo.ift.org.mx/docs/recomendaciones/2021/iii_2_recomendacion_para_promover_economia_digital_vf.pdf

revisan algunas consideraciones, tales como las acciones recientes en esta materia que están llevándose a cabo en otros países, nuevas metodologías propuestas por organismos de estandarización e internacionales, así como la creciente adopción del cómputo en la nube. La sección final recomienda al IFT algunas acciones que podría emprender para reforzar su actuación en este ámbito de su competencia.[14]

II. PRINCIPALES ACCIONES REALIZADAS POR EL IFT RELACIONADAS CON LOS OBJETIVOS ESTRATÉGICOS INSTITUCIONALES DESCRITOS EN EL PLAN DE ACCIONES EN MATERIA DE CIBERSEGURIDAD[15]

Es importante reconocer que, a pesar de que el IFT aún no divulgó una versión final del Plan que puso a consulta pública en 2018, eso no fue un impedimento para que el IFT llevara a cabo diversas acciones propuestas en él que buscan mejorar la habilidad de las empresas de anticipar, soportar, recuperarse de y adaptarse a ataques cibernéticos. Lo anterior, principalmente a través de la elaboración de estudios, códigos de mejores prácticas y diversas guías para los usuarios:

- En julio de 2020, con el fin de implementar el uso de los servicios en la nube a gran escala en el país, el IFT publicó el "Estudio de *Cloud Computing* en México"[16]. En ese estudio se identifican los tipos de configuración de los servicios en la nube, recursos de red e infraestructura necesarios para su desarrollo; se expone la evolución de las actividades que realiza esta nueva plataforma de servicios y su vinculación con las redes de telecomunicaciones; y se identifican diversas regulaciones y mejores prácticas para promover la innovación, así como el desarrollo de la infraestructura y operaciones de las redes actuales y futuras. Se trata de un estudio que explica de manera clara y

[14] El capítulo 4 del Plan de Acciones en materia de Ciberseguridad del IFT contiene una discusión muy completa acerca de la competencia del Instituto para la emisión de disposiciones relacionadas con aspectos técnicos, evaluación de la conformidad y homologación; inclusión digital y cobertura universal; privacidad de los usuarios y seguridad de la red; y colaboración con la justicia (páginas 12 a 16).
[15] Para conocer de manera más pormenorizada las acciones en materia de ciber resiliencia realizadas por el Instituto, el pasado 23 de mayo algunos miembros del VII Consejo Consultivo del IFT se reunieron con titulares y colaboradores de la Coordinación General de Política del Usuario, la Unidad de Administración, la Unidad de Asuntos Jurídicos y la Unidad de Política Regulatoria donde les plantearon una serie de preguntas al respecto.
[16] Disponible a través de la liga: https://www.ift.org.mx/sites/default/files/dgci_estudio-cloud_computing.pdf

completa cómo está estructurada la oferta de estos servicios y algunas estimaciones sobre el crecimiento de su demanda, en términos del tráfico de datos. Cabe destacar que el estudio contiene, dentro del capítulo "Mercados y Regulación", una sección breve acerca de los principales arreglos de ciberseguridad con que opera el cómputo en la nube. En materia de ciberseguridad y ciber resiliencia es relevante un mejor conocimiento sobre el cómputo en la nube debido a que su adopción, además de impactar la forma en que operan las empresas, también conlleva valorar potenciales riesgos de diversa índole, inclusive para su cumplimiento con algunas regulaciones sectoriales.[17]

- En 2021, por la relevancia de la seguridad en redes de telecomunicaciones y radiodifusión, en el espectro radioeléctrico y en equipos y dispositivos que se conectan a la red, el IFT **participó en la primera reunión del subgrupo de ciberseguridad de la Subsecretaría de Comercio Exterior de la Secretaría de Economía (SE) donde se presentó el "Protocolo Nacional Homologado para la gestión de incidentes de Ciberseguridad"**[18] (Protocolo). Este Protocolo, elaborado por Coordinación de Estrategia Digital Nacional de la Presidencia de la República, la Secretaría de Seguridad y Protección Ciudadana, y la Guardia Nacional, establece las actividades para las fases de preparación, detección, respuesta y recuperación ante incidentes cibernéticos en activos esenciales de información a cargo de las dependencias federales, entidades federativas, organismos constitucionales autónomos, academia e instancias del sector privado[19] del país.

---

[17] Véanse, por ejemplo, los documentos "Guidance on Cyber Reslilience", Reserve Bank of New Zealand, May 2021 (disponible a través de la liga https://www.rbnz.govt.nz/-/media/project/sites/rbnz/files/consultations/cyber-resilience/guidance-on-cyber-resilience.pdf) o "*Improving cyber resilience for regulated entities", Reserve Bank of New Zealand*, February 2022 (disponible a través de la liga: https://www.rbnz.govt.nz/regulation-and-supervision/cross-sector-oversight/improving-cyber-resilience-for-regular-entities)

[18] Disponible a través de la liga: https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf. Cabe mencionar que este protocolo toma el marco de referencia sobre Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de Estados Unidos de América (Cybersecurity Framework CSF, por sus siglas en inglés).

[19] Véase como un ejemplo del tipo de guías que están desarrollando instancias del sector privado el documento Guía de Buenas prácticas para auditar la Ciberseguridad, Asociación Bancaria y de Entidades

- El Protocolo considera fases de **preparación, detección, respuesta y recuperación**; con las siguientes funciones:

  i. **Identificar**, orienta en la identificación del contexto del Múltiple Involucrado, los activos esenciales de información que soportan los servicios esenciales, y los riesgos en materia de Ciberseguridad para la construcción de una estrategia de gestión de riesgos alineada a las necesidades de la institución.

  ii. **Proteger**, orienta en el desarrollo de un plan apropiado de seguridad que garantice la entrega de los servicios esenciales proporcionados por los activos esenciales de información. Esta función tiene la finalidad de establecer estrategias para limitar o contener el impacto de un eventual ataque cibernético.

  iii. **Detectar**, orienta en el desarrollo de acciones apropiadas para la detección de eventos que afecten la Ciberseguridad de los activos esenciales de información y en consecuencia puedan afectar los servicios esenciales que prestan. La función de detección permite el descubrimiento oportuno de incidentes de Ciberseguridad.

  iv. **Responder**, orienta en el desarrollo e implementación de acciones apropiadas respecto de la atención de eventos de Ciberseguridad que puedan afectar los servicios esenciales. La función soporta la habilidad para contener el impacto de un ataque cibernético.

  v. **Recuperar**, orienta en el desarrollo e implementación del plan de resiliencia que permita la restauración en el menor tiempo posible de cualquier capacidad o servicio esencial que haya sido impactado por un ataque cibernético para reducir la afectación en los activos esenciales de información.

Financieras de Colombia, Asobancaria, 2022 (disponible a través de la liga: https://www.asobancaria.com/wp-content/uploads/2022/06/Guia_de_Buenas_Practicas_para_Auditar_la_Ciberseguridad_2022_V1.pdf

- En diciembre de 2022, se ***publicaron en el sitio web del IFT el "Código de Mejores Prácticas para la Ciberseguridad en Equipos Terminales Móviles (ETM)"[20] y el "Código de Mejores Prácticas para la Ciberseguridad de los Dispositivos del Internet de las Cosas (IoT)"***[21]. Estos dos códigos establecen, de manera respectiva, recomendaciones para los ETM y Dispositivos IoT que puedan hacer uso del espectro radioeléctrico o ser conectados a redes de telecomunicaciones, los cuales se encuentran expuestos a amenazas, vulnerabilidades, riesgos y ataques dentro del ecosistema móvil.
- También se levantó una "Encuesta de percepción en materia de ciberseguridad"[22], la cual ofrece "***un panorama general acerca de la percepción y el conocimiento en materia de ciberseguridad en el uso de las plataformas digitales de compras y banca en línea, redes sociales, correo electrónico y servicio de almacenamiento en la nube, los riesgos que identifican las personas usuarias, así como las medidas de seguridad que toman para protegerse al navegar en estas plataformas***." Este tipo de ejercicios son muy útiles para que tanto autoridades como empresas preocupadas por la ciberseguridad de los usuarios puedan enfocar mejor sus esfuerzos.
- Entre las acciones para promover la confianza en el ecosistema digital realizadas por el Instituto, del 29 de agosto al 2 de septiembre de 2022 se llevó a cabo ***un ciclo de conferencias sobre ciberseguridad***[23] que tuvo como propósito crear un espacio de diálogo en materia de ciberseguridad entre las instituciones, la industria y la academia, para compartir con el público diferentes recomendaciones y acciones que los usuarios pueden realizar para promover el uso seguro del acceso a internet, crear una cultura de ciberseguridad y promover la confianza en el entorno digital.

[20] Disponible a través de la liga:
https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_etm.pdf
[21] Disponible a través de la liga:
https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf
[22] Disponible a través de la liga
https://ciberseguridad.ift.org.mx/files/guias_y_estudios/percepcion_de_las_personas_en_ciberseguridad.pdf
[23] El informe de este evento está disponible a través de la liga
https://ciberseguridad.ift.org.mx/files/guias_y_estudios/informe_de_las_conferencias_de_ciberseguridad_2022.pdf

- Finalmente, la Coordinación General de Política del Usuario (CGPU) del IFT mantiene un micrositio sobre ciberseguridad[24] en donde ***ha puesto a disposición del público usuario, diversas guías con recomendaciones generales sobre seguridad para ecommerce y servicios financieros, apps y software, protección de datos personales y seguridad digital, entre otros temas***. Además, en ese micrositio se pueden consultar diversos materiales dirigidos a grupos de población específicos, tales como mipymes, mujeres, niños y adolescentes, y padres de familia. La inspección somera de los materiales disponible revela que los contenidos enfatizan acciones relacionadas con identificación y protección (ver Figura 1), lo cual coincide en buena medida con el enfoque que en muchas jurisdicciones adoptaron las autoridades de inicio para enfrentar los riesgos de ciberseguridad. ***Mientras que la "primera generación" de regulaciones de ciberseguridad se enfocaron en establecer enfoques y controles para la administración de ciber riesgos (es decir, en reducir la vulnerabilidad contra ataques cibernéticos), en años recientes se han emitido regulaciones nuevas o adicionales de "segunda generación" basadas en el supuesto de que algunos ataques ocurrirán y tendrán éxito***. En consecuencia, ***están más dirigidas hacia mejorar la ciber resiliencia y proveer herramientas para lograrla***.[25]

Por otro lado, el Instituto en su plan de trabajo anual para 2023, como parte del "Objetivo 3. Promover el desarrollo del ecosistema digital y la adopción de nuevas tecnologías y casos de uso digitales", la "ESTRATEGIA 3.1: Promover la seguridad, confianza e innovación para el desarrollo del ecosistema digital" establece dos líneas de acción "regulatoria":

> LAR 3.1.1: ***Desarrollar y difundir recomendaciones, lineamientos, disposiciones técnicas y/o buenas prácticas*** en materia de ciberseguridad.

[24] https://ciberseguridad.ift.org.mx/seccion/recomendaciones_generales

[25] Para una discusión sobre esta tendencia dentro del sector bancario, véase Juan Carlos Crisanto, Jefferson Umebara Pelegrini and Jermy Prenio (2023), "*Banks' cyber security – a second generation of regulatory approaches, Bank of International Settlements Financial Stability Institute*, June 2023 (disponible a través de la liga: https://www.bis.org/fsi/publ/insights50.htm)

LAR 3.1.4: Colaborar con los organismos nacionales relevantes en la ***promoción de la alfabetización digital y fomentar la confianza de los usuarios acerca de los servicios y dispositivos disponibles en el ecosistema digital***, así como en el uso responsable y seguro de los mismos.

Según el informe de actividades trimestrales del Instituto correspondiente al primer trimestre del 2023, durante ese periodo, el IFT participó en el Foro de Ciberseguridad *American Chamber* realizado por la *American Chamber Mexico* con el objetivo de dialogar acerca de diferentes temas relacionados con la ciberseguridad y su rol en las redes sociales, el impacto de la protección de la infraestructura crítica; así como la cooperación regional en la materia; en las Consultas intersesionales del Comité Ad Hoc de la Organización de las Naciones Unidas (ONU) encargado de elaborar una convención internacional contra el uso de las tecnologías de la información con fines criminales; y firmó el Convenio con el propósito de impulsar y promover acciones que fomenten la participación ciudadana en materia de alfabetización e inclusión digital, promoción de los derechos de los usuarios y audiencias; así como de la cultura de la ciberseguridad y el uso responsable de los servicios digitales, conforme a las atribuciones y facultades de las partes.

Por consiguiente, como se detallará en la sección IV el IFT debería jugar un rol más activo en cuanto a la definición de políticas de ciberseguridad que deben aplicarse en el sector de telecomunicaciones y radiodifusión, impulsando iniciativas que permitan incorporar las mejores prácticas internacionales en materia de ciberseguridad y ciber resiliencia. Específicamente, el IFT debería **priorizar las acciones de seguridad en general en el ámbito de las telecomunicaciones y radiodifusión, sin importar qué tipo de organizaciones sean** (públicas, privadas, empresas, academia, sociedad civil, o gobiernos, entre otras) y fortalecer su colaboración con otros reguladores y entidades.

III. CONSIDERACIONES

A. Experiencia de reciente de algunos países

i. Estados Unidos

El 9 de diciembre de 2021, NIST divulgó una actualización mayor de su guía para desarrollar sistemas ciber resilientes (SP 800-160 Vol. 2, Revision 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach)[26, 27]. El documento presenta un marco de ingeniería en ciber resiliencia que ayuda a comprender y aplicar los conceptos en la implementación de ciber resiliencia en un sistema. Contiene metas, objetivos, técnicas, enfoques de implementación y principios de diseño que las organizaciones pueden seleccionar, adaptar y usar en parte o en su totalidad para construir los ambientes técnicos, operativos y de amenazas para los que se deben diseñar los sistemas. De esta forma, la guía ayuda a las organizaciones a anticipar, soportar, recuperarse de y adaptarse a condiciones adversas, tensiones o fallas en sistemas, incluyendo ciberataques hostiles y crecientemente destructivos provenientes de naciones-estado, bandas criminales e individuos descontentos. En particular, actualiza controles en materia de ciber resiliencia propuestos mediante:

- Estandarización de la taxonomía y marco de análisis de amenazas[28];
- Provisión de un mapa detallado y análisis de los enfoques para implementar la ciber resiliencia, incluyendo controles de apoyo para los marcos de mitigación;

[26] Disponible a través de la liga: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

[27] Algunos especialistas consideran que los estándares de NIST son a la vez muy completos y genéricos, lo cual los hace adecuados para establecimientos que no desean dedicar demasiado tiempo a ajustar el estándar a su propia industria. Se enfoca en la seguridad de la información y puede no ser suficientemente para mejorar la eficacia del programa de ciberseguridad de una empresa entre todo su personal, procesos y tecnología. Véase para más detalles "NIST, ISO, COBIT, ITIL – Which Cyber Framework Rules Them All?", ORNA, Sep. 6, 2022, (ORNA, 2022) disponible a través de la liga: https://www.orna.app/post/nist-iso-cobit-itil-which-cyber-framework-rules-them-all

[28] Cabe agregar que el marco de análisis de amenazas que contempla esta normativa incluye la existencia de un plan de recuperación ante desastres naturales y perturbaciones, disrupciones o ciberataques. Además, la seguridad de la Información es distinta de la ciberseguridad.

- Análisis de los efectos potenciales de la ciber resiliencia en las tácticas, técnicas y procedimientos que utilizan los adversarios para atacar tecnologías operacionales, incluyendo los sistemas de control industrial.

Asimismo, el pasado 13 de julio de 2023 la administración del presidente Joe Biden anunció una nueva estrategia nacional de ciberseguridad de Estados Unidos que busca dos modificaciones fundamentales en la asignación de roles, responsabilidades y recursos en el ciberespacio: 1. Asegurar que las entidades de los sectores público y privado más grandes, capaces y posicionadas asuman una mayor carga en la mitigación de los riesgos cibernéticos. 2. Incrementar los incentivos para las inversiones de largo plazo en ciberseguridad.[29] El plan de implementación de la estrategia nacional de seguridad (*National Cybersecurity Strategy Implementation Plan*, NCSIP) detalla más de 65 iniciativas federales, desde la protección de empleos mediante el combate de los cibercrímenes hasta la construcción de una fuerza laboral calificada y equipada para sobresalir en la economía digital, que buscan complementar otras iniciativas gubernamentales enfocadas en propiciar las inversiones necesarias para reconstruir la infraestructura actual de ese país, desarrollar su sector de energías limpias y concentrar dentro de su territorio su base tecnológica y manufacturera. Cabe destacar algunas iniciativas del NCSPI con el objetivo de propiciar que las fuerzas de mercado conduzcan hacia mayor una seguridad y resiliencia de productos y servicios de hardware y software, tales como:

- crear asociaciones público-privadas con fabricantes de tecnología, educadores, organizaciones sin fines de lucro, la academia y la comunidad de creadores de software de código abierto, entre otros, para promover el desarrollo de software y hardware que sean seguros (*secure-by-design and secure-by-default*);
- explorar enfoques para desarrollar un marco de responsabilidad para productos de software,

[29] Para más detalles véase FACT SHEET: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan, The White House, 13 July 2023 (disponible a través de la liga: https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/

- promulgar una ley sobre componentes de software (*Software Bill of Materials*, SBOM[30]) que mitigue los riesgos asociados al uso de softwares que carezcan de respaldo en infraestructuras críticas, y
- divulgar reglas para el reporte de incidentes de ciberseguridad, estandarización de requerimientos de ciberseguridad en contratos y software seguro.

ii. Unión Europea

En septiembre de 2022 en la Unión Europea se promulgó una ley sobre ciber resiliencia (*Cyber Resilience Act*, CRA)[31] que busca reforzar las reglas de ciberseguridad existentes en los países miembros para contar con productos de *hardware* y *software* más seguros, toda vez que dichos productos cada vez son objeto de más ciberataques exitosos, los cuales en 2021 tuvieron un costo estimado global anual de 5.5 trillones de euros. Los principales problemas que se detectaron en estos productos son un bajo nivel de ciberseguridad, reflejado en amplias vulnerabilidades y una provisión de actualizaciones de seguridad para atenderlas insuficiente e inconsistente, y una comprensión y acceso a información insuficientes por parte de los usuarios, los cuales les impiden escoger productos con características de ciberseguridad adecuadas o utilizarlos de manera segura. La causa identificada es que la mayor parte de los productos de hardware y software no estaban regulados por alguna legislación europea enfocada en sus características de ciberseguridad, por tratarse de software no integrado (*non-embeded software*); lo anterior, a pesar de que han incrementado los ciberataques dirigidos a estos productos.

En consecuencia, entre otros objetivos la CRA busca asegurar un marco de ciberseguridad coherente, que facilite el cumplimiento de los productores de *hardware* y *software*; mejorar

[30] La SBOM consiste en diversas normativas sobre componentes para software para diseñar, buscar, construir, analizar y desplegar sistemas. El trabajo en la SBOM ha avanzado desde 2018 mediante un esfuerzo de colaboración comunitario entre múltiples partes interesadas y dirigido por la *National Telecommunications and Information Administration* (NTIA). Para más detalles, consúltese el sitio del Software Bill of Materials (disponible a través de la liga: https://www.cisa.gov/sbom)

[31] Véase para más detalles *Cyber Resilience Act Shaping Europe's digital future*, *European Commission*, 15 September 2022 (disponible a través de la liga https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act)

la transparencia de las características de seguridad de los productos con elementos digitales; y empoderar el uso seguro de productos con elementos digitales por parte de empresas y personas. Para ello, se identifican categorías de productos críticos por su funcionalidad (por ejemplo, administradores de contraseñas, interfases de red, cortafuegos de sistemas de red y microcontroladores), uso intencionado (sistemas operativos, cortafuegos industriales, CPUs y elementos de seguridad, entre otros) u otros criterios (extensión del impacto) para los cuales se requerirá la aplicación de algún estándar o evaluación de terceros.[32]

B. Organismos de estandarización e internacionales

i. Organismos de estandarización

La Organización Internacional para la Estandarización (International Organization for Standardization, ISO) publicó en 2022 el estándar ISO/IEC 27001 para sistemas de administración de información de seguridad (Information Security Management Systems, ISMS)[33] . Este estándar provee a las empresas de cualquier tamaño y sector de actividad guías para establecer, implementar, mantener y mejorar de manera continua sus ISMS. La conformidad con el estándar ISO/IEC 27001 significa que una organización o negocio ha implantado un sistema para administrar riesgos relacionados con la seguridad de los datos que posee o maneja, y que ese sistema respeta las mejores prácticas y principios contenidos en este estándar internacional. Este estándar ayuda a que las organizaciones sean más conscientes de los riesgos que enfrentan y proactivas en su identificación y eliminación de vulnerabilidades a través de la selección, prueba e inspección de personal, políticas y

[32] La Comisión Europea estima que las categorías de productos críticos agrupen al 10% de los productos de hardware y software. Para el restante 90% de productos no críticos se establece una auto evaluación. Op Cit.
[33] Véase para más detalles ISO/IEC 27001 Standard – Information Security Management Systems (disponible a través de la liga: https://www.iso.org/standard/27001)

tecnologías. Los ISMS implementados conforme a este estándar son una herramienta para la administración de riesgos, la ciber resiliencia y la excelencia operativa.[34]

Otros dos marcos que contienen buenas prácticas y estándares para propiciar una ciber protección eficaz son COBIT [35], e ITIL[36]. La versión de COBIT de 2019 es un marco sólido para guiar los procesos de una manera que permita a los negocios implementar políticas y procedimientos en estrategia, innovación, administración de riesgo y administración de activos, entre otros ámbitos. En contraste con los estándares NIST e ISO, COBIT define componentes y factores de diseño para construir y sustentar un sistema de gobernanza general. Finalmente, ITIL 4 es un estándar que se enfoca en fines del sector público pero aceptado por muchas organizaciones del sector privado. Se enfoca en la cultura de las organizaciones e integra las TI en la estructura de los negocios de una manera que propicia la colaboración entre el área de TI y las demás en lo que concierne a la colaboración para funciones conjuntas.[37]

ii. Organismos internacionales

En julio de 2022 el Foro Económico Mundial (*World Economic Forum*, WEF) publicó el documento en el que propone un índice de ciber resiliencia (*The Cyber Resilience Index: Advancing Organizational Cyber Resilience White Paper*).[38] Este documento detalla un marco conceptual de ciber resiliencia (*Cyber Resilience Framework*, CRF) y el índice de ciber

[34] Los estándares ISO 27001/27002 usualmente se utilizan de manera conjunta para proveer tener infraestructuras de TI y de administración de seguridad congruentes. Véase para más detalles ORNA (2022)

[35] La organización estadounidense Information Systems Audit and Control Association (ISACA) diseñó un estándar para control de objetivos de tecnologías de información (Control Objectives for Information Technologies, COBIT 5) enfocado en ayudar a las organizaciones a atender retos de negocio en materia de cumplimiento regulatorio, administración de riesgos y alineación de la estrategia de tecnologías de información con las metas organizacionales. Para más detalles sobre ISACA véase el sitio https://www.isaca.org/

[36] El estándar Information Technology Infrastructure Library (ITIL) es un conjunto de mejores prácticas desarrollado por el (Central Computer and Telecommunications Agency, CCTA) del gobierno británico en los ochenta de manera específica para propósitos del sector público. Véase para más detalles ORNA (2022).

[37] Estos dos marcos se pueden complementar entre sí para aplicar un enfoque más holístico para la administración de riesgos de ciberseguridad. Véase para más detalles ORNA (2022).

[38] Disponible a través de la liga: https://www.weforum.org/whitepapers/the-cyber-resilience-index-advancing-organizational-cyber-resilience/?DAG=3&gclid=CjwKCAjwwb6lBhBJEiwAbuVUSmuSlpxCd61AGz9zpmmxofiycmT8HiRvZbErgw1gPYJBZN50g085SRoCKKoQAvD_BwE.

resiliencia (*Cyber Resilience Index*, CRI) como una guía para que las organizaciones adopten prácticas de ciber resiliencia más efectivas en los ecosistemas digitales. De manera conjunta el CRF y el CRI buscan mejorar la transparencia y visibilidad de los esfuerzos en materia de ciber resiliencia con el fin de crear confianza en los ecosistemas digitales.

El CRF consiste en seis principios claves que se asocian a prácticas y sub-prácticas en las cuales los ciber líderes pueden definir una organización ciber resiliente. Sirve como un estándar no específico a industria alguna con resultados definidos que pueden servir como métrica para todas las organizaciones, sin distinguir por geografía o tamaño. A su vez, el CRI es una herramienta para ayudar a las organizaciones a medir de manera cuantitativa su ciber resiliencia mediante mediciones de desempeño con respecto a las mejores prácticas que propone el CRF. De manera conjunta el CRF y el CRI transparentan el estado actual de ciber resiliencia de una organización y, de manera subsecuente, del ecosistema digital más amplio en que ésta participa.

Para el sector financiero, un veloz adoptante de nuevas tecnologías y modelos de negocio para aprovecharlas, el Consejo de Estabilidad Financiera (*Financial Stability Board*, FSB) mantiene entre sus principales líneas de trabajo la ciber resiliencia.[39] Entre ellas destacan, además de posicionamientos respecto a regulaciones de ciberseguridad, guías y prácticas de supervisión para sus jurisdicciones miembro (México es una de ellas), diversos reportes sobre buenas prácticas para responder a y recuperarse de ciber ataques, así como para incrementar la convergencia en el reporte de ciber ataques.

C. Cómputo en la nube

Para algunas instituciones internacionales, el cómputo en la nube enfrenta diversos retos de gobernanza y regulación altamente complejo debido a su rápida y creciente centralidad para muchas funciones económicas y la constante innovación. [40] **Entre los retos asociados**

[39] Véase para más detalles *Cyber Resilience - Financial Stability Board* (https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/cyber-resilience/)
[40] Véase para más detalles Ariel E. Levite and Gaurv Kalwani (2020), "*Cloud Governance Challenges: A Survey of Policy and Regulatory Issues*", Carnegie Endowment for International Peace Working Paper, November

a la seguridad, robustez y resiliencia del cómputo en la nube se identifica como un área clave de regulación aquella que se refiere a la delineación de las responsabilidades compartidas entre los proveedores de los servicios de cómputo en la nube, sus clientes y, en algunos casos, también los operadores de las redes de telecomunicaciones. Los diversos modelos de negocios para el cómputo en la nube definen distintas responsabilidades para cada parte en la seguridad de los datos y la infraestructura subyacente. **El proceso de migración de datos y servicios a la nube**, la seguridad y prácticas de administración de riesgos de los proveedores de cómputo en la nube, incluyendo tanto controles sistémicos como medidas de defensa operacional, han emergido como una de las preocupaciones más sensibles.[41] También hay una preocupación creciente de que la **asimetría en el poder del mercado de los proveedores del cómputo en la nube con respecto a sus clientes** puede producir resultados desfavorables. En especial porque **algunos de los clientes más grandes de los proveedores de cómputo en la nube *figuran empresas de telecomunicaciones***, instituciones financieras, empresas productoras y proveedoras de servicios de energía y agua (*utilities*) que en varias jurisdicciones han sido designadas como infraestructuras críticas.[42]

Por otro lado, según un estudio reciente acerca del potencial de la adopción del cómputo en México para incrementar la inclusión, innovación y crecimiento[43], entre las principales

2020 (disponible a través de la liga https://carnegieendowment.org/files/Levite_Kalwani_Cloud_Governance.pdf.

[41] Véase, por ejemplo, *Third-party dependencies in cloud services: Considerations on financial stability implications*, Financial Stability Board, 9 December 2019 (disponible a través de la liga: https://www.fsb.org/2019/12/third-party-dependencies-in-cloud-services-considerations-on-financial-stability-implications/

[42] Según el documento de Levite y Kalwani (2020), es importante señalar que los proveedores de cómputo en la nube no solo enfrentan amenazas de actores maliciosos (hacktivistas, criminales, terroristas, personal interno o, en algunos casos estados nacionales belicistas y sus proxies), sino accidentes y disfunciones técnicas detonadas por desastres naturales (terremotos, inundaciones y tormentas, entre otros) que han provocado numerosas interrupciones en los servicios de cómputo en la nube y los centros de datos. Si bien su debida atención podría requerir la agrupación de los temas en la cartera regulatoria de una sola entidad, en ausencia de ella los reguladores sectoriales deberían utilizar las facultades que tengan en la materia.

[43] Mexico Powered by the Cloud: Inclusivity, Innovation and Growth, Ernesto Flores Roux and Alejandra Palacios, U. S. – Mexico Foundation, July 2022 (disponible a través de la liga: https://static1.squarespace.com/static/61b0f3857a9adc5a5722b68f/t/62e97f092fe0ee5ef54b128e/165946

limitaciones para la adopción del cómputo en la nube que ***deben resolverse*** figuran ***el desconocimiento de las empresas, tanto del gobierno como privadas, y los consumidores sobre los costos y beneficios que puede ofrecerles esa tecnología, el cual es atribuible a los diversos modelos de negocio para su adopción***; así como el ***exceso de regulaciones y requisitos para que las empresas de ciertos sectores trasladen cargas de trabajo o almacenen datos en la nube***.

Por lo que se refiere al primer tema, el estudio sobre "Percepción y conocimiento de las personas usuarios de los servicios de telecomunicaciones en materia de ciberseguridad en plataformas digitales para compras y banca en línea, redes sociales, correo electrónico y servicio de almacenamiento en la nube" [44] que realizó el IFT en 2022 documenta que los servicios de almacenamiento en la nube gratuitos suelen ser utilizados para archivos personales, mientras que los de paga tienen una tendencia a ser más para uso laboral entre las personas entrevistadas. Sin embargo, "cuando se mencionaron plataformas de servicio de almacenamiento en la nube, [los usuarios] señalaron tener poco conocimiento sobre riesgos que existen y sobre medidas de seguridad" y "en cuanto a los TyC de las plataformas de servicio de almacenamiento en la nube… la mayoría mencionó no haberlas leído, pero saben que son importantes."

Por lo que se refiere al exceso de regulaciones y requisitos, existen manuales de mejores prácticas para evaluar si afectan de manera indebida la competencia que podrían utilizarse para que el IFT realice por cuenta propia o a través de terceros un análisis acerca de las barreras para el traslado de cargas y almacenamiento en la nube que se encuentran de manera más frecuente en las normativas sectoriales a nivel federal, de las entidades federativas y municipios, a fin de que pueda promoverse su eliminación.

9586548/Inclusiveness%2C+Innovations%2C+and+Growth+Powered+by+the+Cloud+in+Mexico+DESIGN_VF+%281%29.pdf.

[44] Disponible a través de la liga: Percepción y conocimiento de las personas usuarias de los servicios de telecomunicaciones en materia de ciberseguridad en plataformas digitales para compras y banca en línea, redes sociales, correo electrónico y servicio de almacenamiento en la nube (ift.org.mx): https://ciberseguridad.ift.org.mx/files/guias_y_estudios/percepcion_de_las_personas_en_ciberseguridad.pdf

IV. RECOMENDACIONES

Sin dejar de reconocer la destacada labor en materia de ciberseguridad que ha venido desarrollando el IFT, los miembros de este VII Consejo Consultivo del IFT proponen que, en el ámbito de su competencia:

1. Evalúe las actividades del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos para determinar cuáles considera necesarias y convenientes para fortalecer su capacidad institucional en materia de ciberseguridad y para gestionar los ataques cibernéticos de que sea objeto[45];
2. Identifique lo que respecta a sus funciones regulatorias y, de conformidad con los cinco objetivos estratégicos institucionales listados en los antecedentes, refuerce las acciones de ciberseguridad y ciberresiliencia, e identifique aquellas actividades en las que desde el ámbito de su competencia puede colaborar con otras autoridades que se sumen a gestionar de forma coordinada los incidentes cibernéticos de mayor criticidad e impacto en activos esenciales de información, mediante la aplicación de procedimientos y mejores prácticas de ciberseguridad y para la contención y mitigación de amenazas cibernéticas, a fin de mantener niveles de riesgo aceptables;
3. Desarrolle un marco de referencia en colaboración con la industria y la academia incorporando mejores prácticas de ciberseguridad y ciber resiliencia, para que sus regulados puedan usarlo al elaborar sus planes de gestión de riesgos de ciberseguridad y ciber resiliencia en los que se incluya entre otros la adopción de estándares internacionales (ISO, IEC, COBIT, NIST, ITIL, entre otros) para: a) ciberseguridad, seguridad de la información, planes de recuperación en caso de desastres (Disaster

[45] Cabe recordar que el 24 de octubre de 2022 la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT) sufrió un ciber ataque que obligó a esa dependencia a suspender hasta el 31 de diciembre de ese año "las diligencias y actuaciones en los procedimientos que se tramiten, o deban tramitarse, ante distintas áreas de su jurisdicción". Véase para más detalles "La SICT suspende trámites en lo que resta del año por hackeo" El Economista, 2 de noviembre de 2022 (disponible a través de la liga https://www.eleconomista.com.mx/empresas/La-SICT-suspende-tramites-en-lo-que-resta-del-ano-por-hackeo-20221102-0005.html)

Recovery Plan, DRP) y ciber resiliencia; b) procesos de auditorías internas; c) monitoreo permanente de su infraestructura e información crítica; d) esquemas de protección de la seguridad perimetral y las conexiones remotas (por ejemplo para el teletrabajo); e) actualización de herramientas colaborativas de operación y *software*, *firmware*, *middleware* y *hardware* que utilicen para fines de la provisión de los servicios de telecomunicaciones y radiodifusión y el acceso a Internet; f) protección de la privacidad de los datos y encriptación; g) resguardos; y h) capacitación permanente al personal, entre otros. Cabe recalcar el gobierno de ciberseguridad y ciber resiliencia a través de un programa de mejora continua de la ciberseguridad y la ciber resiliencia es un esfuerzo permanente, no son acciones aisladas e intermitentes;

4. Incorpore en su Plan de Acciones en Materia de Ciberseguridad y sus planes anuales de trabajo actividades de divulgación en materia de ciber resiliencia entre empresas y consumidores; con énfasis en aquellas relacionadas con la detección, respuesta y recuperación de sus actividades después de sufrir algún ciber ataque, y en la concientización de los riesgos cibernéticos al utilizar dispositivos de acceso y aquellos que se encuentran conectados a redes de telecomunicaciones, radiodifusión e Internet. Esta propuesta representa una evolución natural del enfoque actual de promoción de la cultura de ciberseguridad del Instituto, el cual en sus materiales de divulgación para usuarios ha puesto énfasis en que las empresas y consumidores puedan identificar y protegerse contra posibles ciberataques. También es necesario informar al usuario, a través de comunicados, acerca de los nuevos riesgos que aparezcan en las redes públicas de telecomunicaciones;

5. Diseñe una caja de herramientas (“*toolkit*”) para que las mipymes puedan prepararse para anticipar, soportar, recuperarse de y adaptarse a un entorno donde los ciberataques serán frecuentes. Para ello el Instituto podría considerar el estándar ISO/IEC 27001 antes mencionado o el Índice de ciber resiliencia del WEF. Asimismo, en materia de protección de datos personales, también podría tomar como referencia alguno de los documentos elaborados por el INAI o desarrollarlo conjuntamente con el

INAI[46]. De manera inicial, esta caja de herramientas o guía podría enfocarse en las necesidades de los pequeños operadores y operadores comunitarios. Para ello, el IFT podría apoyar a los operadores comunitarios, sociales, indígenas y WISPs, a través del Comité de Pequeños Operadores;

6. Explore y describa con mayor detalle las condiciones en que se están comercializando dentro del país los servicios de cómputo en la nube en sus distintas modalidades, así como los costos y beneficios que deben ponderar los usuarios al momento de evaluar la contratación de estos servicios para transferir y almacenar datos a través de las redes de telecomunicaciones e internet; en especial, aquellos atributos que pueden afectar la capacidad de los usuarios del cómputo en la nube para recuperar su capacidad operativa y su información almacenada, en caso de sufrir algún ciber ataque. Para ello, el IFT podría realizar un estudio de mercado conforme al Artículo 12 fracción XXII de la Ley Federal de Competencia Económica o un nuevo estudio sobre cómputo en la nube en el cual se actualicen algunos de los principales indicadores y estadísticas del estudio de 2020. Un estudio de este tipo podría contribuir al mejor entendimiento entre empresas y usuarios de esta tecnología e incluir recomendaciones pertinentes para que autoridades y oferentes reduzcan barreras de adopción que les atañan, y
7. Colabore para mejorar la interacción entre los CERT (*Computer Emergency Response Team*) establecidos en México, de acuerdo con las recomendaciones de anteriores Consejos Consultivos, y organice anualmente una conferencia para coordinar los esfuerzos de los actores regulatorios, de seguridad nacional, académico e industrial para proponer acciones a corto plazo que mejoren la ciberseguridad y resiliencia de cualquier usuario y red en México.

[46] Véase, por ejemplo, el "Toolkit de Concientización de Seguridad de Datos Personales para Responsables del Sector Privado" disponible a través de la liga: https://home.inai.org.mx/wp-content/uploads/TOOLKIT-PDP.zip

Finalmente, cabe señalar que estos esfuerzos difícilmente rendirán frutos si alguna infraestructura crítica o alguno de sus participantes relevantes no se suma a las acciones de reforzamiento de la ciberseguridad y de la ciber resiliencia.

Lilia Eurídice Palma Salas

Presidenta del VII Consejo Consultivo

Mtra. Rebeca Escobar Briones

Secretaria del Consejo Consultivo

La Recomendación fue aprobada, en lo general, por el VII Consejo Consultivo del Instituto Federal de Telecomunicaciones por mayoría de votos de los consejeros: Alejandro Ildefonso Castañeda Sabido, Sara Gabriela Castellanos Pascacio, Ernesto M. Flores-Roux, Mario Germán Fromow Rangel, Gerardo Francisco González Abarca, Ali Bernard Haddou Ruíz, Erik Huesca Morales, Salma Leticia Jalife Villalón, Luis Miguel Martínez Cervantes, Edgar Olvera Jiménez, Lucía Ojeda Cárdenas, Eurídice Palma Salas y Cynthia Gabriela Solís Arredondo. Lo anterior, en la IX Sesión Ordinaria celebrada el 7 de septiembre de 2023 y reiterada vía correo electrónico el 14 de septiembre del mismo año, mediante Acuerdo CC/VII/IFT/090723/23. De forma adicional y en línea con los Artículos 17 y 18 de las Reglas de Operación de este Consejo Consultivo, el razonamiento de los votos particulares formará parte de la propuesta u opinión correspondiente.

El Grupo de Trabajo que desarrolló el proyecto de Recomendación está integrado por su coordinadora Sara Gabriela Castellanos Pascacio, con la participación de Ali Bernard Haddou Ruíz, Luis Miguel Martínez Cervantes y Cynthia Gabriela Solís Arredondo. Los consejeros Ernesto M. Flores-Roux, Mario Germán Fromow Rangel, Gerardo Francisco González Abarca, Erik Huesca Morales, Salma Leticia Jalife Villalón, Edgar Olvera Jiménez, Lucía Ojeda Cárdenas y Eurídice Palma Salas aportaron comentarios muy útiles para darle a la recomendación su forma final.

ANEXO

Diferencias entre Seguridad de la Información y Ciberseguridad

Seguridad de la información	Ciberseguridad
Son los procesos y procedimientos de para preservar la seguridad de la información que puede encontrarse no tan sólo en medios digitales, es decir, la información de una organización en todas sus formas. Incluye archivos y registros físicos.	Es la seguridad de los sistemas informáticos y todo lo que contienen, incluyendo las redes de telecomunicaciones y sus equipos de trasmisión.
Protege la información contra el acceso, robo, copias no autorizadas que podría resultar en la modificación o eliminación no deseada de información.	Protege los datos y sus tecnologías relacionadas para su operación y resguardo y las fuentes de almacenamiento.
Incluye accesos físicos y procesos y procedimientos de comportamiento de las personas que son responsables de la información.	Regula por lo general el acceso a equipos de telecomunicaciones y cómputo y lleva registros de las amenazas que se han presentado y la forma en que se han resuelto

Fuente: Elaborado por Erik Huesca, basado en el material didáctico para cursos de teoría de la información a nivel licenciatura en el ITAM.

VOTOS PARTICULARES

Edgar Olvera Jiménez

De: olverae@
A: Rebeca Escobar Briones;
drhipo@me.com; jmegretep; ioc; euripal; cynsol
Cc: Maria Isabel Reza Meneses; Jorge Israel Rosas Velasco; Llusvy Amairani Peralta Rojo
Asunto: RE: Nueva versión de la recomendación de ciber resiliencia para solicitar votos de los Consejeros
Fecha: martes, 12 de septiembre de 2023 01:39:16 p. m.
Archivos adjuntos:

Con excepción de las recomendaciones 1 y 2, mi voto es en contra.

La razón fundamental es que tales recomendaciones desbordan del ámbito de competencia del Instituto Federal de Telecomunicaciones.

Saludos

Edgar Olvera

Eurídice Palma Salas

De: euridice palma
A: Rebeca Escobar Briones
Cc:

Asunto: Re: Nueva versión de la recomendación de ciber resiliencia para solicitar votos de los Consejeros
Fecha: martes, 12 de septiembre de 2023 09:21:55 p. m.

Estimada Rebeca,

Por este medio confirmo mi voto a favor en lo general de las recomendaciones y emito mi voto a favor en lo particular, y expongo a continuación los razonamientos para mi voto a favor.

En las discusiones sostenidas en el Consejo Consultivo en relación con las recomendaciones algunos miembros externaron su preocupación porque las recomendaciones excedieran el ámbito de competencia del Instituto. Al respecto, es importante destacar lo siguiente:

- La introducción refiere en forma expresa (ver nota al pie 14) al capítulo 4 del Plan de Acciones en materia de Ciberseguridad del IFT que contiene un análisis sobre la competencia del Instituto para la emisión de disposiciones técnicas, evaluación de la conformidad y homologación; inclusión digital y cobertura universal; privacidad de los usuarios, seguridad de la red; y colaboración con la justicia (páginas 12 a 16).

- Las 7 recomendaciones están basadas en lo previsto en los artículos 2, 6 y 7 Constitucionales y las atribuciones del Instituto previstas en la Ley.

- Las recomendaciones 1, 2 y 3 están acotadas en su alcance; la recomendación 1 al ámbito interno del IFT; la recomendación 2 a sus funciones regulatorias en el ámbito de su competencia para colaborar con otras autoridades; elaborar un marco de referencia para sus regulados.

- La 4 es de divulgación, la 5 está vinculada a la divulgación por tratarse del diseño de un toolkit para las mipymes; podría haberse dicho que solo para el sector pero el toolkit con ese perfil puede ser empleado indistintamente por otras mipymes y no solo regulados, además que las mipymes no cuentan con los recursos de las grandes empresas y su relevancia es indiscutible dado que aportan más del 50% del PIB a nuestra economía y generan más del 70% del empleo en el país.

- La 6a está dirigida a la divulgación para informar a los usuarios. La 7a se refiere a colaborar para mejorar la interacción entre los CERT en México.

- En conclusión, ninguna de las recomendaciones sugiere ni conlleva restringir derechos o imponer obligaciones y están orientadas a los principios establecidos en los artículos 2o, 6o y 7o Constitucionales.

Por último, las recomendaciones surgen también del reconocimiento a las capacidades del Instituto, al nivel de especialización de su personal y los materiales que está generando para difundir. Los riesgos y daños por ciberataques se incrementan cada día y es importante que nuestras autoridades contribuyan a prevenir y desarrollar capacidades de ciberseguridad y ciber resiliencia en nuestro país.

Saludos cordiales.

Euridice Palma

Salma Leticia Jalife Villalón

De: Salma Jalife
A: Rebeca Escobar Briones
Cc:

Asunto: Re: Nueva versión de la recomendación de ciber resiliencia para solicitar votos de los Consejeros
Fecha: martes, 12 de septiembre de 2023 09:40:10 p. m.

Estimadas Eurídice y Rebeca,
Les envío a continuación mi voto particular respecto de la Recomendación en materia de ciber resiliencia, por favor incluirla en las actas correspondientes.

Voto particular de Salma Jalife a la Recomendación en materia de ciber resiliencia.

Mi voto es a favor a excepción de la recomendación 6. que debe eliminarse porque se refiere a que el IFT desarrolle acciones más allá de su ámbito de competencia debido a que el cómputo en la nube no es una infraestructura de telecomunicaciones ni de radiodifusión, sino una infraestructura de tecnologías de información. En el texto de la recomendación se menciona que el IFT debe "jugar un rol más activo en la definición de políticas de ciberseguridad", tampoco es facultad del IFT establecer políticas públicas ya que éstas son competencia de la Secretaría de Infraestructura, Comunicaciones y Transportes.
El ámbito de competencia del IFT está claramente descrito en el artículo 7. de la Ley Federal de Telecomunicaciones y Radiodifusión. El artículo 9 fracción IV de la misma ley indica que es facultad exclusiva de la Secretaría elaborar las políticas de telecomunicaciones y radiodifusión del Gobierno Federal.
En todo caso en el párrafo que inicia con la siguiente frase: "Por consiguiente, como se detallará en la sección IV el IFT debería jugar un rol más activo en cuanto a la definición de políticas de ciberseguridad que deben aplicarse en el sector de telecomunicaciones y radiodifusión...", se debió sustituir la frase "la definición de políticas de ciberseguridad" por la frase " desarrollar acciones regulatorias derivadas de las políticas de ciberseguridad que establezca el Gobierno Federal que deben aplicarse en el sector telecomunicaciones y radiodifusión... ".
Es un hecho que el IFT es un actor coadyuvante y promotor de la ciberseguridad y la ciber resiliencia, porque su competencia radica en regular y vigilar el buen desempeño de las redes de telecomunicaciones y las que usan el espectro radioeléctrico (terrestres y satelitales).

Saludos cordiales,
Salma Jalife

Lucía Ojeda Cárdenas

De: Lucia Ojeda Cárdenas
A: Rebeca Escobar Briones;

Asunto: RE: Nueva versión de la recomendación de ciber resiliencia para solicitar votos de los Consejeros
Fecha: martes, 12 de septiembre de 2023 10:49:16 p. m.

Estimada Rebeca

Confirmo mi voto en favor de la recomendación de referencia.

En efecto, comparto el análisis que hace la Consejera Eurídice Palma en su voto particular. Esto es, considero todas las recomendaciones están, ya sea, acotadas al propio alcance del Instituto; están relacionadas con sus regulados; o se trata tareas de divulgación que están en concordancia e íntimamente relacionadas con los principios contenidos en los artículos 2o, 6o y 7o de la Constitución.

En particular por lo que se refiere a la recomendación 6, añado que tal y como lo mencionó la Magistrada Rosa Elena González Tirado en su voto particular en el expediente relativo al Conflicto competencial 1/2021, los servicios de cómputo en la nube requieren para su desarrollo el uso de infraestructura de telecomunicaciones, por lo que personalmente desprendo que al menos se trata de servicios que se encuentran en mercados relacionados a los servicios de telecomunicaciones. En consecuencia, su análisis pudiera tener relevancia para los mercados de telecomunicaciones que claramente caen dentro del ámbito competencial del Instituto sin que ello implique que la recomendación pretenda ampliar las atr buciones del Instituto para regular estos servicios.

Ahora bien, coincido con la Consejera Salma Jalife quien señala la facultad de elaborar políticas de telecomunicaciones y radiodifusión recae en la Secretaría de Infraestructura, Comunicaciones y Transportes; sin embargo, en la formulación de las recomendaciones -más allá del párrafo identificado por la propia Consejera- no aprecio que se invada esta atribución.

Finalmente, las recomendaciones del Consejo Consultivo no son vinculantes para el Instituto quien podrá en todo momento evaluar la pertinencia de adoptarlas considerando el análisis propio que haya hecho del alcance de sus propias atribuciones.

Saludos

Lucía Ojeda Cárdenas

Erik Huesca Morales

De: Erik Huesca
A: loc
Cc: Rebeca Escobar Briones;

Asunto: Re: Nueva versión de la recomendación de ciber resiliencia para solicitar votos de los Consejeros
Fecha: martes, 12 de septiembre de 2023 11:46:11 p. m.

Las primeras dos recomendaciones las veo bien, las demás no. Por lo que en un balance no es adecuada para ser votada hasta que sufra cambios radicales. La idea de recomendar al IFT valorar sus planes de ciber-seguridad y ciber resiliencia es buena, pero no en la forma que lo aborda la recomendación. Mi voto es en contra hasta hacer cambios radicales y mantener solamente las dos primeras recomendaciones.

Comento:

Arguntar de ITIL, ISO 27001 y muchos otros marcos de referencia, están orientados fundamentalmente a la operación de software y servidores que se encuentran fuera del ámbito del Instituto debido que está enfocado a los sistemas y datos de una organización y no a su transmisión. En todo caso hay un marco de referencia específico que es eTOM (Enhanced Telecom Operations Map) ahora evolucionado a Frameworx y que está diseñando para las empresas prestadoras de servicio de telecomunicaciones. Sin embargo, este mismo marco va más allá de su ámbito de competencia.

Finalmente como nota aclaratoria el cuadro elaborado es resultado de mi experiencia en las clases de maestría de la MTIA del ITAM.

Erik S. Huesca

Gerardo Francisco González Abarca

De: Gerardo Francisco Gonzàlez
A: Rebeca Escobar Briones
Cc:

Asunto: Re: Nueva versión de la recomendación de ciber resiliencia para solicitar votos de los Consejeros
Fecha: miércoles, 13 de septiembre de 2023 12:56:54 p. m.

REITERO MI VOTO A FAVOR EN PARTICULAR, CON LA MENCIÓN DE QUE LAS NOTAS AL PIE DE PAGINA DEBERIAN ESTAR TODAS AL FINAL DEL DOCUMENTO.
FUNDAMENTO MI MENCIÓN, A QUE DE ESA FORMA EL DOCUMENTO ES CONCISO EN LO QUE SE RECOMIENDA Y LAS REFERENCIAS SON PARA CONSULTA SEGUN EL INTERES INDIVIDUAL DE QUIEN LA LEA.
GRACIAS

Mario Germán Fromow Rangel

De: Mario Germán Fromow Rangel
A: Rebeca Escobar Briones;

Asunto: Re: Nueva versión de la recomendación de ciber resiliencia para solicitar votos de los Consejeros
Fecha: jueves, 14 de septiembre de 2023 03:53:02 a. m.

Estimad@s tod@s:

Reitero mi voto a favor de la Recomendación en cuestión.

Considero que todas la recomendaciones que se hacen en el apartado IV son relevantes y caen dentro del ámbito de competencia y atribuciones conferidas por la CPEUM y la LFTR al IFT, además de que el Instituto cuenta con el alto grado de especialización técnica que se requiere para la definición de políticas de ciberseguridad y ciber resiliencia, así como incidir en la implementación efectiva de dichas políticas, con base en su objeto constitutucional de propiciar el desarrollo eficiente de la radiodifusión y las telecomunicaciones en nuestro país.

Por lo anterior, coincido totalmente con la aseveración que se hace en el apartado II respecto a que "el IFT debería jugar un rol más activo en cuanto a la **definición de políticas de ciberseguridad** que deben aplicarse en el sector de telecomunicaciones y radiodifusión, impulsando iniciativas que permitan incorporar las mejores prácticas internacionales en materia de ciberseguridad y ciber resiliencia."

Si bien la LFTR señala en su artículo 9 fracción IV que le corresponde a la Secretaría elaborar **las políticas de telecomunicaciones y radiodifusión del Gobierno Federal**, considero que esto no se puede interpretar como una facultad exclusiva del Ejecutivo Federal, dejando de lado los poderes quasi-legislativos, quasi-ejecutivos y quasi-judiciales que se le otorgaron al IFT en la Reforma Constitucional en materia de Telecomunicaciones de 2013, conforme a lo manifestado por la SCJN en la "Sentencia mediante la cual se resuelve la Controversia Constitucional 117/2014, promovida por el Congreso de la Unión por conducto de la Cámara de Senadores, en contra del Instituto Federal de Telecomunicaciones, por la emisión del Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones emite las Reglas de Portabilidad Numérica y modifica el Plan Técnico Fundamental de numeración, el Plan Técnico Fundamental de Señalización y las especificaciones operativas para la implantación de Portabilidad de números geográficos y no geográficos, publicado en el Diario Oficial de la Federación el doce de noviembre de dos mil catorce".

La Setencia de la SCJN en la Controversia Constitucional 117/2014 fue una "gran victoria legal" para el IFT en la defensa de sus facultades constitucionales.

Una disculpa por la extensión, pero me permitiré reproducir algunos párrafos tomados de dicha sentencia (se incluyen los números de los párrafos para pronta referencia), que considero relevantes para resaltar la **"Facultad Regulatoria"** que el

Constituyente le otorgó al IFT, dentro del andamiaje jurídico que se definió en la Reforma Constitucional en materia de Telecomunicaciones de 2013 y que a mi entender, posibilita también al IFT para definir políticas públicas dentro del ámbito de sus facultades constitucionales.

239. Por tanto, para determinar cuál es el sector de competencia del IFT es necesario precisar el criterio rector de su ámbito material de actuación, lo que, una vez más, se establece de manera expresa en el artículo 28 constitucional en tres rubros:
a) El desarrollo eficiente de la radiodifusión y las telecomunicaciones, conforme a lo dispuesto en esta Constitución y en los términos que fijen las leyes,
b) La regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de radiodifusión y telecomunicaciones, así como del acceso a infraestructura activa, pasiva y otros insumos esenciales, garantizando lo establecido en los artículos 6° y 7° de esta Constitución y
c) En materia de competencia económica de los sectores de radiodifusión y telecomunicaciones.

255. Del análisis del proceso, se observa que el Constituyente Permanente pretendió investir al IFT de facultades regulatorias de suma importancia en el sector de telecomunicaciones y radiodifusión. No sólo para regular cuestiones técnicas y económicas, sino también para resolver cuestiones regulatorias sustantivas que condicionan el ejercicio robusto y desinhibido de los derechos humanos a la libertad de expresión y acceso a la información en la actual época de las tecnologías.

256. Esta doble responsabilidad institucional finalmente investida sobre el IFT debe considerarse en todo ejercicio interpretativo de su nueva nómina de competencias constitucionales, pues son los fines para los cuales ***se le otorgaron poderes quasi legislativos, quasi ejecutivos y quasi judiciales*** *(énfasis añadido).*

275. Para quienes detonaron el proceso de reforma constitucional era importante precisar el fin buscado con la nómina de facultades a otorgar al IFT, al concluir:
Todas estas facultades están dirigidas a garantizar los derechos previstos en los artículos 2º, 3º, 6º y 7º de la Constitución *(énfasis añadido) y a fortalecer la competencia y libre concurrencia, de manera que, en última instancia, se ofrezcan al público productos y servicios de calidad y a precios accesibles y, así, se facilite y* ***procure que todos los mexicanos puedan integrarse a la sociedad de la información y el conocimiento. En suma, las facultades del Instituto Federal de Telecomunicaciones, desde la Constitución misma, son un instrumento para hacer efectivos los derechos fundamentales referidos*** *(énfasis añadido).*

279. En la iniciativa de la reforma constitucional se dijo:
La presente iniciativa tiene por objeto garantizar la libertad de expresión y de difusión y el derecho a la información, así como el derecho de acceso efectivo y de calidad a las tecnologías de la información y la comunicación y a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha.

280. Esto se justificó en la especial naturaleza de las telecomunicaciones, de las que se dijo:
Las tecnologías de la información y los servicios de radiodifusión y telecomunicaciones se han convertido en un instrumento básico de las democracias *(énfasis añadido). Representan un elemento fundamental de participación social y de desarrollo económico. Esto es así porque favorecen las libertades de expresión y difusión, el acceso a la información y potencializan el crecimiento económico, la competitividad, la educación, la salud, la seguridad, el conocimiento, la difusión de ideas y la cultura, entre otros aspectos.*

314. Por ejemplo, se ha establecido que si desde antes de que existieran los órganos constitucionales autónomos, los poderes clásicos (legislativo, ejecutivo y judicial) no podían reclamar la titularidad exclusiva de la función jurídica que tenían asignada sólo preponderantemente y con supremacía, esto es, las funciones legislativa, ejecutiva y jurisdiccional, por mayoría de razón, ahora, los órganos constitucionales autónomos no pueden reclamar la titularidad de una función jurídica exclusiva, ni, a contrario sensu, ser demandados por haber usurpado alguna de esas funciones solo por la razón de que esa función deba resultar exclusiva de alguno de los tres poderes clásicos del Estado *(énfasis añadido).*

315. Por el contrario —se ha concluido— los órganos constitucionales autónomos son titulares de competencias mixtas en las que confluyen las tres funciones, por lo que pueden ejercer funciones quasi-legislativas, quasi-jurisdiccionales y quasi, ejecutivas, siendo irrelevante la específica combinación utilizada por el Constituyente, pues, una vez más, en nuestro país la división funcional de atribuciones no opera de manera tajante y rígida identificada con los órganos que las ejercen, sino que se estructura con la finalidad de establecer un adecuado equilibrio de fuerzas, mediante un régimen de cooperación y coordinación que funcionan como medios de control recíproco, limitando y evitando el abuso en el ejercicio del poder público, garantizando así la unidad del Estado y asegurando el establecimiento y la preservación del estado de derecho *(énfasis añadido).*

316. Así, el estándar mínimo de revisión competencial de los actos y normas de los órganos constitucionales autónomos se ha establecido de la siguiente manera:
De este modo, para que un órgano ejerza ciertas funciones es necesario que expresamente así lo disponga la Constitución Federal o que la función respectiva resulte estrictamente necesaria para hacer efectivas las facultades que le son exclusivas por efectos de la propia Constitución, así como que la función se ejerza en los casos expresamente autorizados o indispensables para hacer efectiva la facultad propia.

317. En el caso, como se había anticipado, el artículo 28, párrafo veinte, fracción IV de la Constitución Federal establece que el IFT, como órgano constitucional autónomo, tiene la facultad propia de "emitir las disposiciones administrativas de carácter general exclusivamente para el cumplimiento de su función regulatoria en el

sector de su competencia", ***lo que implica que esta Suprema Corte debe reconocer que este órgano constitucional tiene la facultad quasi-legislativa necesaria para su fin institucional, la que hemos denominado facultad regulatoria*** *(énfasis añadido).*

319. Sin embargo, desde ahora cabe rechazar cualquier afirmación en contrario de la parte actora, que gire alrededor del reclamo que el IFT ejerció una facultad de producción normativa de carácter general que debe considerarse inconstitucional, por la única razón que la facultad legislativa sea monopolio exclusivo del poder legislativo, pues la concepción del principio de división de poderes, cualquiera que apoye esta conclusión, debe ser rechazada desde ahora. El IFT tiene asignada en el texto constitucional una facultad regulatoria que debe garantizarse en el margen necesario para cumplir sus fines institucionales a costa de lo que decidan en contrario los otros poderes, lo que incluye necesariamente la capacidad de emitir reglas generales, abstractas e impersonales.

320. Si el poder legislativo alega que el IFT emitió una norma general extralimitándose en el ejercicio de su facultad regulatoria, debe acreditar que ese ejercicio de facultades quasi-legislativa no está permitido por la Constitución y ello exige un cuidadoso estudio del texto constitucional en cada caso concreto.

321. Al final, ***este Pleno concluye que lo relevante para determinar la validez de un acto o norma del IFT es determinar si actuó dentro de su órbita de competencias constitucionales establecida en el artículo 28*** *(énfasis añadido). La validez competencial de sus actos y normas se condiciona a que se inserten en el ámbito material de la regulación y no se extralimite invadiendo la facultad legislativa del Congreso de la Unión, definida en el artículo 73 de la Constitución Federal.*

*325. De la exposición de las razones del Constituyente se observa que nuestro modelo constitucional adopta en su artículo 28, **la concepción del Estado Regulador** (énfasis añadido), entendido como el modelo de diseño estatal insertado por el Constituyente Permanente para atender necesidades muy específicas de la sociedad postindustrial (suscitadas por el funcionamiento de mercados complejos), que deposita en ciertas agencias independientes —de los órganos políticos y de los entes regulados— la regulación de ciertas cuestiones especializadas sobre la base de disciplinas/o racionalidades técnicas. Este modelo de Estado Regulador, por regla general, exige la convivencia de dos fines: la existencia eficiente de mercados, al mismo tiempo que la consecución de condiciones equitativas que permitan el disfrute más amplio de todo el catálogo de derechos humanos con jerarquía constitucional. De ahí, que a estos órganos se les otorgue funciones regulatorias, diferenciadas de las legislativas, otorgadas al Congreso de la Unión y de las reglamentarias otorgadas al Ejecutivo por el artículo 89, fracción I de la Constitución Federal.*

***329. Subyacente a la facultad reglamentaria de la administración pública federal subsiste una concepción constitucional de distribución de poderes de producción normativa entre el legislador y el ejecutivo que claramente se pronuncia por depositar en el primero las principales decisiones de política pública, reservando al segundo exclusivamente una facultad de ejecución y desarrollo, no de innovación o configuración normativa** (énfasis añadido).*

333. Según lo ha sostenido este Alto Tribunal en numerosos precedentes, el artículo 89, fracción I, constitucional, faculta al presidente de la República para expedir normas reglamentarias de las leyes emanadas del Congreso de la Unión, y aunque desde el punto de vista material ambas normas son similares, aquéllas se distinguen de éstas básicamente, en que provienen de un órgano que al emitirlas no expresa la voluntad general, sino que está instituido para acatarla en cuanto dimana del Legislativo.

*335. Así, no pudiendo el reglamento más que ejecutar y desarrollar la ley, sin la cual no podría existir, la jurisprudencia de **esta Suprema Corte ha establecido que la ley y el reglamento se relacionan mediante dos principios que dan cuenta no sólo de la superioridad jerárquica de la ley, sino también de la imposibilidad de los reglamentos de producir innovaciones de contenidos en el ordenamiento jurídico: los principios de reserva de ley y de subordinación jerárquica** (énfasis añadido).*

337. En otras palabras, como lo ha señalado la Primera Sala, "[e]l principio de reserva de ley que encuentra su justificación en la necesidad de preservar los bienes jurídicos de mayor valía de los gobernados (tradicionalmente su libertad personal y propiedad) prohíbe que en el reglamento se aborden materias reservadas en exclusiva a las leyes del Congreso, como son las relativas a la definición de los tipos penales, las causas de expropiación y la determinación de los elementos de los tributos, mientras que el principio de subordinación jerárquica, exige que el reglamento esté precedido por una ley cuyas disposiciones desarrolle, complemente o pormenorice y en las que encuentre su justificación y medida."

339. En suma, los principios de reserva de ley y de supremacía jerárquica de la ley exigen dos tipos de consecuencias sobre los reglamentos del ejecutivo, a saber, que de acuerdo con el primero de los sub-principios, los reglamentos no aborden de manera innovadora ningún tópico material relevante, al corresponder en exclusiva su regulación a la fuente legal y por lo que respecta al segundo de los sub-principios, que el reglamento siempre esté precedido de una ley que se le limite a ejecutar y a desarrollar, de tal forma que, por regla general, no queda hablar de reglamentos autónomos.

340. Pues bien, este Pleno rechaza que estos dos principios —en todo su alcance— constituyan un parámetro de control constitucional de las normas generales emitidas por el IFT con fundamento en el párrafo vigésimo de la fracción IV del artículo 28 constitucional. La racionalidad que sustenta el diseño de los reglamentos no es transportable al artículo 28 constitucional, ya que éste responde a una narrativa estatal diversa, que justamente busca el fortalecimiento de un órgano regulador autónomo con el poder suficiente de regulación que innove el ordenamiento jurídico *(énfasis añadido).*

341. En efecto, este Tribunal Pleno considera que los precedentes referidos a la facultad reglamentaria del Ejecutivo, conforme el artículo 89, fracción I,

constitucional no son aplicables a las disposiciones de carácter general del IFT por una razón de diseño institucional: el Constituyente reservó para el IFT un balance de distribución de poder público distinto, ya que, a diferencia del reglamento, en las disposiciones de carácter general del IFT sí se deposita un umbral de poderes de decisión que invisten a ese órgano de un poder de innovación o configuración normativa ausente en el Ejecutivo. Dicha facultad es regulatoria y constituye una instancia de producción normativa diferenciada de la legislación, conforme al artículo 73 constitucional, de los reglamentos del Ejecutivo del artículo 89, fracción I constitucional, y de las cláusulas habilitantes que esta Suprema Corte ha reconocido puede establecer el Congreso de la Unión, para habilitar a ciertos órganos administrativos para emitir reglamentación, emitidas con fundamento en los artículos 73, fracción XXX y 90 de la Constitución Federal *(énfasis añadido).*

346. Por tanto, en principio, no existe razón constitucional para afirmar que ante la ausencia de una ley no sea dable constitucionalmente que el IFT emita regulación autónoma de carácter general, siempre y cuando sea "exclusivamente para el cumplimiento de su función reguladora en el sector de su competencia".

347. Así, no cabe aplicar a las disposiciones administrativas de carácter general del IFT los principios de reserva de ley ni de subordinación jerárquica de la ley, al menos, no con el mismo grado de exigencia aplicable a los reglamentos del Ejecutivo.

405. El principio de no contradicción al que se debe ajustar el IFT al emitir regulación, con fundamento en el artículo 28 constitucional, responde a la decisión del Constituyente de establecer un esquema de división de trabajo de producción normativa entre el legislador y el órgano constitucional autónomo —uno para legislar y el otro para regular—, que no incluye un criterio material para distinguir con nitidez un espacio apartado y diferenciado reservado a cada uno de ellos, sino que se dispone de un espacio material común —denominado como sectores de telecomunicaciones y radiodifusión— a los que ambos están llamados a desplegar sus facultades de producción normativa de una manera concurrente. Esto se demuestra, pues el constituyente escogió caracterizar la facultad legislativa del Congreso de la Unión con un lenguaje general capaz de abarcar todo el ámbito material igualmente destinado al IFT para emitir disposiciones regulatorias *(énfasis añadido).*

406. Así, ante la decisión del Constituyente de establecer un espacio material de proyección de facultades legislativas y regulatorias traslapadas para proveer de un marco normativo a los sectores de telecomunicaciones y radiodifusión, se insiste, el Congreso mediante legislación y el IFT mediante regulación, este Tribunal Pleno concluye que el IFT está sujeto al principio de no contradicción de las leyes de la materia, toda vez que el artículo 28 constitucional establece que su objeto lo debe realizar "conforme a lo dispuesto en esta Constitución y en los términos que fijen las leyes".

407. En consecuencia, en cumplimiento al referido principio de no contradicción,

para determinar la validez de la regulación del IFT debe acudirse a la ley de la materia y determinar si el legislador abordó directamente la cuestión a debate y aportó una solución normativa a la misma. Si la respuesta es positiva, debe hacerse explícita la solución apoyada por el legislador y confrontarla con la o las disposiciones de carácter general del IFT y sólo en caso de resultar contradictorias, debe declararse la invalidez de la disposición impugnada. ***Lo anterior, en el entendido que el IFT no es un órgano subordinado jerárquicamente al poder legislativo, sino un órgano con competencias propias apto para configurar el ordenamiento jurídico con regulación propia, sin embargo, toda vez que debe ajustarse a los términos que establezcan las leyes, es claro que el IFT no puede contradecir la legislación del Congreso emitida con fundamento en el artículo 73 constitucional*** *(énfasis añadido).*

408. Si la respuesta es negativa, esto es, que la ley de la materia no otorgue una respuesta normativa sobre el punto en cuestión, esta Suprema Corte debe reconocer la validez de la disposición de carácter general impugnada, siempre y cuando la norma general del IFT sea una opción normativa inserta en el ámbito regulatorio asignado a su esfera de competencias en su carácter de órgano constitucional autónomo, en términos del artículo 28 constitucional, siendo innecesario, por tanto, que a la regulación impugnada le sea precedida una ley.

409. Lo anterior no implica que el IFT esté habilitando para emitir la regulación que desee con cualquier contenido, libre de escrutinio constitucional, pues el artículo 28 constitucional establece claramente que su mandato, como órgano constitucional autónomo, "tiene por objeto el desarrollo eficiente de la radiodifusión y las telecomunicaciones". En consecuencia, la regulación del IFT debe proveer a la realización de dicho fin constitucional de una manera no arbitraria ni caprichosa, lo que deberá analizarse caso por caso *(énfasis añadido).*

Por todo lo anterior, reitero que coincido con la aseveración de que "el IFT debería jugar un rol más activo en cuanto a la **definición de políticas de ciberseguridad** que deben aplicarse en el sector de telecomunicaciones y radiodifusión, impulsando iniciativas que permitan incorporar las mejores prácticas internacionales en materia de ciberseguridad y ciber resiliencia", ejerciendo las funciones quasi-legislativas, quasi-jurisdiccionales y quasi-ejecutivas que le fueron conferidas a nivel constitucional.

Asimismo, considero muy relevante que el IFT aborde lo planteado en la Recomendación 6 respecto a los servicios de cómputo en la nube en sus distintas modalidades, derivado de su mandato constitucional de garantizar el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet, estableciendo condiciones de competencia efectiva en la prestación de dichos servicios (artículos 6o. y 28 de la CPEUM).

Finalmente, cabe resaltar que la relevancia de los temas de ciberseguridad y ciber resiliencia está contemplada de cierta forma en el Reglamento de las

Telecomunicaciones Internacionales, uno de los instrumentos vinculantes de la UIT bajo el derecho Internacional, resultado de la Conferencia Mundial de Telecomunicaciones Internacionales celebrada en Dubái, Emiratos árabes Unidos en 2012.

El "ARTÍCULO 5A Seguridad y robustez de las redes" del mencionado reglamento estipula lo siguiente:
"Los Estados Miembros procurarán garantizar, individual y colectivamente, la seguridad y robustez de las redes de telecomunicación internacionales a fin de lograr su utilización eficaz y evitar perjuicios técnicos a las mismas, así como el desarrollo armonioso de los servicios internacionales de telecomunicación ofrecidos al público."

Sin más por el momento, aprovecho la oportunidad para enviarles un cordial saludo.

FIRMADO POR: LILIA EURIDICE PALMA SALAS
FECHA FIRMA: 2023/10/15 10:41 PM
AC: AUTORIDAD CERTIFICADORA
ID: 72364
HASH:
2DFEDBDDBC8A8D7DEFEF42D60178253955238E9610B402
6BDF5B2DF93D04D43C

FIRMADO POR: REBECA ESCOBAR BRIONES
FECHA FIRMA: 2023/10/17 7:09 PM
AC: AUTORIDAD CERTIFICADORA
ID: 72364
HASH:
2DFEDBDDBC8A8D7DEFEF42D60178253955238E9610B402
6BDF5B2DF93D04D43C

RECOMENDACIÓN QUE EMITE EL VII CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES SOBRE EL MARCO ÉTICO INSTITUCIONAL Y SU IMPACTO EN EL SECTOR DE LAS TELECOMUNICACIONES Y LA RADIODIFUSIÓN

Reconocemos el papel proactivo del Instituto Federal de Telecomunicaciones (IFT, Instituto) en la adopción de prácticas éticas para la regulación del sector. Apenas un año después de la publicación de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR, 2014), el IFT adoptó los tres instrumentos que conforman su marco ético institucional: a) la Declaración de Principios, b) el Código de Ética del Instituto y c) el Código de Conducta de los Trabajadores. Los peritos en telecomunicaciones y radiodifusión -reconocidos como profesionales expertos y capaces, y que son acreditados por el Instituto – también están obligados a conocer y acatar un código de ética (Lineamientos para la Acreditación de Peritos en Materia de Telecomunicaciones y Radiodifusión, 2023, LAP).

También reconocemos el trabajo del Instituto en promover la adopción de principios éticos en el sector de las telecomunicaciones y la radiodifusión (STR), mediante la inclusión en el Plan Anual de Trabajo 2023, de la estrategia 3.3.6[1]. que a la letra dice:

> "Garantizar las condiciones de competencia en el mercado interno, fomentar el desarrollo y adopción de códigos de ética y políticas de integridad y anticorrupción en el sector empresarial, y combatir otras distorsiones que afectan la asignación eficiente de los recursos".

Por otra parte, del corpus pericial del Instituto resulta de una obligación legal, para garantizar la consistencia de actividad pericial como coadyuvante del Instituto para el cumplimiento de la ley, en la homologación de dispositivos o acreditación de los sistemas

[1] Que se origina en la Estrategia 2.1: "Propiciar un entorno de competencia efectiva a través del monitoreo y análisis de los mercados de TyR en el contexto del ecosistema digital, considerando las nuevas tecnologías y los nuevos modelos de negocio que corresponden al ámbito competencial del Instituto".

de telecomunicaciones y de radiodifusión, a través de la verificación del cumplimiento de las disposiciones técnicas con la práctica generalizada en el IFT.

El marco legal existente obliga a algunos de los regulados (y peritos) a adoptar ciertos principios éticos, pero no obliga a todos los regulados. Diversos concesionarios cuentan y difunden sus principios éticos de negocio como parte de sus estrategias para cumplir la llamada práctica ESG[2]. Por ejemplo, un concesionario de telecomunicaciones deja claro que tiene el compromiso para actuar con honestidad, integridad y transparencia. Otro operador, indica la honestidad, legalidad, integridad y el respeto a los derechos humanos como principios éticos en su negocio.

Finalmente, al constituirse como un sistema, el STR depende de una cultura[3] propia que al interior se genera[4]. Las diversas interacciones de los actores en un sistema siempre terminarán por definir la profundidad y características de las relaciones éticas entre estos y eventualmente, los requisitos éticos de pertenencia e interacción.

MONITOREO DEL CUMPLIMIENTO DEL MARCO ÉTICO INSTITUCIONAL

Como se ha mencionado, las características regulatorias y autorregulatorias del STR permiten apreciar la importancia de las estructuras éticas de los actores y de las interacciones entre ellas. Algunas son formales como el marco ético institucional, mientras que otras se dan por las relaciones de inversión y negocio. Aquello que es establecido por los ordenamientos legales (relaciones éticas formales) han quedado bajo la supervisión del Instituto. Por una parte, el seguimiento del cumplimiento de las obligaciones legales de los

[2] Pese a no existir una definición universal de ESG, la práctica observada muestra elementos a considerar en su definición, v.g. Perez et al. (2022), "… *The 'how' of a company's environmental, social, and governance (ESG) proposition starts with recognizing what companies should be solving for: maintaining and reinforcing their social license to operate, in the face of rising externalities*".

[3] Ardichvili et al. (2009) nos deja ver que en la investigación antropológica sugiere que la cultura "son los comportamientos aceptados en los confines de un grupo específico y guiados por un patrón común de creencias, tradiciones y principios".

[4] De acuerdo con Armstrong (2020), los principios éticos "guían las acciones y las prácticas que están dirigidas a mejorar el bienestar de la sociedad". Sin lugar a duda, en el sector telecomunicaciones y radiodifusión, cada organización puede establecer sus valores y principios éticos, aunque pueden existir algunos comunes, por ejemplo, conducir los negocios con honradez y legalidad.

trabajadores del IFT se lleva a cabo como se ha descrito en la "Recomendación para fortalecer la actuación del Comité de Ética del IFT" del VII Consejo Consultivo del IFT (CCIFT, 2023). Por otra parte, el resto de las obligaciones legales impuestas a los regulados también deben ser monitoreados por el Instituto. De esta forma, en el caso del Comité Consultivo de Acreditación de Peritos en Telecomunicaciones y Radiodifusión los lineamientos obligan al órgano a "emitir la Declaración de Principios del Comité Consultivo, misma que deberá reflejar los valores y las reglas bajo los cuales se conducirán los integrantes del mismo" (Lineamientos Cap. IV 2023) misma que no se encontró en registro público. También, este comité tiene la función de "proponer al Instituto el código de ética para los Peritos Acreditados, el cual será aprobado por el Titular de la Unidad Administrativa del Instituto responsable de la Acreditación de Peritos". De esta forma, el corpus pericial cuenta con un código de ética (2018) que se compone de 15 artículos que explícitamente promueven la "responsabilidad, probidad, rectitud, solvencia moral y profesional" (CEP, 2018) y en general lo previsto en la Declaración de Principios.

SOBRE LAS SANCIONES DE LO ÉTICO EN EL STR

Diversos códigos de ética incluyen sanciones a su incumplimiento. Esto depende en gran medida de la teoría ética de la que se originan[5]. Aquellas conductas no-éticas que "merecen" una sanción resultan también del marco legal laboral, civil, administrativo e incluso penal.

Como apunta la "Recomendación para fortalecer la actuación del Comité de Ética del IFT" del VII Consejo Consultivo del IFT (CCIFT, 2023), además de los casos en que los incumplimientos requieran sanciones administrativas, puedan darse incumplimientos que no impliquen una responsabilidad administrativa y, consecuentemente, que las medidas de

[5] Armstrong (2020) sugiere que la diversidad de estas teorías puede ser clasificadas como: teleológicas, deontológicas y la de las partes interesadas. La naturaleza tecnológica de los objetos que componen al STR sugiere que esta última podría ser la más utilizada sin embargo la investigación actual reporta que la más utilizada es el utilitarismo (teoría teleológica). Esto afirmaría que junto a un juicio ético y moral sobre lo "bueno" o "malo" de la conducta debe existir una "sanción" o consecuencia a la misma.

solución no sean necesariamente punitivas y pueden considerarse la adopción de medidas preventivas y correctivas que sean proporcionales y apropiadas.

Con respecto al uso de mecanismos sancionatorios o medidas de solución para promover un ambiente de altos estándares éticos, en casos particulares como el del corpus pericial dada la particularidad de las disposiciones éticas del ejercicio profesional que se originaron en una obra colegiada, parece apropiado que el propio Comité Consultivo de Acreditación de Peritos en Telecomunicaciones y Radiodifusión determine el manejo de las sanciones por faltas éticas graves mediante la implementación de una comisión que atienda las denuncias correspondientes (de forma análoga a la del Órgano Interno de Control en el Instituto). En el caso de los concesionarios de radiodifusión que están obligados a contar con un código de ética, al ser esta una disposición legal que emana de la propia LFTR, sus reglamentos y lineamientos ya consideran las sanciones que resultan por la omisión del cumplimiento.

RECOMENDACIONES

El VII Consejo Consultivo del Instituto Federal de Telecomunicaciones reconoce la importancia de un marco ético para las actividades del sector de las telecomunicaciones y de la radiodifusión. Este Consejo invita al Pleno del Instituto Federal de Telecomunicaciones a promover la adopción de principios y valores éticos que contribuyan a la cultura de la legalidad en el sector de las telecomunicaciones y la radiodifusión, y fomentar la innovación, el crecimiento, la competencia y el beneficio de la sociedad. De esta forma, este Consejo recomienda al Instituto:

PRIMERO. Continuar con el liderazgo ético en el sector de las telecomunicaciones y la radiodifusión en México mediante la promoción y divulgación de su marco ético institucional. Para lo cual, podría retomar las campañas de difusión entre todos los actores del sector y de forma amplia a través de los recursos electrónicos de Instituto.

SEGUNDO. Considerar en la revisión periódica del marco ético institucional compuesto por el Código de Ética, la Declaración de Principios y el Código de Conducta de los Trabajadores del Instituto Federal de Telecomunicaciones, aquellas prácticas que reflejan la cultura de lo ético en el sector de las telecomunicaciones y la radiodifusión.

TERCERO. Sugerir al Comité Consultivo de Acreditación de Peritos en Telecomunicaciones y Radiodifusión la revisión del Código de Ética para Peritos en Materia de Telecomunicaciones y Radiodifusión acreditados por el Instituto Federal de Telecomunicaciones para incorporar los principios y valores contenidos en el marco ético institucional.

Lilia Eurídice Palma Salas

Presidenta del VII Consejo Consultivo

Mtra. Rebeca Escobar Briones

Secretaria del Consejo Consultivo

La Recomendación fue aprobada por el VII Consejo Consultivo del Instituto Federal de Telecomunicaciones por unanimidad de votos de los consejeros: Alejandro Ildefonso Castañeda Sabido, Sara Gabriela Castellanos Pascacio, Ernesto M. Flores-Roux, Mario Germán Fromow Rangel, Gerardo Francisco González Abarca, Ali Bernard Haddou Ruiz, Salma Leticia Jalife Villalón[6], Luis Miguel Martínez Cervantes, Jorge Fernando Negrete Pacheco, Eurídice Palma Salas y Cynthia Gabriela Solís Arredondo, mediante Acuerdo CC/VII/IFT/280923/30. Lo anterior, de acuerdo con el artículo 17 de las Reglas de Operación del CCIFT, en la X Sesión Ordinaria celebrada el 28 de septiembre de 2023.

El Grupo de Trabajo que desarrolló el proyecto de Recomendación está integrado por su coordinador el consejero Luis Miguel Martinez Cervantes y los consejeros Eurídice Palma Salas, Ernesto M. Flores-Roux y Gerardo Francisco González Abarca.

[6] La consejera Salma Leticia Jalife Villalón voto vía WhatsApp en el grupo del VII CCIFT el 28 de septiembre de 2023.

REFERENCIAS

1. A. Ardichvili, JA. Mitchell, D. Jondle. "Characteristics of ethical business cultures." Journal of Business Ethics 85: 445-451, 2009.
2. A. Armstrong, “Ethics and ESG”, AABFJ | Volume 14, No.3, 2020
3. Gobierno de México, “Ley Federal de Telecomunicaciones y Radiodifusión”, 2021
4. Instituto Federal de Telecomunicaciones, “Código de Ética para Peritos en Materia de Telecomunicaciones y Radiodifusión acreditados por el Instituto Federal de Telecomunicaciones conforme a los lineamientos para la acreditación de peritos en materia de telecomunicaciones y radiodifusión”, 2018.
5. Instituto Federal de Telecomunicaciones, “Lineamientos para la Acreditación de Peritos en Materia de Telecomunicaciones y Radiodifusión”, 2023.
6. Instituto Federal de Telecomunicaciones, “Programa Anual de Trabajo”, 2023.
7. Pérez, Lucy, et al. "How to make ESG real." The McKinsey Quarterly. 2022.
8. VII Consejo Consultivo del IFT. “Recomendación para fortalecer la actuación del Comité de Ética del IFT”. México. 2023.

BIBLIOGRAFÍA COMPLEMENTARIA

1. “Órgano Interno de Control,” IFT. [En línea]. Disponible: https://www.ift.org.mx/transparencia/oic/denuncias. [Acceso: 06-Jul-2023].
2. “The IBE Business Ethics Framework,” Home. [En línea]. Disponible: https://www.ibe.org.uk/knowledge-hub/ibe-business-ethics-framework.html. [Acceso: 06-Jul-2023].
3. A. Chadegani, A. Aghaei, and A. Jari, "Corporate ethical culture: Review of literature and introducing pp model", Procedia Economics and Finance 36: 51-61, 2016.
4. AA. Kobylko, "Telecommunication ecosystems: Special features of management and interaction," Upravlenets, Ural State University of Economics, vol. 11(1), 2020.

5. AA. Kobylko, "Telecommunication ecosystems: Special features of management and interaction." Управленец 11.1: 15-23, 2020.
6. Auditoria Superior de la Federación, “Auditoría Cumplimiento Financiero: 2017-0-43100-15-0132-2018”, 2018.
7. C. Manning, & S. Manning, “Ethical Challenge in Telecommunications”, The International Information & Library Review, 32(3-4), 2000. doi:10.1006/iilr.2000.0144
8. G.B. Kleiner, “A New Theory of Economic Systems and Its Applications”, Herald of the Russian Academy of Sciences, Vol. 81, No. 5, 2011.
9. Global Symposium for Regulators (GSR), “Best Practice Guidelines Regulatory and economic incentives for an inclusive sustainable digital future”, 2023.
10. H. Bril, G. Kell, A. Rasche “Sustainability, Technology, and Finance: Rethinking How Markets Integrate ESG”, Routledge, 2022, ISBN: 9781032200569; 1032200561.
11. IBM, “Reshaping the telecommunications ecosystem and business models”, https://www.ibm.com/blog/reshaping-the-telecommunications-ecosystem-and-business-models/
12. Instituto Federal de Telecomunicaciones, “Acuerdo mediante el cual el Titular del Órgano Interno de Control emite el Código de Ética del Instituto Federal de Telecomunicaciones”, Diario Oficial de la Federación, 2019.
13. Instituto Federal de Telecomunicaciones, “Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones aprueba y emite los Lineamientos para la Entrega, Inscripción y Consulta de Información para la conformación del Sistema Nacional de Información de Infraestructura”. Diario Oficial de la Federación, 2019.
14. Instituto Federal de Telecomunicaciones, “Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones modifica y adiciona el Código de Conducta de los trabajadores del Instituto Federal de Telecomunicaciones para armonizarlo con la Ley General del Sistema Nacional Anticorrupción, la Ley General de Responsabilidades Administrativas, la Ley Federal de Telecomunicaciones y

Radiodifusión y el Código de ética del Instituto Federal de Telecomunicaciones", 2019.

15. Instituto Federal de Telecomunicaciones, "Comunicado de Prensa No. 70/2017: se efectúa la primera sesión del Comité Consultivo de Acreditación de peritos en Telecomunicaciones y Radiodifusión del Instituto Federal de Telecomunicaciones", 2017.

16. Instituto Federal de Telecomunicaciones, "Estatuto Orgánico del Instituto Federal de Telecomunicaciones", Diario Oficial de la Federación, 2020.

17. Instituto Federal de Telecomunicaciones, "Normas de Control Interno del Instituto Federal de Telecomunicaciones", 2022.

18. Instituto Federal de Telecomunicaciones, "Reglas de Operación del Consejo Consultivo del Instituto Federal de Telecomunicaciones", 2019.

19. Instituto Federal de Telecomunicaciones, "Reglas de Operación del Comité Técnico en materia de espectro radioeléctrico", 2017.

20. Instituto Federal de Telecomunicaciones, "Reglas de operación del Comité Técnico en Materia de Despliegue de 5G en México", 2019.

21. JD. DeBode, AA. Armenakis, HS. Feild, H. S., AG. Walker, "Assessing Ethical Organizational Culture", The Journal of Applied Behavioral Science, 49(4), 2013. doi:10.1177/0021886313500987

22. K. Sarikakis, K. Rozgonyi, "Ethics in the governance of telecommunications: accountability of global industrial actors, 27th European Regional Conference of the International Telecommunications Society (ITS): "The Evolution of the NorthSouth Telecommunications Divide: The Role for Europe", Cambridge, United Kingdom, 7th-9th September, 2016.

23. M. Ellman, P. Pezanis-Christou, "Organizational Structure, Communication, and Group Ethics." American Economic Review, 100 (5): 2478-91, 2010. DOI: 10.1257/aer.100.5.2478

24. M. Kamel, and K. Morrell. "The ethical business: Challenges and controversias". Bloomsbury Publishing, 2017.

25. M. Kaptein, "Developing and testing a measure for the ethical culture of organizations: The corporate ethical virtues model." Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior 29.7, 2008.

26. P. Cabrera, J. Oriol, “La gobernanza de las telecomunicaciones: hacia la economía digital”, Monografía del Banco Interamericano de Desarrollo, Washington, EEUU, 20217.

27. S. Sengupta, “Models of Business Ethics”, Management Weekly, 2020, https://managementweekly.org/models-of-business-ethics/

28. Unión Internacional de Telecomunicaciones, “Global Digital Regulatory Outlook”, 2023.

29. XM. Xie, T.Lv and G.J. Liu, "The Research on Telecommunication Industry Business Ecosystem," 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, 2008, pp. 1-5, doi: 10.1109/WiCom.2008.1590.

FIRMADO POR: LILIA EURIDICE PALMA SALAS
FECHA FIRMA: 2023/10/16 6:49 PM
AC: AUTORIDAD CERTIFICADORA
ID: 72305
HASH:
B1F70468FED5ADA4CE72997E056AB74D7945772E74162D
18B1A1E651D0A8C0C2

FIRMADO POR: REBECA ESCOBAR BRIONES
FECHA FIRMA: 2023/10/17 7:09 PM
AC: AUTORIDAD CERTIFICADORA
ID: 72305
HASH:
B1F70468FED5ADA4CE72997E056AB74D7945772E74162D
18B1A1E651D0A8C0C2

RECOMENDACIÓN QUE EMITE EL VII CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES SOBRE LA PARTICIPACIÓN ACTIVA DEL INSTITUTO EN LAS DISCUSIONES EN TORNO A LA CREACIÓN DE LA LEGISLACIÓN EN MATERIA DE CIBERSEGURIDAD PROPUESTA POR DIFERENTES PARTIDOS POLÍTICOS DADAS LAS POSIBLES IMPLICACIONES QUE TUVIERA PARA EL INSTITUTO

El VII Consejo Consultivo del Instituto Federal de Telecomunicaciones emite la presente recomendación al Pleno del Instituto Federal de Telecomunicaciones ("IFT o Instituto"), para intervenir proactivamente en la redacción final de la iniciativa de una Ley Federal de Ciberseguridad dada la importancia que este tema significa para el futuro de las telecomunicaciones, el ordenamiento jurídico nacional aplicable y la actividad del propio Instituto.

I. ANTECEDENTES

1. La Ciberseguridad puede ser entendida como el conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicaciones, en términos de la Estrategia Nacional de Ciberseguridad de 2017[1] (ENA).

El objetivo primordial de la ENA al momento de su creación y publicación era establecer la visión del Estado Mexicano en la materia. Es un concepto que involucra esfuerzos de distinta naturaleza, no únicamente aspectos legislativos o técnicos. Por lo que la normativa sobre ciberseguridad que en su momento se expida a nivel federal, deberá contar con un enfoque integral, principalmente apelando a una

[1] Estrategia Nacional de Ciberseguridad, última vez consultado el día 30 de junio de 2023.

correcta gestión de riesgos y preponderando la visión preventiva más que correctiva y punitiva.

2. Hablando estrictamente de legislación federal, el primer antecedente legislativo que se encuentra aún en vigor, lo podemos encontrar en el Código Penal Federal, en el CAPÍTULO II del TÍTULO NOVENO, artículos 211 BIS I a 211 BIS 7, enfocados a sancionar las conductas de acceso ilícito a Sistemas y Equipos de informática publicado en el Diario Oficial de la Federación el 17 de mayo de 1999[2]. En esa misma Reforma también el legislador se encargó de adicionar el artículo 168 BIS para prever las sanciones aplicables a conductas ilícitas tendientes a descifrar las señales de telecomunicaciones. Esto ilustra que desde hace más de 20 años ha sido de interés del legislador federal abordar y sancionar las conductas ilícitas en contra de los Sistemas de Informática y las Telecomunicaciones, y hace patente que dicha legislación continúa vigente y desmitifica la idea de que no existe legislación aplicable en materia de ciberseguridad.

3. A nivel estatal, podemos destacar amplios esfuerzos legislativos desde el año 2000, por ejemplo, el Código Penal del Estado de Sinaloa, en su Capítulo V artículo 217 sanciona lo que se entiende por Delito Informático; a lo largo del tiempo y de la República Mexicana, los legisladores de distintas entidades federativas han ido reformando y adicionando artículos tendientes a sancionar estas conductas, como ejemplo, presentamos una tabla elaborada con una muestra representativa:

[2] https://www.dof.gob.mx/nota_detalle.php?codigo=4948419&fecha=17/05/1999#gsc.tab=0

ESTADO	ARTÍCULOS	NOMENCLATURA	FECHA DE PUBLICACIÓN
AGUASCALIENTES	ARTÍCULO 181	Acceso informático indebido	Reformado el 28 de noviembre de 2019
BAJA CALIFORNIA	TÍTULO TERCERO, CAPÍTULO SEGUNDO	Delitos Contra la Inviolabilidad Del Secreto y de los Sistemas y Equipos de Cómputo y Protección de los Datos Personales	14 de septiembre de 2007
CHIHUAHUA	CAPÍTULO IV	Del Uso y Acceso Ilícito a los Sistemas y Equipos Informáticos y de Comunicación	19 de noviembre de 2011
COLIMA	Artículo 201	Se equipara al delito de fraude en la fracción VII y se considera como agravante que el sujeto activo cuente con formación o grado relacionado con la informática	22 de noviembre 2016

JALISCO	CAPÍTULO II	La Obtención Ilícita de Información Electrónica	4 de mayo de 2012
QUERÉTARO	CAPÍTULO II	Acceso Ilícito a Sistemas de Informática	22 de abril de 2011
YUCATÁN	CAPÍTULO V TER	Delitos Informáticos	26 de noviembre de 2019

4. Adicionalmente, desde hace más de una década se han promulgado otras Leyes Federales que estipulan de manera preventiva y correctiva, obligaciones en materia de ciberseguridad, algunas de ellas son:

NORMA	**ARTÍCULO (S)**	**NOMENCLATURA**	**FECHA DE PUBLICACIÓN**
Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Artículos 19, 20 y 21 CAPÍTULO XI	Medidas de Seguridad, deberes de seguridad y confidencialidad De los Delitos en Materia del Tratamiento Indebido de Datos Personales	5 de julio de 2010

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Artículo 50 Artículo 52 Capítulo III	Obligaciones del encargado Tratamiento de datos personales en el denominado cómputo en la nube De las Medidas de Seguridad en el Tratamiento de Datos Personales	21 de diciembre de 2011
Ley Federal de Telecomunicaciones y Radiodifusión	Artículos 2, 56, 117, 145, 150, 183, 185, 189, 190,		14 de julio de 2014
Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados	Artículo 3, fracciones XIV, XX, XI, XX, XXIII, Artículo 12 Artículos 30, 31, 32, 33, 34, 35, 36, 37, 38, 39 y 42	 Deber de seguridad	26 de enero de 2017

5. Los ataques a infraestructuras gubernamentales son una de las razones por las cuales se ha hablado de la materia de ciberseguridad como prioridad al final de esta administración del gobierno federal. Ha habido un incremento en el número de ciberataques que han sufrido diversas entidades gubernamentales, tanto federales como estatales, comprometiendo infraestructuras críticas, como fue el caso del ciberataque de *Ransomware* en contra de PEMEX en el 2019[3], varios ciberataques dirigidos al SAT[4] en lo que va del sexenio[5], y aquel del que no ha podido recuperarse CONAGUA[6,7], entre otros. Sin duda alguna, el más famoso que aceleró el debate legislativo en torno a la materia de Ciberseguridad, ha sido el sufrido por SEDENA[8], mejor conocido como Guacamaya *Leaks*[9], de proporciones aún inestimables, por la cantidad de información comprometida, mucha de ella sensible o de seguridad nacional.

6. Estos ciberataques se han cometido a pesar de que existe la legislación vigente tendiente a prevenir y combatir estos delitos. Esta situación deja claro que no es precisamente legislación lo que falta, sino muchos otros elementos, tales como presupuesto, capacitación, enfoque de gestión de riesgos, y correcta implementación de las medidas obligatorias por Ley, entre otras.

---

[3] El rescate por el hackeo a Pemex es el segundo mayor por *ransomware*.

[4] SAT Servicio de Administración Tributaria
[5] SAT ha recibido más ciberataques con AMLO que en otro sexenio.

[6] Conagua, Comisión Nacional del Agua
[7] Conagua bajo ataque cibernético: Resaltando el déficit de la ciberseguridad en el sector del agua en México.

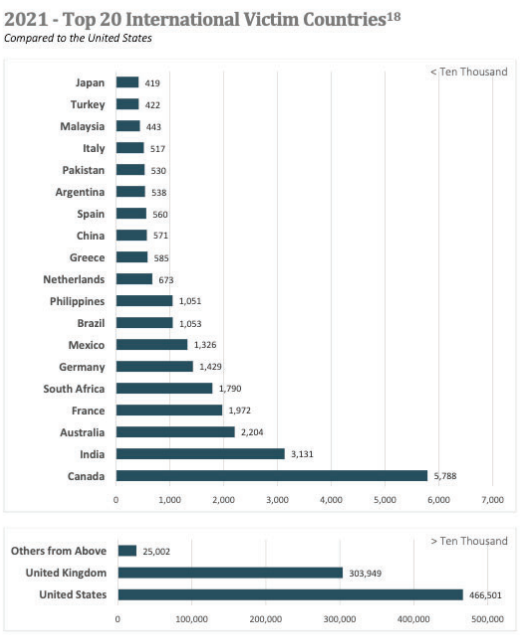
[8] SEDENA Secretaría de la Defensa Nacional
[9] Guacamaya *Leaks*: 5 revelaciones del hackeo masivo que sufrió el ejército de México - BBC News Mundo.

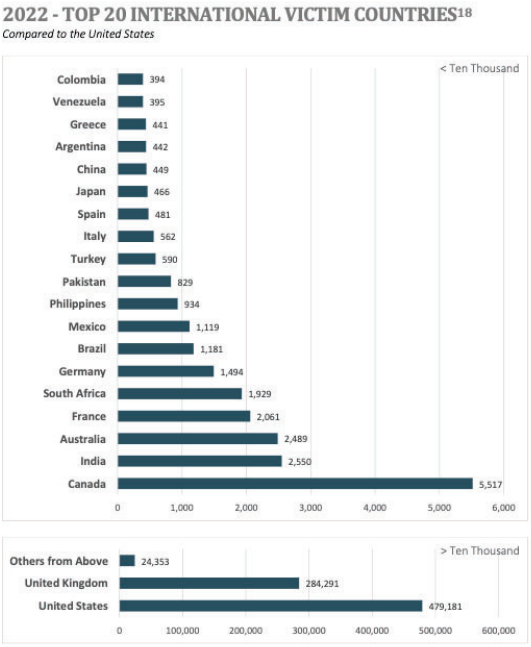
II. SITUACIÓN ACTUAL E INICIATIVAS

2.1 ESTADO DE LA CIBERSEGURIDAD EN MÉXICO

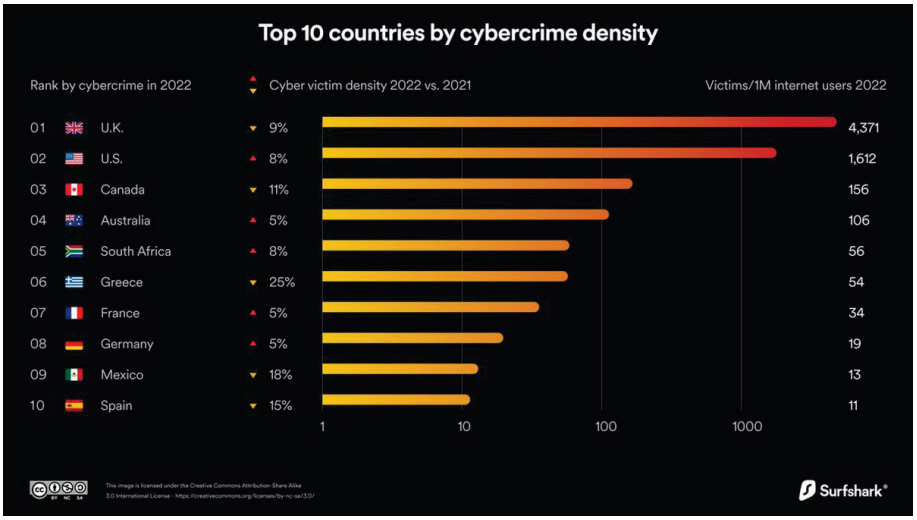
El estado de la ciberseguridad que guarda México actualmente es preocupante tanto del punto de vista nacional como el internacional. Cada año o dos, el FBI[10] publica su "*Internet Crime Report*"[11], el cual es un reporte completo acerca del estado que guarda la ciberseguridad en Estados Unidos en cada uno de sus estados, por tipo de crimen y también frente a otros países, y elabora estadísticas que muestran cuáles son los países que conforman el Top 20 por número de víctimas. En los últimos 3 años, México ha ocupado los lugares 7, 8 y 9 según el año en dicho reporte, junto con Brasil el cual se disputa el lugar año con año, a continuación, mostramos las gráficas de 2020, 2021 y 2022 tomadas de ese reporte:

[10] FBI *Federal Bureau of Investigation*
[11] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf





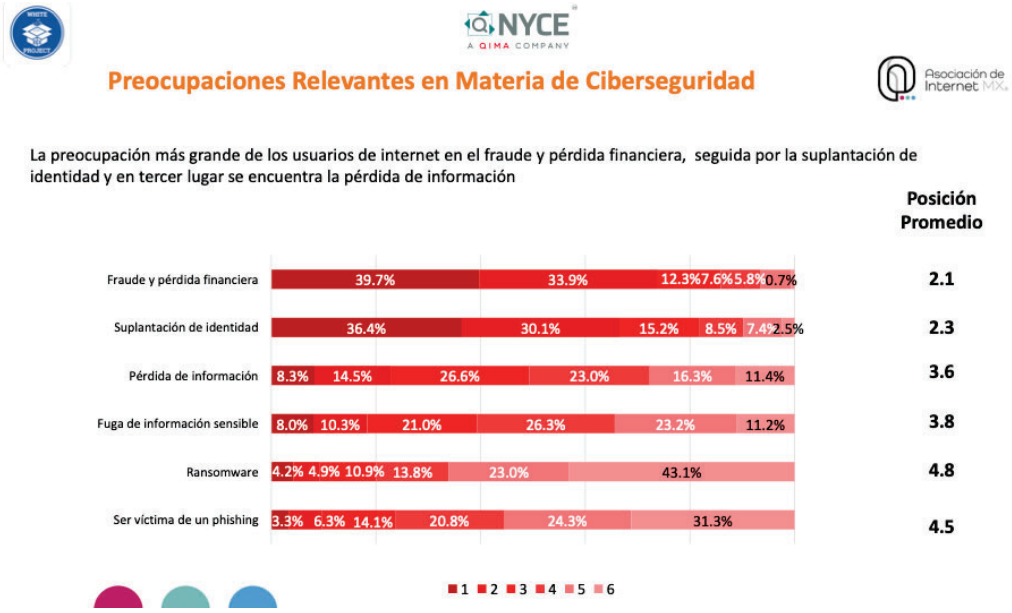
De igual manera, en la siguiente estadística elaborada por Surfshark[12] respecto al 2022, se muestra cómo México forma parte del Top 10 de países por densidad de víctimas del cibercrimen:



[12] https://surfshark.com/research/data-breach-impact/statistics

Respecto a las estadísticas en México, el último reporte de incidencia delictiva a nivel federal al mes julio de este 2023 publicado por el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, no muestra específicamente aquellos delitos que hayan sido cometidos a través de Internet o utilizando alguna otra tecnología[13].

Sin embargo, se cuenta con algunos estudios recientes elaborados por la Asociación de Internet MX, entre ellos: el "Estudio sobre ciberseguridad en empresas, personas usuarias de Internet y padres de familia en México"[14] cuya segunda edición contiene las siguientes tablas acerca de las preocupaciones relevantes en materia de ciberseguridad, el número de víctimas reportado por tipo de conducta y las experiencias negativas que se han presentado en menores de edad, entre otros aspectos importantes:

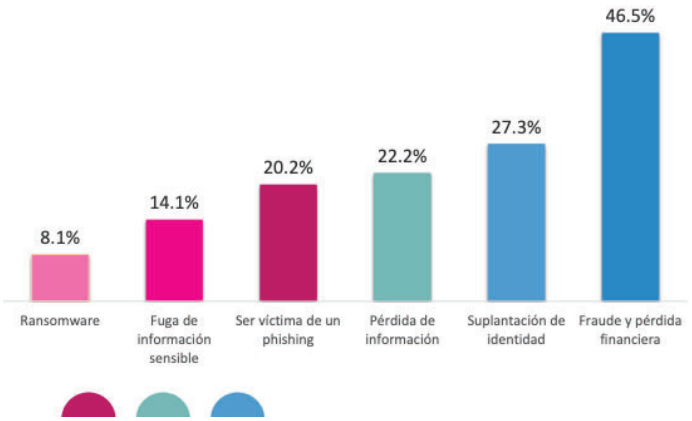


[13] https://drive.google.com/file/d/17tCln7WfBE4O3Ullv1q3AJYmvxehotC-/view
[14] https://irp.cdn-website.com/81280eda/files/uploaded/Encuesta Ciberseguridad 2022 pública 20230119.pdf

Victimas de Alguna Vulneración

Delincuentes han migrado al mundo digital para cometer delitos

- **22.1% de los usuarios han sido víctimas de alguna vulneración en los últimos 12 meses**



Afectaciones reportadas por parte de los usuarios:

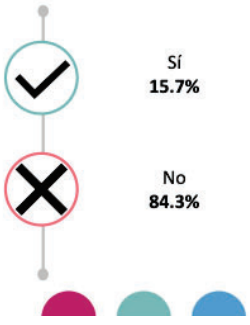
- Principalmente de pérdida de información, fraudes y pérdidas financieras
- 1 de cada 3 víctimas ha sufrido de suplantación de identidad, lo cual puede derivar en otro tipo de problemas legales

Experiencias Negativas con terceros a través de internet por parte de sus hijas o hijos

Baja proporción de menores que perciben haber tenido experiencias negativas mediante internet **(15.7%)**

- Aproximadamente, **7 de cada 10** hijos reportan acoso por parte de otros menores de edad
- Las Redes sociales y los servicios de mensajería son los principales medios por los que se han visto afectados

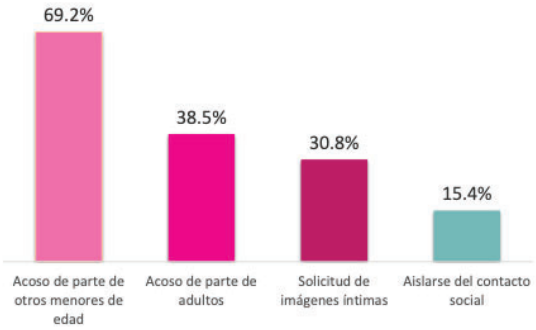
¿Sus hijas o hijos han tenido experiencias negativas con terceros a través de internet?



Sí **15.7%**

No **84.3%**

Experiencias negativas han tenido sus hijas o hijos con terceros a través de internet



Los incidentes con terceros se han dado a través de:

Redes sociales **46.2%**

Servicios de mensajería **46.2%**

Videojuegos en línea **23.1%**

Asimismo, este mismo año se presentó el "Estado de las Políticas Públicas y Regulación sobre la Ciberseguridad para NNA en México. 2022". Ese reporte nos presenta estadísticas muy relevantes de incidencia en ese grupo poblacional[15].

Por lo anterior, podemos concluir en este rubro que el estado que guarda la ciberseguridad en nuestro país es preocupante y debe atenderse desde una perspectiva multifactorial, en lo particular, consideramos de relevancia la actuación del Instituto conforme a su normativa aplicable, en particular la Ley y los Lineamientos para la gestión de tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet.

2.2 INICIATIVAS IDENTIFICADAS

En este momento, tanto nivel federal como estatal se tienen identificadas alrededor de 24 iniciativas en los congresos locales y el federal.

Una de las principales razones por las que, a pesar de haber existido múltiples intentos en otras legislaturas y sexenios por contar con una normativa enfocada al cien por ciento en la materia, es el desconocimiento del funcionamiento de la tecnología, por ejemplo, la presentada en octubre del 2015 por el entonces Senador del PRI Omar Fayad[16], que prácticamente criminalizaba a la tecnología en sí misma al darles el carácter de "arma informática"; pero más aún, atentaba contra derechos fundamentales como la libertad de expresión al incorporar los tipos penales de terrorismo informático, la intimidación, divulgación indebida de información y una recopilación excesiva de información de los

[15] https://irp.cdn-website.com/81280eda/files/uploaded/Internet_Seguro_para_Tod_s_AIMX_octubre.2022.pdf
[16] Omar Fayad retira iniciativa contra ciberdelitos

usuarios. Evidentemente, al ser ampliamente criticada por los medios de comunicación, la industria y los propios usuarios, tuvo que retirar su iniciativa.

Llama la atención que el término Delito Cibernético o Ciberdelito, ya se encuentra definido en el documento de la Estrategia Nacional de Ciberseguridad, que no ha quedado sin efecto o ha sido modificado, entendiendo como éste a las *"Acciones 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."*

Entonces, la necesidad imperiosa de contar con una normativa enfocada a sancionar estas conductas, que ya se encuentran contempladas en diversos ordenamientos, hace plantearnos la verdadera necesidad de contar con una Ley Federal en la materia, y más importante aún, corroborar que se cuenten con las facultades precisas para un proyecto de norma con alcances tan amplios y dispersos.

III. CONSIDERACIONES GENERALES

De manera general consideramos que cualquier regulación que se genere o modifique el marco regulatorio existente debe ajustarse a ciertos criterios basados tanto en la Constitución Política de los Estados Unidos Mexicanos como en instrumentos internacionales de los que México es parte, así como en algunos ejemplos de derecho comparado. Por lo anterior, sería deseable:

1. Generar la normativa conforme al ámbito de competencias previsto en el artículo 73 Constitucional fracción XXI, cuidando que no se invadan competencias del fuero común, por lo que se estima

relevante que se orienten los trabajos hacia una Ley General y no una Ley Federal;

2. Que conforme al artículo 1 Constitucional párrafos segundo y tercero, se respeten, protejan y garanticen los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad favoreciendo en todo momento la protección más amplia;
3. Que su redacción no genere duplicación, antinomias o conflictos de aplicación normativa, al pretender incorporar materias especiales que ya se encuentran debidamente reguladas, tales como la protección de datos personales, la propiedad intelectual y las telecomunicaciones;
4. Que se delimite perfectamente el ámbito de facultades y competencias de las autoridades que pretendan crearse, respetando el ámbito de las existentes, con la finalidad de prevenir una futura controversia constitucional, hacer un uso eficiente de los recursos públicos, y
5. Que se garantice el respeto al derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal conforme a las obligaciones contraídas por el Gobierno de México en el Convenio 108 (Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal).

En particular nos inquieta la premura que se ha manifestado públicamente para que en el presente periodo de sesiones se dictamine y posteriormente vote en el pleno una Ley de Ciberseguridad, siendo que no se tiene un proyecto debidamente analizado y maduro.

En primer lugar consideramos que se debe definir si será una propuesta de Ley de carácter federal que contempla la incorporación de diversos tipos penales que no son facultad exclusiva del legislador federal o que incluso ya se encuentran tipificados en los ordenamientos locales, podrían generar un entorno óptimo para el planteamiento de controversias constitucionales, además esto se refuerza al invadir las esferas de competencia de los Órganos Constitucionales Autónomos como el IFT o el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI).

Estudiando las iniciativas que se encuentran en este momento analizándose, no queda claro si en realidad se tratará de una Ley General o Federal.

En una de las iniciativas más socializadas, le son supletorias, entre otras, las leyes en materia de protección de datos personales y la Ley Federal de Telecomunicaciones y Radiodifusión, sin embargo, plantea cuestiones que invaden el ámbito de facultades constitucionales otorgadas al IFT, por ejemplo, en el TÍTULO CUARTO, PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES CAPÍTULO I.

Aunado a lo anterior, se menciona en la exposición de motivos que "*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.*"

Lo cual es impreciso, ya que las policías cibernéticas llevan operando más de diez años, incluso, el sexenio pasado se creó el Modelo Homologado de Unidades de Policía

Cibernética[17] para profesionalizar a todas las unidades del país y que trabajaran de forma estandarizada.

Asimismo, miembros de diversas organizaciones tales como la Cámara Internacional de Comercio, la propia Asociación de Internet MX y la CANIETI[18] que albergan a algunos de los sujetos regulados, han manifestado públicamente a través de un comunicado[19] el día 5 de septiembre, sus inquietudes respecto de esta iniciativa y de la urgencia con la que pretende aprobarse en este período de sesiones con base en la Agenda Legislativa del Partido MORENA[20].

A continuación, se presenta una tabla con observaciones precisas que consideramos importantes:

ARTÍCULO	CONTENIDO	OBSERVACIONES
Artículo 1 fracciones IX y X	Establecer las bases para sancionar conductas ilícitas en materia de Ciberseguridad; y	Estas conductas ya se encuentran tipificadas en diversos ordenamientos jurídicos estatales, lo cual además de ser redundante

[17] Modelo homologado de unidades de policía cibernética

[18] Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la información (CANIETI)

[19] https://newsreportmx.com/2023/09/05/la-pone-en-riesgo-derechos-humanos-e-incumple-obligaciones-internacionales-en-la-materia/

[20] https://infosen.senado.gob.mx/sgsp/gaceta/65/2/2023-02-09-1/assets/documentos/Angenda_Legislativa_MORENA_2do_Ano_de_Ejercicio.pdf

	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	generaría un conflicto competencial nocivo para los sujetos pasivos y para el Estado de Derecho.
Artículo 3	Glosario o definiciones de la Ley	Remitir a las leyes que han previamente definido estos conceptos o bien, a estándares internacionales evitaría generar confusión en la aplicación de la norma.
CAPÍTULO I DE LA COMISIÓN INTERSECRETARIAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, Y DE LA SEGURIDAD	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	Si bien está previsto invitar a representantes de los Órganos Constitucionales Autónomos, el Instituto Federal de Telecomunicaciones debería incorporarse por Ley como invitado permanente; ya que, por sus atribuciones su

DE LA INFORMACIÓN	equivalentes de otras entidades de la Administración Pública Federal; II. Representantes de los órganos constitucionales autónomos;	participación es fundamental en las tareas encomendadas a esta CITICSI.
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: XIX. Integrar y mantener actualizado un Catálogo Nacional de Infraestructuras Críticas de Información; así como salvaguardar su confidencialidad, integridad y disponibilidad;	Hay una invasión de competencias del Instituto Federal de Telecomunicaciones y una duplicación de actividades. Lo anterior es contrario a la eficiencia para el uso de recursos públicos y tiene otras desventajas operativas; por ejemplo, no establece reglas claras para la baja inmediata de proveedores de servicio o administradores, de direcciones IP, aplicaciones, dominios y sitios de internet.

	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; 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	Esto derivaría también en potenciales actos de autoridad inconstitucionales, así como en posibles conflictos competenciales.
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:	De estas disposiciones también se vislumbran posibles conflictos competenciales.

	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; VII. Acciones para la prevención de riesgos, amenazas y vulnerabilidades de los sistemas informáticos, digitales y de las telecomunicaciones tanto públicas como privadas; 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.	
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;	En general, todo el capítulo I y el II de este Título Cuarto parecen innecesarios toda vez que son derechos previamente reconocidos en la Constitución y regulados en las normas en la materia, por lo que no habría lugar a incorporarlos en esta normativa, además de que, en algunos puntos invade facultades exclusivas del IFT y el INAI.

	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.	
TÍTULO QUINTO DE LA PRESTACIÓN DE SERVICIOS, USO DE INFRAESTRUCTURA DIGITAL Y	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	Varias de las obligaciones que se imponen en los términos de este título a los prestadores de servicios de telecomunicaciones pueden considerarse excesivas y van más allá de lo dispuesto

TELECOMUNICACIONES	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;	en la Ley que regula su actividad; es decir, la LFTR e incluso parecieran desconocer las obligaciones y marco legal para la colaboración con la justicia prevista en el Título Octavo de la LFTR.

	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.	
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	Además de ser poco claros los tipos penales, lo cual haría impugnable su aplicación y sanción, se invaden las facultades del IFT.

	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	

IV. RECOMENDACIÓN

Por lo anteriormente expuesto, este Consejo Consultivo recomienda que el Instituto participe de forma proactiva buscando que la redacción final de la norma que se desarrolle en pro de la ciberseguridad:

(i) no invada competencias que le corresponden en exclusiva y como garante de los derechos de los usuarios en términos del artículo 6 Constitucional Apartado B, fracción V; y los artículos 7 y 145 fracción III de la Ley Federal de Telecomunicaciones y Radiodifusión;

(ii) considere la participación del Instituto en el ámbito de su competencia para contribuir a la ciberseguridad en el país con sus capacidades regulatorias, humanas y técnicas, así como para coadyuvar y promover la ciberseguridad en el país;

(iii) promueva la coordinación de las autoridades a nivel nacional e internacional;

(iv) no duplique las obligaciones en materia de colaboración con la justicia que prevé la Ley Federal de Telecomunicaciones y Radiodifusión en su Título Octavo, y

(v) considere la importancia de tener presente el desarrollo tecnológico y la innovación por una parte para garantizar que sus disposiciones sean generales y abstractas y por otra para que las medidas que se adopten no sean excesivas y generen obstáculos a la innovación.

Lilia Eurídice Palma Salas

Presidenta del VII Consejo Consultivo

Mtra. Rebeca Escobar Briones

Secretaria del Consejo Consultivo

La Recomendación fue aprobada por el VII Consejo Consultivo del Instituto Federal de Telecomunicaciones por unanimidad de votos de los consejeros: Alejandro Ildefonso Castañeda Sabido, Sara Gabriela Castellanos Pascacio, Ernesto M. Flores-Roux, Mario Germán Fromow Rangel, Gerardo Francisco González Abarca, Misha Leonel Granados Fernández[21], Erik Huesca Morales, Salma Leticia Jalife Villalón, Luis Miguel Martínez Cervantes, Lucía Ojeda Cárdenas, Eurídice Palma Salas y Cynthia Gabriela Solís Arredondo. Lo anterior, en la I Sesión Extraordinaria celebrada el 21 de septiembre de 2023, mediante Acuerdo CC/VII/IFT/210923/28, en términos del artículo 17 último párrafo de las Reglas de Operación del Consejo Consultivo del Instituto Federal de Telecomunicaciones.

La Recomendación fue desarrollada por la consejera Cynthia Gabriela Solís Arredondo, con la contribución de los consejeros Sara Gabriela Castellanos Pascacio, Eurídice Palma Salas y Luis Miguel Martínez Cervantes.

[21] El consejero Misha Leonel Granados Fernández emitió su voto favorable vía correo electrónico el 4 de octubre de 2023.

ANEXO

Se resaltan los elementos que pueden significar un riesgo sustancial para los derechos humanos en relación con las limitaciones, restricciones o medidas de control que se tendrían que implementar a las telecomunicaciones.

INICIATIVA	CONTENIDO	FECHA
INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD La suscrita Juanita Guerra Mena Diputada Federal integrante del Grupo Parlamentario de MORENA en la LXV Legislatura	LEY GENERAL DE CIBERSEGURIDAD TÍTULO PRIMERO DISPOSICIONES GENERALES Capítulo Único Disposiciones Generales Artículo 4. Para garantizar la protección de los derechos humanos de los cibernautas, las autoridades deberán atender los siguientes principios: … … V. La vigilancia e intervención de comunicaciones privadas deben estar fundadas en la legislación aplicable, atendiendo a los principios de necesidad y proporcionalidad, utilizando mecanismos de control, transparencia y rendición de cuentas; VI. Deberán promover el mejoramiento y adopción del cifrado como medida para mitigar riesgos y fortalecer la Ciberseguridad;	03-10-22

	X. Las políticas de Ciberseguridad deben sustentarse en la disponibilidad continua de la conectividad, y XI. La regulación de la vigilancia y monitoreo de la red y de la investigación y persecución de los ciberdelitos, se hará con absoluto respeto a los derechos humanos y garantías individuales. Artículo 5. Para los efectos de la presente Ley, se entiende por: … VII. Ciberespacio.- Es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico; XIX. Hiperconectividad.- Conexión a los sistemas de información a través de diferentes dispositivos; XX. Internet.- Conjunto de redes de telecomunicaciones que a través de la red pública de telecomunicaciones ofertan servicios y comunicaciones digitales;	

	XXVII. TIC.- Tecnologías de Información y Comunicaciones, que comprende los equipos de cómputo, programas de computación, servicios y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video; XXVIII. Virtual.- Todo lo que tiene lugar en los medios digitales,… TÍTULO SEGUNDO DE LOS ÁMBITOS DE COMPETENCIA EN CIBERSEGURIDAD Capítulo I Distribución de competencias Artículo 7. Las autoridades en materia de Ciberseguridad son: V. Las demás que con ese carácter determinen la presente Ley y otras disposiciones legales aplicables. Artículo 10. Son auxiliares en materia de Ciberseguridad, cuando sean requeridos por algunas de las autoridades en el cumplimiento de sus atribuciones, los siguientes:	

	V. Las demás que dispongan los ordenamientos legales aplicables, cuando su colaboración resulte necesaria para el cumplimiento de los fines de esta Ley. Sección Primera De la Dirección General de Investigación Cibernética y Operaciones Tecnológicas Artículo 16. Son atribuciones de la Dirección General de Investigación Cibernética y Operaciones Tecnológicas, en materia de Ciberseguridad: II. Monitorear la red pública de Internet con el fin de prevenir conductas delictivas; III. Coordinar y autorizar los métodos de análisis y monitoreo en medios electrónicos u otras plataformas tecnológicas que pudieran ser utilizadas para cometer un hecho probablemente constitutivo de delito; X. Solicitar la baja de información, sitios o páginas electrónicas que representen un riesgo, amenaza o peligro para la seguridad ciudadana, conforme a las disposiciones aplicables;	

	XXIII. Desarrollar mecanismos para la instalación de equipo tecnológico para vigilancias en puntos fijos y móviles;	
INICIATIVA DE LA SENADORA JESÚS LUCÍA TRASVIÑA WALDENRATH, CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD Y SE DEROGAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL	LEY GENERAL DE CIBERSEGURIDAD LIBRO PRIMERO TÍTULO PRIMERO CAPÍTULO I Disposiciones Preliminares Artículo 1.- La presente Ley es reglamentaria de los artículos 6 y 21 de la Constitución Política de los Estados Unidos Mexicanos en materia de Ciberseguridad y tiene por objeto regular la integración, organización y funcionamiento de la Comisión Nacional de Ciberseguridad y de la Agencia Nacional de Ciberseguridad, así como establecer la distribución de competencias y las bases de coordinación entre la Federación, las Entidades Federativas y los Municipios, en esta materia. XXI. Delitos cibernéticos o ciberdelitos: Acciones 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. XXII. Dispositivo: Aparato, artificio, mecanismo, artefacto, órgano, periférico, gadget, producto,	23 de marzo de 2021

	elemento de un sistema o componente electrónico. Dispositivo de Acceso: Es toda tarjeta, placa, código, número, u otros medios o formas de acceso, a un sistema o parte de éste, que puedan ser usados independientemente o en conjunto con otros dispositivos, para lograr acceso a un sistema de información o a cualquiera de sus componentes. XXIV. Dominio: Espacio de aplicabilidad intangible que define el campo de acción del ciberdelito. XXV. Nombre de dominio: Es un nombre fácil de recordar asociado a una dirección física de internet. XXVI. Emisiones Electromagnéticas: Combinación de campos eléctricos y magnéticos oscilantes, que no necesitan un canal o medio para su propagación de un lugar a otro. XXVII. Entorno Digital: Conjunto de canales, plataformas y herramientas que disponen cualquier individuo, marcas o negocios para tener presencia en Internet. Internet: Conjunto de redes de telecomunicaciones que a través de la red pública de telecomunicaciones ofertan servicios y comunicaciones digitales	

	XLIV. Proveedor de Servicios de Internet: Es la empresa que proporciona una conexión de acceso a Internet a sus clientes (ISP), que incluye tránsito y registro de nombres de dominio. XLV. Proveedor de contenidos en Internet: Persona física o moral que brinda servicios, aplicaciones, almacenamiento, infraestructura y soporte técnico de diversos productos basados en Internet, entre otros, bajo las políticas de privacidad y condiciones que él mismo establece. XLVI. Radiofrecuencia: También denominado espectro de radiofrecuencia, es la distribución energética del conjunto de las ondas electromagnéticas, es decir, la radiación electromagnética que emite una antena de radiocomunicación. XLVIII. Red Pública de Internet: Es un tipo de red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. XLIX. Red Social: Comunidad virtual que permite la interacción entre personas u organizaciones que se conectan a partir de intereses o valores comunes, basados en la estructura de conocido ha conocido.	

	LX. Sistema de Telecomunicaciones: Conjunto de dispositivos relacionados, conectados o no, cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales, señales electromagnéticas, signos, escritos, imágenes fijas o en movimiento, video, voz, sonidos, datos o informaciones de cualquier naturaleza, por medio óptico, celular, radioeléctrico, electromagnético o cualquiera otra plataforma útil a tales fines. Este concepto incluye servicios de telefonía fija y móvil, servicios de valor agregado, televisión por cable, servicios espaciales, servicios satelitales y otros. LXIII. Sistema Telemático: Sistema que combina los sistemas de telecomunicaciones e informáticos como método para transmitir la información. LXIV. Tecnologías de la Información y Comunicación: Conjunto de herramientas, sistemas, programas, recursos, procedimientos que sirven para el almacenamiento y facilitar la emisión, acceso y tratamiento de la información mediante códigos variados que pueden corresponder a textos, imágenes, videos, sonidos, entre otros.	

	LXIX. Wi Fi: Es una red de dispositivos inalámbricos interconectados entre sí y generalmente conectados a Internet a través de un punto de acceso inalámbrico. Se trata de una red LAN que no utiliza un cable físico para el envío de la información. Tecnología de interconexión de dispositivos electrónicos de forma inalámbrica, que funciona en base al estándar 802.11, que regula las transmisiones inalámbricas. Capítulo IV De los delitos a la propiedad intelectual Artículo 39.- Cuando las conductas descritas en la Ley Federal de Derechos de Autor y en la Ley de Propiedad Industrial, vigentes al momento de los hechos, 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 (UMA), 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. Capítulo V De los delitos contra la Nación	

	Artículo 40.- Serán considerados también delitos contra la Nación, los actos que se realicen a través de un sistema informático, electrónico, telemático o de telecomunicaciones, que atenten contra los intereses fundamentales y de Seguridad de la Nación, tales como los siguientes: Capítulo VII Disposiciones comunes a los delitos en materia de las tecnologías de la Información y comunicación, que afectan redes de sistemas informáticos, electrónicos o telemáticos. Artículo 52.- Las Policías, la Guardia Nacional y el Ministerio Público, en apego a lo establecido en el Código Nacional de Procedimientos Penales, podrán solicitar sin intervención de la autoridad judicial: I. La cooperación con empresas proveedoras de servicios de Internet, y de servicios en la Red Pública de Internet nacionales e internacionales, para neutralizar sitios, páginas electrónicas y perfiles de redes sociales, siempre y cuando no se afecte la libertad de expresión, en los siguientes casos: a) Inciten al terrorismo realicen la apología del odio nacional, racial, sexual o religioso;	

	b) Que constituya incitación a la discriminación, la hostilidad o la violencia; c) La instigación directa y pública a cometer genocidio y pornografía infantil; d) Suplantación de identidad para fraude, y robo de datos personales; e) Dañe la imagen pública y la reputación de una persona o Institución; II. La preservación de la información, a los proveedores de servicios y contenidos en Internet, nacionales e internacionales. III. En los hechos relacionados con el presente Título, y de conformidad con las políticas de privacidad de los proveedores de servicios y contenidos en Internet y cualquier otra entidad que contenga en su infraestructura indicios de hechos delictivos que pongan en riesgo las libertades, derechos humanos y otras garantías, la información correspondiente por los mecanismos establecidos por dichas personas físicas o morales. En los casos de que los indicios se refieran a datos de contenido o datos personales deberá de solicitarse por control judicial y en caso de que se encuentren fuera del país también se deberá	

	recurrir a los Tratados de Asistencia Jurídica Mutua o de Carta Rogatoria, según corresponda en términos de las disposiciones de Derecho Internacional. De igual forma se podrá solicitar la colaboración de los proveedores de servicios de Internet en términos de lo dispuesto en la Ley Federal de Telecomunicaciones y Radiodifusión y sus Lineamientos de Colaboración en Materia de Seguridad y Justicia. Así mismo, dichas peticiones podrán ser realizadas por las policías, la Guardia Nacional y el Ministerio Público en casos de urgencia, de conformidad a lo establecido en el Código Nacional de Procedimientos Penales. Solicitar a una persona física o moral preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos. Artículo 53.- El Ministerio Público atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de	

	agentes encubiertos a efectos 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, de conformidad con lo establecido en los ordenamientos jurídicos aplicables.	
Senadora Alejandra Lagunes Soto Ruiz INICIATIVA CON PROYECTO DE DECRETO PARA REFORMAR Y ADICIONAR DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL EN MATERIA DE CIBERSEGURIDAD	Artículo 168 Bis.- Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho: I. Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas, o II. Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas. III. Produzca, transmita la propiedad, obtenga para su utilización o usufructo, importación, difusión u otra forma de puesta a disposición de: a) Dispositivos, incluidos programas informáticos diseñados o adoptados principalmente para la intervención de comunicaciones privadas, geolocalización o la interceptación de datos de navegación en internet sin consentimiento;	Abril 2019

	b) Contraseñas, códigos de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático. IV. Produzca, transmita la propiedad, obtenga para su utilización o usufructo, importación, difusión u otra forma de puesta a disposición de dispositivos, programas de computación especializados en señales, redes y aplicativos de cualquier aparato portátil o casero que atenten contra la privacidad. V. Posea alguno de los elementos contemplados en la fracción anterior, con la intención de ser utilizados para cometer ilícitos relacionados con la violación de confidencialidad, integridad, privacidad y disponibilidad de la información y sistemas informáticos. Artículo 177.- A quien intervenga comunicaciones privadas o los datos de tráfico de las telecomunicaciones realizadas por cualquier vía telefónica, medios digitales o cualquier medio de comunicación de orden público, sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa. La pena prevista en este artículo se duplicará para el caso de servidores públicos que en	

	ejercicio de sus funciones o aprovechando el cargo, ordene, permita, autorice o realice las conductas señaladas en este artículo, además de la privación del cargo o inhabilitación para ocupar otro hasta por cinco años. Artículo 211 Bis 7.- A quien intercepte, por cualquier medio o método, información o datos informáticos en transmisiones dirigidas a un sistema o equipo informático físico o digital, originadas desde otro sistema o equipo o realizadas dentro del mismo, incluidas las emisiones electromagnéticas y radiofrecuencias provenientes de un sistema o equipo informático que transporten dicha información o datos informáticos, se le impondrá de seis meses a cuatro años de prisión y de cien a seiscientos días multa.	
Miguel Ángel Mancera Espinosa INICIATIVA CON AVAL DEL GRUPO PARLAMENTARIO QUE CONTIENE PROYECTO DE DECRETO POR EL QUE SE MODIFICA LA	Artículo 22 Bis. El Centro Nacional de Ciberseguridad tendrá, entre otras, las siguientes atribuciones: V. Coordinarse con el Instituto Federal de Telecomunicaciones para determinar la política en la materia de Ciberseguridad.	1 de septiembre 2020

DENOMINACIÓN DEL CAPÍTULO II, DEL TÍTULO NOVENO, DEL LIBRO SEGUNDO Y SE REFORMA EL ARTÍCULO 211 BIS 1 Y SE DEROGAN DIVERSOS ARTÍCULOS DEL CÓDIGO PENAL FEDERAL; SE REFORMAN Y ADICIONAN DIVERSOS ARTÍCULOS DE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA; SE ADICIONA UNA FRACCIÓN XIV AL ARTÍCULO 5° DE LA LEY DE SEGURIDAD NACIONAL; Y SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD	TERCERO.- Se adiciona una fracción XIV al artículo 5° de la Ley de Seguridad Nacional para quedar como sigue: Artículo 5.- ... I a la XIII. ... XIV. Actos tendentes a amenazar, afectar, inhabilitar o destruir la infraestructura activa o pasiva de telecomunicaciones que sean indispensable para la provisión de bienes o servicios públicos o para el adecuado funcionamiento de las instituciones del Estado. Artículo 3.- La presente ley tiene por objeto: I. Establecer los tipos penales en la materia e integrar la forma y los términos en que las autoridades de las entidades federativas y los municipios colaborarán con la Federación en dicha tarea, con el fin de garantizar el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de telecomunicaciones, incluido el de banda ancha e internet en forma segura;	

	Artículo 8.- El Centro Nacional se coordinará con el Instituto Federal de Telecomunicaciones, para determinar la política en la materia de Ciberseguridad. TÍTULO V DE LAS AMENAZAS A LA CIBERSEGURIDAD Y LA SEGURIDAD DE LA INFORMACIÓN EN LA RED Artículo 25.- El Centro Nacional deberá publicar e informar al Secretario Ejecutivo del Sistema Nacional de Seguridad Pública de manera continua un reporte de amenazas a la ciberseguridad para la población en general y generar un informe anual sobre el estado que guarda la ciberseguridad, con el fin de que las personas conozcan los mayores riesgos a los que están expuestos por el uso de sistemas de telecomunicación, información y comunicación. Artículo 26.- El Centro Nacional deberá informar a las autoridades de las ciberamenazas que enfrentan en el desempeño de sus funciones, así como establecer los lineamientos de capacitación de las y los servidores públicos en la materia. Artículo 27.- Los operadores de red deberán de implementar sistemas de protección para garantizar la confidencialidad de la información de las personas usuarias.	

	Artículo 28.- Los operadores de red adoptarán las acciones necesarias para garantizar al máximo la seguridad de la información personal que recopilan y para evitar que la información personal se divulgue, destruya o se pierda. Artículo 29.- Todas las personas y empresas serán responsables del uso de sus sitios web y por ningún motivo deberán establecer sitios de internet o grupos de comunicación para realizar actividades ilícitas, difundir o perpetrar fraudes, impartir métodos criminales, elaborar o comercializar artículos prohibidos o controlados, u otras actividades ilegales. Artículo 30.- Los operadores de red gestionarán la información publicada por las personas usuarias y, al descubrir que está prohibida la publicación o transmisión, deberán detener inmediatamente la transmisión de esa información, evitar la difusión de la información, guardar registros e informar de forma inmediata a las autoridades competentes.	
Cristóbal Arias Solís INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN LOS ARTÍCULOS 6 Y 73 DE	DECRETO POR EL QUE SE REFORMAN LOS ARTÍCULOS 6 Y 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS ÚNICO. Se reforma el artículo 6, tercer párrafo, y fracciones I y II del Apartado B; y se adiciona la fracción XXIII Ter al artículo 73 de la Constitución	04 de noviembre de 2022

LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS EN MATERIA DE SEGURIDAD CIBERNÉTICA	Política de los Estados Unidos Mexicanos, para quedar como sigue: Artículo 6. ... El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios. La Ley establecerá los mecanismos de cooperación y coordinación institucional para prevenir y combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos, así como garantizar la protección, seguridad y desarrollo del ecosistema digital y la prevención de riesgos o amenazas en el entorno digital o ciberespacio. A) ... B. En materia de radiodifusión y telecomunicaciones: I. El Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales, de alfabetización digital y el establecimiento de la Estrategia Nacional Digital y de Ciberseguridad	

	con perspectiva de derechos humanos y enfoque basado en prevención y gestión de riesgos, así como de eficiencia en los procesos digitales, combate a la corrupción, seguridad en la información y soberanía tecnológica. II. Las telecomunicaciones son servicios públicos de interés general, por lo que el Estado garantizará que sean prestados en condiciones de competencia, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre, seguridad y sin riesgos o amenazas e injerencias arbitrarias. III. a VI. ... Artículo 73. ... I. a XXIII BIS. ... XXIII Ter. Para expedir leyes que, con respeto a los derechos humanos, establezcan los principios y las bases sobre las cuales la Federación, las entidades federativas y los Municipios en el ámbito de sus respectivas competencias coordinarán sus acciones para prevenir y combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos, de conformidad con lo establecido en el artículo 6 de esta Constitución. XXIV a XXXI. ...	

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMA LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA EN MA TERIA DE SEGURIDAD CIBERNÉTICA	DECRETO POR EL QUE SE REFORMA LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA ÚNICO. Se reforma el artículo 17 de la Ley General del Sistema Nacional de Seguridad Pública y, se adiciona el artículo 20 Bis a dicho ordenamiento, para quedar como sigue: Artículo 17. El Secretariado Ejecutivo es el órgano operativo del Sistema y gozará de autonomía técnica, de gestión y presupuestal. Contara con los Centros Nacionales de Información, de Prevención del Delito y Participación Ciudadana, de Seguridad Cibernética, así como de Certificación y Acreditación. El Titular del Ejecutivo Federal expedirá el Reglamento del Secretariado, que establecerá las atribuciones y articulación de estos Centros. Artículo 20 Bis. El Centro Nacional de Seguridad Cibernética tendrá, como principales atribuciones: l. Proponer al Consejo Nacional lineamientos y políticas transversales de prevención del Cibercrimen, con perspectiva de derechos humanos y enfoque basado en gestión de riesgos, a fin de preservar un entorno digital seguro y	

	resiliente, cuyas acciones tendrán el carácter de permanentes y estratégicas; 11. Promover el uso adecuado de las Tecnologías de la Información y Comunicaciones, a través de una cultura de información y concientización sobre el uso adecuado de las herramientas tecnológicas que se encuentran al alcance de la ciudadanía y los riesgos en el uso de la red de Internet; en general, promover una cultura del autocuidado, civismo y alfabetización digitales. III. Emitir opiniones y recomendaciones, dar seguimiento y evaluar los programas implementados por las Instituciones de Seguridad Pública, en los tres órdenes de gobierno para: a) Prevenir el cibercrimen y los delitos en el espacio digital. b) Promover el uso adecuado de las Tecnologías de la Información y Comunicaciones.	

FIRMADO POR: LILIA EURIDICE PALMA SALAS
FECHA FIRMA: 2023/10/17 6:26 PM
AC: AUTORIDAD CERTIFICADORA
ID: 73011
HASH:
AB44E86C0E6B647B7DA1316B6DB4915F45B76A8BA92255
CDE24C0267A4F0AD74

FIRMADO POR: REBECA ESCOBAR BRIONES
FECHA FIRMA: 2023/10/17 7:09 PM
AC: AUTORIDAD CERTIFICADORA
ID: 73011
HASH:
AB44E86C0E6B647B7DA1316B6DB4915F45B76A8BA92255
CDE24C0267A4F0AD74

OPINIÓN QUE EMITE EL VII CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES SOBRE EL DESPLIEGUE SOSTENIBLE DE LAS TELECOMUNICACIONES Y LA RADIODIFUSIÓN PARA LA EXPLORACIÓN DE GUÍAS DE REGULACIÓN DEL SECTOR DESDE LA PERSPECTIVA DEL IMPACTO AL AMBIENTE, LA SOCIEDAD Y LOS ASPECTOS TÉCNICOS

INTRODUCCIÓN

En los últimos años, el enfoque de sostenibilidad[1] del sector se ha dirigido al aspecto económico y de mercado, y en esos aspectos tienen mayor énfasis las dos recomendaciones anteriores que ha emitido este Consejo Consultivo del Instituto Federal de Telecomunicaciones (CC-IFT). El campo de análisis es muy amplio como para agotarlo en un solo periodo del Consejo Consultivo, por ello esta opinión tiene como propósito delinear algunos elementos a considerar en la política regulatoria e indicadores en el sector telecomunicaciones y radiodifusión desde la perspectiva del impacto al ambiente, la sociedad y los aspectos técnicos.

I. ANTECEDENTES

El CC-IFT ha abordado la temática de la sostenibilidad en dos consejos previos, el V Consejo Consultivo abordó la sostenibilidad en el sector con la *Recomendación que emite el Consejo Consultivo del Instituto Federal de Telecomunicaciones sobre el estudio de la sustentabilidad del sector telecomunicaciones y radiodifusión y su aprovechamiento para la mejora regulatoria* ("Recomendación sobre el estudio de la sustentabilidad del sector del V CC-

[1] Objetivos de Desarrollo Sostenible de acuerdo con la ONU. Disponibles en: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

IFT"). En dicha recomendación se refiere que en una reunión efectuada con expertos se concluyó que el término "sustentabilidad" es más amplio que el de "sostenibilidad" que al parecer se limita a una dimensión económica. Igualmente, la recomendación refiere que "la sustentabilidad requiere un enfoque integral de sistemas para una efectiva toma de decisiones".[2] Sin caer en controversias, nos referimos en esta opinión a sostenible en relación con el desarrollo y en su acepción en ecología y economía, "es decir que se puede mantener durante largo tiempo sin agotar los recursos o causar grave daño al medio ambiente".[3] A su vez, el VI Consejo Consultivo elaboró la *Recomendación que emite el Consejo Consultivo del Instituto Federal de* Telecomunicaciones *sobre acciones de impacto positivo a la transformación digital en un entorno sustentable*.[4]

II. ALCANCE

Sin embargo, la sostenibilidad tiene otros dos aspectos, el ambiental y el social que se han dejado de forma lateral. El desarrollo sostenible es un concepto que se refiere al desarrollo que satisface las necesidades del presente sin comprometer la capacidad de las generaciones futuras para satisfacer sus propias necesidades; lo cual es consistente con las responsabilidades de la generaciones actuales con las futuras, que a su vez han sido mencionadas en distintos instrumentos internacionales y que se desarrollan con mayor detalle en la Declaración sobre las Responsabilidades de las Generaciones Actuales para con las Generaciones Futuras de 1997.[5]

---

[2] La recomendación se encuentra disponible en https://consejoconsultivo.ift.org.mx/docs/recomendaciones/2021/recomendacion_que_emite_el_cc_del_ift_sobre_el_estudio_de_la_sustentabilidad_del_sector_telecomunicaciones_y_radiodifusio%CC%81n_para_mejora_regulatoria.pdf

[3] Diccionario de la Real Academia de la Lengua Española, https://dle.rae.es/sostenible?m=form

[4] La recomendación se encuentra disponible en https://consejoconsultivo.ift.org.mx/docs/recomendaciones/2022/14__recomendacion_sobre_acciones_de_impacto_positivo_a_la_transformacion_digital_en_un_entorno_sustentable.pdf

[5] La Declaración establece la responsabilidad de garantizar la plena salvaguarda de las necesidades y los intereses de las generaciones presentes y futuras, respetando los derechos humanos, las libertades fundamentales, incluidas la libertad de elección de su sistema político, económico y social y preservar su diversidad cultural y religiosa, asegurar que se perpetúe la humanidad, respetando la dignidad de la persona humana, no atentar contra la naturaleza ni la vida humana, preservando el planeta, la utilización racional de

El desarrollo sostenible se basa en tres ejes: el ambiental, el social y el económico.

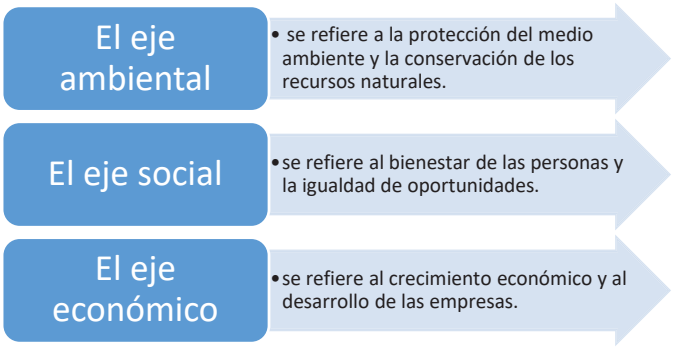


Figura 1. Componentes del desarrollo sostenible

1. EJE AMBIENTAL

Con respecto a lo ambiental, por parte de los fabricantes de equipos de telecomunicaciones y radiodifusión, la mira se ha desplazado hacia el consumo de energía y el propio impacto ambiental de las telecomunicaciones y radiodifusión en términos del despliegue de tecnologías que son altamente demandantes de energía eléctrica. Aunado al consumo existen otros problemas por resolver de forma adecuada como son: la obsolescencia tecnológica forzada[6], el uso de recursos escasos y el impacto ambiental de su explotación (p. ej. litio), el manejo de los desechos de equipos, especialmente cuando contienen componentes de alto riesgo ambiental y requieren de un proceso especial de desecho y la

los recursos naturales, preservando la calidad e integridad del medio ambiente, entre otros. El texto de la Declaración está disponible en: https://es.unesco.org/about-us/legal-affairs/declaracion-responsabilidades-generaciones-actuales-generaciones-futuras#:~:text=Las%20generaciones%20actuales%20deben%20esforzarse,forma%20de%20la%20vida%20humana.

[6] Este proceso de fabricantes de equipos de telecomunicaciones y radiodifusión incluyendo los equipos terminales de usuarios.

contaminación asociada de radiaciones no ionizantes[7] que contribuyen al consumo de energía y como consecuencia al calentamiento global.

El Acuerdo de París reconoce la importancia de reducir las emisiones del sector de las telecomunicaciones y la radiodifusión. El acuerdo establece el objetivo de reducir las emisiones de gases de efecto invernadero en un 45% para 2030, y en un 100% para 2050 (conocido como Net Zero).

En términos de comparación con otros sectores que tienen quema directa de combustibles fósiles, la operación de las telecomunicaciones y radiodifusión tienen un impacto en nuestro planeta aproximadamente del doble de la operación por un año de la aviación civil, siendo esta una industria catalogada en emisiones de alcance tipo 1[8]. Si bien las empresas de telecomunicaciones y radiodifusión generan pocas emisiones de las llamadas de alcance tipo 1, son consideradas grandes contribuyentes en emisiones de alcance tipo 2 y responsables del crecimiento exponencial del tipo 3. Pues es irremediable que para el 2030 existan más de 5,300 millones de equipos tipo IoT (Internet de los Objetos) que estarán conectados a redes celulares en donde China contribuirá con un tercio del consumo de energía debido al uso de estos equipos, a pesar de que busquen fuentes alternativas de energía.

[7] En los documentos del VI CC-IFT puede consultarse la *Recomendación que emite el Consejo Consultivo del Instituto Federal de Telecomunicaciones relativa a la información sobre los riesgos de las radiaciones no-ionizantes* disponible en https://consejoconsultivo.ift.org.mx/docs/recomendaciones/2022/11__recomendacion_relativa_a_la_informacion_sobre_los_riesgos_de_las_radiaciones_no_ionizantes.pdf

[8] Clases de emisiones de alcance:
- Tipo 1, aquellas generadas por la quema directa de combustibles fósiles.
- Tipo 2, resultan de la compra de energía para una empresa de telecomunicaciones.
- Tipo 3, son causadas por actividades comunes por el uso del servicio, como el consumo de energía de dispositivos de telecomunicaciones en los usuarios.

Se puede consultar en: https://es.weforum.org/agenda/2022/09/cual-es-la-diferencia-entre-las-emisiones-de-alcance-1-2-y-3-y-que-hacen-las-empresas-para-reducir-las-tres/ recuperado en sept 28, 2023

Por ello, los acuerdos de París de la Convención para el cambio climático de las Naciones Unidas de 2015[9] invitan al sector a que se tenga una reducción del 45% en las emisiones de CO_2 para el año 2025.

A pesar de estos desafíos, el sector de las telecomunicaciones y radiodifusión tiene por otra parte el potencial de contribuir a la sostenibilidad y también el de ser más sostenible.

Para reducir su impacto ambiental las empresas del sector pueden adoptar medidas como: utilizar energías renovables; mejorar la eficiencia energética; reciclar y reutilizar equipos; manejar los desechos tecnológicos de forma adecuada; pedir a los fabricantes de equipo que no introduzcan la obsolescencia tecnológica forzada y reducir el desperdicio de energía; además de hacer público e informar el gasto energético, al menos de forma mensual, y el probable impacto ambiental; instalar sus redes alámbricas de forma segura sobre todo en donde el territorio es sujeto a desastres naturales periódicos; también, la recolección de cables aéreos en desuso que hayan sido desplegados para sus servicios de última milla, tal como el acuerdo que ya firmó el Instituto Federal de Telecomunicaciones (IFT o Instituto) con el gobierno de la CDMX en agosto de 2023.[10]

Se puede lograr un esfuerzo adicional si, además, se consolida la compartición de infraestructura no solo para reducir espacios donde hay contaminación visual causada por antenas y radiobases, sino también para maximizar el uso de los canales de comunicación que de otra forma pudieran mantener periodos de baja o nula capacidad de tráfico prolongados.

[9] El Acuerdo de París es un tratado internacional jurídicamente vinculante sobre el cambio climático. Fue adoptado por 196 países en la Conferencia de las Partes de la Convención Marco de las Naciones Unidas sobre el Cambio Climático (COP21) en París el 12 de diciembre de 2015 y entró en vigor el 4 de noviembre de 2016.
[10] En exhorto del 14 de octubre de 2021 el Congreso de la Ciudad de México pide al Instituto Federal de Telecomunicaciones (IFT) que implemente una política con sus regulados para el retiro del cableado aéreo La supervisión del cumplimiento de la legislación.

2. EJE SOCIAL

En el aspecto social, de continuar las tendencias de consumo y hábitos de uso de la población, las demandas se incrementarán, el alto despliegue de redes 5G y 6G, IoT, Wi-Fi 6 y aplicaciones vinculadas al consumo de información[11] lo que crea importantes desafíos para la salud, la privacidad, la libertad, la información y la democracia. Estas tecnologías podrían utilizarse para hacer sostenible nuestra sociedad, o afectar su sostenibilidad y también, podrían ser usadas para incrementar las desigualdades existentes o fuera de los gobiernos establecidos; igualmente pueden ser empleadas para mejorar los aspectos de nuestras relaciones sociales y la democracia y la mejora en la calidad de vida de todos los mexicanos.

Es decir, al ser esenciales para las actividades y el desarrollo de las sociedades su uso conlleva una ambivalencia en el resultado de su aplicación y operación.

Por ello, en nuestra opinión, ante el advenimiento de cambios no previstos en nuestras relaciones con el medio ambiente y en el ámbito social, que generalmente se obvia en pos de mercados y regulación económica, estos dos sectores se encuentran en una zona gris para la regulación bajo el marco legal actual. Es en este punto que el IFT podría transformar su práctica y visión de regulador a través de la aplicación de un enfoque más integral y que considere la sostenibilidad con una visión más amplia, en la que se incorpore la sociedad y ambiente para las futuras generaciones.

3. ECONÓMICO

La pandemia de COVID-19 ha acelerado aún más la demanda de servicios de telecomunicaciones, ya que las personas han pasado más tiempo en línea para trabajar,

[11] La información multimedial para cualquier fin que los usuarios requieran.

estudiar, comunicarse y entretenerse. Como resultado, el sector de las telecomunicaciones se espera que continúe creciendo en los próximos años.

Sin embargo, el sector de las telecomunicaciones y radiodifusión también se enfrenta a una serie de oportunidades, como la competencia creciente, los altos costes de inversión y la participación en una regulación dinámica[12] en conjunto con el IFT, tal como se recomendó en el quinto Consejo Consultivo[13]. Estos retos pueden poner en riesgo la sostenibilidad económica del sector en los próximos años.

A pesar de los retos, el sector de las telecomunicaciones tiene el potencial de seguir creciendo y generando riqueza en los próximos años. Para que el sector sea sostenible, es importante que las empresas de telecomunicaciones adopten una serie de medidas, como:

- Invertir en nuevas tecnologías y servicios que satisfagan las necesidades cambiantes de los consumidores y las empresas;
- Introducir estrategias de bonos verdes o bonos de carbón;
- Reducir costos de operación;
- Mejorar la eficiencia y la productividad;
- Desarrollar nuevos modelos de negocio que sean más rentables, y
- Trabajar con los gobiernos para crear un entorno regulatorio favorable para el sector.

[11] Knieps, Günter (2011): Regulatory unbundling in telecommunications, Diskussionsbeiträge // Institut für Verkehrswissenschaft und Regionalpolitik, No. 137, http:// hdl.handle.net/10419/47437

[13] Recomendación que emite el Consejo Consultivo del Instituto Federal de telecomunicaciones (Instituto) sobre el estudio de la sustentabilidad del sector telecomunicaciones y radiodifusión y su aprovechamiento para la mejora regulatoria, disponible en https://consejoconsultivo.ift.org.mx/docs/recomendaciones/2021/recomendacion_que_emite_el_cc_del_ift_sobre_el_estudio_de_la_sustentabilidad_del_sector_telecomunicaciones_y_radiodifusio%CC%81n_para_mejora_regulatoria.pdf

III. OPINIÓN

Para avanzar en este proceso, el Consejo Consultivo considera que el Instituto puede abordar el análisis de los aspectos social y ambiental del sector telecomunicaciones para identificar en cuáles puede, desde el ámbito de su competencia, contribuir a la sostenibilidad, individualmente o en colaboración con otras autoridades, adoptando medidas y acciones de las cuales se enlistan algunos ejemplos a continuación:

1. Colaborar con otras instituciones que mantienen información respecto al cambio climático, con datos que le permita a la población conocer su huella de carbón como resultado del consumo de energía de sus dispositivos, desechos de equipos, servicios de telecomunicaciones, etcétera.[14] Así como colaborar en la elaboración y/o difusión de lineamientos y guías para el consumo de energía de dispositivos que se conecten a redes de telecomunicaciones que sean acordes con una política de reducción de consumo de energía para el 2050 tal y como lo plantea el Acuerdo de París, y promoverlos ante la Unión Internacional de Telecomunicaciones si lo considera conveniente Además de alentar con sus regulados la creación de indicadores de emisiones de gases efecto invernadero en el sector;

2. Emitir un reporte anual del consumo de energía de las redes de los operadores y crear un tablero de posicionamiento sobre cuáles redes consumen más energía, así como en cuáles se implementan medidas para sustitución por energías limpias. Se pueden crear indicadores que lleven a la creación de un "índice verde.";[15]

[14] Por ejemplo, ver el sitio México ante el cambio climático, accesible a través de la liga https://cambioclimatico.gob.mx/tag/inegi/ que mantiene el Instituto Nacional de Estadística y Geografía (INEGI). El INEGI y el Instituto Nacional de Ecología y Cambio Climático (INECC) también mantienen el Sistema de Indicadores sobre Cambio Climático (accesible a través de la liga http://gaia.inegi.org.mx/sicc/

[15] INEGI realiza cálculos de PIB ajustados para "deducir del Producto Interno Bruto (PIB) dos tipos de costos: el consumo de capital fijo y los costos imputados por los usos ambientales, estos últimos causados por el agotamiento de los recursos naturales y por la degradación ambiental, resulta el Producto Interno Neto Ajustado Ambientalmente". Estos cálculos incluyen todos los sectores económicos y se realizan cada cinco años, dado que no es un ejercicio sencillo (véase, Comunicado de Prensa. Cuentas Económicas y Ecológicas de México, 2018, disponible a través de la liga:

3. Colaborar con otros reguladores sectoriales en la creación de esquemas de incentivos para el desarrollo de:

a) Redes inteligentes de electricidad: las redes inteligentes utilizan las telecomunicaciones para gestionar la generación, distribución y consumo de electricidad de manera más eficiente, que ayudan a reducir las emisiones de gases de efecto invernadero y mejorar la eficiencia energética;

b) Agricultura de precisión: que utiliza las telecomunicaciones para optimizar el rendimiento de los cultivos y minimizar el uso de recursos como el agua y los fertilizantes. Contribuye a reducir el impacto ambiental de la agricultura;

c) Edificios inteligentes: utilizan las telecomunicaciones para optimizar el consumo de energía y reducir los residuos. Contribuyen a reducir las emisiones de gases de efecto invernadero y mejorar la eficiencia energética;

d) Vehículos eléctricos: utilizan las telecomunicaciones para optimizar la carga y descarga de las baterías, lo que ayuda a reducir las emisiones de gases de efecto invernadero y mejorar la eficiencia energética;

e) Industria 4.0 Además de mejorar la eficiencia las telecomunicaciones proveen un soporte para la recopilación de datos, potenciar la automatización, optimizar

https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2019/StmaCntaNal/CtasEcmcasEcolgicas2018.pdf)

el consumo energético, y apoyar en la creación de nuevos modelos de negocio, y

4. Crear incentivos en los usuarios para la demanda de productos de IoT verdes[16] que benefician a la población.[17]

Lilia Eurídice Palma Salas
Presidenta del VII Consejo Consultivo

Mtra. Rebeca Escobar Briones
Secretaria del Consejo Consultivo

La Opinión fue aprobada, en lo general, por el VII Consejo Consultivo del Instituto Federal de Telecomunicaciones por unanimidad de votos de los consejeros: Alejandro Ildefonso Castañeda Sabido, Sara Gabriela Castellanos Pascacio, Ernesto M. Flores-Roux, Mario Germán Fromow Rangel, Gerardo Francisco González Abarca, Misha Leonel Granados Fernández, Ali Bernard Haddou Ruiz, Erik Huesca Morales, Salma Leticia Jalife Villalón, Luis Miguel Martínez Cervantes, Jorge Fernando Negrete Pacheco, Lucía Ojeda Cárdenas, Edgar Olvera Jiménez, Eurídice Palma Salas y Cynthia Gabriela Solís Arredondo. Lo anterior, en la X Sesión Ordinaria celebrada el 28 de septiembre de 2023, y reiterada vía correo electrónico, mediante Acuerdo CC/VII/IFT/280923/33, en términos del artículo 17 último párrafo de las Reglas de Operación del CCIFT

El Grupo de Trabajo que desarrolló el proyecto de Opinión está integrado por su coordinador el consejero Erik Huesca Morales, con la participación de las consejeras Eurídice Palma Salas y Salma Leticia Jalife Villalón.

[16] IoT verde se define como: el IoT que se centra en la sostenibilidad y la reducción del impacto ambiental. El IoT verde se basa en la idea de que el IoT puede utilizarse para mejorar la eficiencia de los recursos y reducir las emisiones de gases de efecto invernadero.
[17] Tal como lo reporta Shava en su artículo The economic and environmental impacts of information and communication technology: A state-of-the-art review and prospects.

BIBLIOGRAFÍA ADICIONAL

1. Anders S. G. Andrae y Tomas Edler., Sobre el uso global de electricidad de la tecnología de la comunicación: tendencias para 2030. Huawei 2016
2. Ericsson (2022). 5G energy efficiency: A roadmap to 2030.
3. Vertiv (2022). 5G: The future of connectivity and sustainability.
4. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future in the age of the new machines. New York: Public Affairs.
5. Morozov, E. (2013). To save everything, click here: Technology, solutionism, and the urge to fix problems that don't exist. New York: Public Affairs.
6. Schneier, B. (2018). Data and Goliath: The hidden dangers of big data. New York: W.W. Norton & Company.
7. POST (2023). Energy consumption of the UK telecommunications sector. London: POST.
8. POST (2022). The energy transition in the UK telecommunications sector. London: POST.
9. POST (2021). The climate impact of the UK telecommunications sector. London: POST.
10. GSMA (2023). The mobile economy. 2023.
11. GSMA (2020). 5G energy efficiencies. Green is the new Black.
12. Heikkilä, *Melissa*. El último desafío de la IA: calcular su propia huella de carbono, MIT Technology Review, noviembre de 2022.
13. Friedrich, R., Hoffman, S., Lampe, T., Ullrich, S. (2021), Putting Sustainability at the Top of the Telco Agenda. Boston Consulting Group. Junio, 2021.
14. Xiaoyuan C., Yukun H., Varga, L (2022), 5G network deployment and the associated energy consumption in the UK: A complex systems' exploration, Technological Forecasting & Social Change, Elsevier.
15. Andreev, S., Petrov, V., Dohler, M., Yanikomeroglu, H., (2019). Future of Ultra-Dense Networks Beyond 5G: harnessing Heterogeneous Moving Cells. IEEE Commun. Mag. 57, 66–92
16. Schoenen,R., & Yanikomeroglu, H., (2014) User-in-the-loop: spatial and temporal demand shaping for sustainable wireless networks, *IEEE Communications Magazine*, vol. 52, pp. 196–203, February 2014.
17. IRENA, (2022). Tracking the transition to low-carbon ICT: The role of renewable energy.
18. IRENA, (2021). The energy transition in the ICT sector: A roadmap to 2050.
19. IRENA (2021). The digitalization of energy: Opportunities and challenges for the ICT sector.
20. Wang et al (2018). The environmental impact of ICT: A comprehensive review.

21. Zhang, X., & Wei, C. (2022). The economic and environmental impacts of information and communication technology: A state-of-the-art review and prospects. *Resources, Conservation and Recycling*, *185*, 106477.
22. Shava, H., (2022) The economic and environmental impacts of information and communication technology: A state-of-the-art review and prospects.
23. Freitag, C., (2020) The Climate impact of ICT: A review of estimates, trends and regulations December 2020.
24. Cunliff, C., (2022) Beyond the Energy Techlash: The Real Climate Impacts of Information Technology, ITIF.
25. Zhang, Y. G-Networks and the Performance of ICT with Renewable Energy. *SN COMPUT. SCI.* 1, 56 (2020).
26. Malmodin, J., & Lundén, D. The Energy and Carbon Footprint of the Global ICT and E&M Sectors 2010–2015. *Sustainability*, *10*(9), 3027.
27. Gergs, L., & Mavrakis, D., (2021) 5G Sustainability, ABIresearch / interdigital
28. Andrae, A, & Edler, T.,(2015) On Global Electricity Usage of Communication Technology: Trends to 2030, Challeges Basel, Switzerland

REPORTES DE ORGANISMOS

- *Ambiental:*

"The environmental impact of the information and communication technology (ICT) sector: A review of the evidence" (2015), International Telecommunication Union (ITU)

"The impact of ICT on the environment" (2017), United Nations Environment Programme (UNEP)

"ICT and sustainability: A roadmap for the future" (2018), World Economic Forum

- *Social:*

"ICT for development: A review of the evidence" (2016), World Bank

"The role of ICT in education" (2017), UNESCO

"The impact of ICT on health" (2018), World Health Organization (WHO)

- *Económico:*

"The economic impact of ICT" (2017), International Monetary Fund (IMF)

"The impact of ICT on employment" (2018), International Labour Organization (ILO)

"The impact of ICT on trade" (2019), World Trade Organization (WTO)

REPORTES DE REGULADORES

Ofcom: "5G: la próxima generación de tecnología móvil" (2020)

Ofcom: "Seguridad 5G: una guía para empresas" (2021)

FCC: "5G: El futuro de la tecnología inalámbrica" (2020)

FCC: Informe preliminar sobre los efectos en la salud de 5G" (2021)

IFT: "5G: Los desafíos y oportunidades de la próxima generación de tecnología móvil" (2020)

IFT: “Lineamientos para el despliegue de redes 5G" (2021**)**

FIRMADO POR: LILIA EURIDICE PALMA SALAS
FECHA FIRMA: 2023/10/16 1:36 PM
AC: AUTORIDAD CERTIFICADORA
ID: 72369
HASH:
FADCFDE648DD742FEB0C665468425C9ECC4FDA2DEB1239
7FABFB1AF20C237000

FIRMADO POR: REBECA ESCOBAR BRIONES
FECHA FIRMA: 2023/10/17 7:09 PM
AC: AUTORIDAD CERTIFICADORA
ID: 72369
HASH:
FADCFDE648DD742FEB0C665468425C9ECC4FDA2DEB1239
7FABFB1AF20C237000

OPINIÓN QUE EMITE EL VII CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES SOBRE LA EVOLUCIÓN DE LAS REDES PRIVADAS, RETOS LEGALES Y REGULATORIOS

INTRODUCCIÓN

Las nuevas tecnologías inalámbricas – en especial IMT/5G – han detonado la aparición de nuevas aplicaciones y usos que permiten cambios a los modelos de negocio de usuarios industriales y usuarios de misión crítica. La tecnología 5G es adecuada para aquellos usuarios que tienen necesidades de desempeño predecible y confiable. Sin embargo, por múltiples razones, las redes públicas pueden en ocasiones no satisfacer plenamente dichas necesidades; esto ha dado origen al surgimiento de redes privadas con esta tecnología en varias partes del mundo. Como estas redes necesariamente utilizan el espectro radioeléctrico, emanan una serie de desafíos regulatorios.

Este texto aborda algunos de estos desafíos, para así apoyar al Instituto Federal de Telecomunicaciones (IFT o Instituto) en su proceso de reflexión y deliberación sobre cómo proceder para promover, en un ambiente de sana competencia e innovación, el despliegue de redes privadas inalámbricas. Partimos de algunas generalidades sobre el concepto de redes privadas, describimos someramente dos casos internacionales relevantes para el caso mexicano, destacamos la problemática y algunos cuestionamientos fundamentales, y concluimos con algunas recomendaciones de alto nivel. Sabemos que el IFT ha estudiado detalladamente este tipo de redes y los desafíos que presentan, tanto en la Unidad de Espectro Radioeléctrico (UER) como en el seno del Comité 5G, ya que claramente es materia del Instituto, por lo que de manera breve tratamos de resaltar únicamente lo que a juicio de este Consejo Consultivo resulta más relevante.

I. ¿QUÉ SON LAS REDES PRIVADAS?

De manera muy general, una red privada de telecomunicaciones puede definirse como una red para la cual existen restricciones de entrada y salida de comunicación a otras redes. No es una definición asociada a la tecnología de la red, sino que está asociada al uso de la red. Los elementos que generalmente conforman una red pública y una red privada son prácticamente los mismos.

Existen muchas razones que sustentan la existencia de una red privada, siendo las principales la seguridad, el costo, la confiabilidad, la calidad, la instalación y uso de tecnología diferenciada (de punta o no disponible en la red pública) y la customización a un uso o cliente específico. Estas redes han existido desde antaño y han sido siempre desafiantes para la actividad regulatoria, al potencialmente reducir el tamaño de mercado servido por los proveedores tradicionales (que están asociadas a reservas de mercado), deteriorar la calidad del servicio telefónico[1], reducir el control gubernamental sobre el desarrollo del sector e incluso promover el incumplimiento de reglas o rodear imposiciones regulatorias (p.ej., el *by-pass* o las tarifas internacionales de liquidación).

Una red privada puede estar conformada por elementos de red propios o de terceros, los cuales muchas veces provienen de empresas que prestan el servicio público (p.ej., enlaces dedicados). Las redes pueden ser, entonces, físicas o virtuales (una VPN o *virtual private network*). En la práctica, estas redes tienden a ser una mezcla de elementos que interoperan correctamente para mejor alcanzar el objetivo deseado.

[1] Véase, por ejemplo, la argumentación de AT&T en el caso Hush-A-Phone Corp. v. United States (1956), la "Carterphone decision" de la FCC en 1968 e, incluso, el permitir la interconexión de la red de MCI como mandatado por la FCC en 1971.

II. REGULACIÓN ACTUAL DE LAS REDES PRIVADAS EN MÉXICO

Si una red privada no requiere de ningún elemento regulado, más allá de la homologación del equipo (y en ocasiones también excluyéndolo[2]), el papel del regulador es mínimo: ¿cuál sería, por ejemplo, el rol del regulador en la instalación de un sistema de interfón en un condominio o de un conmutador (PBX[3]) en una empresa, en especial si éste no está interconectado con la red pública de telecomunicaciones?

En una red que no utiliza recursos escasos, los argumentos en contra del despliegue de una red privada no se sustentan desde el punto de vista de competencia y estructura de mercado. Sin embargo, cuando es necesaria la utilización de recursos escasos, comienzan a surgir cierto tipo de cuestionamientos que necesitan ser resueltos. El recurso escaso más evidente que puede ser requerido para desplegar una red privada es el espectro radioeléctrico, lo cual está claramente abordado en varios artículos de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTyR) (en específico, los artículos 68 y 78). Existen otros elementos que, aunque menos comunes en los aspectos regulatorios de despliegue de redes privadas, también son escasos, al menos en el corto plazo (p.ej., fibra óptica oscura, ductos, postes y torres, derechos de vía); sin embargo, éstos ameritan un tratamiento regulatorio diferente al que se la da al espectro y no son materia de la presente opinión.

Una red privada sólo requiere concesión única si busca utilizar recursos orbitales o bandas de frecuencia que no sean de uso libre. En la mayoría de las redes privadas que existen actualmente y que utilizan espectro, o bien usan espectro libre, o bien rentan enlaces,

[2] Este comentario sólo busca reconocer que existen elementos instalados asociados a la red que, por diversas razones, no están debidamente homologados. Por ejemplo, los casos de excepción que pueda prever el propio Instituto, aquellos que derivan de la falta de una disposición técnica emitida por el IFT o bien por una situación de facto ante el incumplimiento por parte del usuario.
[3] *Private Branch Exchange*

generalmente punto a punto, de las empresas que tienen la concesión de uso de espectro, quedando así la red privada exenta de buscar concesión. Son pocos aquellos que optan por seguir el camino de obtener una concesión para que les sean asignadas frecuencias por el IFT (p.ej., Pemex).

Sin embargo, la llegada de las redes inalámbricas basadas en tecnologías de última generación (5G y en menor grado Wi-Fi 6 y Wi-Fi 7) han levantado un nuevo interés en las redes privadas, ya que se visualiza que potencien un gran número de nuevas aplicaciones y nuevas utilizaciones de las telecomunicaciones sustentadas en mejorías en capacidad, latencia, fluctuación de la latencia (*jitter*) y seguridad. Estas redes pueden ser importantes catalizadores de cambios en los modelos de negocio de usuarios industriales y usuarios de misión crítica. Pueden potencializar, de acuerdo con los proveedores de las tecnologías, la "industria 4.0" y los "sistemas intercomunicados de manufactura inteligente".
Estas nuevas tecnologías son adecuadas para aquellos grandes usuarios que necesitan un desempeño predecible y confiable para avanzar en la automatización de fábricas, almacenes inteligentes, puertos, plantas químicas, generación y distribución de energía, transporte e industrias de gas y petróleo, por citar sólo algunos.

III. PROBLEMÁTICA

Algunas empresas en México y en otros países han comenzado a solicitar el desarrollo de modelos regulatorios flexibles para poder construir y operar redes privadas que utilizan espectro, ya que consideran que los modelos actuales no son adecuados para el desarrollo de estas redes. De manera previsible, solicitan que se les garantice certeza jurídica en el largo plazo, que existan mecanismos de protección contra interferencias que no tienen cuando acceden a espectro cuyo servicio está atribuido a título secundario o son de uso libre, e incluso solicitan exclusividad en el uso del espectro al menos en una zona o área definida. Para estos requerimientos señalan como principal justificación las fuertes inversiones para su despliegue y las necesidades de mayor control y precisión de sus redes.

Los principales argumentos que esbozan giran alrededor del esquema legal y regulatorio de acceso al espectro y su uso. Aunque los esquemas regulatorios en esta materia varían de país en país, la problemática es muy parecida en todo el mundo:

- Las concesiones generalmente son otorgadas a través de un proceso de licitación pública;
- En el caso de utilizar espectro de uso libre, no existe protección contra interferencias al no haber en la práctica mecanismos que garanticen el cumplimiento de ciertos parámetros técnicos que las impidan;
- La utilización en un esquema de uso secundario no sólo los pone como segundos en prioridad de uso, sino que también otorga poca certidumbre jurídica;
- Si proceden a arrendar espectro concesionado, están supeditados a la suerte del título de concesión de quien lo arrienda, disminuyendo la certeza en cuanto al plazo de utilización.

En este contexto, han comenzado análisis técnicos no sólo en el seno de la Unión Internacional de Telecomunicaciones (UIT) sino a nivel nacional. Varios países han comenzado a estudiar el problema e incluso algunos (p.ej., Brasil y Alemania) han hecho modificaciones a sus modelos regulatorios. Estados Unidos ha ido aún más lejos al haber licitado espectro para acomodar la existencia de redes privadas.

III.1 UIT

La Recomendación ITU-R M.2083 de 2015 provee el marco de referencia y objetivos generales del desarrollo de las telecomunicaciones móviles internacionales para el 2020. Entre sus considerandos refiere la expansión de las aplicaciones de comunicaciones inalámbricas a nuevos segmentos del mercado para facilitar la economía digital, como las redes eléctricas inteligentes, la cibersalud y los sistemas de transporte y de control del

tráfico inteligentes. En las tendencias se preveía que el diseño de nuevas aplicaciones estaría basado en la comunicación máquina a máquina (M2M) con prescripciones en tiempo real. Con respecto a las comunicaciones de gran fiabilidad y baja latencia refiere que tiene requisitos muy estrictos en cuanto a capacidades tales como el caudal, la latencia y la disponibilidad; aporta como ejemplos el control inalámbrico de procesos industriales de fabricación o producción, la cirugía a distancia, la automatización de la distribución en una red eléctrica inteligente y la seguridad del transporte. Una de las premisas de los estudios es la eficiencia espectral.[4]

En el seno de los grupos de estudio (grupo de trabajo 5) de la UIT se analizan por ejemplo la *CUESTIÓN UIT-R 262/5, Utilización de la componente terrenal de los sistemas IMT*[5] *para aplicaciones específicas*, y desde 2019 se trabaja en responder preguntas específicas respecto a las aplicaciones industriales y empresariales específicas, utilizaciones emergentes y funcionalidades que pueden soportar redes IMT, las características técnicas, los aspectos operativos y las capacidades asociadas a aplicaciones industriales y empresariales específicas.[6] El resultado de los estudios será incluido en recomendaciones, informes y manuales; es de preverse que algunos serán conocidos al finalizar la Conferencia Mundial de Radiocomunicaciones 2023.

[4] Recomendación ITU-R M.2083 de 2015 páginas 2, 4, 13 y disponible en https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-S.pdf
[5] *International Mobile Telecommunications*, témino genérico empleado por la UIT para referirse a los sistemas de banda ancha móvil. Incluye IMT-2000, IMT-Advanced e IMT-2020.
[6] El documento se encuentra disponible en el siguiente vínculo https://www.itu.int/pub/R-QUE-SG05.262-2019

III.2 INICIATIVA CBRS DE LA FCC (COMPARTICIÓN DE ESPECTRO) [7]

La iniciativa CBRS (*Citizens Broadband Radio Service*[8]) de la FCC (*Federal Communications Commission*) es un marco para la compartición de espectro para hacer uso de los 150 MHz en la banda de 3.5 GHz (3.550-3.700 GHz) para diversos servicios de comunicación inalámbrica. Aunque las discusiones iniciales se dieron desde 2012, no fue sino hasta 2017 que fueron publicadas las primeras reglas. La última modificación fue realizada en 2022.

De acuerdo con la FCC, la iniciativa CBRS tiene como objetivo promover la eficiencia del espectro, fomentar la innovación y ampliar el acceso a la banda ancha en los Estados Unidos. Permite que varios proveedores de servicios inalámbricos, empresas y organizaciones utilicen la banda de 3.5 GHz para una variedad de aplicaciones, incluidos datos móviles, Internet de las cosas (IoT), banda ancha inalámbrica fija y más.

Para el uso de ese espectro, se estableció un marco con tres niveles de licenciatarios– usuarios actuales (sistemas de radar del gobierno y operaciones satelitales), licenciatarios con acceso prioritario (PAL[9]) y acceso autorizado general (GAA[10]) – para permitir el acceso de nuevos usuarios protegiendo a los usuarios que ya ocupaban la banda. La asignación en cada momento se hace a través de un sistema de coordinación automático de frecuencias (AFC[11]) llamado SAS[12], siguiendo la priorización de los 3 niveles de licenciatarios. Los usuarios de la banda pagan por este servicio.

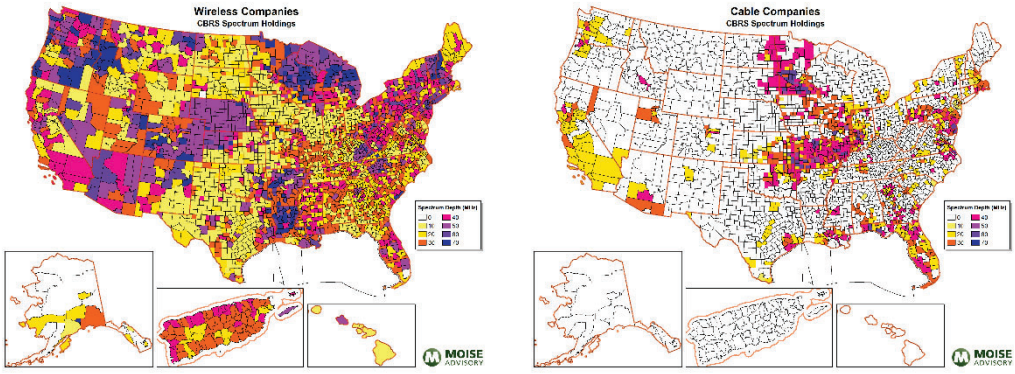
La iniciativa tiene su parte más innovadora en la asignación de las licencias PAL. Cada licencia PAL consta de 10 MHz en la sub-banda de 3.55 a 3.65 MHz para cada área

[7] https://auctiondata.fcc.gov/public/projects/auction105
[8] Servicio Ciudadano de Radio de Banda Ancha.
[9] *Priority Access Licensees*
[10] *General Authorized Access*
[11] *Automated Frequency Coordination*
[12] *Spectrum Access System*

geoestadística básica[13], pudiendo asignar en cada área un máximo de 7, restringiendo a un máximo de 4 para un mismo postor. Originalmente se consideraron que serían licencias con una vigencia de 3 años, pero ésta fue extendida a 10 años. En la subasta 105 (FCC Auction 105) llevada a cabo del 23 de julio al 25 de agosto de 2020, en 76 rondas, se presentaron 271 postores, 228 de los cuales obtuvieron al menos una licencia. Fueron asignadas 20,625 licencias de un total 22,631 puestas a disposición. Fueron recaudados 4,545 millones de dólares.[14]

Vale la pena resaltar algunos de los resultados de este proceso. No sorprende que los principales ganadores de la subasta hayan sido empresas de telecomunicaciones; de los 20 mayores ganadores, 16 son empresas de servicios móviles y cableras. La figura 1 muestra la obtención de licencias CBRS por parte de estas empresas. Muchos otros postores fueron empresas de prestación de servicios de banda ancha de porte local.

Figura 1. Licencias CBRS obtenidas por empresas móviles y cableras



Fuente: Moise Advisory, tomado de Dano, M. "CBRS spectrum auction maps: who won what, and where"[15]

[13] *Census tract.* Es un concepto similar al utilizado por el INEGI. En México hay 64,000 Áreas Geoestadísticas Básicas (AGEB), mientras que en EUA hay poco más de 85,000.
[14] FCC (https://www.fcc.gov/auction/105). Un análisis detallado de los resultados de la subasta puede encontrarse en https://sashajavid.com/FCC_Auction105.php
[15] Dano, Mike. "CBRS spectrum auction maps: Who won what, and where", publicado en LightReading. Disponible en https://www.lightreading.com/5g/cbrs-spectrum-auction-maps-who-won-what-and-where/d/d-id/763837

Llama la atención, sin embargo, la asignación de cerca de 500 licencias PAL (alrededor de 2.5% del total) a muchas otras entidades pertenecientes a ramos diferentes a las telecomunicaciones y que, sin eliminar la posibilidad de que con este espectro quisieran prestar servicios al público, su uso esté destinado básicamente a la construcción de redes privadas[16]:

- **Empresas eléctricas:** 10 empresas eléctricas obtuvieron 375 licencias PAL en 150 condados, pagando $174 millones (cobertura de 10% de la población). Entre estas empresas destacan Southern California Edison (20 PAL, $119 millones), Sempre Energy (3 PAL, $21.3 millones) y Alabama Power (271 PAL, $18.9 millones).
- **Una FIBRA[17]:** JBG Smith, un desarrollador de bienes raíces en el área de Washington D.C. a quien fue encomendado el desarrollo del complejo de Amazon en el área, obtuvo 7 PAL en Arlington y Alexandria, Virginia por $25.3 millones.
- **Empresas petroleras y químicas:** Chevron obtuvo 26 PAL en Colorado, Luisiana, Misuri, Nuevo México y principalmente Texas pagando $1.1 millones. Oxy USA Inc. (producción de energía y productos químicos) obtuvo 31 PAL por $4.8 millones en Colorado, Nuevo México, Texas y Wyoming. Pioneer Natural Resources obtuvo 24 PAL en Texas por $1.18 millones.
- **Una armadora de tractores:** John Deere (Deere & Company) obtuvo 5 PAL en Illinois y Iowa pagando $0.55 millones.
- **Universidades:** Texas A&M (College Station, Texas) obtuvo una licencia por $39,000 y University of Virginia Foundation (Virgina) obtuvo 6 licencias por $118,000.
- **Una ciudad:** La Ciudad de Donalsonville en Georgia obtuvo 2 licencias por $15,980.
- **Una agencia de educación:** Newaygo County Regional Educational Service Agency, la agencia encargada de prestar varios servicios a los distritos escolares en el condado de Newaygo, Michigan, obtuvo 2 PAL por $51,000.

[16] Fuente: FCC (https://auctiondata.fcc.gov/public/projects/auction105). Análisis del equipo de trabajo
[17] Fideicomiso de Inversión en Bienes Raíces (REIT – *real estate investment trust*).

- **Una empresa de integración de redes:** Xtreme Enterprises, LLC, dedicada a la construcción e integración de redes de telecomunicaciones (WISP y otras), obtuvo 17 PAL por $145,000 en Nueva York y Pensilvania.

De lo anterior, parece haber evidencia sólida para decir que las redes privadas que prefieren contar con espectro concesionado para su despliegue ya es una realidad. La combinación de espectro licenciado y acceso libre en un modelo de 3 niveles ha generado ya mucha investigación y literatura en la optimización en el proceso de compartición de infraestructura, así como en cuestiones de privacidad y ciberseguridad. El tema es relativamente nuevo, por lo que es de esperarse que su entendimiento evolucione rápidamente en un futuro cercano.

III.3 CANADÁ

Canadá ha reconocido la importancia de las redes privadas y la necesidad de poner espectro a disposición de potenciales usuarios. Innovación, Ciencia y Desarrollo Económico Canadá (ISED o ISDE[18]), parte del Ministerio de Innovación, Ciencia e Industria, sometió en 2022 a consulta pública[19] un proceso de asignación de 80 MHz de espectro en la banda de 3,900-3,980 MHz y bandas milimétricas (26 GHz, 28 GHz y 38 GHz) con el objetivo de facilitar el acceso de manera flexible a este recurso escaso a un amplio grupo de potenciales usuarios, entre los cuales se encuentran empresas de telecomunicaciones y pequeños proveedores (p.ej., WISP), así como para negocios e industrias verticales, tales como agricultura, minería, manufactura, servicios de salud, seguridad pública y transporte.

[18] Innovation, Science and Economic Development Canada (ISED) o Innovation, Sciences et Développement Économique Canada (ISDE) en https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/learn-more/key-documents/consultations/consultation-non-competitive-local-licensing-framework-including-spectrum-3900-3980-mhz-band-and

[19] ISDE. (Agosto 2022). “Consultation on a Non-Competitive Local Licensing Framework, Including Spectrum in the 3900-3980 MHz Band and Portions of the 26, 28 and 38 GHz Bands”

El gobierno de Canadá sometió a consulta pública un proceso de licenciamiento local no competitivo (NCL[20]) para el cual delineó tres opciones:

- **Todos servidos** (ACAS – *all-come all served*): Es un método de compartición de espectro sin que ningún operador tenga prioridad sobre el resto; no existe restricción para obtener licencias en diferentes áreas geográficas. Se reconoce la importancia de la interferencia, sin para ello dar una solución. Sus ventajas serían la baja carga administrativa para ISED y los operadores, reduce las barreras de entrada y maximiza el número de operadores que pueden utilizar el espectro. Sus desventajas son la posibilidad de interferencia y el congestionamiento, lo que impacta la calidad de servicio y la posible existencia de interferencia perjudicial.
- **Primero en llegar, primero en ser atendido** (FCFS – *first-come first-served*): Es un modelo de licenciamiento para permitir la compartición de espectro que sería gestionado por ISED. Como ventajas tiene que habría un nivel pre-especificado de protección de interferencias y mitigaría el posible congestionamiento e interferencia que pueden ocurrir con ACAS. Daría, además, cierto grado de certidumbre para la planeación de inversiones. Como desventaja, se destaca que disminuiría el número de operadores que podrían obtenerse con ACAS, además de que implicaría una carga administrativa mayor tanto para ISED como para los operadores, aunque potencialmente podría reducirse automatizando algunos de los procesos asociados al licenciamiento.
- **Acceso espectral dinámico** (DSA – *dynamic spectrum access*): Es un sistema de compartición de espectro que soporta un uso intensivo del espectro asignando frecuencias basadas en disponibilidad y necesidad inmediata. El espectro es asignado por la duración deseada de uso, quedando disponible para otros usuarios una vez que ha sido dejado de usar. Sus ventajas con respecto al modelo FCFS están en la versatilidad y eficiencia en el uso del espectro, la disminución de barreras de

[20] *Non-Competitive Local Licensing process*

entrada, la reducción en la carga administrativa y la posibilidad de que los operadores paguen por el uso del espectro sólo cuando realmente lo están utilizando. ISED reconoce que un ecosistema DSA para las bandas consideradas no estaba disponible en el momento de la consulta y que lo promoverá en un futuro cuando sea técnicamente factible.

Como resultado de la consulta[21], ISED decidió utilizar un sistema de FCFS. Asimismo, dado que reconoce que el espectro tendrá al menos tres tipos de potenciales interesados (nueva capacidad para sistemas inalámbricos fijos en áreas rurales y remotas, redes privadas de banda ancha en complejos empresariales tales como campus universitarios, estadios, centros comerciales y edificios de oficinas, así como redes privadas para servir de soporte a usos industriales tales como agricultura, manufactura y minería), decidió definir las áreas de licenciamiento de manera flexible, utilizando un sistema basado en vectores (*custom vector-based license areas*), de tal manera que las áreas de licenciamiento tendrían una frontera definida por el usuario y no estaría predeterminadas por ISED. Los precios fueron fijados en términos de área cubierta y tipo de área (área urbana: C$1.80/MHz/km^2; rural: C$0.45/MHz/km^2; remota: C$0.01/MHz/km^2). El proceso de licenciamiento aún no comienza.

El sistema adoptado en Canadá es novedoso y aún es difícil prever cuáles serán los resultados. ISED ha sido criticado por tratar de implementar un marco de referencia ambicioso tratando de satisfacer los usos de muchos usuarios con necesidades diferentes de manera simultánea, lo cual generará beneficios no homogéneos a todas las partes.

[21] ISDE. (Mayo 2023). “Decision on a Non-Competitive Local Licensing Framework, Including Spectrum in the 3900-3980 MHz Band and Portions of the 26, 28 and 38 GHz Bands”

IV. MÉXICO

México no es ajeno al problema. Varias entidades han levantado ya la necesidad de crear un marco regulatorio que permita y promueva la existencia de redes privadas, especialmente con tecnologías IMT. Para ello es necesario encontrar mecanismos que permitan acceder al espectro de una manera satisfactoria.

Varias instancias, entre las que destaca la UER y el Comité 5G organizado por el IFT, ya han comenzado a analizar en detalle el tema y han comenzado a proponer algunas soluciones. En un documento desarrollado por la UER[22] fechado septiembre de 2022, ya se delinean algunas de las preguntas que deben ser respondidas:

- ¿Cuál es el plazo óptimo para estas concesiones? ¿Sería necesario un plazo de 10 o 15 años u otro plazo?
- ¿Las autorizaciones de uso secundario satisfarían la demanda para redes privadas a actividades vinculadas con la industria 4.0?
- ¿El arrendamiento de espectro es la vía para satisfacer la demanda de estas industrias?
- ¿La oferta de los operadores atiende las necesidades específicas de las industrias?
- ¿Se requiere modificar la Ley Federal de Telecomunicaciones y Radiodifusión para poder lograr la asignación eficiente de concesiones de espectro radioeléctrico para uso privado?
- ¿Se deberían definir segmentos específicos de espectro radioeléctrico para redes privadas? ¿Deberían incluirse en el programa anual de uso y aprovechamiento de bandas de frecuencias?
- ¿Resulta viable la evaluación mediante *Beauty Contest* para determinar a un participante ganador en licitación?

[22] UER-IFT. (Septiembre, 2022). "Reflexiones respecto a la asignación eficiente de espectro para redes privadas"

- ¿Es posible que se demuestre el interés legítimo del interesado para poder participar en la licitación pública?
- En la comprobación del interés legítimo, respecto del área en donde se quieren prestar los servicios, ¿qué pasaría si hubiere áreas traslapadas o contenidas unas en otras?

Este Consejo Consultivo ha identificado algunas problemáticas adicionales, aunque con intersecciones relevantes con las preguntas planteadas por la UER. No es una lista que pretende ser exhaustiva, sino que creemos que resalta parte de la problemática y el desafío:

- El conflicto con el marco legal, especialmente con respecto a la necesidad de un proceso licitatorio (artículos 69 y 78[23] de la LFTyR) cuando se asigna espectro. Bajo el entendimiento generalizado, si se plantea una asignación de espectro para el desarrollo de redes privadas con procedimientos distintos a la licitación, se estaría en abierta contradicción con el artículo 78 primer párrafo y fracción I de la LFTyR;
- La necesidad de contar con un plazo largo preestablecido para utilización del espectro, para con ello dar certidumbre a las inversiones. Las concesiones pueden darse hasta por 30 años, con posibilidad de prórroga. Un plazo tan largo podría ser innecesario para muchos proyectos asociados a redes privadas, especialmente con la velocidad del cambio tecnológico, por lo que probablemente los plazos deberían

[23] Artículo 78. Las concesiones para el uso, aprovechamiento o explotación del espectro radioeléctrico para uso comercial o privado, en este último caso para los propósitos previstos en el artículo 76, fracción III, inciso a), se otorgarán únicamente a través de un procedimiento de licitación pública previo pago de una contraprestación, para lo cual, se deberán observar los criterios previstos en los artículos 6o., 7o., 28 y 134 de la Constitución y lo establecido en la Sección VII del Capítulo III del presente Título, así como los siguientes:
I. Para el otorgamiento de concesiones en materia de telecomunicaciones, el Instituto podrá tomar en cuenta, entre otros, los siguientes factores:
a) La propuesta económica;
b) La cobertura, calidad e innovación;
c) El favorecimiento de menores precios en los servicios al usuario final;
d) La prevención de fenómenos de concentración que contraríen el interés público;
e) La posible entrada de nuevos competidores al mercado, y
f) La consistencia con el programa de concesionamiento.

estar asociados a criterios basados en variables objetivas (p.ej., inversión, amortización, relevancia al proceso para el cual se pretende construir una red privada, etc.). Asimismo, cualquier concesión debe estar sujeta a condiciones de terminación anticipada (p.ej., *use it or lose it*).

- El potencial conflicto o riesgo de interferencias con otros usos y usuarios actuales por el interés manifestado para la identificación de bandas específicas para uso empresarial (uso privado para comunicación privada). Dentro del Comité 5G se ha planteado la posibilidad de usar las siguientes bandas (el Anexo 1 presenta usos actualmente atribuidos a dichas bandas en el Cuadro Nacional de Atribución de Frecuencias, los cuales podrían ser la fuente de conflictos y riesgos):
    - 410-430 MHz
    - 450-470 MHz
    - Banda L (1,427-1,518 MHz)
    - 2,300 MHz
    - 2,483.5-2,495 MHz (B53)
    - 2,570-2,640 MHz (2.6 GHz TDD)
    - 3.7-3.8 GHz
    - Partes de las bandas de 26 GHz y 28 GHz;
- En caso de arrendamiento de espectro, dependencia de la concesión de un tercero, lo que disminuye la certeza a las inversiones, a los plazos y a las interferencias;
- Eficiencia espectral y administración eficiente del uso del espectro; licitaciones que otorgan uso exclusivo impiden el acceso de terceros interesados al uso del espectro, lo que puede llevar a un uso ineficiente del recurso;
- Utilización de redes existentes (operadores actuales) y casos en los que no es posible o no satisfacen adecuadamente las necesidades demandadas por el usuario potencial de una red privada; esto está íntimamente ligado a la existencia de potenciales reservas de mercado, que no deberían existir;

- Conflicto con derechos adquiridos. Cuando una red privada opera en uso secundario, generalmente puede zanjarse el conflicto potencial de derechos adquiridos, además de poder prevenir una gama importante de conflictos a través de condiciones técnicas (i.e., áreas de cobertura, límites de potencia, especificaciones de los equipos, etc.).
- Posible conflicto con el precio (guante+derechos) del espectro. La motivación para desplegar una red privada no debe ser el arbitraje que podría existir debido al costo del espectro que pagan los operadores móviles y lo que pagarían por el uso del espectro. Sin embargo, la variable precio, dada la distorsión existente en el modelo de cobro por el uso del espectro en México, no debería inhibir el desarrollo de las redes privadas, ya que potencialmente podrán traer enormes beneficios en productividad como consecuencia de la transformación digital;
- Necesidad de información detallada actualizada en un sistema informático de administración del espectro (previsto en el artículo 62[24] de la LFTyR), para así poder acceder a información oportuna para el diseño de redes e identificación del origen de posibles interferencias;
- Necesidad de supervisión y resolución de conflictos. Dada la naturaleza de los dueños de las redes privadas, la supervisión de cumplimiento de condiciones puede ser, en la mayoría de los casos, relativamente laxa, ya que son los usuarios y propietarios de las redes que comparten espectro los que estarán proactivamente verificando que la red funciona correctamente. Sin embargo, esto sólo es eficiente si existe un proceso de recepción de quejas, resolución de conflictos e imposición

[24] *Artículo 62. El Instituto estará obligado a implementar, operar y mantener actualizado un sistema informático de administración del espectro, así como a establecer los mecanismos y criterios para hacer público el acceso a la información contenida en las bases de datos correspondientes, en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.*

En el sistema mencionado se incluirá toda la información relativa a la titularidad de las concesiones incluyendo la tecnología, localización y características de las emisiones, así como la relativa al despliegue de la infraestructura instalada y empleada para tales fines.

Los concesionarios se encuentran obligados a entregar al Instituto, en el plazo, formato y medio que para tal efecto se indique, la información referente a dicho uso, aprovechamiento o explotación.

de multas realmente expedito y certero. En caso contrario, será necesario que el IFT cuente con los recursos para llevar a cabo monitoreo y las verificaciones.

V. ASUNTOS QUE REQUIEREN DE MAYOR ESTUDIO Y ESBOZO DE RECOMENDACIONES PRELIMINARES

Este Consejo Consultivo plantea algunas cuestiones que requieren ser entendidas a profundidad, emitiendo una opinión al respecto. No nos estamos pronunciando sobre una banda del espectro en particular; la presente opinión es acerca de principios y conceptos, los cuales son independientes de las bandas específicas que pudieran ser consideradas. Tampoco pretendemos que sean exhaustivas, sino que buscamos resaltar parte de la problemática y el desafío existente

- **Sobre soluciones alternativas**: Como parte del análisis y búsqueda de soluciones alternativas para atender los requerimientos de las redes privadas es importante que se analice la forma en que se podrían modificar, en su caso, los esquemas que se emplean actualmente para evaluar si es posible hacer ajustes que resuelvan sus necesidades, entre ellos el arrendamiento del espectro radioeléctrico previsto en el artículo 104 de la Ley. Un ejemplo puede ser que, ante la extinción de pleno derecho del arrendamiento, el IFT pueda establecer un régimen transitorio que permita al arrendatario migrar su red privada a otro concesionario (p.ej., a través de esquemas de colaboración).
- **Sobre la oferta de los operadores y la brecha de las necesidades específicas de las industrias:** Es necesario analizar e identificar por qué la oferta de los operadores actuales no cubre las necesidades específicas de las industrias y cómo sí podría satisfacer dichas necesidades, en específico, desde el punto de vista regulatorio, para evaluar si es posible abordar el tema desde esta perspectiva.

- **Sobre las áreas de servicio:** La definición del tamaño de las áreas de servicio es fundamental para una potencial asignación de espectro. El IFT divide a México en 65 ABS[25], pero para poder satisfacer la necesidad de espectro para redes privadas, la extensión de las áreas de la unidad básica de concesionamiento debe ser sustancialmente menor a las definiciones utilizadas actualmente[26], ya que prácticamente ningún potencial usuario estaría interesado en adquirir espectro en una enorme zona geográfica. Además de la falta de interés, implicaría un uso muy ineficiente del espectro, pues probablemente las áreas de sombra en espectro reservado serían muy grandes. Para ilustrar el punto del tamaño del área de servicio, puede tomarse a manera de ejemplo la licitación de CBRS, que utilizó como base los 85,000 *census tracts.*
- **Sobre el proceso de asignación:** Aunque bajo el entendimiento generalizado del marco legal mexicano, si se plantea una asignación de espectro para el desarrollo de redes privadas con procedimientos distintos a la licitación, se estaría en abierta contradicción con el artículo 78 primer párrafo y fracción I de la LFTyR), este Consejo Consultivo recomienda al Instituto que analice con detalle esquemas novedosos que han venido desarrollándose en otros países (de los cuales describimos someramente apenas dos en el presente texto) para satisfacer la necesidad de espectro para el despliegue de redes privadas. Un modelo parecido al CBRS de Estados Unidos podría ser compatible con el marco mexicano. Modelos de grupos (*tiered models)* probablemente ayudan a solventar la restricción de acceso por licitación.
- **Sobre la necesidad de promover la compartición de espectro (acceso dinámico y uso compartido)[27].** Varias de las soluciones para la asignación de espectro para usos

[25] Áreas Básicas de Servicio
[26] El VI Consejo Consultivo del IFT abordó la reducción de las áreas básicas de servicio en la "Recomendación para mejorar el diseño de subastas de espectro radioeléctrico". Disponible en: https://consejoconsultivo.ift.org.mx/docs/recomendaciones/2022/07__recomendaci%C3%B3n_para_mejorar_el_dise%C3%B1o_de_subastas_de_espectro_radioel%C3%A9ctrico_que_lleva_a_cabo_add.pdf)
[27] El VI Consejo Consultivo del IFT abordó la reducción de las áreas básicas de servicio en el texto "Recomendaciones específicas que emite el Consejo Consultivo del Instituto Federal de Telecomunicaciones relacionadas con el mandato del IFT en materia de regulación y supervisión del uso del espectro

de redes privadas pasan por la coordinación automática de frecuencias (AFC). Sin embargo, AFC tiene muchas otras virtudes en muchas otras situaciones (p.ej., espectro satelital vs espectro de redes terrestres), ya que permite la utilización concomitante del espectro por varios usuarios, aumentando de manera sustancial la eficiencia del uso del espectro. La definición de *tiers* en CBRS depende de una solución de este tipo; en Canadá se está estudiando su implementación después de reconocer que es la solución óptima para el problema bajo análisis; Europa lo utiliza casi de manera generalizada. Entendemos que el IFT ya ha comenzado a estudiar el tema[28], pero queremos hacer hincapié en que es de primerísima importancia desarrollar en el corto plazo una ruta crítica para la implementación de AFC y DSA, con mecanismos que consideren evitar conflictos para su implementación, identificando exhaustivamente la infraestructura existente y las entidades que las ocupan, previendo y haciendo pruebas adecuadas para evitar interferencias perjudiciales a los concesionarios actuales y afectaciones a los usuarios finales. Este tema ya ha sido abordado por el Consejo Consultivo en el pasado[29].

- **Sobre el precio del espectro.** Sea cual fuere la solución que IFT decida implementar, deberá minimizar las oportunidades de arbitraje que podrían surgir por el esquema de cobro del espectro en México, cuidando, sin embargo, que no se desincentive el crecimiento de redes privadas, que no se proteja innecesariamente a concesionarios públicos y que no se tengan consecuencias adversas a la competencia. Es un tópico muy delicado y la solución probablemente no es trivial y mucho menos estática, ya que las variables que inciden son muchas y están en cambio constante.

---

radioeléctrico, en particular con el monitoreo del uso del espectro y solución de interferencias perjudiciales en el contexto del uso dinámico y el uso compartido". Disponible en: https://consejoconsultivo.ift.org.mx/docs/recomendaciones/2022/17__recomendaciones_relacionadas_con_el_mandato_del_ift_en_materia_de_regulacion_y_supervision_del_uso_del_espectro_radioelectrico.pdf

[28] Véase, por ejemplo, el documento titulado "Análisis en materia de acceso dinámico y uso compartido del espectro radioeléctrico y las alternativas regulatorias para su habilitación", publicado por la UER-IFT en junio de 2023.

[29] El documento está publicado en https://consejoconsultivo.ift.org.mx/docs/recomendaciones/2022/17__recomendaciones_relacionadas_con_el_mandato_del_ift_en_materia_de_regulacion_y_supervision_del_uso_del_espectro_radioelectrico.pdf

- **Sobre la resolución de conflictos.** Dada la naturaleza de las redes privadas y la enorme preocupación surgida por la posibilidad de interferencias, sin minimizar su importancia, este Consejo Consultivo es de la opinión que al implementar la solución es necesario un proceso de verificación eficiente. Sin embargo, para reducir esa necesidad de fiscalización, el IFT deberá contar con un esquema de aceptación de quejas y resolución de conflictos verdaderamente expedito, considerando la posibilidad de esquemas de solución alternativa de controversias como (p.ej., el arbitraje y la mediación).

Lilia Eurídice Palma Salas
Presidenta del VII Consejo Consultivo

Mtra. Rebeca Escobar Briones
Secretaria del Consejo Consultivo

La Opinión fue aprobada por el VII Consejo Consultivo del Instituto Federal de Telecomunicaciones por unanimidad de votos de los consejeros: Alejandro Ildefonso Castañeda Sabido, Sara Gabriela Castellanos Pascacio, Ernesto M. Flores-Roux, Mario Germán Fromow Rangel, Gerardo Francisco González Abarca, Misha Leonel Granados Fernández, Ali Bernard Haddou Ruiz, Erik Huesca Morales, Salma Leticia Jalife Villalón, Luis Miguel Martínez Cervantes, Jorge Fernando Negrete Pacheco[30], Lucía Ojeda Cárdenas, Eurídice Palma Salas y Cynthia Gabriela Solís Arredondo, en términos del artículo 17 de las Reglas de Operación de este Consejo Consultivo, en la X Sesión Ordinaria celebrada el 28 de septiembre de 2023, mediante Acuerdo CC/VII/IFT/280923/32.

La Opinión fue elaborada por los consejeros Ernesto M. Flores-Roux y Eurídice Palma Salas.

[30] El consejero Jorge Fernando Negrete Pacheco manifestó su voto a través del grupo de WhatsApp del VII CCIFT. Se dio cuenta del voto de viva de la voz de la consejera presidenta en la X Sesión Ordinaria del VII CCIFT celebrada el 28 de septiembre de 2023.

Referencias

1. Bauer, Johannes M. y Erik Bohlin. (Julio 15, 2019). "The Role of Regulation in 5G Market Design". Quello Center Working Paper, TPRC47: The 47th Research Conference on Communication, Information and Internet Policy 2019, Disponible en: SSRN:https://ssrn.com/abstract=3421024 or http://dx.doi.org/10.2139/ssrn.3421024

2. Brown, Gabriel. (2019). "Private 5G Mobile Networks for Industrial IoT". Heavy Reading White Paper. Disponible en: https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/private_5g_networks_for_industrial_iot.pdf

3. Consejo Consultivo del Instituto Federal de Telecomunicaciones. (Junio, 2022). "Recomendaciones específicas que emite el Consejo Consultivo del Instituto Federal de Telecomunicaciones relacionadas con el mandato del IFT en materia de regulación y supervisión del uso del espectro radioeléctrico, en particular con el monitoreo del uso del espectro y solución de interferencias perjudiciales en el contexto del uso dinámico y el uso compartido". Disponible en: https://consejoconsultivo.ift.org.mx/docs/recomendaciones/2022/17_recomendaciones_relacionadas_con_el_mandato_del_ift_en_materia_de_regulacion_y_supervision_del_uso_del_espectro_radioelectrico.pdf

4. Consejo Consultivo del Instituto Federal de Telecomunicaciones. (Marzo, 2022). "Recomendación para mejorar el diseño de subastas de espectro radioeléctrico". Disponible en: https://consejoconsultivo.ift.org.mx/docs/recomendaciones/2022/07_recomendaci%C3%B3n_para_mejorar_el_dise%C3%B1o_de_subastas_de_espectro_radioel%C3%A9ctrico_que_lleva_a_cabo_add.pdf)

5. Dano, Mike. “CBRS spectrum auction maps: Who won what, and where”, publicado en LightReading. Disponible en: https://www.lightreading.com/5g/cbrs-spectrum-auction-maps-who-won-what-and-where/d/d-id/763837

6. FCC. Micrositio de la subasta 105. Disponible en: https://auctiondata.fcc.gov/public/projects/auction105

7. IFT. (Diciembre 30, 2021). Cuadro Nacional de Atribución de Frecuencias. Diario Oficial de la Federación del 30 de diciembre de 2021.

8. ISDE. Gobierno de Canadá (Agosto, 2022). “Consultation on a Non-Competitive Local Licensing Framework, Including Spectrum in the 3900-3980 MHz Band and Portions of the 26, 28 and 38 GHz Bands”. Disponible en: https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/learn-more/key-documents/consultations/consultation-non-competitive-local-licensing-framework-including-spectrum-3900-3980-mhz-band-and

9. ISDE. Gobierno de Canadá. (Mayo, 2023). “Decision on a Non-Competitive Local Licensing Framework, Including Spectrum in the 3900-3980 MHz Band and Portions of the 26, 28 and 38 GHz Bands”. Disponible en: https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/spectrum-allocation/decision-non-competitive-local-licensing-framework-including-spectrum-3900-3980-mhz-band-and

10. Javid, Sasha. (Sin fecha). “Auction 105 Summary (2550-2650 MHz Band)”. Página personal del autor. Disponible en: https://sashajavid.com/FCC_Auction105.php

11. México. Ley Federal de Telecomunicaciones y Radiodifusión

12. RCRWireless News. (Agosto, 2023). “Private Network Global Forum. Key Findings Report”. Disponible en: https://content.rcrwireless.com/private-networks-forum-key-findings-report

13. UER-IFT. (Septiembre, 2022). “Reflexiones respecto a la asignación eficiente de espectro para redes privadas”.

14. UER-IFT. (Junio, 2023). “Análisis en materia de acceso dinámico y uso compartido del espectro radioeléctrico y las alternativas regulatorias para su habilitación”. Disponible en https://www.ift.org.mx/sites/default/files/analisis_en_materia_de_acceso_dinamico_y_uso_compartido_del_espectro_radioelectrico.pdf

15. UIT-R. (Septiembre, 2015). “Recomendación ITU-R M.2083 de 2015”. Disponible en: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-S.pdf

16. UIT-R. (Noviembre, 2019). “CUESTIÓN UIT-R 262/5, Utilización de la componente terrenal de los sistemas IMT para aplicaciones específicas”. Disponible en https://www.itu.int/pub/R-QUE-SG05.262-2019

17. UIT-R. (Febrero, 2022). “ITU-R FAQ on International Telecommunications (IMT)”. Disponible en https://www.itu.int/en/ITU-R/Documents/ITU-R-FAQ-IMT.pdf

Anexo I

410-430 MHz, 450-470 MHz

INTERNACIONAL MHz			**MÉXICO MHz**
Región 1	**Región 2**	**Región 3**	
405 – 415 RADIONAVEGACIÓN 5.76	**405 – 415** RADIONAVEGACIÓN 5.76 Móvil aeronáutico		**405 – 415** RADIONAVEGACIÓN Móvil aeronáutico **MX8 MX15**
415 – 435 MÓVIL MARÍTIMO 5.79 RADIONAVEGACIÓN AERONÁUTICA	**415 – 472** MÓVIL MARÍTIMO 5.79 Radionavegación aeronáutica 5.77 5.80 5.78 5.82		**415 – 435** MÓVIL MARÍTIMO RADIONAVEGACIÓN AERONÁUTICA **MX8 MX16** **MX16A**
435- 472 MÓVIL MARÍTIMO 5.79 Radionavegación aeronáutica 5.77 5.82	**415 – 472** (continúa) MÓVIL MARÍTIMO 5.79 Radionavegación aeronáutica 5.77 5.80 5.78 5.82		**435- 472** MÓVIL MARÍTIMO Radionavegación aeronáutica **MX16A**
	525 -535		**525 -535**
526.5 -1606.5 RADIODIFUSIÓN	RADIODIFUSIÓN RADIONAVEGACIÓN AERONÁUTICA	**526.5 -535** RADIODIFUSIÓN Móvil 5.88	RADIONAVEGACIÓN AERONÁUTICA **MX8 MX19**

5.87 5.87A	**535 – 1605** RADIODIFUSIÓN	**535 – 1605.5** RADIODIFUSIÓN	**535 – 1605** RADIODIFUSIÓN **MX20 MX21 MX22** **MX23** **MX25**

2300 -2498 FIJO MÓVIL salvo móvil aeronáutico (R) RADIODIFUSIÓN 5.113 5.103	**2300 -2498** FIJO MÓVIL RADIODIFUSIÓN 5.113	**2300 -2495** FIJO MÓVIL RADIODIFUSIÓN

2502 -2625 FIJO MÓVIL salvo móvil aeronáutico (R 5.92 5.103. 5.114)	**2502 -2505** FRECUENCIAS PATRÓN Y SEÑALES HORARIAS	**2502 -2505** FRECUENCIAS PATRÓN Y SEÑALES HORARIAS
	2505 – 2850 FIJO MÓVIL	**2505 – 2850** FIJO MÓVIL

3.5 - 3.8 AFICIONADOS FIJO	**3.5 - 3.75** AFICIONADOS	3.5 - 3.9 AFICIONADOS FIJO	**3.5 - 3.75** AFICIONADOS

MÓVIL salvo móvil aeronáutico 5.92	5.119	MÓVIL	**MX28**

Rango de frecuencias: 25.01 - 29.7 MHz

INTERNACIONAL MHz			**MÉXICO MHz**
Región 1	**Región 2**	**Región 3**	
25.67 - 26.1 RADIODIFUSIÓN			**25.67 - 26.1** RADIODIFUSIÓN
26.1 - 26.175 MÓVIL MARÍTIMO 5.132			**26.1 - 26.175** MÓVIL MARÍTIMO **MX84**
26.175 - 26.2 FIJO MÓVIL salvo móvil aeronáutico			**26.175 - 26.2** FIJO MÓVIL salvo móvil aeronáutico
26.2 - 26.35 FIJO MÓVIL salvo móvil aeronáutico Radiolocalización 5.132A	**26.2 - 26.42** FIJO MÓVIL salvo móvil aeronáutico RADIOLOCALIZACIÓN 5.132A	**26.2 - 26.35** FIJO MÓVIL salvo móvil aeronáutico Radiolocalización5.132A	**26.2 - 26.42** FIJO MÓVIL salvo móvil aeronáutico RADIOLOCALIZACIÓN 5.132A

5.1323A			**MX38A**
26.35 -27.5 FIJO MÓVIL salvo móvil Aeronáutico 5.150	**26.42. -27.5** FIJO MÓVIL salvo móvil Aeronáutico 5.150	**26.35 -27.5** FIJO MÓVIL salvo móvil Aeronáutico 5.150	**26.42. -27.5** FIJO MÓVIL salvo móvil Aeronáutico **MX68 MX85**

28 - 29.7 AFICIONADOS AFICIONADOS POR SATÉLITE	**28 - 29.7** AFICIONADOS AFICIONADOS POR SATÉLITE **MX28**

MX8 El 26 de abril de 1996 se firmó en Morelia, Michoacán, el Protocolo entre México y los Estados Unidos de América, relativo al uso de las bandas atribuidas a los servicios de radionavegación aeronáutica y de comunicaciones aeronáuticas a lo largo de la frontera común. En este documento se establecen procedimientos de coordinación, criterios técnicos y condiciones de uso de las bandas de frecuencias que se enlistan a continuación:

190 - 285 kHz	328.6 - 335.4 MHz	5.35 - 5.47 GHz
285 - 435 kHz	960 - 1215 MHz	9 - 9.2 GHz
510 - 535 kHz	1215 - 1400 MHz	13.25 - 13.4 GHz
74.8 - 75.2 MHz	2700 - 2900 MHz	15.4 - 15.7 GHz
108 - 118 MHz	4.2 - 4.4 GHz	
118 - 137 MHz	5 - 5.25 GHz	

MX15 Por encontrarse atribuida a título primario al servicio de radionavegación, la banda de frecuencias 405 - 415 kHz se clasifica como espectro protegido. Dentro de dicha banda, el segmento de frecuencias 406.5 - 413.5 kHz se encuentra destinada para su uso por la radiogoniometría, de conformidad con el número 5.76 del RR.

MX16 Por encontrarse atribuida a título primario al servicio de radionavegación aeronáutica, la banda de frecuencias 415 - 435 kHz se clasifica como espectro protegido. La utilización de esta banda de frecuencias por el servicio móvil marítimo no deberá causar interferencias perjudiciales a la operación del servicio de radionavegación aeronáutica, ni deberá reclamar protección contra interferencias perjudiciales provenientes de dicho servicio.

MX16A La utilización de las bandas de frecuencias 415 - 495 kHz y 505 - 525 kHz por el servicio móvil marítimo se encuentra limitada para radiotelegrafía y podrán utilizarse también por estaciones de transmisión del sistema NAVDAT limitadas a estaciones costeras, de conformidad el número 5.79 del RR.

MX19 Por encontrarse atribuida a título primario al servicio de radionavegación aeronáutica, la banda de frecuencias 525 - 535 kHz se clasifica como espectro protegido.

MX20 La banda de frecuencias 535 - 1705 kHz se emplea para la prestación del servicio de radiodifusión sonora en AM.

MX21 El 31 de agosto de 2015 se publicó en el DOF el Acuerdo por el cual se expide la Disposición Técnica IFT-001-2015: Especificaciones y requerimientos para la instalación y operación de las estaciones de radiodifusión sonora en amplitud modulada en la banda de 535 kHz a 1705 kHz.

MX22 El 28 de agosto de 1986 se firmó en la Ciudad de México, el Convenio entre México y los Estados Unidos de América, relativo al uso de la banda 535 - 1605 kHz por el servicio de radiodifusión en AM.

MX23 La coordinación para la operación de la banda de 535 - 1605 kHz, con otros países de América exceptuando los Estados Unidos de América, se realiza con base en el Acuerdo Regional sobre el servicio de radiodifusión por ondas hectométricas en la Región 2, firmado en Río de Janeiro, Brasil el 19 de diciembre de 1981, mismo que entró en vigor el 1 de julio de 1983.

MX25 El 11 de agosto de 1992 se firmó en Querétaro, Querétaro, el Acuerdo entre México y los Estados Unidos de América, relativo al uso de la banda de 1605 - 1705 kHz por el servicio de radiodifusión de AM. Las disposiciones del Acuerdo se aplican también para asegurar la compatibilidad entre estaciones de radiodifusión en esta banda y en el segmento de 1585 - 1605 kHz.

MX28 El 14 de agosto de 1987 se firmó en Lima, Perú, el Convenio Interamericano sobre el Servicio de Aficionados, cuyo propósito es autorizar temporalmente el ejercicio del Servicio de Aficionados en el territorio de un país cuando lo solicite otro Estado Miembro.

MX38A Las bandas de frecuencias 4.438 - 4.488 MHz, 5.25 - 5.275 MHz, 13.45 - 13.55 MHz, 16.1 - 16.2 MHz, 24.45 - 24.65, 26.2 - 26.42 MHz, 41.015 - 41.665 MHz y 43.35 - 44 MHz bajo la atribución al servicio de radiolocalización, se limitan a los radares oceanográficos que funcionan con arreglo a lo dispuesto en la Resolución 612 (Rev.CMR-12). La utilización de estas bandas de frecuencias por estaciones del servicio de radiolocalización no deberá causar interferencia perjudicial a las estaciones de los servicios fijo y móvil, ni deberá

reclamar protección contra interferencias perjudiciales provenientes de dichos servicios, de conformidad con los números 5.132A, 5.145A y 5.161A del RR.

MX68 Las bandas de frecuencias que se enlistan a continuación se encuentran designadas para aplicaciones industriales, científicas y médicas (ICM):

13.553 - 13.567 MHz	902 - 928 MHz	24 - 24.25 GHz
26.957 - 27.283 MHz	2400 - 2500 MHz	
40.66 - 40.70 MHz	5.725 - 5.875 GHz	

Los servicios de radiocomunicación que funcionan en estas bandas deben aceptar la interferencia perjudicial resultante de estas aplicaciones, de conformidad con el número 5.150 del RR. Los equipos ICM que funcionen en estas bandas estarán sujetos a las disposiciones del número 15.13 del RR.

MX84 La frecuencia portadora 26.1005 MHz es una frecuencia internacional de transmisión de información relativa a la seguridad marítima, de conformidad con el número 5.132 y los Apéndices 15 y 17 del RR. Esta frecuencia portadora se clasifica como espectro protegido.

MX85 El uso de la banda de frecuencias 26.96 - 27.41 MHz deberá sujetarse al Acuerdo por el que se fijan las condiciones de operación del servicio compartido para cortas distancias, Banda Civil. Dicho Acuerdo fue publicado en el DOF el 7 de febrero de 197**8**.

FIRMADO POR: LILIA EURIDICE PALMA SALAS
FECHA FIRMA: 2023/10/17 6:51 PM
AC: AUTORIDAD CERTIFICADORA
ID: 73010
HASH:
4F02A0485E4384ECA7CB88639732366C5DDFED21486A4C
7FF7098D997F10B6D9

FIRMADO POR: REBECA ESCOBAR BRIONES
FECHA FIRMA: 2023/10/17 7:09 PM
AC: AUTORIDAD CERTIFICADORA
ID: 73010
HASH:
4F02A0485E4384ECA7CB88639732366C5DDFED21486A4C
7FF7098D997F10B6D9