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