

Política General de Ciberseguridad y Seguridad de la Información del Instituto Federal de Telecomunicaciones.

Considerando

Primero.- Que el Instituto Federal de Telecomunicaciones (“IFT” o “Instituto”) es un órgano público autónomo, independiente en sus decisiones y funcionamiento, con personalidad jurídica y patrimonio propio, que tiene por objeto regular y promover la competencia y el desarrollo eficiente de las telecomunicaciones y la radiodifusión en el ámbito de las atribuciones que le confieren la Constitución Política de los Estados Unidos Mexicanos y en los términos que fijan la Ley Federal de Telecomunicaciones y Radiodifusión y demás disposiciones aplicables.

Segundo.- Que tiene a su cargo la regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, los recursos orbitales, los servicios satelitales, las redes de telecomunicaciones, incluyendo las redes públicas de telecomunicaciones, y la prestación de los servicios públicos de interés general de radiodifusión y de telecomunicaciones, así como del acceso a la infraestructura activa y pasiva y otros insumos esenciales, garantizando lo establecido en los artículos 6o. y 7o. de la Constitución Política de los Estados Unidos Mexicanos.

Tercero.- Que, adicionalmente, es la autoridad en materia de competencia económica de los sectores de radiodifusión y telecomunicaciones, por lo que en éstos ejercerá en forma exclusiva las facultades que el artículo 28 de la Constitución Política de los Estados Unidos Mexicanos, la Ley Federal de Competencia Económica y demás disposiciones legales aplicables establecen para la Comisión Federal de Competencia Económica y es la autoridad en materia de lineamientos técnicos relativos a la infraestructura y los equipos que se conectan a las redes de telecomunicaciones, así como en materia de homologación y evaluación de la conformidad de dicha infraestructura y equipos.

Cuarto.- Que de conformidad con la “Hoja de Ruta del Instituto Federal de Telecomunicaciones para el periodo 2021-2025”¹ (“Hoja de Ruta 2021-2025”), la visión del Instituto es ser una autoridad reguladora y de competencia independiente, eficaz y transparente, que contribuye al desarrollo de las telecomunicaciones y la radiodifusión y del ecosistema digital, al avance de la sociedad de la información y del conocimiento en nuestro país, así como el mejoramiento de la calidad de vida y las oportunidades de desarrollo para la sociedad, incluyendo usuarios, audiencias y sectores productivos.

Quinto.- Que en la Hoja de Ruta 2021-2025, como parte de las líneas de acción para “Asegurar la eficiencia interna en el desarrollo de las funciones regulatorias” se estableció la necesidad de “Fomentar la sistematización y digitalización de los procesos de trabajo internos y externos,

¹ Aprobada mediante Acuerdo P/IFT/161220/567 del Pleno del IFT.

minimizando el impacto administrativo y promoviendo un gobierno digital y abierto dentro del Instituto”.²

Sexto.- Que, en concordancia con los objetivos y estrategias fijadas en la Hoja de Ruta 2021-2025 y con las acciones previas en materia de gobierno electrónico, el Instituto ha implementado diversas acciones encaminadas a sistematizar y digitalizar sus procesos de trabajo internos, así como sus procedimientos y trámites disponibles al público en general, lo que ha dado como resultado, entre otros, que actualmente más del 99 % del total de trámites a cargo del Instituto se puedan realizar por medios electrónicos. Adicionalmente, a nivel interno el Instituto ha implementado diversas medidas para favorecer el trabajo en línea y ha fomentado el uso de herramientas electrónicas que faciliten los procesos internos de trabajo, con la finalidad de hacerlos más eficientes y ágiles.

Séptimo.- Que conforme a dicha Hoja de Ruta, el Instituto considera que por su adecuado posicionamiento en los temas relacionados con la seguridad, confianza e innovación, su extenso conocimiento de las redes e infraestructura de telecomunicaciones y sus atribuciones legales, debe tomar un rol activo en materia de ciberseguridad, a través del desarrollo y difusión de recomendaciones, lineamientos, disposiciones técnicas y/o buenas prácticas en materia de ciberseguridad, a partir de un enfoque basado en la gestión de riesgos y aumento de la resiliencia de los dispositivos y redes de telecomunicaciones³.

Octavo.- Que las acciones descritas en párrafos anteriores, aunadas a otras medidas transversales que ha adoptado el Instituto durante los últimos años en materia de digitalización, son un reflejo del compromiso que ha asumido el IFT haciéndolo un regulador de vanguardia, que fomenta el gobierno electrónico y la digitalización interna, en consistencia con su misión como órgano autónomo que tiene por objeto el desarrollo eficiente de las telecomunicaciones y radiodifusión y del ecosistema digital para el beneficio de la sociedad, incluyendo entre otros a usuarios, audiencias y sectores productivos.⁴

Noveno.- Que en función de lo anterior y en línea con las acciones y medidas transversales adoptadas en los últimos años en materia de gobierno digital y abierto, el Pleno del Instituto como órgano máximo de gobierno y decisión, considera que para el mejor desarrollo de los procesos de sistematización y digitalización organizacional, es indispensable fortalecer las medidas de protección de la información y de los recursos tecnológicos que garanticen una adecuada gestión de los riesgos en materia de ciberseguridad y, de manera más amplia, de seguridad de la información, que involucra la protección de equipos, servidores, dispositivos, sistemas electrónicos, redes y datos de la organización⁵ a través de una Política general de ciberseguridad y seguridad de la información.

² Línea de Acción Regulatoria T.1.2. para la Estrategia T.1.

³ Hoja de Ruta 2021-2025. p. 79.

⁴ *Ibidem*, p. 151.

⁵ Kaspersky. ¿Qué es la Ciberseguridad? Disponible en: <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>

Décimo.- Que si bien las políticas descritas en el párrafo anterior, contribuyen a crear conciencia y generar mecanismos, reglas y procesos relativos a la gestión de riesgos para la seguridad de la información, es importante reconocer que para generar una cultura organizacional de ciberseguridad, que permee a todas las áreas que integran el Instituto, resulta fundamental contar con directrices fijadas por su órgano máximo de gobierno, especialmente cuando estas políticas impactan de manera transversal a la organización e involucran, desde su confección, la clasificación y organización de información y archivos del Instituto, tanto para garantizar su seguridad y preservación, como para salvaguardar la accesibilidad a dicha información y archivos, cuando éstos sean de naturaleza pública, en términos de la legislación aplicable.

Décimo Primero.- En ese sentido, organismos como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) afirman que, en materia de políticas de seguridad digital, los organismos públicos deben predicar con el ejemplo, incluyendo la adopción de mejores prácticas de gestión de riesgos para la seguridad digital, con la finalidad de proteger las actividades gubernamentales.⁶

Décimo Segundo.- En el mismo sentido, la OCDE enfatiza que los riesgos a la seguridad digital son extremadamente dinámicos, con amenazas y vulnerabilidades en constante evolución que afectan a las tecnologías, productos y servicios utilizados de numerosas formas innovadoras en la economía y la sociedad,⁷ por lo que se recomienda establecer una serie de objetivos y directrices que permanezcan en el tiempo y que permitan a los involucrados coordinar sus acciones y progreso bajo esas directrices, es decir, con cierta flexibilidad.

Décimo Tercero.- Bajo estas consideraciones, se estima necesario fijar una serie de directrices institucionales, que fortalezcan las acciones de ciberseguridad y seguridad de la información del IFT, con la finalidad de generar, promover y garantizar una cultura organizacional en esta materia y sentar las bases generales para la adopción de las herramientas, procesos y mecanismos necesarios para su implementación.

En virtud de lo anterior y con fundamento en los artículos 1, 6, 7, 15 fracciones LII y LXIII, 16 y 17 fracciones X y XV de la Ley Federal de Telecomunicaciones y Radiodifusión; 118 de la Ley Federal de Competencia Económica; 158 de las Disposiciones Regulatorias de la Ley Federal de Competencia Económica para los sectores de telecomunicaciones y radiodifusión; y 1, 4 fracción I y 6 fracciones XXXII, XXXIII, y XXXVII del Estatuto Orgánico del Instituto Federal de Telecomunicaciones, el Pleno del Instituto Federal de Telecomunicaciones emite el siguiente:

⁶ OECD (2022), OECD Policy Framework on Digital Security, OECD Publishing, Paris, <https://doi.org/10.1787/a69df866-en> p. 21

⁷ *Idem*.

Acuerdo

Único.- Se expide la Política General de Ciberseguridad y Seguridad de la Información del Instituto Federal de Telecomunicaciones, para quedar como sigue:

Política General de Ciberseguridad y Seguridad de la Información del Instituto Federal de Telecomunicaciones

Artículo 1.- El objeto de la presente política es establecer las directrices generales en materia de ciberseguridad y seguridad de la información del Instituto Federal de Telecomunicaciones (“Instituto” o “IFT”), que contribuyan a la adecuada gestión de los riesgos para la protección de la información, del ecosistema digital institucional y de los recursos tecnológicos que dan soporte al cumplimiento de los objetivos del Instituto.

Artículo 2.- La presente política es de observancia obligatoria para todas las personas servidoras públicas del IFT al hacer uso de los recursos de tecnologías de la información y comunicaciones (“TIC”) del Instituto, y/o al utilizar Información que se encuentra bajo resguardo del Instituto.

Artículo 3.- Para efectos de la presente Política, las personas servidoras públicas a que se refiere el artículo anterior, serán consideradas Personas Usuarias.

Artículo 4.- El Pleno del Instituto reconoce que la información es uno de los activos esenciales para supervisar y promover el desarrollo eficiente de la radiodifusión y las telecomunicaciones, garantizando lo dispuesto en los artículos 6o y 7o de la Constitución Política de los Estados Unidos Mexicanos, así como para ejercer sus atribuciones en materia de competencia económica en estos sectores, por lo que está comprometido a implementar acciones que impliquen su protección en medios de almacenamiento físico y en el entorno digital.

Artículo 5.- En este sentido, se emiten las siguientes directrices en materia de ciberseguridad y seguridad de la información:

- I. El Instituto implementará las herramientas tecnológicas, mecanismos y controles que permitan preservar la seguridad de la información física y digital que se encuentre en posesión del Instituto.
- II. La información deberá categorizarse y preservarse conforme a los parámetros técnicos que en materia informática deriven de la presente política.
- III. El acceso a la información, por parte de las Personas Usuarias, se limitará a los permisos indispensables para el cumplimiento de sus funciones.

- IV. El Instituto promoverá la cultura de la seguridad de la información entre las Personas Usuarias y establecerá los mecanismos para capacitar y concientizar acerca de su relevancia.
- V. Se fortalecerán y mantendrán actualizados los mecanismos de ciberseguridad y seguridad de la información para la protección de las instalaciones, el Centro de Procesamiento de Datos, los equipos de cómputo y dispositivos móviles proporcionados por el IFT, así como la infraestructura de comunicaciones, sistemas de información y cualquier servicio tecnológico del Instituto.
- VI. La transferencia, almacenamiento y procesamiento de la información se realizará exclusivamente, y en todo caso, a través de los medios habilitados para tal efecto por el Instituto. Cuando dicha transferencia se realice a terceros que no sean Personas Usuarias, se establecerán los mecanismos tecnológicos que permitan identificar el origen, destino y conserven el registro del envío de la información.
- VII. El Instituto adoptará las medidas necesarias para evitar el almacenamiento y/o procesamiento de la información en servicios o dispositivos distintos a los proporcionados a las Personas Usuarias por el Instituto para el desempeño de sus funciones.
- VIII. Se implementarán mecanismos de monitoreo de los servicios tecnológicos, sistemas, infraestructura y redes institucionales a efecto de identificar de manera oportuna cualquier evento que pueda afectar la seguridad de la información.
- IX. Las Personas Usuarias son responsables de notificar de manera inmediata cualquier incidente identificado que afecte la seguridad de la información. Dicha notificación, será realizada a través de los mecanismos que el Instituto establezca para dicho propósito.
- X. El Instituto se reserva el derecho de suspender los privilegios de acceso a la información y/o cualquier recurso de TIC del Instituto, cuando se identifique que algún evento o acción realizada por las Personas Usuarias, pueda afectar la seguridad de la información.
- XI. El incumplimiento a la presente política tendrá como consecuencia las responsabilidades administrativas, civiles o penales a las que haya lugar.

Artículo 6.- Sin perjuicio del ejercicio de las atribuciones que correspondan a otras Unidades Administrativas o instancias del Instituto, corresponderá a la Unidad de Administración difundir y dar a conocer la presente política a todas las personas servidoras públicas del Instituto.

Artículo 7.- La aplicación e interpretación de la presente política corresponde a la Unidad de Administración, a través de la Dirección General de Tecnologías de la Información y Comunicaciones.

Transitorios

Primero.- La presente política entrará en vigor a los diez días hábiles a partir de su aprobación por el Pleno del Instituto.

Segundo.- Se instruye a la Unidad de Administración a llevar a cabo la difusión de la Política General de Ciberseguridad y Seguridad de la Información del Instituto Federal de Telecomunicaciones a través de los medios institucionales internos a partir de la aprobación del presente Acuerdo.

Javier Juárez Mojica
Comisionado Presidente*

Arturo Robles Rovalo
Comisionado

Sóstenes Díaz González
Comisionado

Ramiro Camacho Castillo
Comisionado

Acuerdo P/IFT/140224/61, aprobado por unanimidad en la V Sesión Ordinaria del Pleno del Instituto Federal de Telecomunicaciones, celebrada el 14 de febrero de 2024.

Lo anterior, con fundamento en los artículos 28, párrafos décimo quinto, décimo sexto y vigésimo, fracción I de la Constitución Política de los Estados Unidos Mexicanos; 7, 16, 23, fracción I y 45 de la Ley Federal de Telecomunicaciones y Radiodifusión, y 1, 7, 8 y 12 del Estatuto Orgánico del Instituto Federal de Telecomunicaciones.

*En suplencia por ausencia del Comisionado Presidente del Instituto Federal de Telecomunicaciones, suscribe el Comisionado Javier Juárez Mojica, con fundamento en el artículo 19 de la Ley Federal de Telecomunicaciones y Radiodifusión.

FIRMADO POR: RAMIRO CAMACHO CASTILLO
FECHA FIRMA: 2024/02/15 4:28 PM
AC: AUTORIDAD CERTIFICADORA
ID: 86767
HASH:
2E2EB5F4295F8C72AE898DC03DD5EB413060F3DA1C4EE7
A4A528EB256E88738E

FIRMADO POR: JAVIER JUAREZ MOJICA
FECHA FIRMA: 2024/02/15 4:38 PM
AC: AUTORIDAD CERTIFICADORA
ID: 86767
HASH:
2E2EB5F4295F8C72AE898DC03DD5EB413060F3DA1C4EE7
A4A528EB256E88738E

FIRMADO POR: SOSTENES DIAZ GONZALEZ
FECHA FIRMA: 2024/02/15 4:43 PM
AC: AUTORIDAD CERTIFICADORA
ID: 86767
HASH:
2E2EB5F4295F8C72AE898DC03DD5EB413060F3DA1C4EE7
A4A528EB256E88738E

FIRMADO POR: ARTURO ROBLES ROVALO
FECHA FIRMA: 2024/02/15 5:08 PM
AC: AUTORIDAD CERTIFICADORA
ID: 86767
HASH:
2E2EB5F4295F8C72AE898DC03DD5EB413060F3DA1C4EE7
A4A528EB256E88738E