**RECOMENDACIÓN QUE EMITE EL CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES RESPECTO CIBERSEGURIDAD.**

## Concepto de ciberseguridad.

La Unión Internacional de Telecomunicaciones (UIT), en su Recomendación UIT–T X.1205, define la ciberseguridad como:

> *La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:*
>
> - *disponibilidad;*
> - *integridad, que puede incluir la autenticidad y el no repudio;*
> - *confidencialidad."*

Fuente: http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

En el glosario del Programa Sectorial de Marina 2013-2018 (Diario Oficial de la Federación, 16 de diciembre de 2013), se define a la ciberseguridad como: Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno (Se asume ciberentorno como sinónimo de ciberespacio).

En forma práctica y sencilla, puede considerarse que ciberseguridad es la seguridad en el ciberespacio.

## Los riesgos en el ciberespacio.

El ciberespacio proporciona amplios beneficios en todos los ámbitos de la vida, no obstante, éste como cualquier otro espacio está sujeto a amenazas y vulnerabilidades.

A fin de lograr una mejor convivencia en el ciberespacio, es necesario conocer la triada amenaza-vulnerabilidad-riesgo: Amenaza es cualquier elemento o acción que pueda causar algún efecto negativo, pueden ser humanas, naturales, operacionales, tecnológicas o sociales; vulnerabilidad es la debilidad, falla o ausencia de controles de seguridad, que puede ser

explotada o aprovechada por una amenaza. Al identificar, analizar y evaluar ambos conceptos, se determinan los riegos y sus niveles, así como posibles grados de afectación. Si el riego no fue debidamente atendido, el resultado podrían ser afectaciones de diversas magnitudes, que se pueden traducir en pérdidas económicas, robo de información, afectación de las operaciones, daño de la imagen pública, entre otros.

Los ataques en el ciberespacio van más allá de una afectación de carácter técnico o tecnológico a una infraestructura o dispositivo conectado, pueden transgredir incluso psicológicamente a las personas que utilizan el ciberespacio para comunicarse, entretenerse o trabajar, ocasionado afectaciones como el ciberacoso, la cibermanipulación que son cada vez más evidentes en las redes sociales.

A las actividades malintencionadas, ilícitas o delincuenciales a través del ciberespacio, se les ha acuñado con nuevos conceptos, muchos de ellos sin definición formal pero que se han adoptado en forma convencional; por ejemplo, terrorismo es el concepto en el mundo físico, ciberterrorismo es el concepto en el ciberespacio.

Recientemente, el ***Foro Económico Mundial publicó su Informe de Riesgos Globales 2018***, que aborda algunos de los retos más fuertes que enfrentamos, como la pérdida de biodiversidad, las amenazas para la ciberseguridad, el aumento de las tensiones geopolíticas y el riesgo de que estalle otra crisis financiera; en materia de ciberseguridad indica que los ciberataques ocupan el lugar 3 en probabilidad de ocurrencia y el lugar 6 por su impacto negativo.

**Estudios sobre ciberseguridad.**

A fin de conocer el estado de la ciberseguridad en México, se hace referencia a estudios recientes elaborados por Organismos Internacionales:

El ***Informe de Ciberseguridad 2016*** elaborado por la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), se tienen 49 indicadores en 5 grupos: 1) Política y estrategia, 2) Cultura y sociedad, 3) Educación, 4) Marcos Legales y 5) Tecnología; señalando 5 grados de madurez (inicial, formativo, establecido, estratégico y dinámico) con los cuales el más bajo implica un grado de capacidad con la disposición a adoptar la seguridad, y el nivel más alto con capacidad de adaptarse dinámicamente. Por lo que respecta a México, 3 indicadores están en madurez inicial, 29 en formativo, 14 en establecido y 3 en estratégico.

El ***Índice Global de Ciberseguridad***, elaborado por la UIT, tiene cinco indicadores críticos para medir las capacidades nacionales de ciberseguridad, debido a que forman los elementos constructivos intrínsecos de cada cultura nacional: 1) Medidas Jurídicas, 2) Medidas Técnicas, 3) Medidas Organizativas, 4) Creación de Capacidades y 5) Cooperación; el índice más bajo que se puede obtener es 0 y el más alto es 1. En el índice publicado en **2015**, México obtuvo 0.3235; y en el índice publicado en **2017**, indica que México obtuvo 0.66; lo que significa que se tuvo una mejoría casi del doble, sin embargo, sigue siendo un índice lejano del 1.

**Política pública para ciberseguridad en México.**

En la presente Administración Pública Federal, se han realizado principalmente los siguientes planteamientos:

En el ***Plan Nacional de Desarrollo 2013-2018***, dentro de la meta nacional "México en paz", objetivo 1.2 "Garantizar la Seguridad Nacional", estrategia 1.2.3 "Fortalecer la inteligencia del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la Seguridad Nacional", están las siguientes líneas de acción: 1) Impulsar, mediante la realización de estudios e investigaciones, iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para fortalecer la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad. 2) Diseñar e impulsar una estrategia de seguridad de la información, a efecto de garantizar la integridad, confidencialidad y disponibilidad de la información de las personas e instituciones públicas y privadas en México.

El 08 de mayo de 2014 se publicó en el Diario Oficial de la Federación, la ***Política en materia de TIC de la Estrategia Digital Nacional, así como el Manual Administrativo de Aplicación General en las materias de Tecnologías de la información y Comunicaciones y de Seguridad de la Información (MAAGTICSI)***, que contiene un apartado de seguridad de la información, que establece el Sistema de Gestión de Seguridad de la Información (SGSI) para las dependencias de la Administración Pública Federal y la Procuraduría General de la República.

El ***Programa Nacional de Seguridad Pública 2014–2018***, contempla la estrategia 2.7 "Detectar y atender oportunamente los delitos cibernéticos". ***El Programa para la Seguridad Nacional 2014–2018***, cuenta con un apartado que contempla la Estrategia 2.1.2. "Desarrollar una política de Estado en materia de seguridad cibernética y ciberdefensa, para proteger y promover los intereses y objetivos nacionales".

En noviembre del 2017, durante la 3ª. Semana Nacional de Ciberseguridad, se publicó la ***Estrategia Nacional de Ciberseguridad para México***, un documento de 30 páginas, que plantea 1 objetivo general, 5 objetivos estratégicos, 3 principios rectores y 8 ejes transversales:

El **objetivo general** de la Estrategia Nacional de Ciberseguridad es identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano.

Para cumplir con el objetivo general, se establecen **5 objetivos estratégicos**:

1. Sociedad y derechos.
2. Economía e innovación.
3. Instituciones públicas.
4. Seguridad pública.
5. Seguridad nacional.

Para el desarrollo de la ENCS se consideran tres **principios rectores**:

A. Perspectiva de derechos humanos.
B. Enfoque basado en gestión de riesgos.
C. Colaboración multidisciplinaria y de múltiples actores.

Para alcanzar los objetivos estratégicos se desarrollarán **8 ejes transversales**:

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


Fuente: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Para la implementación de la Estrategia Nacional de Ciberseguridad, la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico "CIDGE", a través de la Subcomisión de Ciberseguridad, invitó al IFT a liderar el grupo de trabajo correspondiente al Objetivo Estratégico "Sociedad y Derechos" que indica: Generar las condiciones para que la población realice sus actividades de manera responsable, libre y confiable en el ciberespacio, con la finalidad de mejorar su calidad de vida mediante el desarrollo digital en un marco de respeto a los derechos humanos como la libertad de expresión, vida privada y protección de datos personales, entre otros. El pasado 29 de mayo se realizaron mesas de trabajo con objeto de diseñar la ruta crítica y plan de trabajo de cada uno de los temas que conforman el mencionado objetivo estratégico.

**Consideraciones.**

- En Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) publicada en el Diario Oficial de la Federación el 14 de julio de 2014, no se hace referencia específica a la ciberseguridad; sin embargo, el espectro, la infraestructura, equipos, servicios de telecomunicaciones y radiodifusión, son parte del ciberespacio, por lo que todos éstos deben contar con ciberseguridad.

- El IFT en su comunicado de prensa número 012/2018 del 15 de febrero de 2018, informó que aprobó su Programa Anual de Trabajo 2018, indicando que entre los estudios e informes que tiene programados para este año destaca el plan de acciones en materia de ciberseguridad.

**Recomendaciones.**

***Se recomienda que el IFT***, además del grupo de trabajo que dirige para implementar el objetivo estratégico "Sociedad y Derechos" de la Estrategia Nacional de Ciberseguridad, ***tenga una participación más activa en materia de ciberseguridad con base en sus atribuciones que le confiere la LFTR,*** como se indica a continuación:

A. Con base al segundo párrafo del Artículo 2: "El Estado, al ejercer la rectoría en la materia, protegerá la seguridad y la soberanía de la Nación y garantizará la eficiente prestación de los servicios públicos de interés general de telecomunicaciones y radiodifusión..."; y al cuarto párrafo del Artículo 7: "El Instituto es la autoridad en materia de lineamientos técnicos relativos a la infraestructura y los equipos que se conecten a las redes de telecomunicaciones, así como en materia de homologación y evaluación de la conformidad de dicha infraestructura y equipos".

   Se recomienda que el IFT analice y en su caso emita lineamientos técnicos indicando la seguridad que debiera cumplirse en la prestación de los servicios públicos de telecomunicaciones y radiodifusión, así como en la homologación y evaluación de la infraestructura y equipos correspondientes.

B. Derivado de la fracción XIV del Artículo 9: "Proponer a la Secretaría de Relaciones Exteriores la posición del país y participar, con apoyo del Instituto, en la negociación de tratados y convenios internacionales en materia de telecomunicaciones y radiodifusión"; y de la fracción XXXIV del Artículo 15: "Colaborar con el Ejecutivo Federal en la negociación de tratados y convenios internacionales en materia de telecomunicaciones y radiodifusión y vigilar su observancia en el ámbito de sus atribuciones".

   Se recomienda que el IFT proponga al Ejecutivo Federal, su apoyo y colaboración en materia de telecomunicaciones y radiodifusión, en las actividades que se están realizando para que nuestro país se adhiera al Convenio de Colaboración Internacional en materia de ciberseguridad conocido como Convenio de Budapest; en las correspondientes Comisiones de Estudio de la UIT que realizan trabajos sobre ciberseguridad, tales como

los derivados de la Resolución 50 sobre ciberseguridad (AMNT-16-Resoluciòn 50); así como a otros posibles acuerdos o convenios internacionales de ciberseguridad,

C. Referente a la fracción XXXVIII del Artículo 15: "Establecer y operar laboratorios de pruebas o autorizar a terceros a que lo hagan, a fin de fortalecer la autoridad regulatoria técnica en materias de validación de los métodos de prueba de las normas y disposiciones técnicas, aplicación de lineamientos para la homologación de productos destinados a telecomunicaciones y radiodifusión, así como sustento a estudios e investigaciones de prospectiva regulatoria en estas materias y las demás que determine, en el ámbito de su competencia, de conformidad con la disponibilidad presupuestaria autorizada"; y a la fracción XXXIX del mismo Artículo 15: "Realizar estudios e investigaciones en materia de telecomunicaciones y radiodifusión, así como elaborar proyectos de actualización de las disposiciones legales y administrativas que resulten pertinentes".

   Se recomienda que el IFT analice la posibilidad de establecer y operar laboratorios de pruebas, para llevar a cabo pruebas de vulnerabilidades a la infraestructura y equipos de las redes de telecomunicaciones y radiodifusión. También que el IFT realice estudios e investigaciones que contribuyan a conocer en forma periódica el estado de la ciberseguridad en México, así como para propiciar desarrollos encaminados a generar capacidades propias en ciencia y tecnología para la ciberseguridad. Como parte de los estudios e investigaciones que realice el IFT, se analice la creación de un Centro de Respuesta a Incidentes de Seguridad en la infraestructura de telecomunicaciones y radiodifusión.

D. Por lo que respecta al cuarto párrafo del Artículo 54: "Al administrar el espectro, el Instituto perseguirá los siguientes objetivos generales en beneficio de los usuarios:", fracción I: "La seguridad de la vida".

   Se recomienda que el IFT analice y en su caso defina los requisitos y/o actividades, que deben cumplirse para lograr la seguridad de la vida en la administración del espectro; inclusive se considere la posibilidad de realizar monitoreo que verifique el buen uso del espectro.

E. Se recomienda que el IFT cuente con un área específica encargada del tema de ciberseguridad, a efecto de que realice los análisis, estudios, investigaciones, pruebas, proyectos y propuestas de política regulatoria en materia de ciberseguridad.

F. Derivado de propuestas por parte de diversas organizaciones y especialistas, podría crearse una Agencia Nacional de Ciberseguridad en nuestro país; por lo que en caso de que se constituya dicha Agencia o similar, se recomienda que el IFT proponga al Ejecutivo Federal su apoyo y colaboración en materia de telecomunicaciones y radiodifusión en las actividades que se realicen en la citada Agencia.

**Conclusiones.**

Es muy complejo contener los riesgos en el ciberespacio, porque en gran medida son impredecibles, constantemente cambian, evolucionan, cada vez son más potentes, son de carácter transnacional y aprovechan los canales de la globalización. En virtud de que las telecomunicaciones y radiodifusión forman parte del ciberespacio, es indispensable que sus infraestructuras, equipos y servicios cuenten con ciberseguridad; por lo que es conveniente que el IFT conforme a sus atribuciones, tenga una mayor participación en las actividades que realizan para lograr la ciberseguridad en nuestro país y a nivel internacional.

***"La seguridad es indispensable en el mundo real y en el mundo virtual. Por un México Ciberseguro".***

**Dr. Ernesto M. Flores-Roux**
**Presidente**

**Lic. Juan José Crispín Borbolla**
**Secretario**

La Recomendación fue aprobada por el III Consejo Consultivo del Instituto Federal de Telecomunicaciones por unanimidad de votos de los Consejeros presentes: Rodolfo De la Rosa Rábago, Ernesto M. Flores-Roux, Gerardo Francisco González Abarca, Santiago Gutiérrez Fernández, Erik Huesca Morales, Salma Leticia Jalife Villalón, Federico Kuhlmann Rodríguez, Luis Miguel Martínez Cervantes, Alejandro Ulises Mendoza Pérez, Jorge Fernando Negrete Pacheco y Paola Ricaurte Quijano, en su V Sesión Ordinaria celebrada el 31 de mayo de 2018, mediante Acuerdo CC/IFT/310518/8.