

Competencias en materia de ciberseguridad

1. ¿En el marco de las competencias del ente regulador de telecomunicaciones de su país, tienen alcance para tratar los temas de ciberseguridad o es competencia de otra autoridad? Si es el caso especificar el nombre del ente.

<p>ANACOM Portugal</p>	<p>Regarding the cyber security issues, there is a cross-sector legal framework that identifies the Portuguese National Cybersecurity Centre (CNCS, https://www.cncs.gov.pt/certpt/) as the entity in charge for the continuous improvement of the national cyber security and the international cooperation, in coordination with all the competent authorities, and the implementation of measures and instruments required for the management of incidents or cyber attacks. For further information, consult the National Strategy for Cyberspace, at https://www.cncs.gov.pt/content/files/rcm_36-2015.pdf.</p> <p>To what refers specifically the electronic communications sector and according to the sector specific law (cf. English version at https://www.anacom.pt/render.jsp?contentId=975162&languageId=1), ANACOM is responsible to ensure the continuity in the integrity and security of public communications networks and publicly available services, including national and international interconnections (see chapter V, articles from 54A to 54G).</p>
<p>INDOTEL República Dominicana</p>	<p>De manera general, se tiene previsto que el Centro Nacional de Ciberseguridad (actualmente en creación) sea el órgano encargado del tema de ciberseguridad a nivel nacional. Sin embargo, de manera sectorial el INDOTEL tiene competencias y facultades para regular los aspectos de ciberseguridad que tocan directamente el sector de las telecomunicaciones.</p>
<p>SUTEL Costa Rica</p>	<p>Al respecto del tema de Ciberseguridad, la institución que lo lidera es el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Este año se integró un Comité Consultivo de Ciberseguridad, el cual es directamente coordinado por el MICITT. El Viceministro Sander Pacheco Araya es el encargo a nivel del Micitt de darle seguimiento al tema.</p>
<p>MINCOM Cuba</p>	<p>Si, Ministerio de Comunicaciones.</p>
<p>ENACOM Argentina</p>	<p>En materia de ciberseguridad el ENACOM trabaja junto con otros organismos nacionales en el tema, sin tener ninguno de ellos competencias exclusivas.</p>
<p>CNMC España</p>	<p>No. El Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional es el organismo competente en temas de ciberseguridad.</p>
<p>CONATEL Paraguay</p>	<p>la Secretaria de las Tics (Senatics), que a través del Plan Nacional de Ciberseguridad compromete a todos los entes públicos para lograr el objetivo. La Conatel tiene competencia en la Parte privada y la fiscalía tiene competencia en el Cibercrimen.</p>

<p>OSIPTEL Perú</p>	<p>El OSIPTEL no mantiene competencia sobre temas de ciberseguridad, en el Perú el ente normativo en dichos temas es la Secretaria de Gobierno Digital de la Presidencia del Consejo de Ministros</p>
<p>IFT México</p>	<p>En el caso del IFT sólo se encuentra relacionado con el aprovechamiento y explotación de las redes, como se expresa en la fracción IV del Artículo 28 de la Constitución Política de los Estados Unidos Mexicanos que dicta:</p> <p>«El Instituto Federal de Telecomunicaciones es un órgano autónomo, con personalidad jurídica y patrimonio propio, que tiene por objeto el desarrollo eficiente de la radiodifusión y las telecomunicaciones, conforme a lo dispuesto en esta Constitución y en los términos que fijen las leyes. Para tal efecto, tendrá a su cargo 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.</p> <p>Se debe considerar que desde 2005 se creó la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), un órgano colegiado que tiene por objetivo promover y consolidar el uso y aprovechamiento de las TIC en la Administración Pública Federal. La CIDGE en octubre del 2017, mediante acuerdo adoptado por unanimidad, creó la Subcomisión de Ciberseguridad, la cual está presidida por la Secretaría de Gobernación a través de la Comisión Nacional de Seguridad (CNS) por la División Científica de la Policía Federal.</p> <p>Uno de los objetivos de la subcomisión es articular los esfuerzos del Ejecutivo Federal y generar los criterios generales para que todas las dependencias y entidades de la Administración Pública Federal contribuyan a la generación de la Estrategia Nacional de Ciberseguridad (ENCS) y den seguimiento a la misma mediante acciones generales y específicas. Como resultado, la ENCS (https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf) fue publicada el 13 de noviembre de 2017. La ENCS es de naturaleza transversal y se articula con otros programas y estrategias y se desprende de lo señalado en el propio Plan Nacional de Desarrollo 2013-2018, en apego a los valores y principios que establece la Constitución Política de los Estados Unidos Mexicanos.</p> <p>Derivado de la publicación de la ENCS se establecieron ocho ejes transversales a efecto de fortalecer las acciones en materia de ciberseguridad que permitan el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano. Atendiendo al aumento de riesgos, ataques cibernéticos y al surgimiento de nuevas técnicas para aprovechar vulnerabilidades de los productos TIC.</p>

	<p>En este último punto sobre surgimiento de nuevas técnicas para aprovechar vulnerabilidades de los productos TIC, el Instituto tiene atribuciones de acuerdo al Estatuto Orgánico del IFT en su artículo 23, que dicta que la Dirección General de Regulación Técnica –de la Unidad de Política Regulatoria (UPR)- “tendrá a su cargo la elaboración y proposición de normas y disposiciones técnicas, reglas, procedimientos de evaluación de la conformidad, procedimientos de homologación y certificación, lineamientos y planes técnicos generales, lineamientos relativos a la aplicación del reconocimiento mutuo de la evaluación de la conformidad, así como la emisión de opiniones técnicas que le soliciten, [...] Coadyuvar en el ámbito técnico en la coordinación de los estudios e investigaciones que realicen los concesionarios y que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones, para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional”.</p>
CRC Colombia	<p>La CRC tiene unas competencias en materia de ciberseguridad que le otorgó la POLÍTICA NACIONAL DE SEGURIDAD DIGITAL, el documento CONPES 3854 disponible en (https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf). de acuerdo con lo anterior el año pasado se presentó un proyecto de gestión de riesgos de seguridad digital para operadores de telecomunicaciones.</p>