#CubaInformatiza #Cuba ACTUALIZA SU MARCO JURÍDICO EN MATERIA DE TELECOMUNICACIONES Y TIPIFICA INCIDENTES DE CIBERSEGURIDAD EN LA GACETA OFICIAL No. 92 DE 2021…



¿Cuáles son los instrumentos jurídicos que se ponen en vigor en la Gaceta Oficial No. 92 de 2021?

El Decreto-Ley No 35 de las Telecomunicaciones, las Tecnologías de la Información y la Comunicación (TIC) y del Uso del Espectro Radioeléctrico; del 13 de abril de 2021.

El Decreto 42 "Reglamento General de Telecomunicaciones y de las Tecnologías de la Información y la Comunicación", del 24 de mayo de 2021.

El Decreto 43 "Reglamento sobre el Uso del Espectro Radioeléctrico", del 24 de mayo de 2021.

La Resolución No. 108 "Reglamento de Interconexión, acceso e instalaciones esenciales de redes de telecomunicaciones", del 9 de agosto de 2021, del Ministerio de Comunicaciones.

La Resolución No. 107 "Reglamento para el uso de los servicios de radiocomunicaciones por satélite" del 9 de agosto de 2021, del Ministerio de Comunicaciones.

La Resolución No. 105 "Modelo de Actuación Nacional para la respuesta a

incidentes de Ciberseguridad", del 9 de agosto de 2021, del Ministerio de Comunicaciones.

Todas estas normativas puestas en vigor es la Gaceta Oficial No. 92 de 2021, es importante y necesario que los cubanos las conozcamos, aunque por la extensión de su contenido al leerlas pudieran surgirles interrogantes. Estas pueden ser algunas de ellas:

¿Qué ventajas nos reporta a los cubanos la puesta en vigor del Decreto Ley No 35 de las Telecomunicaciones, las Tecnologías de la Información y la Comunicación (TIC) y del Uso del Espectro Radioeléctrico y sus normativas?

• Ordena de forma coherente en un solo documento, los objetivos del Estado Cubano en relación con la infraestructura y los servicios de Telecomunicaciones y las TIC, y el uso del espectro radioeléctrico para la construcción de una sociedad de la información y el conocimiento, centrado en la persona, con visión integradora y orientada al desarrollo sostenible, en la que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento en la mejora de su calidad de vida.

• Establece los derechos y deberes de los operadores nacionales (Etecsa, Radio Cuba, Movitel y Telecable Internacional), los proveedores y de los usuarios, lo cual posibilita un ordenamiento armónico en función de elevar la calidad en la prestación de estos servicios.

• Define los servicios que se encuentran considerados como Servicio Universal de Telecomunicaciones, que el Estado cubano, a través del operador público (Etecsa), debe garantizarle a los ciudadanos.

¿Qué implica para los cubanos la aprobación del Modelo de Actuación Nacional para la respuesta a incidentes de Ciberseguridad?

• Habilita a la persona para ejercer sus derechos de notificar o denunciar ante los órganos, órganismos de la Aministración del Estado (OACE) y entidades, cualquier afectación que pueda ser tipificada como incidente, y que lo afecte en lo personal, a su familia, o a la sociedad en general.

• El derecho a recibir una respuesta, que puede ser una orientación concreta inmediata o una posterior a la investigación.

• Forma parte de la creación de valores de conducta cívica de los ciudadanos, de respeto, disciplina y contribución al bienestar social.

• En caso de notificaciones o acusaciones falsas, se procederá según la Ley contra el infractor.

¿Qué debemos hacer los cubanos para notificar un incidente de ciberseguridad?

• Si la notificación proviene de una persona natural, no está obligada a emplear la tipificación establecida, aunque es muy favorable que conozca cuáles son las categorías y subcategorías contempladas, lo que ayuda culturalmente a identificar las amenazas. En el caso de las personas jurídicas, estas tienen la responsabilidad de notificar usando la tipificación con independencia de que pueda ser rectificada

por la Oficina de Seguridad de Redes Informáticas (OSRI).
• Asumir la responsabilidad de la información que se aporte, para lo que se identificará con sus datos personales y de la entidad que representa (si fuese el caso), así como tributar detalles que faciliten la gestión, incluidos en el Anexo III del Reglamento. La vía podrá ser cualquiera de las que se publiquen por la OSRI.
• Los interesados se pueden comunicar con la OSRI a través de los siguientes canales de comunicación:
Sitio web www.osri.gob.cu en el acápite incidentes.
Correo electrónico reportes@osri.gob.cu
Número único de atención a la población 18810.
¿Puede una notificación convertirse en un proceso penal?
Si como resultado de la investigación, existen los elementos que justifiquen una acusación que pueda dar lugar a uno o más delitos tipificados en el código penal vigente, procede iniciar un proceso penal.
¿Qué justifica que un evento de carácter social, político, económico o de otra índole, se coincidente de ciberseguridad sin repercusión tecnológica en la seguridad?
La definición de incidente de ciberseguridad, aunque se ratifica en el Reglamento, está dada por una norma superior (Decreto 360/2019) y refiere textualmente: "Se considera un incidente de ciberseguridad cualquier evento que se produzca de forma accidental o intencional, que afecte o ponga en peligro las tecnologías de la información y la comunicación o los procesos que con ellas se realizan". Lo que significa en términos prácticos que un incidente puede estar asociado a cualquier proceso con independencia de su naturaleza, siempre y cuando se soporte sobre las TIC.
Otro elemento a tener en cuenta es que los referidos procesos tienen lugar en el ciberespacio, conceptualizado como "el ambiente virtual y dinámico, definido por tecnologías, equipos, procesos, sistemas de información, control y comunicaciones que interactúan entre sí, y con las personas, y en el que la información se crea, procesa y trasmite".
Es una práctica mundial con resultados probados a favor de la tranquilidad ciudadana, el orden interior y la seguridad de los Estados. Todos los Estados se protegen a lo interno, aunque algunos disimuladamente aboguen por libertades en lo internacional con marcados intereses de injerencia, así como de facilitar la labor de sus agencias de inteligencia.
¿Qué relación tiene el modelo con el régimen de contravenciones?
Cualquier incidente que, al ser investigado y dictaminado por la entidad facultada, puede conllevar a la aplicación de sanciones administrativas, contravenciones o proceso penal.
¿Qué aspectos debemos tener en cuenta los cubanos al emplear las TIC, para evitar incidentes de ciberseguridad?

Es muy importante conocer las buenas prácticas y medidas de seguridad en el empleo de las Telecomunicaciones y las TIC, fundamentalmente en el manejo de terminales (computadoras, celulares, tabletas y otros dispositivos), para actuar responsablemente.

Conocer las amenazas que pueden estar presentes al consumir un servicio (conectarse una red, crearse un perfil, colocar una información en cualquier formato, establecer un intercambio de mensajería, video llamadas, o cualquier otra facilidad). Por ejemplo, en las plataformas internacionales incluidas las redes sociales y servicios administrados por operadores y proveedores extranjeros, operan y se administran desde sus infraestructuras en el exterior del país y por sus funcionarios, lo que implica que la gestión de incidentes en este contexto es muy limitada.

Tener en cuenta que, aunque existen relaciones entre los países para gestionar incidentes, estos se corresponden con aquellos que representan alta peligrosidad o impacto sobre los estados y sus infraestructuras vitales, no asociados como regla a personas naturales.

Crear una cultura de consultar sitios destinados a la divulgación de vulnerabilidades y formación de habilidades para proteger la información personal y garantizar seguridad durante la interacción en el ciberespacio, debe ser una premisa para el empleo responsable de las Telecomunicaciones y las TIC. Es muy nociva la práctica de consumir servicios sin antes conocerlos.

¿Cómo se aborda la actuación ante incidentes de ciberseguridad en otros países?

Son muchos los estados que han creado normas jurídicas de alto nivel para reglamentar estos temas, todos bajo las mismas premisas: garantizar su defensa y seguridad nacional, con énfasis en la tranquilidad ciudadana.

En el caso concreto del modelo de actuación, es una práctica internacional, tener establecida la conceptualización de sistemas de trabajo que contribuyan a la dirección (coordinación, gestión) cada vez más eficaz de las organizaciones que según sus roles están involucradas con la protección de sus ciberespacios nacionales, e incluso en su inserción en mecanismos regionales y globales para gestionar incidentes de ciberseguridad.

Por ejemplo, en España existe el Real Decreto 12, del 7 de septiembre de 2018, “De seguridad de las redes y sistemas de información”, el cual regula la seguridad de las redes y los sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establece un sistema de notificación de incidentes. El referido Decreto establece además un marco institucional para la aplicación del decreto y la coordinación entre las autoridades competentes.

Finalmente, sugerimos a los interesados en estos temas que para mayor información consulten en el portal web #Cubadetate el siguiente link: http://www.cubadebate.cu/…/cuba-actualiza-marco…/

Para esclarecer sus dudas también pueden contactar con el Ministerio de Comunicaciones (MINCOM) a través del sitio web www.mincom.gob.cu; por el correo electrónico atención.poblacion@mincom.gob.cu; y por la línea única de atención a la ciudadanía 80011011.