Cuba celebra la II Jornada Nacional de Ciberseguridad del 20 al 30 de noviembre con la voluntad política de **#CiberseguridadParaTodos**

A través de los avances tecnológicos y la aparición de nuevas plataformas tecnológicas y aplicaciones incrementan el acceso a la información y al conocimiento

La irrupción de Internet y las Tecnologías de Información y Comunicación en todas las esferas del desarrollo humano, ha sido sin dudas, uno de las mayores y más importantes transformaciones, no sólo en los hábitos de consumo, también en los del desarrollo cognitivo y acceso a la información.

- **Ver además:** II Jornada Nacional de Ciberseguridad

Es necesario desarrollar políticas de acuerdo con el vertiginoso desarrollo y alcance que tienen algunos procesos virtuales, que conocemos de la vida física. Entre ellos, la gestión de la participación ciudadana, hechos de violencia, bullying y linchamientos virtuales y, entre otros, la ciberseguridad.

> El termino ciberseguridad de un país se relaciona con varios aspectos, como su capacidad para responder a eventos de seguridad a gran escala, su marco legal en esa área, la

protección de sus infraestructuras críticas, su capacidad para colaborar con otros países y la cultura de seguridad que pueda existir entre su población. Esa es una tarea compleja al requerir iniciativas a gran escala, pero que resultan imprescindibles en la actualidad, debido a las amenazas y ataques informáticos que aumentan cada día, en cantidad, frecuencia, impacto y nivel de sofisticación.

- Ver además: 30 de noviembre: Día Internacional de la Seguridad de la Información

La ciberseguridad constituye una prioridad para el Estado cubano desde todos los ámbitos de la sociedad. Así se ha expresado en disímiles acciones emprendidas, entre ellas la búsqueda de soluciones legales en correspondencia con los niveles tecnológicos alcanzados.

Entre las primeras, destaca la Política para el perfeccionamiento del sistema de la informatización de la sociedad. De esta forma, se ha incrementado el acceso a la información y al conocimiento a través de los avances tecnológicos, no solo con el incremento de conectividad y la telefonía móvil, también por la aparición de nuevas plataformas tecnológicas y aplicaciones.

Sobre la protección de datos personales, la estrategia gubernamental ha estado caracterizada por concebir la protección de la información

en un sentido general orientada a la preservación de la confidencialidad, la integridad y disponibilidad de esta sin percibir los daños que desde lo individual se le ocasionan al titular de los datos personales.

Aun cuando había referencia en la Constitución del ‘40 a lo que, de manera universal, se reconoce como derecho fundamental basado en la inherencia de la dignidad humana de las personas, lo cierto es que no fue hasta el año 2019, con la aprobación de la Constitución de la República de Cuba , que se reconoció dicha necesidad.

> ARTÍCULO 48: "Todas las personas tienen derecho a que se les respete su intimidad personal y familiar, su propia imagen y voz, su honor e identidad personal”

Desde entonces, se han desarrollado paulatinamente acciones para dar cumplimiento a lo legislado en la Ley de Leyes, muestra de ello es la Ley 149 "De Protección de Datos Personales" que garantiza a los cubanos el control sobre sus datos y evita cualquier invasión en la transmisión de sus derechos personales, íntimos o no.

> «La Ley de Protección de Datos Personales es la concreción de la prioridad que exige para Cuba contar con una regulación jurídica de este tipo, donde se delimiten los principios y garantías fundamentales para la protección del titular de la información personal y elevar la percepción ciudadana de riesgo ante el destino y tratamiento de sus datos»

El país también cuenta con una norma jurídica donde se asocian incidentes de ciberseguridad y tipificaciones que superan los límites de lo tecnológico.

El Decreto-Ley No 35 de “las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y del Uso del Espectro Radioeléctrico” y la Resolución 105 “Modelo de Actuación Nacional para la respuesta a incidentes de Ciberseguridad” establecen un grupo de objetivos, normas y procedimientos en los que se refleja el compromiso contraído con el pueblo cubano y cómo se implementan para alcanzarlos.

> **El decreto ley “Sobre la Seguridad y Protección de la Información Clasificada y Limitada”** establece las reglas para

garantizar la seguridad y protección de aquella información y datos en cualquier soporte, que reflejen la actividad del Estado o información emitida por otra persona jurídica o natural, siempre que sea reconocida legalmente por el Estado cubano, cuando su divulgación o conocimiento no autorizado, alteración o no disponibilidad, le represente un riesgo, amenaza o daño.

Por su parte el Decreto ley **"Sobre el Desarrollo, la Aplicación y Uso de los Dispositivos de Protección Criptográfica y Servicios en la Esfera de la Criptografía en la República de Cuba"** estipula el ordenamiento del desarrollo científico y técnico, la aplicación y el uso de los dispositivos de protección criptográfica, la organización y funcionamiento de los servicios en la esfera de la criptografía, y el funcionamiento del sistema de trabajo nacional para asegurar integralmente la calidad de los citados productos y servicios; informaron los ponentes del Ministerio del Interior.

¿Qué hacer 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.

Se pueden comunicar con la OSRI a través de su sitio web https://www.osri.gob.cu/en el acápite incidentes , por el correo electrónico reportes@osri.gob.cu ó por el número único de atención a la población 18810

Aun cuando son necesarias las leyes para regular lo que concierne a

esta temática, es importante también que la ciudadanía tome conciencia de la importancia de proteger sus datos. Por ello, hoy queremos traerte algunos consejos que puedes poner en práctica en tu centro de trabajo, estudio o en la familia.

- Confirma la identidad de quien te solicite información: Seguro has recibido o conocido de aquellos ciberataques de personas que piden números de cuenta, te envían enlaces diciendo que vieron una foto tuya en tal sitio, o te solicitan cualquier otra información personal. Para ello se hacen pasar por proveedores, donantes u otros miembros de la entidad que tienen una excusa aparentemente legítima, o incluso, haciéndose pasar por persona cercanas a ti. Desconfía siempre, comunícate con esa persona y asegúrate de qué es lo que te pide y con qué fines.
- Mantente informado por fuentes oficiales sobre los principales —y más comunes— ciberataques, ciberamenazas y vulnerabilidades: Busca ayuda profesional, si la necesitas, ante una situación de estas.
- Cuidado con las contraseñas: Estas son de uso personal y privado. No la compartas a menos que necesites una urgencia. No utilices la misma en todos los programas y/o sistemas. Si necesitas anotarla o guardarla, hazlo en un sitio seguro y privado. Actualízala con frecuencia.
- Lee cuidadosamente las políticas de privacidad: En la actualidad, la mayoría de los sitios y aplicaciones, una vez los abres o instalas, contienen una serie de requisitos de utilización. En ellos se deja claro los fines de utilización de tus datos personales.
- No instales programas de fuentes desconocidas: Los avances tecnológicos y la inteligencia artificial de muchos dispositivos ya son capaces de reconocer si un programa, software o aplicación es seguro o no. Asegúrate de estar instalando correctamente la versión oficial; este consejo está muy relacionado con el anterior.
- Utiliza antivirus: Antes de utilizar cualquier dispositivo electrónico con acceso a Internet (móviles, computadoras) debes instalar un antivirus. Es importante también que lo tenga actualizado.

Descargar

Gaceta Oficial No. 90 Ordinaria de 25 de agosto de 2022

- Ley 149/2022 “De Protección de Datos Personales”
- Resolución 58/2022 “Reglamento para la Seguridad y Protección de los Datos Personales en Soporte Electrónico”

Gaceta Oficial No. 92 Ordinaria de 17 de agosto de 2021

- Decreto-Ley 35/2021 “De las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y el uso del Espectro Radioeléctrico”
- Decreto 42/2021 “Reglamento General de Telecomunicaciones y las Tecnologías de la Información y la Comunicación”
- Decreto 43/2021 “Reglamento sobre el uso del Espectro Radioeléctrico
- Resolución 105/2021 “Reglamento sobre el Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad”
- Resolución 107/2021 “Reglamento para el uso de los Servicios de Radiocomunicaciones por Satélites”
- Resolución 108/2021 “Reglamento de Interconexión, Acceso e Instalaciones Esenciales de Redes de Telecomunicaciones”

Con información de CUBAHORA y GRANMA