La ciberseguridad: Reto crucial de las Telecomunicaciones

14/11/2019



Inmersos en el proceso de Informatización de la sociedad cubana y con la importancia que revierte la misma en el desarrollo futuro de la nación descorrió sus cortinas el II Taller Ciberseguridad en las Telecomunicaciones.

Mayra Arevich, presidenta de ETECSA, significó el peso que en la actualidad tiene generar espacios de socialización del conocimiento para aprender a dar soluciones y pasos sólidos en el camino hacia una internet segura.

Destacó la responsabilidad de la empresa, en medio de un escenario hostil, de ataque cibernéticos y recrudecimiento del bloqueo económico impuesto por Estados Unidos en todos los frentes, y urge estar preparados para coexistir bajo semejante entorno y cualquier otro que pueda presentarse.

Exhortó a trabajar bien y rápido en busca de asegurar con cada acción el propósito encomendado por la dirección del país, adentrarnos en cuestiones como el comercio electrónico, mejorar las plataformas e infraestructura…

Asimismo sentenció que Ciberseguridad no es más que un puente para entre todos llegar a un proyecto de sociedad informatizada de forma segura.

Enrtrando en materia, el II Taller Ciberseguridad en las Telecomunicaciones Etecsa 2019, contó este miércoles con la ponencia Internet de los Objetos, Retos y Tendencias de la Ciberseguridad, de Ricardo Maceo.

El internet de los objetos que cotidianamente utilizan las personas es el más conocido, pero donde este alcanza su mayor desarrollo actualmente es en los elementos de uso industrial, el cual precisa mayores inversiones y demanda gastos superiores de energía.

En este campo el reto fundamental consiste en el logro de la seguridad, elemento que más preocupa a desarrolladores y clientes en todo el mundo en cuanto a la conectividad, pues impide su progreso.

“Cuando se realiza un ataque a las industrias se perjudica también a las personas. Es por esta razón que los centros esenciales donde atacan los cibercriminales son las empresas de telecomunicación y de servicios en general”, explicó Maceo.

El ponente señaló entre las principales formas de ataque las configuraciones y redes inseguras, identificaciones falsas, falta de actualizaciones de los dispositivos y las violaciones de conectividad físicas de los mismos.

Dispositivos móviles seguros

La conferencia Seguridad en dispositivos móviles de Noslen Olavarrieta estuvo centrada en la evolución de estos artefactos tecnológicos y las formas en que en la actualidad pueden ser objetos de ciberataques.

La mayor parte del consumo de internet se realiza hoy desde los dispositivos móviles. Con el paso de los años ha ido creciendo el número de usuarios de teléfonos inteligentes a nivel global, los que principalmente se utilizan para acceder a las redes sociales, sitios de compra en internet y para la búsqueda de información.

“Google Play y AppStore son las fundamentales tiendas de aplicaciones que emplean las plataformas de los teléfonos y tienen una serie de mecanismos que garantizan hasta cierto punto que las aplicaciones que se compren aquí y se instalen en ellos sean seguras, pero no es totalmente confiable. Existen otras alternativas para realizar esta misma función, que facilitan los ataques de los dispositivos” dijo Olavarrieta.

Según informó Noslen Olavarrieta, para contribuir a la seguridad en este caso es importante establecer mecanismos de bloqueos en los teléfonos personales, mantener actualizados sus sistemas operativos, descargar las aplicaciones de tiendas oficiales, no abrir correos de dudosa procedencia y tener cuidado con el acceso a las Wifi.