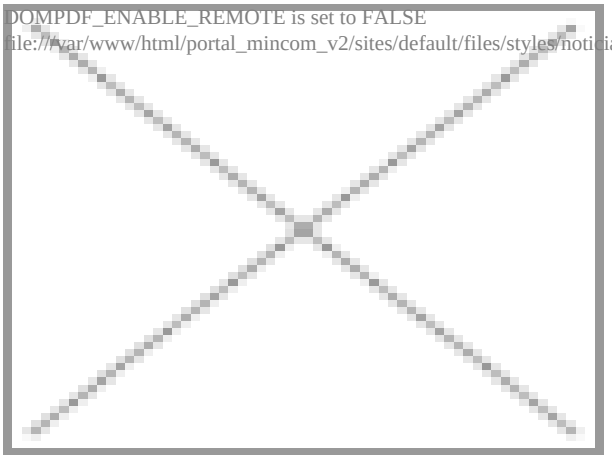

Source:
Tomado de CubaSí

El crecimiento en el uso de las Tecnologías de la Información y la Comunicación, TIC, en Cuba, con más de 8,4 millones de usuarios conectados a internet, de ellos más de 6,8 millones a través de celulares y un incremento de los pagos electrónicos mediante las pasarelas Transfermóvil y EnZona, han creado condiciones para que también se incrementen las amenazas cibernéticas, abarcando desde ataques básicos de malware hasta intrusiones más complejas. En este contexto, estaremos dialogando con Daniel Ramos Fernández, director de negocios digitales de la Empresa de Telecomunicaciones de Cuba (ETECSA) y experto en sistemas informáticos y ciberseguridad, sobre algunos de los desafíos que se prevén en el campo de la ciberseguridad para el presente año.

OPS: Según la empresa de seguridad cibernética, Kaspersky, en el último año en América Latina los ataques de malware contra computadoras y dispositivos móviles han experimentado un aumento en cuanto a intentos de ataques de phishing y troyanos bancarios. Los sectores de gobierno y finanzas han sido los más afectados, al igual que los internautas. De enero a septiembre de 2023, a través del Centro Nacional de Ciberseguridad y del Centro de Operaciones de Seguridad de la Empresa de Telecomunicaciones de Cuba, ETECSA, se detectaron y gestionaron más de 2600 incidentes, un 70% en personas naturales.

Estos estuvieron asociados a la ocurrencia de ciberataques de denegación de servicios, el envío y recepción de correos no deseados, tráfico malicioso generado por códigos malignos, escaneos de servicios y explotación de vulnerabilidades que han comprometido sitios web y otros elementos informáticos y en el caso de las personas naturales, ciberacoso, suplantación de identidad, y estafas a través de las redes sociales digitales y canales electrónicos de pago. El principal desafío para este año es la implementación de acciones efectivas para crear una cultura en el uso seguro y responsable de las TIC en directivos, especialistas y la población.

DRF: El año 2023 estuvo marcado por un incremento de los ciberataques a nivel mundial, poniendo en riesgo la seguridad de las empresas y los datos de las personas. El error humano es una de las principales causas de ciberincidentes en las entidades, donde prevalecen violaciones de las políticas de seguridad de la información por parte de los responsables de seguridad informática y de los usuarios de estas tecnologías. Se usan contraseñas débiles y no se cambian de manera oportuna; el personal visita sitios web no seguros y no se actualiza el software del sistema o las aplicaciones cuando es necesario.

El uso de servicios o dispositivos sin una garantía de seguridad es otro factor importante que ocasiona ciberincidentes. En este sentido hemos detectado la utilización de sistemas y dispositivos no autorizados para compartir datos que tienen un carácter confidencial. Otra acción reportada fue la instalación de software no oficial en dispositivos de trabajo. A todas estas problemáticas debemos prestarle una atención particular en la próxima etapa.

En varios organismos y entidades es necesario crear las estructuras para la atención a la ciberseguridad; en otras avanzar en el completamiento, preparación y gestión del personal del área. En este año se gradúan los primeros ingenieros que cursan la carrera de ciberseguridad en la Universidad de las Ciencias Informáticas, UCI; pero hay que agilizar la formación emergente de especialistas en cursos cortos, ampliar la cantidad de universidades con planes de formación en pregrado, posgrado y técnico superior universitario.

OPS: Un reto de primer orden es avanzar en la investigación, el desarrollo y la innovación (I+D+i) en temas de ciberseguridad, con la participación de los actores con posibilidades de aportar en este asunto. Si bien es cierto que los ciberdelincuentes continuarán aprovechando los avances en Inteligencia Artificial (IA) para cumplir sus propósitos delictivos, se abren nuevas oportunidades para el desarrollo de soluciones innovadoras y eficaces para proteger a nuestras redes y servicios aprovechando la IA y la analítica de datos.

Es imprescindible que en este año se potencie la creación de entidades estatales de ciberseguridad que den soluciones integrales e incrementen la prestación de servicios en los diferentes sectores. Una prioridad será el acompañamiento al proceso de bancarización con altos niveles de seguridad en las organizaciones tecnológicas involucradas.

DRF: La continuidad en el fortalecimiento de la seguridad tecnológica en el sistema bancario; en las infraestructuras críticas vinculadas a las TIC, las Tecnologías Operacionales (TO) y la automática; el desarrollo del antivirus nacional, Segurmática; la consolidación de plataformas nacionales como toDus, Picta y Apklis que garantizan una mayor soberanía tecnológica y el perfeccionamiento del modelo de actuación ante incidentes, son asuntos que requieren de la mayor atención.
Agregaría que las normas jurídicas en esta materia, precisan de una actualización permanente, porque surgen a una gran velocidad nuevas problemáticas y tecnologías que impactan de inmediato en la seguridad cibernética. Hoy la norma principal es el Decreto No.360; pero tenemos que aspirar a tener una ley como norma superior.

OPS: Este será un año de consolidación del trabajo del Grupo Nacional de Ciberseguridad y de sus grupos provinciales en el propósito de implementar las medidas que correspondan, para la protección del ciberespacio en cada provincia y municipio. En noviembre de 2024 se realizará la III Jornada Nacional de Ciberseguridad, con la participación de expertos y especialistas de varios organismos y territorios. El resultado esperado debe estar en correspondencia con el crecimiento logrado en los servicios de la telefonía móvil, internet, la informatización de los procesos y la transformación digital de la sociedad cubana.