DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png
Ministry of Communications
Published on *Ministry of Communications* (https://www.mincom.gob.cu)

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/seguridad_28_de_mayo.jpg
Seguridad
Source:
tomado del periódico Granma

Ante la llamada infodemia y los millones de noticias que circulan en la red acerca del nuevo coronavirus, los ciberdelincuentes han encontrado una nueva manera de «atrapar» a los usuarios

Aunque quizá sea demasiado temprano para hablar de las consecuencias que ha dejado el SARS-COV-2, más allá del lamentable efecto en la salud humana o, incluso, en la esfera de las finanzas y la economía mundial, esta pandemia ha puesto de relieve la necesidad de acelerar los procesos de transformación digital.

En el actual contexto, donde actividades tan cotidianas como ir al trabajo o la escuela han tenido una expresión desde el plano virtual, se confirma la necesidad de encontrar vías alternativas y mecanismos no tradicionales que faciliten la operatividad de ciertas labores, aunque estas se desarrollen desde la comodidad del hogar.

Cambiar estos paradigmas conlleva no solo darle un nuevo sentido a las actividades profesionales y los entornos en que se desarrollan, sino también pensar en la infraestructura, accesibilidad a datos y seguridad informática, que deben tener las empresas y sus trabajadores para asumir esa metamorfosis.

Y es que, ante la llamada infodemia y los millones de noticias que circulan en la red acerca del nuevo coronavirus, los ciberdelincuentes han encontrado una nueva manera de «atrapar» a los usuarios.
Ante esta realidad, que es también un problema global, es bueno recordar algunas de las nociones que defiende y aplica Cuba en materia de seguridad informática.
«Lo primero sería entender que la informatización de la sociedad es compleja y transversal, pues impacta prácticamente en todos los ámbitos de la vida del país e implica, entre otras cuestiones, habilitar aplicaciones, procesos digitalizados, trámites y servicios en el entorno de internet.

«No obstante, para hacer todo eso, resulta necesaria la implementación de tecnologías de seguridad para la autenticación o legitimación de las personas que interactúan con dichas plataformas informatizadas; el trabajo con documentos, también digitales, y la validación de datos personales e institucionales», comentó a nuestro diario, Miguel Gutiérrez Rodríguez, director general de Informática del Ministerio de Comunicaciones (Mincom).
Existen, además, servicios básicos como la electricidad, el agua y las comunicaciones, entre otros, cada vez más dependientes de las tecnologías de la información y las comunicaciones (TIC), y asegurar su funcionamiento seguro y estable es un objetivo clave de la informatización de la sociedad, lo cual requiere de altos niveles de ciberseguridad, aseveró. «En pocas palabras, la seguridad constituye una dimensión primordial en la calidad de los servicios digitales».

En aras de actualizar el marco regulatorio que define la protección de las tic y el ciberespacio nacional frente a las amenazas, el año pasado el Mincom emitió el decreto No. 360/2019 que, precisamente, establece una estrategia para la sostenibilidad y el fortalecimiento de las infraestructuras críticas; además de crear capacidades para prevenir y gestionar incidentes en la red, y la obligación de proteger los datos personales en soporte electrónico.

Por otra parte, señaló, desde el año 2019 el Consejo de Ministros aprobó un sistema de trabajo con medidas para la defensa del ciberespacio nacional, cuyas premisas están expresadas en el decreto antes referido, y se orientan hacia el fortalecimiento de la vigilancia tecnológica, entendida como un proceso de perfeccionamiento continuo y la necesidad de preparar y preservar el capital humano para esas funciones.
«Del mismo modo, se puntualiza lo imprescindible de elevar la seguridad de las tic, mediante el desarrollo de la industria nacional de programas y aplicaciones informáticas para asegurar la disponibilidad de soluciones

y productos cubanos», afirmó.

¿CÓMO PROCEDE CUBA ANTE UN ATAQUE INFORMÁTICO?

Los ciberataques casi siempre tienen como objetivo principal causar afectaciones a servicios y aplicaciones, a los que se accede a través de internet, dadas las vulnerabilidades que presentan en su estructura y en el entorno digital, donde se encuentran ubicadas, precisó Gutiérrez Rodríguez.

«Una vez detectado un incidente de ciberseguridad en nuestro país por una entidad jurídica o una persona natural, con independencia de su tipo, debe reportarse a la Oficina de Seguridad para las Redes Informáticas (OSRI), entidad que pertenece al Mincom.

«A partir de la recepción del incidente, se activa un procedimiento para su investigación, con el propósito de esclarecer las causas y condiciones existentes, determinar las responsabilidades implicadas y, lo más importante, fortalecer los sistemas de prevención y control a partir de las experiencias obtenidas durante el proceso», puntualizó.

Sin embargo, en un escenario en el cual cada vez hay mayor número de usuarios conectados, infoalfabetizar a la ciudadanía respecto a estos temas adquiere igual relevancia.

«En ese sentido, el Ministerio de Comunicaciones incluyó recientemente, como uno de los pilares en el proceso de informatización, la cultura en el uso de las TIC, teniendo en cuenta que si los ciudadanos tienen una mejor y mayor preparación para interactuar en el espacio virtual, consecuentemente podrán hacer un uso más responsable y creativo de internet y sus servicios, proteger mejor las tecnologías que se utilizan para acceder, así como cuidar sus datos personales».

Para lograr esto, añadió el funcionario, se implementan también acciones de formación en varios niveles de enseñanza, tales como la gestión de redes y su seguridad en los cursos de ciclo corto (Técnico Superior Universitario), la especialidad de posgrado en Seguridad Informática y la Ingeniería en Ciberseguridad, que acogerá la Universidad de las Ciencias Informáticas, por citar solo algunos esfuerzos.

Pero más allá de lo que puede hacerse a nivel de país en función de la seguridad informática, en el plano individual, nosotros –los usuarios– debemos conocer e implementar ciertas medidas para no ser víctimas de delitos informáticos como el phishing o robo de información. En tal propósito, recalcó el director de Informática del Mincom, lo más importante es conocer en qué lugar ponemos nuestros datos y qué ubicaciones electrónicas visitamos desde nuestros dispositivos.

No es buena práctica entregar datos o información de valor identificativo a individuos o aplicaciones de cuya autenticidad no estemos seguros, advirtió. «Generalmente, ese tipo de conductas nocivas son exitosas, porque se actúa con ingenuidad o desconocimiento, algo en lo que todos debemos trabajar por minimizar, en particular cuando Cuba avanza en proyectos como el gobierno y comercio electrónicos, y se incrementan las posibilidades de acceso al ciberespacio».

https://bit.ly/3esVtkb [1]

Links
[1] https://bit.ly/3esVtkb