Seguridad informática en el hogar

Alberto Vanegas Gallardo

Actualmente, la tecnología se emplea como un elemento de comunicación en la familia y la computadora se ha convertido en una herramienta inherente al ser humano que es usada por todos los miembros del hogar; sin embargo, no muchas personas saben qué medidas tomar para contrarrestar los riesgos y amenazas tecnológicas que implica tener estos objetos tecnológicos.

Ante este panorama, el pasado 22 de marzo se llevó a cabo la ponencia *Seguridad informática en el hogar,* perteneciente a las Pláticas sobre Seguridad Informática, impartidas por la Secretaría de Telecomunicaciones e Informática del Instituto de Ingeniería. La charla, presentada por el maestro Cuauhtémoc Vélez Martínez y el ingeniero Mauricio Velázquez Álvarez, trató sobre conceptos y recomendaciones básicas para evitar poner en riesgo la información, *hardware* y *software* de equipos en el hogar.

Por qué hablar de seguridad en el hogar

Las tecnologías de la información se han diversificado, ahora ya no se usa únicamente la PC, sino también teléfonos inteligentes, tabletas y otros objetos domésticos con posibilidad de conectividad a Internet. Lo

anterior encierra un nivel de riesgo. Si no se conocen las amenazas, se puede vulnerar la integridad, no sólo de los equipos, sino de la familia.

Según datos de la Asociación de Internet, en diez años, se ha triplicado la cantidad de usuarios de Internet en el país, de 20 millones en 2006 a más de 70 millones en 2016. El uso primordial de los mexicanos es el acceso a redes sociales, en segundo lugar, se utiliza para ver y descargar contenidos multimedia. Además, la edad del perfil de los usuarios ha disminuido.

Los delitos informáticos en México presentan un incremento de 14 millones en 2010 a 22.4 millones en 2016, lo que representa un aumento en el costo de 60 por ciento. Las transgresiones más comunes son: robo de dispositivo móvil, 30 por ciento; robo de contraseña, 26 por ciento, y el *hackeo* del correo electrónico, 20 por ciento.

Amenazas

Dentro de las amenazas se mostró el mal uso de los equipos. Esto puede ser por descuido o por agentes externos. Las amenazas que atañen directamente al software se enlistan en: *spam*, *adware*, *phishing*, *malware*, *ransonware*, *spyware*, programas *keylogger* y virus. Sin embargo, los padres de familia deben poner atención especial en las siguientes amenazas: *sexting*, pornografía infantil, *cyberbullyng*, *creepweare*, *grooming* y foros de pedofilia.

Los nativos digitales son jóvenes que aprenden a usar las nuevas tecnologías rápidamente pero no necesariamente son conscientes de los peligros que corren en la red.

El anonimato en la red es un gancho para cometer actos delictivos sin ser detectados, aunado a la poca o nula supervisión, ya que los padres no están al tanto de lo que sus hijos hacen con los *gadgets*. Esto puede darse por la falta de conocimientos de la misma familia, el escaso interés en temas de seguridad y el uso indiscriminado de Internet a corta edad.

A continuación se presentan las medidas preventivas y correctivas recomendadas en la plática, divididas en los temas tratados: *hardware*, *software*, información y familia.

	Medidas preventivas	Medidas correctivas
Hardware	• Aplicar mantenimiento frecuente • Garantizar la ventilación adecuada • Contar con alimentación eléctrica apropiada • Usar adecuadamente el equipo	• Soporte técnico • Mantenimiento correctivo
Software	• Actualizar el sistema operativo • Aplicar controles de acceso (contraseñas) • Instalar antimalware • Verificar que las unidades externas no tengan malware • No instalar aplicaciones de dudosa procedencia (piratería) • Estar atento a los correos electrónicos • No visitar páginas web fraudulentas o poco confiables • Proteger la red interna	• Apagar el equipo • Someterlo a revisión • Acudir al soporte técnico
Información	• Depurar archivos • No compartir información confidencial con desconocidos • No abrir archivos adjuntos que despierten cierto grado de sospecha • Romper los documentos • Revisar cuidadosamente el correo electrónico • Verificar la autenticidad del email en caso de sospecha • No publicar información confidencial en redes sociales • No subir documentos sensibles a la nube • Tener al menos un respaldo de información actualizado • No llenar formatos en páginas web poco confiables	• Cambiar contraseñas • Informar si ha sido víctima de robo • Reubicar información
Familia	• Activar controles de privacidad en redes sociales para familiares y amigos cercanos • Utilizar el control parental (sistema operativo y aplicaciones) • No aceptar gente desconocida en redes sociales • Difundir cualquier situación (*phishing*, *vishing*, *impersonation*, etc.) a la comunidad • Platicar con la familia sobre los cuidados a seguir • Procurar ser intuitivo y desconfiado • Tomar consciencia de que la seguridad la hacemos todos.	• Comisión Nacional de Seguridad • Centro Nacional de Respuesta a incidentes cibernéticos de la policía federal (cns.gob.mx)

Recomendaciones finales

Para finalizar, el maestro Vélez enfatizó que “los textos, imágenes y videos que se publican en redes sociales dejan de ser privados en automático”, por lo que insistieron en actualizar, tanto el *software* y los equipos, así como informarse constantemente sobre aspectos de seguridad; concientizar, promover información en cuanto a los riesgos que conlleva el empleo de las nuevas tecnologías; supervisar, verificar las actividades que hacen los menores de casa en Internet; y comunicar, informar a la familia sobre los riesgos que representan el uso de objetos tecnológicos y la publicación de información personal en redes sociales.