RETO EN LA ERA DIGITAL

Guillermo Cárdenas Guzmán
Subdirección de Intercambio Académico
gcardenas@cinvestav.mx

Cuando en marzo de 2008 el ejército colombiano bombardeó un campamento guerrillero de las Fuerzas Armadas Revolucionarias de Colombia (FARC) situado en Ecuador, no sólo asestó un duro golpe al grupo rebelde encabezado por el comandante Raúl Reyes, quien falleció durante el ataque.

Tras la incursión, los militares retuvieron equipo de cómputo que pertenecía al líder guerrillero. El contenido de los archivos, alojados en tres *lap tops*, dos discos duros externos y tres memorias USB, fue revelador, pues según el gobierno colombiano aportó información clave sobre los movimientos, alianzas y compra de armamento de las FARC.

Cinco años después, luego del escándalo mundial por las filtraciones de Edward Snowden (ex empleado de la Agencia de Seguridad de Estados Unidos que en 2013 dio a conocer documentos confidenciales y programas de espionaje masivo) Rusia adoptó una medida muy peculiar para contener estos riesgos.

De acuerdo con la cadena británica BBC, la agencia FSO, encargada de la seguridad de los altos funcionarios rusos, ordenó la compra masiva de máquinas de escribir. El objetivo: redactar en papel los reportes confidenciales que pudieran ser interceptados o alterados en caso de alojarse en computadoras.

Big Brother no es ficción

Por desgracia, no sólo los líderes sociales, las empresas o los funcionarios de gobierno están en la mira de los *hackers*; en la medida que se popularizan las tecnologías digitales y crece el flujo de información a través de ellas, también aumenta el riesgo de convertirse en blanco de un ataque cibernético pasivo o activo (con intervención de equipo). Ahora todos los miembros de la sociedad son vulnerables.

Los dispositivos digitales están enlazados de tal modo a nuestra vida cotidiana que parece imposible prescindir de ellos, como pretende el Estado ruso. Las transacciones bancarias, las compras *on-line*, los sistemas de geolocalización, los teléfonos "inteligentes" o el control del tráfico de vehículos, por citar pocos casos, dependen parcial o totalmente de esos sistemas.

En la medida que se extiende el cómputo ubicuo (*ubicomp*) y se materializa el "internet de las cosas", la

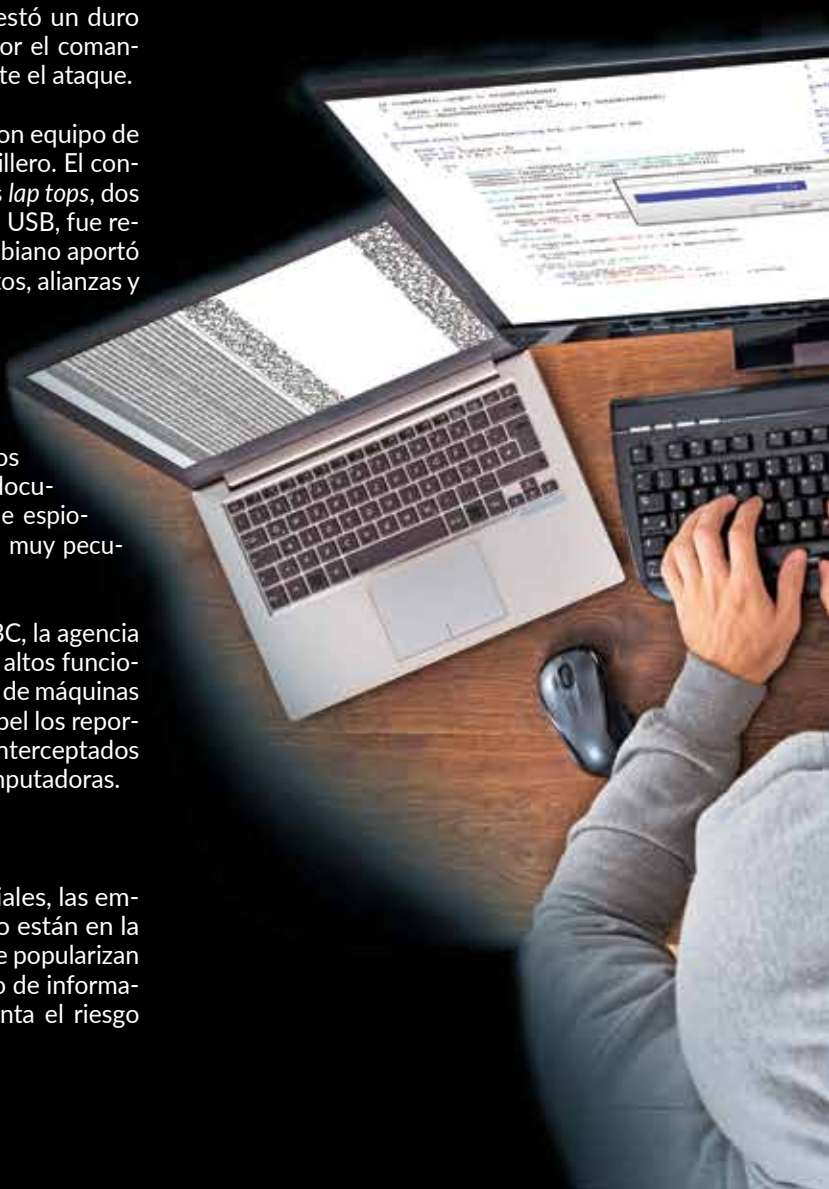

figura del *Big Brother* que todo lo vigila y la policía del pensamiento, descritos en la novela *1984* de George Orwell se hace realidad. "Ahora la única forma de tener privacidad es vivir fuera de la sociedad", considera el investigador Francisco Rodríguez Henríquez, del Departamento de Computación del Cinvestav.

El cómputo ubicuo, que Bill Gates preconizó con su deseo de que algún día, por cada ser humano en el planeta hubiera también una computadora, se refiere a la integración de todos los dispositivos informáticos en el entorno del usuario, de manera que no sean percibidos como objetos diferenciados.

De hecho, el ideal del fundador de Microsoft ha sido superado con creces por el cómputo ubicuo: ahora los expertos calculan que en las ciudades desarrolladas existen entre cien y mil procesadores sirviéndonos constantemente. Además, este servicio se da de manera silenciosa, pues la mayoría de estos dispositivos electrónicos están ocultos en objetos de uso cotidiano como televisores, autos o edificios. Esto ha implicado grandes ventajas, pero también numerosos inconvenientes.

Los expertos recomiendan usar contraseñas con al menos 12 caracteres para evitar el robo de identidad

No se trata sólo del riesgo de exponer información confidencial personal o institucional a través del correo electrónico, los navegadores de internet o las redes sociales digitales; a medida que avanza la tecnología, aparecen nuevas amenazas, como la posibilidad de intervenir la computadoras que llevan a bordo los autos modernos para provocar una falla deliberada o incluso dispositivos médicos como marcapasos o bombas de insulina, como advirtió en su momento el famoso *hacker* neozelandés Barnaby Douglas Jack.

Rodríguez Henríquez indica que la instalación de software malicioso (*malware*), la suplantación del Sistema de Resolución de Nombres de Dominio para conducir al usuario a una página web falsa (*pharming*) y el robo de identidad con el fin de adquirir datos confidenciales (*phishing*) son los principales peligros para los usuarios digitales en México.

Arturo Díaz Pérez, director del Cinvestav Unidad Tamaulipas y experto en seguridad informática, argumenta por su parte que los desafíos en esta área se transforman constantemente, y en esa medida cambian sus prioridades: hace 15 años, el mayor problema eran los virus informáticos, mientras que hoy la principal amenaza es la extracción de datos confidenciales.

Cifras de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) permiten corroborarlo: el número de quejas por robo de identidad (para suplantar a empresas y particulares, así como pedir créditos en su nombre) creció seis veces en el país durante el último lustro, al pasar de 4 mil 564 en el primer semestre de 2011 a 28 mil 258 durante el mismo periodo de 2015.

No hay dispositivos invulnerables

Los costos de la inseguridad informática resultan mayúsculos no sólo en términos de la violación que significa a la privacidad e integridad de las personas y las organizaciones, sino por su impacto económico, que en 2015 ascendió a 400 mil millones de dólares a nivel global, según cálculos de la empresa McAfee.

La misma compañía de software estimó un costo por ciberdelitos de 3 mil millones de dólares para México en 2013, cifra que tiende al alza, con un incremento de 40 por ciento registrado en 2015. Aunado a ello, el país ocupó en 2012 el último lugar en el rubro de ciberseguridad dentro de las naciones integrantes

de la Organización para la Cooperación y el Desarrollo Económicos.

En este contexto, la Unidad de Inteligencia Competitiva elaboró el reporte titulado *Retos de ciberseguridad para México*. El documento de la firma consultora propone diseñar e implementar estrategias y planes nacionales que permitan la transición hacia un ciberespacio libre de riesgos, que permita aprovechar los innegables beneficios que ofrecen las plataformas digitales.

Pero, ¿esto es posible? ¿Podemos transitar sin peligro en el ciberespacio? Francisco Rodríguez aclara que, de acuerdo con la primera Ley de Seguridad Informática no existen dispositivos invulnerables. Andrés Velázquez, experto en cómputo forense y presidente de la compañía mexicana Mattica, ilustra esta idea con una cita de su profesor Eugene Spafford, de la Universidad de Purdue, Estados Unidos.

"Eugene Spafford decía que el único sistema absolutamente seguro es aquel que está apagado y desconectado, guardado en una caja de titanio rodeada por gas venenoso, protegida por guardias armados, y ni aun así apostaría su vida por él", recuerda el experto de Mattica, primer laboratorio de investigación de delitos informáticos en América Latina.

En un mundo cada vez más interconectado crece el riesgo ante el acoso constante de *hackers*, espías electrónicos, software malicioso y otras amenazas similares. ¿Tenemos recursos suficientes para enfrentarlas?

Ante este panorama, apunta Díaz Pérez, es preciso promover una cultura enfocada a la protección de datos confidenciales entre las organizaciones públicas y privadas que custodian información personal o de terceros, además de trabajar en mecanismos de seguridad para las transacciones electrónicas.

"Frecuentemente se piensa que es suficiente con instalar un corta fuegos, pero hay que garantizar desde la obtención de la información hasta su custodia a lo largo del proceso en el que se va a utilizar", advierte el director del Cinvestav Unidad Tamaulipas.

Usuario, el eslabón más débil

Esta vulnerabilidad de los sistemas de cómputo no justifica el descuido o negligencia por parte de los usuarios, quienes con frecuencia constituyen el eslabón más débil en la cadena de la información. Como en el caso de un automóvil: puede existir el modelo más costoso, dotado con los mejores dispositivos de seguridad, pero de poco servirá para evitar accidentes a un mal conductor.

"El eslabón más débil en la informática, las computadoras y los sistemas muchas veces es el usuario, por ejemplo, cuando se dan casos en que le da *click* al archivo adjunto del correo electrónico de un desconocido y éste infecta su computadora", opina Andrés Velázquez.

Francisco Rodríguez comparte esta apreciación. "La principal debilidad es la falta de conciencia de cuán vulnerables somos ante este tipo de ataques". El problema, sostiene el científico del Cinvestav, se agrava por la falta de conocimientos básicos de seguridad informática, tales como la existencia de certificados digitales.

Ante esta situación, ambos expertos insisten en la necesidad de aplicar medidas básicas que por obvias que parezcan, a menudo son ignoradas: usar contraseñas de al menos 12 caracteres y que no sean predecibles; emplear administradores de las mismas y cerciorarse de que existan certificados digitales de seguridad al abrir páginas de internet.

No se trata de utilizar una herramienta de cifrado muy robusta sólo para proteger un mensaje de texto, aclara Arturo Díaz; sin embargo, "como la capacidad de cómputo ha mejorado tanto en los últimos años, ya no resulta descabellado pensar en una máquina de escritorio que incorpore estas técnicas y herramientas como parte de sus servicios".

El experto de la Unidad Tamaulipas reconoce que vigilar a una persona ya se hizo un problema común; lo que no resulta trivial, añade, es cuando la vigilancia se masifica, así sea con el noble fin de combatir delitos como narcotráfico o terrorismo. "Nuestra información está ahí disponible; pero quiénes la usan, cuándo y cómo, son los grandes temas de discusión".

Más instrumentos de protección

Además de mejorar algoritmos de cifrado, que se inventaron antes que las computadoras, los centros de investigación y las compañías de cómputo han desarrollado diversos instrumentos para reducir el impacto negativo de los delitos informáticos

En el Cinvestav, los científicos también están aportando nuevas alternativas para atacar dicho problema. En la Unidad Tamaulipas, un equipo donde colaboran Arturo Díaz, Víctor Sosa y José Luis Rodríguez pretende mejorar la seguridad de los servicios de alojamiento de información en la nube en diferentes escenarios.

"Buscamos procedimientos que permitan la privacidad, la autenticidad y la integridad de la información con mecanismos de control de acceso en los que sólo los usuarios autorizados puedan obtener la información, sin importar que estén en otro país", comenta Díaz Pérez. Otro rubro en el que laboran los expertos

LEYES DE SEGURIDAD INFORMÁTICA

Un entorno digital libre de riesgos no es posible, pero sí es factible minimizarlos, tal como lo enuncian las tres leyes de seguridad informática:

1. Los sistemas absolutamente seguros no existen
2. Disminuir las vulnerabilidades de un sistema a la mitad implica duplicar los costos de seguridad
3. Típicamente la criptografía no es vulnerada, sino "brincada" (los *hackers* buscan resquicios para entrar sin violar el sistema)

ENTROPÍA DEL *PASSWORD*

El término entropía, que en física alude a las leyes de la termodinámica, se usa en computación para medir qué tan vulnerable es una contraseña. Mientras más entrópico o "desordenado" sea, resultará más complicado adivinarlo o forzarlo. Generalmente se expresa en bits. Uno ya conocido tiene cero bits. Otro que podría ser adivinado al primer intento la mitad de las veces tiene un bit y así sucesivamente.

Esta es la razón por la cual los expertos recomiendan cambiar regularmente las contraseñas, hacerlas de al menos doce caracteres con símbolos especiales y sin palabras de uso común en los diccionarios. El investigador Francisco Rodríguez Henríquez advierte que en este punto, el usuario es con frecuencia el eslabón más débil en la cadena de seguridad informática.

Ante ello, el científico del Laboratorio de Criptografía del Departamento de Cómputo del Cinvestav recomienda usar programas administradores de contraseñas (pueden descargarse en Internet o en tiendas de apps para celulares) a fin de facilitar las interacciones *on-line* sin tener que memorizar numerosas y largas contraseñas.

es en el desarrollo de aplicaciones para monitorear el estado de diversos dispositivos (celulares, televisores, memorias), resguardarlos contra ciberataques y controlar su actividad.

En los protocolos de comunicación para internet podríamos incorporar mecanismos de codificación de la información o servicios de autentificación de mensajes, afirma Díaz Pérez. El problema, precisa, es que quienes diseñan estas aplicaciones las incorporen como parte de los estándares de la industria.

José Juan García Hernández, también de la Unidad Tamaulipas, se ha enfocado en evaluar la calidad de marcas de agua digitales (análogas a las que contienen los billetes) en el campo de la imagenología médica, particularmente en las imágenes de ultrasonido de mama, que ayudan a diagnosticar lesiones. Al incorporar metadatos de las pacientes, dichas marcas ayudan a garantizar la fidelidad y autenticidad de los datos.

Recientemente, García Hernández demostró a nivel experimental que un algoritmo, denominado *Ocultamiento de Datos de Alta Capacidad*, es sumamente recomendable para su empleo en el diagnóstico asistido por computadora, ya que mantiene la calidad de las imágenes médicas sin introducir distorsiones.

Por otro lado, en el Laboratorio de Criptografía del Departamento de Computación del Cinvestav, Francisco Rodríguez Henríquez se ha dedicado junto con sus colaboradores a analizar la vulnerabilidad de algoritmos criptográficos que están en uso o serán adoptados como estándar internacional en la industria, para alertar a las autoridades sobre eventuales riesgos.

En este rubro, señala, hay otro gran dilema: seguridad contra compatibilidad, pues regularmente dichos estándares son establecidos a partir de los que aprueban las autoridades de Estados Unidos. Entonces, otras naciones menos desarrolladas en este tipo de tecnologías (como México), aunque tienen libertad para generar sus propios diseños y estándares, podrían afrontar problemas para acoplarse con los que ya están avalados. Además, podrían ser más vulnerables, ya que no recibirían el minucioso análisis que se aplica en los estándares criptográficos estadounidenses.

Por esas razones, Rodríguez Henríquez considera deseable desarrollar tecnologías de seguridad digital propias en México. Pero para lograrlo, advierte, es indispensable contar con la plataforma de un organismo regulatorio de seguridad informática similar al que hay en España, el Instituto Nacional de Ciberseguridad, en el que estén representados los diversos sectores de la sociedad: gobierno, academia e industrias.