Paakat: Revista de Tecnología y Sociedad
ISSN: 2007-3607
Universidad de Guadalajara
Sistema de Universidad Virtual
México
suv.paakat@redudg.udg.mx

Año 6, número 11, septiembre 2016-febrero 2017

Seguridad en internet

José Antonio Amaro López*
Centro Universitario de Ciencias Sociales y Humanidades, Universidad de Guadalajara, México
Citlalli Rosalba Rodríguez Rodríguez**
Universidad de Guadalajara, México

[Recibido 27/05/2016; aceptado para su publicación 4/08/2016]

Resumen
El presente documento aborda la seguridad que existe en internet a través de casos y estadísticas acerca de las principales amenazas, así como de las acciones realizadas por parte de diversos países para regular su participación en la red de redes y otras recomendaciones que los usuarios pueden adoptar para mejorar su experiencia mientras navegan en esta red.

Palabras clave
Seguridad; internet; recomendaciones; comunicaciones; redes de computadoras.

Internet security

Abstract
In this document is an approach about of the security that exists on the Internet, presenting cases and statistics about the major threats and actions that have been made by countries to regulate their participation in this network and the readers we find a few recommendations that users can take to improve their experience while there are surfing the Internet.

Key Words
Security; Internet; recommendations; communications; computers networks.

El incremento anual en cantidad de usuarios que hacen uso de internet (de acuerdo con la página internet *Live Stats*[2] e *internet World Stats*[3]*,* ya somos aproximadamente 3 mil millones de personas conectadas) por razones que van desde ocio, compras, estudiar en línea, transferencias bancarias, mantenerse informadas, entre muchas otras; por lo tanto, este medio obtiene cada día un nivel de importancia tal que en la actualidad sería casi imposible imaginarse la vida sin una conexión a la red de redes.

Incluso una gran parte del comercio mundial es por medio de internet (aún cuando el 85% de las transacciones se lleva mediante el uso de efectivo) de acuerdo con la empresa GlobalWebIndex, en su informe del año 2016; ocho de cada diez consumidores en línea han realizado una compra en internet, de igual manera el diario *Gestión* agrega:

> De acuerdo con una investigación de PayPal e Ipsos, el crecimiento del comercio móvil (compras realizadas con *smartphones* y *tablets*) superará en casi tres veces al del comercio electrónico mundial. De 2013 a 2016, el aumento anual del mCommerce será de 42%, frente a 13% para el eCommerce en general (incluido los móviles). Incluso el comercio a través de redes sociales ha tenido un incremento de 80% según el informe de GlobalWebIndex (2015:2).

Además los usuarios que se conectan de dispositivos móviles también han incrementado de 2.2 a 7.1 mil millones en los últimos diez años y la contratación de anchos de banda para estos mismos dispositivos creció de 0.8 a 3.5 mil millones en los pasados cinco años de acuerdo al *Measuring the information society report 2015* que elaboró la International Telecomunication Union (ITU, 2015:3). Por lo anterior, es posible visualizar que se genera gran cantidad de datos en internet, más la suma de información personal que circula por el uso de redes sociales, como la contenida en plataformas de *Facebook*, *Instagram* o *WhatsApp*.

Toda esta información viaja de manera codificada entre computadoras de usuarios, pero depende del nivel de seguridad que se tenga en los dispositivos que dan vida a internet (servidores, *hubs*, *routers*, *firewalls*, servidores DNS, entre otros), más la seguridad en dispositivos de los usuarios y las reglas que los usuarios observen al transferir o publicar su información, lo que contribuyen a incrementar el nivel de seguridad con la cual se navega en internet.

Aún cuando todos estos datos que viajan por red se encuentran codificados deben y tienen que ser decodificados con la finalidad de que el usuario receptor pueda recibir el mensaje y, por lo tanto, en el camino puede ser interceptada por terceras personas que pueden descubrir la información transmitida.

Si esta información es catalogada entre usuarios con un nivel alto de importancia y privada (contraseñas de cuentas de correos o redes sociales, de cuentas bancarias, información privilegiada entre empresas o gobiernos), resulta grave que usuarios no autorizados tengan acceso a estos datos, ya que podrían vaciar las cuentas bancarias, o vender información clasificada a otros países, como por ejemplo los de planos de bases militares o armamento nuclear.

Un ejemplo es el caso del gran robo bancario cibernético que se realizó en febrero de 2016, donde se extrajeron 81 millones de dólares de los fondos del banco central de Bangladés y que se mantenían en el banco de la reserva federal de Nueva York. Lo anterior se realizó mediante un *malware* que simuló realizar transferencias legítimas de dinero a través de una aplicación llamada *SWIFT,* que utilizan todos los bancos para realizar operaciones entre ellos (Leetaru, 2016).

También en 2007, Estonia soportó el primer ciberataque a gran escala dirigido en contra de su infraestructura crítica, como sus bancos o el parlamento; incluso en diciembre de 2005 parte de Ucrania no tuvo energía eléctrica por aproximadamente seis horas, debido a un ciberataque contra la compañía nacional de energía,perpetrado mediante un *malware* que tenía la capacidad de dar control a un usuario externo de los equipos de cómputo de la compañía y con ello lograr deshabilitar sus sistemas y borrar archivos de computadoras con las que se contaban (Leetaru, 2016).

De acuerdo con el informe *Key findings from the 2015 US State of Cybercrime Survey* de PricewaterhouseCoopers (2015:4-5), los ciberataques en el año 2014 fueron más destructivos, porque los ciberdelincuentes lograron apoderarse de un mil millones de registros de información. Mientras en el 2014 el incidente que más se presentó fue el ataque distribuido de denegación de servicio con 18% de las veces, dirigidos a dañar la reputación de alguna empresa o interrumpir el comercio electrónico y otros procesos de negocios. El 13% de encuestados dijo haber sido víctima de la modalidad de *ransomware*[4]*.*

El estudio *2015 Cyber Security Survey: Major Australian Businesses* que realizó el Australian Cyber Security Centre (2015:71) encontró que 72% de las veces se realizaron ataques a las empresas encuestadas en la modalidad de *ransomware*, 66% *malware*, 59% correos electrónicos maliciosos, 30% infecciones de virus o gusanos, 30% robo de dispositivos móviles o laptops, 27% troyanos, 20% acceso remoto logrado por troyanos (RATs), 25% accesos no autorizados, 23% robo o violación de información confidencial, 17% acceso no autorizado a información de personas ajenas a la empresa, 16% ataques de denegación de servicio y 14% se presentó acceso no autorizado a información privilegiada.

Las intrusiones o violaciones de seguridad a equipos de cómputo o a la red no son nada nuevo, como lo menciona Kabay (2008:4), ya que en los años 60 se dio inicio con los ciberataques en modalidad de sabotaje, donde directamente empleados deshonestos o molestos provocaban daños a computadoras o interferían las líneas telefónicas por diversión o para robar servicios. Este tipo de ataques hasta la fecha se llevan a cabo.

También Kabay (2008:4), menciona que, durante la década de los años ochenta, los programadores comenzaron a desarrollar códigos maliciosos con la finalidad de interferir en computadoras personales con bajo nivel de seguridad, esto para borrar o apoderarse de información o llevar a cabo acciones políticas. Ya para los años noventa, cuando comenzó el uso de internet de manera masiva y por lo tanto se tenía una mayor interconexión de los equipos de cómputo, los criminales atacaban las computadoras para cometer delitos financieros, como el fraude por tarjetas de crédito; hizo su aparición el spam, así como el fraude por medio del envío de correos electrónicos masivos, aparecen los troyanos, los *keyloggers*, y se intensifican los ataques de denegación de servicio.

Es por lo anterior que, cuando un usuario utiliza internet se le debe proveer de un alto grado de seguridad, con la finalidad de que todo lo que por él fluya sólo deba ser recibido por el usuario al que va dirigido y nadie más.

Para incrementar la seguridad en internet, toda la información que viaja se codifica y para ello se han desarrollado algunos métodos con la finalidad de incrementar la seguridad en las comunicaciones y transacciones que se realizan diariamente, algunos métodos criptográficos[5] son:

- Simétricos: este método hace uso de una clave, que se utiliza tanto para ocultar el mensaje y como para descubrirlo.
- Asimétricos: consta de dos claves, una pública que todas las personas conocen y una privada que sólo las personas que envían y reciben la conocen. Para encriptar

se realiza una clave pública y para el proceso inverso es necesaria la clave privada del destinatario.

Estos métodos aseguran que el mensaje sea ilegible, sin embargo no garantizan que el medio por el que se transmiten sea seguro, por lo que se apoyan en sistemas de encriptación para que el mensaje llegue al destinatario por un medio seguro. Para lo anterior se hace uso de sistemas de encriptación como lo son el *Secure Socket Layer* (SSL), protocolo que asegura el transporte de información a través de la red, y el *Secure Hypertext Transfer Protocol* (SHTTP), variante del SSL, brinda mayor seguridad en la transferencia de información por un medio inseguro, internet.

Ahora bien, ya que se asegura que la información es ilegible y que el medio por el que se transmite es confiable, y con la finalidad de que se incremente la seguridad en internet, es necesario identificar con mucha certeza al emisor y receptor de datos, por tal motivo se desarrolla lo que se conoce como firmas digitales, cadena de datos ilegible, en la cual mediante un sistema de encriptación se agregan datos del firmante y se identifica a éste para reconocerlo siempre que envíe o reciba información a través de la red. En la actualidad se busca que esta firma sustituya a la firma autógrafa en documentos oficiales, como en el caso del Sistema de Administración Tributaria de México, donde ya es posible firmar de manera electrónica una declaración de impuestos.

Además de la firma electrónica, recientemente se utilizan certificados digitales que, junto con la firma buscan garantizar al visitante de una página de internet que se encuentra en un sitio confiable. Este certificado muestra la información digital de la empresa, la validez del certificado, fecha de vencimiento, entre otros, lo que permite generar en el usuario la suficiente confianza para poder realizar cualquier transacción con la empresa. Estos certificados son expedidos por una empresa certificadora[6] y para su creación se hace uso de criptografía, firmas digitales y protocolos SSL, para validar que la empresa que tiene una página web es quien dice ser.

La seguridad en internet no sólo tiene que ver con la relación usuario-página web y los distintos métodos de encriptación, aunque la mayor parte de lo tratado hasta el momento así lo demuestra; también la seguridad en internet ha escalado hasta niveles de ser considerado como un tema de seguridad nacional, esto debido a la cantidad de computadoras que los gobiernos en la actualidad tienen conectadas a la red de redes. También existen esfuerzos para asegurar de manera diplomática entre las naciones que no se hará mal uso de la tecnología ni utilizarla para atacar a otras naciones de manera cibernética, como los casos mencionados de la reserva federal de Nueva york y Estonia.

Para mantener un estado cordial entre las naciones se ha firmado el código de conducta para la seguridad de información, creado por los países de China, Kazakstán, Kirguistán, la Federación Rusa, Tayikistán and Uzbekistán, todos miembros de las Naciones Unidas; debido a que en la actualidad se ha presenciado un considerable progreso en el desarrollo y aplicación de tecnologías de la comunicación e información y que potencialmente puede ser utilizado para desestabilizar el orden y la seguridad internacional (ONU, 2015: 1). En este código se identifican los derechos y responsabilidades que tienen los Estados miembros en el espacio de información o ciberespacio.

Incluso no sólo entre los países se han establecido estos códigos, también por parte de empresas del sector privado que desarrollan y proveen de tecnologías de información y comunicación (ICT, por sus siglas en inglés). Como el caso de la empresa Microsoft (Nicholas, 2015), que ha estado inmersa en este asunto y ha colaborado para formalizar normas entre las instituciones de gobierno y el sector tecnológico, con la finalidad

de regular las acciones que puedan realizar tanto empresas privadas hacia el gobierno y viceversa, en el ciberespacio. Nicholas (2015) propone las siguientes reglas:

1. El Estado no puede dirigirse a las empresas de ICT para que agreguen vulnerabilidades o lleven acciones que disminuyan la confianza por parte del público en productos o servicios que prevean las empresas.
2. Los Estados deberán informar de vulnerabilidades encontradas en productos a las empresas antes de explotarlas.
3. Los Estados deben restringir la creación de armas cibernéticas y si las desarrollan deben ser elaboradas para un fin muy específico, limitado, preciso y no deben ser reutilizables.
4. Los Estados deben comprometerse a no realizar actividades que fomenten la proliferación de armas cibernéticas.
5. Evitar participar en ofensivas cibernéticas.
6. El Estado debe ayudar a las empresas de este ramo a detectar, contener, responder y recuperarse de eventos en el ciberespacio.

Estos acuerdos, entre otros[7], buscan dar orden a tantas bondades que nos ofrece la internet y que también puede ser utilizada para otros fines como la ciberguerra.

Los gobiernos realizan trabajos para incrementar la seguridad en internet, como las distintas policías cibernéticas[8] cuya función es identificar, perseguir y atrapar a los delincuentes que cometan delitos dentro del ciberespacio, así también los gobiernos han adaptado sus leyes con la finalidad de poder contar con herramientas jurídicas para poder juzgar a los ciberdelincuentes, como la ley que regula el uso de tecnología para la seguridad pública del Distrito Federal[9], o han creado organismos para abordar el cibercrimen como es el caso *The Council of Europe* que ayuda a proteger a las sociedades en todo el mundo de la amenaza de la delincuencia informática a través de la Convención sobre la Ciberdelincuencia y su Protocolo sobre la Xenofobia y el Racismo, el Comité de la Convención Ciberdelincuencia (T-CY) y los programas de cooperación técnica sobre el delito cibernético (Council of Europe, home).

Incluso los miembros de la APWG[10] realizan esfuerzos para establecer un formato para el registro de crímenes cometidos en internet, cuyo fin es contar con una herramienta que automaticen la gestión de casos de cibercrímenes que se cometan y poder adaptar las leyes a la velocidad con que estos delitos evolucionan.

Ahora bien, ya que los países trabajan para regular internet y las empresas de ICT para proveer soluciones para incrementar la seguridad mientras navegamos, existen algunas recomendaciones que podemos seguir en aras de mejorar nuestra seguridad mientras navegamos en la red, porque "una cadena es tan fuerte tanto como el eslabón más débil". Nosotros formamos parte de esta cadena que es internet y también es nuestra responsabilidad mantener la seguridad en la misma. Por tal motivo, a continuación se presentan algunas buenas prácticas que podemos seguir.

Para evitar que dañen o saboteen nuestra computadora, el US-CERT (Mindi McDowell & Allen Householder, 2009) recomienda:

- Guardar la computadora en un lugar seguro, ya que cualquier persona podría dañar o alterar la información.
- Desconectar la computadora de internet cuando no se esté utilizando, porque existen programas que escanean la red en busca de computadoras con vulnerabilidades que puedan ser explotadas y si ésta presenta estas deficiencias puede ser atacada.
- Evaluar de manera periódica la configuración de seguridad con que se

cuenta. Esto para identificar posibles fallas en la configuración del *firewall*, si el antivirus no se encuentra actualizado, si el sistema operativo necesita ser actualizado, si las licencias de antivirus son válidas, entre otros aspectos.

- Respaldar la información de manera continua, para en caso de que se presente un problema físico en la computadora, contar con la información.
- Proteger el equipo contra descargas eléctricas.

Microsoft recomienda que mientras se navegue en internet:

- Evitar descargar fotos o música o dar clic en ligas de internet que lleguen a correos, redes sociales, o programas de mensajería instantánea que no provengan de un usuario confiable o no se haya solicitado ese tipo de información, ya que podrían contener programas ocultos que tomen el control del dispositivo, del correo electrónico, del programa de mensajería instantánea, espiar lo que se realice en internet u obtener contraseñas o datos financieros que se encuentren en el dispositivo como las cuentas de las tarjetas de crédito.
- Evita descargar cualquier programa que resulte de un anuncio que ofrezca proteger los dispositivos o remover virus de manera gratuita, sobre todo si proviene de un anuncio que aparece de manera sorpresiva mientras navega en internet.
- Instalar actualizaciones de sus dispositivos o programas que tenga instalados, sólo de páginas oficiales.
- Eliminar programas o aplicaciones que no utilice.
- Proteger los dispositivos o cuentas de internet mediante contraseñas largas que combinen letras, números y símbolos.
- Mantener en secreto las contraseñas.
- Evitar utilizar la misma contraseña para ingresar a distintos dispositivos o cuentas de correo o bancarias.
- Evitar dar acceso a información personal a las aplicaciones que se instalen en los dispositivos cuando esto no sea lógico, por ejemplo, no dar acceso a la ubicación o a la lista de contactos a la aplicación de la calculadora en un celular.
- Evitar deshabilitar el antivirus o cualquier programa que provea de seguridad al dispositivo.
- Descargar programas de sitios confiables o directamente de la página del proveedor.
- En caso de recibir una liga de internet que no se solicitó o no es normal que alguien la haya enviado, debe preguntarse al usuario que la envía si la liga es legítima.
- Desactivar todas aquellas funcionalidades que no se estén utilizando de los dispositivos, como por ejemplo el *wifi*, *bluethoot*, geo-localización, etcétera.
- Evitar dar clic en el botón de aceptar sobre anuncios que aparezcan de manera sorpresiva mientras se navega en internet.
- Proteger la contraseña del dispositivo inalámbrico de la casa (*router wireless*), con una contraseña segura.
- Nunca se debe enviar mediante correo, mensajería instantánea, o en las redes sociales información sensible, como contraseñas, domicilios, horarios, planes de viajes, cuentas bancarias, etc.
- Navegar en páginas en cuya dirección al inicio se muestre "https://", ya que estas páginas utilizan métodos de encriptación para el envío y recepción de datos o en páginas donde se muestre una imagen de un candado cerrado a la izquierda de "https://".
- Cuidar la reputación que se tenga en internet, porque en la actualidad muchas de las empresas que contratan personal solicitan tener acceso a las redes sociales como parte del proceso de selección; razón por la cual de manera periódica se debe buscar en internet mediante buscadores como

Google, Yahoo, Duckduckgo, entre otros, la información que existe sobre nosotros como usuario en internet.
- Cultivar y proteger una reputación positiva en internet, publicando sólo aquello que no perjudique nuestra imagen.
- Configurar quien puede y no puede tener acceso a lo que se publica de usted enredes sociales y también quién de sus seguidores puede comentar o publicar en su red.
- Ser selectivo al aceptar amigos en redes sociales, así como vigilar de manera continua lo que publican de usted.
- Con respecto a permitir utilizar internet a niños y adolescentes, se deben establecer guías claras de acuerdo a su edad para el uso correcto de internet.
- Estar al pendiente de las páginas que visitan.
- Tener acceso a redes sociales que frecuentan para identificar problemas de acoso o qué información publican.
- Asegurarse que los niños y adolescentes comprendan la importancia de no compartir información sensible en redes sociales, mensajería instantánea o por correo.
- Disponer de la contraseña de administrador con la finalidad de instalar programas que permitan bloquear aquellas páginas no apropiadas para niños o adolescentes o para investigar el uso y las páginas que visitan de manera frecuente[11].

Poner en practica estas y otras recomendaciones nos permiten navegar con mayor seguridad en internet, sin embargo utilizar nuestro sentido común mientras nos conectamos a internet juega un papel importante, ya que nos permite siempre cuestionar y evaluar si algo puede ser confiable o no, porque los ciberdelincuentes siempre están innovando con la finalidad de que el usuario pueda caer en sus trampas y obtener ganancias.

Conclusiones

Con base en lo descrito, no se puede negar que internet forma parte de nuestro día a día y más con el incremento que se ha tenido en estos últimos años del comercio electrónico cuyas ganancias aumentan cada año[12] y la información que se transmite es de carácter financiero, por lo tanto sensible. Por esto deben establecerse algunas reglas para la sana convivencia en este medio, tanto entre particulares como entre empresas y gobiernos, ya que la invasión al espacio cibernético de alguno de estos entes puede resultar en problemas legales o incluso provocar una problema bélico entre naciones o en su caso, una guerra cibernética.

Todos los conflictos que hasta el siglo XX provocaban algún mal entendido entre particulares, empresas o gobiernos, ahora se han extendido también al aspecto virtual, al internet. Por tal motivo cabría hacer mención a la frase célebre del expresidente de México, Benito Juárez "entre los individuos como entre las naciones el respeto al derecho ajeno es la paz". Y si lo aplicamos al siglo XXI quizás podría extenderse también al hecho de que el respeto al espacio cibernético.

No debemos olvidar que, como usuarios, también tenemos la responsabilidad de asegurarnos que nuestra información llegue a su destino y que serán utilizadas de manera correcta, o para el fin que fueron dados, razón por la cual debemos de contar con buenas prácticas, antivirus, mantener actualizados el *software* que utilicemos, etcétera, mientras navegamos en internet y con esto asegurarnos que todo lo que enviamos no pueda ser interceptado o contar con una buena reputación en internet.

Referencias

Australian Ciber Security Center. (2015). *2015 cyber security survey: Major australian businesses.* Recuperado de: https://www.acsc.gov.au/publications/ACSC_CERT_Cyber_Security_Survey_2015.pdf

Caride, I. (13 de enero de 2015). 5 claves del comercio electrónico en 2015. *Forbes*. Recuperado de http://scl.io/4YYith5E#gs.i=qCMgQ.

Certsuperior. (s/f). *Centro de Información SSL*. Recuperado de https://www.certsuperior.com/InformacionSSL.aspx

Certsuperior. (s/f). *¿Qué es un Certificado Digital?* Recuperado de https://www.certsuperior.com/QueesunCertificadoDigital.aspx

Certsuperior. (s/f). *Qué es un certificado de seguridad*. Recuperado de https://www.certsuperior.com/CertificadosSeguridad.aspx

Council of Europe. (s/f). *Action against cybercrime*. Recuperado de http://www.coe.int/web/cybercrime

Emarketer. Worldwide Retail Ecommerce Sales: eMarketer's Updated Estimates and Forecast Through 2019. (23 de diciembre de 2015). *Report of Emarketer.* Recuperado de http://www.emarketer.com/Report/Worldwide-Retail-Ecommerce-Sales-eMarketers-Updated-Estimates-Forecast-Through-2019/2001716

Eumed.net. (s/f). *Seguridad en internet*. Recuperado de http://www.eumed.net/cursecon/ecoinet/seguridad/index.htm

Gestion.pe. (24 de febrero de 2015). *Crecimiento de comercio móvil triplicará al de e-commerce a nivel mundial*. Recuperado de, http://gestion.pe/tecnologia/crecimiento-comercio-movil-triplicara-al-commerce-nivel-mundial-2124395

Globalwebindex. (2016). *GlobalWebIndex's bi-annual report on the latest trends in online commerce.* . Recuperado de http://cdn2.hubspot.net/hubfs/304927/GWI_Commerce_-_Q1_2016_Summary.pdf

International Telecomunication Union. (2 de diciembre de 2015). *Measuring the information society report 2015*. Recuperado de, https://www.itu.int/en/ITU-D/Statistics/Documents/events/wtis2015/MISR2015_Magpantay.pdf

Kabay, S. M. E. & Whyne, E. (2009). *History of computer crime, computer security handbook*. New York: Wiley. Recuperado de http://www.mekabay.com/overviews/history.pdf

Leetaru, K. (30 de abril de 2016). *What The Bangladesh SWIFT Hack Teaches About The Future Of Cybersecurity And Cyberwar.* Recuperado de, http://www.forbes.com/sites/kalevleetaru/2016/04/30/what-the-bangladesh-swift-hack-teaches-about-the-future-of-cybersecurity-and-cyberwar/

Microsoft. (s/f). *Online safety resources.* Recuperado de https://www.microsoft.com/about/philanthropies/youthspark/youthsparkhub/programs/onlinesafety/resources/

McDowell, M. & Householder, A. (2 de junio de 2009). Good Security Habits. *US-CERT*. Recuperado de https://www.us-cert.gov/ncas/tips/ST04-003

Nicholas, P. (20 de enero de 2015). *Six proposed norms to reduce conflict in cyberspace*. Recuperado de https://blogs.microsoft.com/cybertrust/2015/01/20/six-proposed-norms/

ONU. (13 de enero de 2015). *International code of conduct for information security*. Recuperado de https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf

PayPal. (s/f). *Tres preguntas a Dan Schulman* [Comercio]. Recuperado de https://www.paypal.com/stories/latam/tres-preguntas-a-dan-schulman

PricewaterhouseCoopers. (Julio, 2015). *Key findings from the 2015 US State of cybercrime survey.* Recuperado de http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-cybercrime-survey-2015.htm

Segu-info. (s/f). *Seguridad Informática / Criptografía - Firma Digital*. Recuperado de http://www.segu-info.com.ar/proyectos/p1_firma-digital.htm

*__José Antonio Amaro López__: Licenciado en informática con orientación en sistemas computacionales; maestro en Tecnologías para el Aprendizaje, ambos por la Universidad de Guadalajara. Profesor docente del Departamento de Geografía y Ordenación Territorial del Centro Universitario de Ciencias Sociales y Humanidades de la Universidad de Guadalajara.
**__Citlalli Rosalba Rodríguez Rodríguez__: Licenciada en informática y maestrante en Tecnologías para el Aprendizaje; ha participado en la gestión de proyectos en el ámbito tecnológico dentro de la Universidad de Guadalajara.

[2] http://www.internetlivestats.com/

[3] http://www.internetworldstats.com/stats.htm

[4] Modalidad en la que el ciberdelincuente bloquea el acceso a una computadora y exige un pago por dar otra vez el acceso a ésta.

[5] Proceso mediante el que un texto o una serie de bytes son modificados de tal manera que se vuelven ilegibles para las personas, y sólo el destinatario, quien conoce el procedimiento mediante el cual se volvió ilegible el texto o los *bytes*, pueda leer o comprender el mensaje o archivo que se envió.

[6] Como *Symantec*, *verysign* o la Agencia de Certificación Electrónica (ACE), por mencionar algunas.

[7]http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=/english/&Lang=E
https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states
https://blogs.state.gov/stories/2015/12/03/g20-growing-international-consensus-stability-cyberspace,
https://www.un.org/disarmament/topics/informationsecurity/
http://www.state.gov/secretary/remarks/2015/05/242553.htm
http://cybersummit.info/
https://cybersummit.info/sites/cybersummit.info/files/BGCyberNorms_FINAL.pdf

[8] En el caso de México la policía cibernética está adscrita a la Coordinación General de Inteligencia para la Prevención de la SSP, su página en Facebook es: https://www.facebook.com/policia.ssp

[9] http://info4.juridicas.unam.mx/adprojus/leg/10/401/

[10] https://apwg.org/apwg-news-center/data-logistics/

[11] Otros consejos sobre cómo abordar el *bullying*, evitar fraudes en internet, cuidado de niños y adolescente en internet y sobre cómo mantenerse seguro en internet, consultar en: https://www.microsoft.com/about/philanthropies/youthspark/youthsparkhub/programs/onlinesafety/resources/

[12] La revista *Forbes México*, en su artículo "5 claves del comercio electrónico en 2015", menciona que las ventas en línea globales representaron 5.9% del mercado de menudeo, logrando una facturación de 1.3 mil millones de dólares en 2014, mientras que en el artículo de *Worldwide Retail Ecommerce Sales: eMarketer's Updated Estimates and Forecast Through 2019* de la consultora eMarketer estimó que en 2019 esa proporción saltará a $ 3.578 billones de dólares.