IUS ET SCIENTIA (ISSN: 2444-8478) 2018, Vol.4, nº 1, pp. 19-39
"Tecnologías, seguridad informática y derechos humanos", Evelyn TÉLLEZ CARVAJAL
Universidad Nacional Autónoma de México. evelyn.tellez@infotec.mx
Recibido: 21/06/2018. Aceptado: 01/07/2018
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2018.i01.03

TECNOLOGÍAS, SEGURIDAD INFORMÁTICA Y DERECHOS HUMANOS

TECHNOLOGIES, INFORMATIC SECURITY AND HUMAN RIGHTS

Evelyn TÉLLEZ CARVAJAL[1]

Resumen: En un mundo en el que las tecnologías de la información y comunicación (TIC) parecen estar presentes en casi todas nuestras actividades diarias poco se ha reflexionado sobre los riesgos que pueden representar las mismas para los seres humanos.

Por un lado tenemos a la comunidad internacional promoviendo la implementación de las TIC para impulsar el desarrollo de los menos favorecidos, pero por el otro lado existen riesgos inminentes derivados del uso de estas mismas tecnologías.

El ciudadano hoy día se encuentra expuesto a situaciones en las que sus derechos e incluso su seguridad misma están en riesgo debido al gran cúmulo de información que se concentra en sistemas informáticos que son el blanco de los ataques cibernéticos.

Resulta urgente la necesidad de sensibilizar a la sociedad en general sobre estos riesgos latentes en los que nos encontramos a fin de poder ser parte de la prevención de los mismos.

[1] Profesora – Investigadora en el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), en Av. San Fernando número 37, Colonia Toriello Guerra, Delegació Tlalpán, C.P. 14050, Ciudad de México y profesora en la Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México.
56242800 ext. 6149
iustellez@yahoo.fr y evelyn.tellez@infotec.mx

IUS ET SCIENTIA (ISSN: 2444-8478) 2018, Vol.4, nº 1, pp. 19-39
"Tecnologías, seguridad informática y derechos humanos", Evelyn TÉLLEZ CARVAJAL
Universidad Nacional Autónoma de México. evelyn.tellez@infotec.mx
Recibido: 21/06/2018. Aceptado: 01/07/2018
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2018.i01.03

Abstract: In a world in which information and communication technologies (ICT) seem to be present in almost all our daily activities little has been reflected on the risks that they can represent for human beings.

On the one hand, we have the international community promoting the implementation of ICT in order to grant the development of the less favored, but on the other hand there are imminent risks derived from the use of these same technologies.

Citizens today are exposed to situations in which their rights and even their security itself are at risk due to the large amount of information that its concentrate on computer systems that are the target of cyber attacks.

It is urgent the need to raise awareness in society in general about these latent risks in which we find ourselves in order to be part of their prevention.

Palabras clave: Seguridad, derechos humanos, tecnologías

Keywords: Security, human rights, technologies

Introducción

Las Tecnologías de la Información y Comunicación, también conocidas como TIC, se incorporaron paulatina y vertiginosamente en varias actividades que se realizan en las sociedades en la actualidad.

Nadie preguntó sobre la pertinencia de adoptar tales o cuales tecnologías. Mucho menos en los países menos desarrollados como es el caso de los Estados latinoamericanos que no somos productores de tecnología sino meros importadores de las mismas.

En un mundo globalizado e intercomunicado la sociedad internacional continuamente ha señalado que es menester cooperar para el desarrollo de los menos favorecidos y se ha señalado a las tecnologías como una herramienta idónea que impulse y genere este cambio.

IUS ET SCIENTIA (ISSN: 2444-8478) 2018, Vol.4, nº 1, pp. 19-39
"Tecnologías, seguridad informática y derechos humanos", Evelyn TÉLLEZ CARVAJAL
Universidad Nacional Autónoma de México. evelyn.tellez@infotec.mx
Recibido: 21/06/2018. Aceptado: 01/07/2018
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2018.i01.03

Sin embargo, poco es lo que se ha debatido sobre las consecuencias adversas que las tecnologías en general y el uso de la red de redes específicamente han significado para las sociedades y en particular para los ciudadanos y sus derechos más elementales como es la seguridad.

Hoy en día los ciudadanos estamos expuestos más que nunca a la vulneración de nuestra vida privada, al robo de nuestra información personal, e incluso a que nuestra salud se ponga en riesgo debido a las vulneraciones que pueda haber en los sistemas informáticos.

En la era de las tecnologías es necesario reflexionar en torno al tema de la seguridad informática y con ello abonar en la protección de la información que generamos todos los días.

Seguridad informática y seguridad de la información

La seguridad informática y la seguridad de la información suelen considerarse como sinónimos cuando en realidad son conceptos distintos, aunque se encuentran relacionados.

La seguridad informática (también conocida como seguridad digital) se refiere a las diversas técnicas, aplicaciones y dispositivos encargados de asegurar la confidencialidad, integridad, privacidad y disponibilidad de la información de un sistema informático y por consiguiente de sus usuarios.[2]

Un sistema informático es definido como una serie de componentes que se relacionan con otros conjuntos y cada sistema a su vez tiene una composición, una estructura y un entorno. En el caso de los sistemas informáticos se componen de hardware, software, personal informático, redes, usuarios, datos y procedimientos. Garantizar la ausencia de riesgos en

[2] Véase Gómez Vieites, A., *Seguridad Informática*, 2ª. ed., Madrid, Ra-MA, 2014.

estos conjuntos de componentes es lo que conocemos como seguridad informática y que generalmente se encuentra a cargo de un experto en sistemas informáticos.

Por otro lado la seguridad de la información se relaciona con la ausencia de riesgos sobre específicamente los datos que ya han sido procesados, (es decir recabados, almacenados, eliminados, resguardados, recuperados y en general tratados) y que sirven para construir un mensaje y que de acuerdo a las normas jurídicas esta seguridad de la información se encuentra a cargo de encargados de la información y responsables de la misma.[3]

En esta manera de generar y proteger la información se ha tenido que iniciar un diálogo entre dos lenguajes técnicos que anteriormente se consideraban incompatibles; por un lado el lenguaje de la ingeniería y por el otro el lenguaje jurídico ya que para poder garantizar tanto la seguridad de los sistemas y la seguridad de la información debe de existir un diálogo armónico entre ambos.

En este diálogo es menester comprender los alcances que puede tener el concepto de seguridad en cada uno de los contextos ya que al final parecería que la seguridad informática se diluye cuando los sistemas informáticos de los gobiernos, las empresas o los individuos se conectan con la red de redes.

Esta [in]seguridad de la Internet trae aparejado el riesgo, vulnerabilidades y amenazas no solo hacia los componentes de un sistema informático sino directamente a diversos derechos de los individuos como pueden ser la violación a la privacidad, a la intimidad y o bien a los datos personales.

El concepto de seguridad

Según David A Baldwin, profesor de la Universidad de Princeton, redefinir el concepto de seguridad se ha convertido hoy en día una tarea casi artesanal ya que la mayoría de los

[3] Véase Garriga Dominguez, A., *Tratamiento de datos personales y derechos fundamentales*, España, Dykinson, 2004.

esfuerzos se han concentrado en redefinir agendas políticas de los Estados nación más que preocuparse por el concepto en sí mismo de seguridad.[4]

Encontrar un concepto inequívoco de seguridad es complejo, ya que la seguridad es un valor y depende del contexto su significado, por ejemplo hablar de seguridad ambiental, seguridad alimentaria, seguridad en el empleo es distinto a referirse a la seguridad humana, seguridad nacional o seguridad informática aunque en todos los casos de manera general se haga alusión a la ausencia de riesgos.

En muchos casos, continúa el profesor Baldwin; la palabra seguridad toma forma de propuestas para dar una mayor prioridad a temas como son los derechos humanos, la economía, el medio ambiente, el tráfico de drogas, las epidemias, los crímenes, la injusticia social además de los hechos tradicionales en relación a la seguridad de amenazas militares externas.[5]

De esta manera alrededor de todas estas temáticas se ha ido construyendo un andamiaje jurídico que pretende la protección de todos y cada uno de los aspectos de la vida de los seres humanos que les garantice esta "seguridad" o ausencia de riesgos, esto incluye la seguridad de la que debemos gozar los individuos ante los avances científicos y tecnológicos.

Derechos humanos y tecnologías

La incorporación de los temas tecnológicos en materia de derechos humanos es reciente.

[4] BALDWIN, D. A., «The concept of security» *Review of International Studies*, nº. 23, p. 5. Disponible en: https://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1997)%20The%20Concept%20of%20Security.pdf. Fecha de consulta el 5 de junio de 2018.
En el original puede leerse: "Redefining 'security' has recently become something of a cottage industry. 1 Most such efforts, however, are more concerned with redefining the policy agendas of nation-states than with the concept of security itself". Una cita fue omitida del original. Traducción libre.
[5] Idem.
En el original se lee "Often, this takes the form of proposals for giving high priority to such issues as human rights, economics, the environment, drug traffic, epidemics, crime, or social injustice, in addition to the traditional concern with security from external military threats". Traducción libre.

IUS ET SCIENTIA (ISSN: 2444-8478) 2018, Vol.4, nº 1, pp. 19-39
"Tecnologías, seguridad informática y derechos humanos", Evelyn TÉLLEZ CARVAJAL
Universidad Nacional Autónoma de México. evelyn.tellez@infotec.mx
Recibido: 21/06/2018. Aceptado: 01/07/2018
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2018.i01.03

Como es sabido, la sociedad internacional, consternada por las atrocidades cometidas durante los enfrentamientos bélicos ocasionados por la Segunda Guerra Mundial, y segura de querer evitar este tipo de situaciones en el futuro en contra de los individuos y su integridad, así como su dignidad humana, firmó en 1945 la Carta de San Francisco que diera paso posteriormente a la Carta de Naciones Unidas. El primer instrumento internacional en el que se menciona el concepto de derechos humanos.

Posteriormente en 1948, con la Declaración de Derechos Humanos propuesta por la Asamblea General de las Naciones Unidas, los Estados mostrarían su intención por comprometerse a proteger los derechos humanos que serían reconocidos más adelante en los instrumentos vinculantes conocidos como el Pacto de Derechos Civiles y Políticos y el Pacto de Derechos Económicos, Sociales y Culturales para 1966. Dando con ello paso a la posterior proliferación de diversos instrumentos internacionales que existen hoy día en materia de derechos humanos.

Así, dentro del *corpus iuris* internacional de los derechos humanos que se encuentra vigente actualmente, solamente la Convención sobre los Derechos de las Personas con Discapacidad de 2006, hace referencia a las nuevas tecnologías[6] debido justamente a que

[6] 4 párrafo 1 "g) Emprender o promover la investigación y el desarrollo, y promover la disponibilidad y el uso de *nuevas tecnologías*, incluidas las tecnologías de la información y las comunicaciones, ayudas para la movilidad, dispositivos técnicos y tecnologías de apoyo adecuadas para las personas con discapacidad, dando prioridad a las de precio asequible;…"
La misma Convención en su artículo 9 señala sobre la accesibilidad a las tecnologías:
"A fin de que las personas con discapacidad puedan vivir en forma independiente y participar plenamente en todos los aspectos de la vida, los Estados Partes adoptarán medidas pertinentes para asegurar el acceso de las personas con discapacidad, en igualdad de condiciones con las demás, al entorno físico, el transporte, la información y las comunicaciones, incluidos los sistemas y *las tecnologías de la información y las comunicaciones*, y a otros servicios e instalaciones abiertos al público o de uso público, tanto en zonas urbanas como rurales. Estas medidas, que incluirán la identificación y eliminación de obstáculos y barreras de acceso, se aplicarán, entre otras cosas, a:
a) Los edificios, las vías públicas, el transporte y otras instalaciones exteriores e interiores como escuelas, viviendas, instalaciones médicas y lugares de trabajo;
b) Los servicios de información, comunicaciones y de otro tipo, incluidos los servicios electrónicos y de emergencia".

estos avances tecnológicos pretenden ser herramientas que beneficien a la sociedad como se ha dejado de manifiesto desde la Cumbre del Milenio en el año 2000.[7]

Otro organismo internacional que es necesario destacar en lo que se refiere a la los derechos humanos y las tecnologías es la Unidad Internacional de Telecomunicaciones que es un organismo especializado de Naciones Unidas y que realizó la Cumbre Mundial de la Sociedad de la Información en Ginebra 2003 y Túnez 2005.

En el Plan de Acción de Ginebra se trataba de establecer una cooperación para dar respaldo a la Agenda de Solidaridad Digital[8] (países desarrollados, empresas con capacidades tecnológicas en apoyo a países en desarrollo). En Túnez se habló de la creación de un Fondo de Solidaridad Digital[9] sin ser más específica.

Algunos de los objetivos señalados para alcanzarse en 2015 fue que todas las universidades y escuelas, bibliotecas públicas, centros de salud, hospitales y las oficinas de gobierno y oficinas de correos estuvieran conectados a las tecnologías de la información u comunicación. Lo cual veremos más adelante ha significado también un riesgo para los usuarios de estas tecnologías.

Baste hasta este punto para recordar la relevancia que supone para la sociedad internacional que el desarrollo de los Estados se relacione con la incorporación de las nuevas tecnologías lo que se asume redundará en un beneficio de las sociedades en general. Sin embargo, no estaría demás en reflexionar sobre los efectos adversos de una incorporación a las tecnologías sin información respecto de las mismas.

---

[7] Por medio de la Resolución 55/2 de la Asamblea General de Naciones Unidas la Declaración del Milenio en cuyo punto III. 20 señala en cuanto al desarrollo y erradicación de la pobreza:
"Velar por que todos puedan aprovechar los beneficios de las nuevas tecnologías, en particular de las tecnologías de la información y de las comunicaciones, conforme a las recomendaciones formuladas en la Declaración Ministerial 2000 del Consejo Económico y Social". Resolución aprobada por la Asamblea General 55/2. Declaración del milenio, disponible en http://www.un.org/spanish/milenio/ares552s.htm, última fecha de consulta el 6 de julio de 2018.

[8] Plan de Acción de Ginebra. Disponible en https://www.itu.int/net/wsis/outcome/booklet/plan_action_D-es.html, última fecha de consulta el 6 de julio de 2018.

[9] Foro Mundial de Solidaridad Digital. Disponible en https://www.itu.int/itunews/manager/display.asp?lang=es&year=2005&issue=03&ipage=global_digital&ext=html, última fecha de consulta 6 de julio de 2018.

El derecho a saber

El derecho es un producto cultural que no puede escapar de los valores y la cosmovisión de las personas que constituyen la sociedad que le da origen y, por ello, la regulación en materias como acceso a Internet o bien uso de datos biométricos para la autenticación de usuarios de la banca, por citar algunos ejemplos, son casos que impactan de forma distinta a las sociedades dependiendo del grado de avance tecnológico que posean, así como de la penetración de los ámbitos digitales en su entorno como puede ser en las áreas de la salud (expediente clínico electrónico), educación (educación 2.0), laboral (teletrabajo), etcétera.

Infortunadamente los ciudadanos no hemos sido informados respecto a las consecuencias tanto positivas como adversas que la incorporación de las tecnologías trae a nuestras vidas y, por ello, sería pertinente tomar en cuenta el conocido "derecho a saber" o "right to know".

Fue el biólogo francés Jean Rostand quien utilizara por primera vez la idea de que los humanos que vivimos las consecuencias que generan los avances científicos en nuestro entorno tenemos el derecho a saber. Siguiendo esta idea Yves Briot añade que no solo tenemos el derecho a saber sino que el conocer lo que sucede en nuestro entorno nos da la oportunidad de cambiar lo que está sucediendo. [10]

En el caso de las TIC, se observa que muchas de las consecuencias adversas como es el robo de información o pérdida de la misma, los actos de sexting, o incluso las violaciones a los derechos de autor por el uso incorrecto de obras musicales o fotográficas que se toman desde sitios ubicados en la red, se derivan de la ignorancia de los usuarios de estos medios

[10] Véase Birot, Y., «La science au service de la foresterie en región méditerranéenne: les vois du futur», en *Forêt médoterranéene*, t. XXXII, nº. 4, diciembre 2011, p. 5.
En el original se lee "Dans le contexte actuel et à venir, marqué par un niveau élevé d'incertitudes et de risques liés aux facteurs technologiques, économiques et environnementaux, la connaissance scientifique est considérée comme la meilleure réponse à apporter, comme l'avait d'ailleurs souligné le biologiste français Jean Rostand (1894-1977) : « L'obligation de subir nous donne le droit de savoir. Et le fait de savoir nous offre la possibilité du changement»." El énfasis fue añadido. La traducción es libre Lectura disponible en: http://documents.irevues.inist.fr/bitstream/handle/2042/47148/FM_XXXII-4_349-353.pdf?sequence=1&isAllowed=y. Fecha de consulta 5 de junio de 2018.

tecnológicos en mucho de los casos, inclusive las violaciones a la privacidad o intimidad también se ven propiciadas por la falta de cuidado o pericia al compartir información personal en las redes sociales, poniéndonos los mismos usuarios en situaciones sumamente vulnerables.

Por ello es menester que los gobiernos informen a sus ciudadanos adecuadamente sobre el tipo de tecnologías que se utilizan en su territorio y que tendrán relación con los ciudadanos como es el caso de las cámaras de vigilancia en la vía pública, o bien, el uso de datos como los biométricos para realizar ciertos trámites como puede ser el pasaporte o la credencial de identidad, informar sobre el tratamiento que se da de los mismos y por supuesto, concientizar a los individuos sobre los riesgos que pueden existir en torno al uso de dichas tecnologías.

Seguridad Informática y su relación con diversas áreas del derecho

La seguridad informática como se mencionó con anterioridad consiste en asegurar la ausencia de riesgos en cualquiera de los componentes de un sistema (hardware, software, personal informático, redes, usuarios, datos y procedimientos), impidiendo que cualquier persona sin autorización pueda tener acceso a la información contenida en el sistema y por lo tanto no pueda modificarla, dañarla, alterarla, eliminarla o darle cualquier tratamiento que no esté autorizado.

Los activos que pueden estar en riesgo suponen cualquier bien que compone el patrimonio y el valor para la empresa, gobierno o individuo, como son los equipos, el hardware, los programas informáticos, también las patentes, los procesos que se utilizan y las actividades del negocio.

En este caso existen diversas normas que regulan la protección en cuanto a las vulneraciones como pudiera ser el robo de equipos que en este caso caería en el área del

derecho penal y que se pondría en marcha todo el andamiaje legal penal al ser el robo una conducta tipificada en esta rama del derecho.

En el caso de uso indebido de información obtenida por ejemplo de cámaras de video del gobierno de un Estado, accionaría el derecho a la privacidad y la protección de datos personales.

Por el contrario en el caso de vulneración a una patente estaríamos ante la presencia del derecho de la Propiedad Intelectual que incluye tanto los derechos de autor como los derechos propiedad industrial como pueden ser el uso de marcas o de patentes sin contar con la debida autorización.

También el uso indebido de un programa de cómputo accionaría el derecho de Propiedad Intelectual pero en este caso sería respecto a los derechos de autor ya que en la mayoría de los países, este tipo de programas se protegen por medio de esta figura jurídica a diferencia de los Estados Unidos en donde los programas de cómputo si pueden ser patentados[11] y que por no ser tema de este artículo solo baste con la mención.

Por si no fuera poco existe también el tema de los nombres de dominio que al ser una asignación que se realiza, no por parte de alguna autoridad estatal, sino de una organización que es específicamente la Corporación de Internet para la Asignación de Nombres y Números por sus siglas en inglés ICANN,[12] puede hacer colisionar derechos por ejemplo si alguien es el titular de los derechos de una marca y es distinto al dueño titular del nombre de dominio que usa el nombre de esa marca con alguna de las terminaciones como .com .net o .es.

[11] "La actual controversia en Estados Unidos sobre las patentes de software, muestra las consecuencias que hubiera tenido considerar al software, erróneamente, como producto y no como obra: en ese país, es posible obtener una patente sobre "utilizar un programa para resolver el problema X", y a partir de ese momento el titular de la patente es la única persona con derecho a escribir programas que resuelvan X [3]". Heinz, F., «Software vs. Copyright», en Argentina Copyleft. La crisis del modelo de derecho de autor y las prácticas para democratizar la cultura, Argentina, Fundación Henrich Böll Stiftung. Cono Sur, 2010, pp. 75-76

[12] La página oficial de la Internet Corporation for Assigned Names and Numbers está disponible en: https://www.icann.org/es. Última fecha de consulta el 5 de junio de 2018.

Universidad Nacional Autónoma de México. evelyn.tellez@infotec.mx
Recibido: 21/06/2018. Aceptado: 01/07/2018
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2018.i01.03

Estos casos en la actualidad son cotidianos en la materia y que en general las prácticas de ocupar nombres de dominio para posteriormente venderlas a las personas que son legítimos dueños de las marcas es conocida como cybersquatting, o ciber ocupación y se ha tratado de erradicar por políticas de resolución de disputas.[13]

En el diseño de la seguridad informática es fundamental las detección de las amenazas, es decir que se debe de identificar, algo o alguien que pudiera causar una vulnerabilidad para así poder obtener la información de cómo evitar, disminuir, hacer frente, modificar o impedir el acceso a un activo o comprometerlo.

Se dice entre los encargados de la seguridad informática que pueden existir varias vulnerabilidades y a la vez distintas amenazas derivadas de cada vulnerabilidad. Así al identificar las amenazas se permite conocer el grado de peligro que representa y los controles apropiados para reducir su impacto potencial.

Tipos de amenazas a la seguridad informática

Las amenazas pueden tener lugar: de origen (debido a fallas de algún componente del sistema mismo, mal funcionamiento del equipo como descargas eléctricas, problemas en con el hardware y software que se utilizan, etcétera), por su tipo (amenazas internas o externas, de alto riesgo, de mantenimiento, errores de utilización, omisiones, terremotos, erupciones volcánicas, inundaciones, incendios, etcétera) o bien por alguna motivación (robo, terrorismo, fraude, hackeos, alteración de datos, denegaciones de servicio, virus informáticos, worms, troyanos, atentados, etcétera).

Para el caso de este artículo las que nos interesan son las amenazas que ponen en riesgo la seguridad informática por alguna motivación ya que a diferencia de las amenazas de origen

[13] Para mayor detalle véase el Uniform Domain-Name Dispute Resolution Policy (UDRP) disponible en: https://www.icann.org/resources/pages/help/dndr/udrp-en y el Uniform Rapid Suspension System (USR), disponible en https://www.icann.org/resources/pages/urs-2014-01-09-en. Última fecha de consulta en ambos casos 5 de junio de 2018.

Universidad Nacional Autónoma de México. evelyn.tellez@infotec.mx
Recibido: 21/06/2018. Aceptado: 01/07/2018
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2018.i01.03

que cuentan con las normas específicas que van desde los derechos de consumidor que podemos ejercer al hacer efectiva una garantía por mal funcionamiento de un equipo que hemos adquirido o bien solicitar la intervención de una aseguradora por la pérdida de determinados equipos que fueron asegurados y hubieran sido dañados por alguna descarga o bien por eventos externos como pudieran ser fenómenos de la naturaleza como un huracán o un sismo. Las amenazas a la seguridad informática por alguna motivación, en cambio, pueden accionar normas como las penales en caso de estar como se dijo ante un robo o bien una amenaza terrorista o una extorsión.

Es por esto que hablar de seguridad informática y un solo derecho que le asista o resuelva resulta casi un imposible. Es común escuchar la solicitud de los encargados de la seguridad informática solicitar al encargado del despacho jurídico que le explique cuáles son las leyes que deben de cumplirse para poder cumplir con las obligaciones de una adecuada seguridad informática. La realidad es que el derecho no pretende regular la tecnología y que los riesgos son inherentes al mismo sistema informático, es decir existen vulnerabilidades y riesgos derivado de ellas tanto en el aspecto del hardware, el software y el del personal que los utiliza lo que puede traducirse en una vulnerabilidad como el robo o acceso no autorizado a bases de datos por ejemplo de clientes de un banco. En este caso se estaría frente a un tema de seguridad informática que vulnera también el derecho a la protección de datos. Todo un cuerpo normativo que regula esta temática.

La seguridad informática, no hay duda, requiere de la identificación de riesgos, es decir de las posibilidades de que un evento crítico aparezca y su evaluación permite poder tener acciones específicas para reducir la amenaza. En este caso las vulnerabilidades que nos interesan son las derivadas de las amenazas por motivación y relacionadas con los aspectos legales.

Algunos casos en los que la presencia de este tipo de amenazas y acciones perpetradas en contra de la seguridad informática y de la información ha hecho que las partes involucradas

acudan ante autoridades correspondientes e incluso tribunales internacionales para dirimir las consecuencias derivadas.

Es importante señalar que las normas jurídicas han tenido que ir evolucionando ante el avance científico y tecnológico pues una de las características del derecho es que no es apriorístico por lo que no pude encontrarse a la par del surgimiento de los nuevos descubrimientos.

Casos de seguridad informática

Es relevante considerar que gran parte de los casos sobre seguridad informática se centran en cómo las empresas y gobiernos se ocupan de las infracciones de datos o problemas de privacidad,[14] como puede ser el caso del hackeo que puso en riesgo los números de tarjetas de crédito y débito de 4.2 millones de usuarios por medio de la cadena de supermercado Hannaford Bros., en la costa este de los Estados Unidos que registró 1,800 casos de fraude y cuya vulnerabilidad si bien se identificó en febrero de 2008, en realidad se había venido realizando desde diciembre del año anterior[15] o bien el caso de Edward Snowden[16] relativo

[14] Ayyagari, Ramakrishna y Tyks, Jonathan, Disaster at a University: A case strudy in information security, Journal of information Technology Education: Innovations and practice, vol. 11, 2012. Disponible en https://pdfs.semanticscholar.org/2e74/2e0754841a53d98cefb3cc479e2141e1a2b5.pdf, ultima fecha de consulta 19 de junio de 2018.

[15] Véase Clapper, D. L., «Stolen data and fraud: The Hannaford Brothers Data Brach», en Journal of the International Academy for Case Studies, Vol. 16, Special Issue, nº. 1, 2010, pp. 121-130. Disponible en http://www.alliedacademies.org/articles/jiacsvol16si12010.pdf#page=133. Última fecha de consulta el 5 de junio de 2018.

[16] Rivera, N., Cronología del caso Edward Snowden, el hombre más buscado del mundo, en el newsletter Hipertextual, sección cultura, 15 de marzo de 2016. Disponible en https://hipertextual.com/2016/03/cronologia-edward-snowden, Consultado el 20 de junio de 2016.
2006 Snowden es contratado por la CIA, 2007-2009 es enviado a Suiza y comienza a sentirse desilusionado por como su gobierno controlaba la información del resto del mundo, 2009-2012 tras un reporte de su supervisor Snowden deja de laborar para la CIA e ingresa a la NSA en Hawaii, de diciembre 2012 a enero de 2013 contacta con personas del diario The Guardian, es despedido de su empleo viaja de Hong Kong a Rusia donde es asilado temporalmente.
Cervera, José, Assange contra Snowden: parecidos y diferencias, diario Turning, 6 de enero de 2014. Disponible en https://www.eldiario.es/turing/vigilancia_y_privacidad/Assange-Snowden-parecidos-diferencias_0_215228764.html, útlima fecha de consulta, 20 de junio de 2018.

a sustracción y publicidad de información confidencial de clasificado como TOP Secret por parte del gobierno de Estados Unidos en el cual se han involucrado diversos personajes acusados de espionaje.

De los casos anteriores se desprende que ante una situación que atenta contra la seguridad informática que pone en riesgo la información, se debe de comunicar a los involucrados sobre la situación y hace de su conocimiento los posibles riesgos. Si la situación se deriva del incumplimiento que obliga a los participantes, es menester dar una respuesta y señalar cuál es la estrategia a seguir ante tal situación ya que negarla o tratar de ocultarla puede complicar las situación misma y agravar la responsabilidad. Evidentemente siempre es imprescindible conocer las normas que regulan cada una de las situaciones particulares.

Hoy, la gran dependencia que se tiene del uso de la tecnología puede representar sin lugar a riesgos que impacten a derechos fundamentales. Un ejemplo de esto se ha dado en la industria médica ya que la denegación al acceso a información médica pude poner en un riesgo la vida misma de los pacientes.

Nos referimos al caso de Reino Unido, en donde un ataque a los servicios médicos y registros de ese país resultaron inaccesibles poniendo así en riesgo numerosas vidas mientras los hackers trataron de extorsionar al personal de los hospitales.

El 12 de mayo de 2017 a las 12.30 hora local del Reino Unido un ransomware (nombre en inglés ransom= rescate y ware tomado de software programa), un programa de rescate masivo detuvo el trabajo de 16 hospitales a lo largo de ese país.

El programa encriptó y congeló los sistemas de manera que cuando los trabajadores quisieron acceder a sus ordenadores, se encontraron con el mensaje de que debían pagar 300 bitcoins a cambio de liberarlos de la situación.

La situación se agravó cuando comenzaron numerosas cancelaciones de citas y en general el desorden que se causó pues los hospitales fueron incapaces de acceder a los expedientes

Fernández, Rodrigo, Rusia prorroga a Snowden el permiso de residencia hasta 2020.

médicos básicos. Incluso alguno de estos 16 hospitales tuvo que cancelar todas las cirugías que no fueran consideradas como urgentes teniendo que re-agendar posteriormente.[17]

Lo más grave del asunto recae en lo revelado posteriormente, y es que el ataque (que se realizó a través de un fragmento de software o secuencia de comandos utilizada para aprovechar justamente otro software) tomó ventaja de las vulnerabilidades de la seguridad de un sistema de información para conseguir accesos de forma no autorizada, (control de sistemas de cómputo, y hacer denegaciones de servicios) conocidos por su palabra en inglés como *exploit* que contacta con el software vulnerable de manera ya sea remota (en la red), o local y de esta manera accede al sistema que se va a atacar, aunque también puede realizarse a través de ficheros.

En este caso específico el ataque se realizó a través de vulnerabilidades de Microsoft, Adobe, pero lo más interesante es que al profundizar en el caso se descubrió que el *exploit* fue desarrollado por la Agencia Nacional de Seguridad del gobierno de los Estados Unidos, (National Security Agency) conocido como un software llamado EternalBlue y que fue dirigido para vulnerar la seguridad de Windows.[18]

Es importante que se analice cuál es la responsabilidad Estatal, y en dado caso cómo se deben reparan las afectaciones a las empresas y a los individuos específicamente pues estamos ante un derecho fundamental que fue vulnerado que es el de la salud.

Seguridad informática y factor humano

"De acuerdo con un estudio realizado por The Diffusion Group, dado a conocer por el portal Dinero.com, en el cual se encuestó a pequeñas empresas, el 60% de las que pierden

[17] Véase Mattei, T. A., «Privacy, confidentiality, and security of health care information: Lessons from the recent Wannacry Cyberattack», en World Neurosurgery News, agust 2017, vol. 107, pp. 972-974.
[18] Brandom, R., «UK Hospitals hit with massive ransomwareattck», en The Verge, 12 mayo 2012, disponible en https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin, Última fecha de consulta el 21 de junio de 2018.

información cierran dentro de los seis meses siguientes a la catástrofe. Un estudio similar, pero realizado por la British Chambers of Commerce evidencian que el 93% de los negocios que sufren la pérdida de datos durante más de 10 días, se declaran en quiebra un año después.

La pérdida de datos dentro de una empresa puede, por supuesto, ser causada por varios factores, el principal es el mal funcionamiento del hardware. De hecho, un disco duro muere cada 15 segundos. Otras causas principales de estas pérdidas son el desconocimiento de los empleados al usar incorrectamente las herramientas de almacenamiento o por la corrupción de software, virus, desastres naturales y la piratería".[19]

Un gran porcentaje de pérdida de la información se debe al extravío de equipos portátiles, sean computadoras, celulares, agendas electrónicas, discos compactos, memorias usb. En otros casos estamos ante fugas de información en donde los empleados son los que venden la información confidencial a otras empresas, o un empleado pierde los documentos como se había señalado anteriormente como amenaza por motivación.

Así por un lado habrá que enfrentar en materia de seguridad informática amenazas por motivación de tipo internas derivados por: la falta de integridad de los empleados, el robo de propiedad intelectual, la fuga de información, el espionaje industrial, la interrupción operacional, algún conflicto entre empelados, el crimen corporativo, la conducción de un negocio personal para el cual se extrae la información necesaria o bien por el bajo desempeño del empleado y por otro lado las amenazas por motivación tanto internas como externas de los equipos como es el hackeo y el crimen organizado, los virus, troyanos, worms, exploits, incluso las políticas de seguridad interna.

[19] Beroes Rios, M. A., «60% de las empresas que pierden información quiebran en seis meses», CIO América Latina, 2 de febrero de 2016. Disponible en http://www.cioal.com/2016/02/02/82195/. Última fecha de consulta el 5 de julio de 2018.

IUS ET SCIENTIA (ISSN: 2444-8478) 2018, Vol.4, nº 1, pp. 19-39
"Tecnologías, seguridad informática y derechos humanos", Evelyn TÉLLEZ CARVAJAL
Universidad Nacional Autónoma de México. evelyn.tellez@infotec.mx
Recibido: 21/06/2018. Aceptado: 01/07/2018
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2018.i01.03

Existen estándares internacionales por ejemplo las normas ISO[20] específicamente que abonan al tema de las políticas de seguridad que entre varias cosas debe de incluir en cuanto a:

1) Herramientas Cifrado: el filtrado, control de acceso, perímetro de seguridad;
2) Personas: sensibilización, formación, control y vigilancia;
3) Procedimientos gestión: controles, vigilancia, evaluación seguimiento, actualización respaldo, restauración, seguridad, explotación y conformidad;
4) *Respetar la Legislación*. Las normas van desde qué tipo de datos son manejados, las obligaciones de los particulares, como avisos de privacidad, pero también de los sujetos obligados la disponibilidad de la información: los estándares mínimos de protección así como las consecuencias en el incumplimiento que muchas veces se debe al desconocimiento de las normas, a la oscuridad de su significado o de la falta de pericia de las autoridades e incluso a la ausencia de seguimiento del cumplimiento de las mismas resoluciones.

Como se mencionó anteriormente es menester recordar que el derecho tiene componentes éticos y que por ello antes de realizar alguna actividad que esté relacionada con el tratamiento de la información deben de hacerse las preguntas ¿qué norma faculta que trate la información o que norma sanciona que lo haga?, ¿cuáles son las motivaciones y necesidades para realizar una actividad determinada que involucra información y medios tecnológicos?

Es necesario saber el valor de la información que se posee y de los sistemas que deben proteger dicha información.

[20] Véase ISO/IEC 1779 Tecnología de la Informacíon Técnicas de seguridad. Código de práctica de la gestión de la seguridad de la información. https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

IUS ET SCIENTIA (ISSN: 2444-8478) 2018, Vol.4, nº 1, pp. 19-39
"Tecnologías, seguridad informática y derechos humanos", Evelyn TÉLLEZ CARVAJAL
Universidad Nacional Autónoma de México. evelyn.tellez@infotec.mx
Recibido: 21/06/2018. Aceptado: 01/07/2018
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2018.i01.03

Conclusiones

Las TIC son herramientas de gran utilidad que han permitido automatizar procesos y concentrar grandes cantidades de datos. Los sistemas informáticos que son utilizados en estos procesos se han convertido en el objetivo de ataques cibernéticos que ponen en riesgo la seguridad de las informaciones que se almacenan en dichos sistemas.

El derecho es un componente necesario al momento de hacer frente a las actividades ilícitas que se despliegan en contra tanto de los sistemas informáticos como de la información almacenada en los mismos, sin embargo, aún hoy en día no hay barrera que pueda evitar que la seguridad informática se vea vulnerada sea por amenazas por motivación o bien por amenazas externas como pueden ser los fenómenos naturales.

Sin lugar a dudas los individuos nos encontramos merced a los ataques digitales y en ocasiones como se ha dejado expuesto somos nosotros mismos los que ponemos en riesgo los sistemas informáticos por desconocimiento o falta de pericia. Es por ello que es necesario difundir y tomar conciencia de los derechos y las responsabilidades que como individuos tenemos ante esta realidad en donde las tecnologías pueden representar grandes logros y aciertos pero que también traen aparejados riesgos que tenemos derecho a conocer.

Sin lugar a dudas el derecho a saber es una herramienta que empodera a los individuos y que podemos exigir para así estar aún más conscientes de los riesgos a los que nos enfrentamos con el uso de estas nuevas tecnologías y con ello poder anticipar las amenazas y los riesgos que tenemos hoy por hoy.

Fuentes de consulta

AYYAGARI, R. y TYKS, J., Disaster at a University: A case strudy in information security, Journal of information Technology Education: Innovations and practice, vol. 11, 2012. Disponible en https://pdfs.semanticscholar.org/2e74/2e0754841a53d98cefb3cc479e2141e1a2b5.pdf, ultima fecha de consulta 19 de junio de 2018.

BALDWIN, D. A., «The concept of security» *Review of International Studies*, nº. 23, p. 5. Disponible en: https://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1997)%20The%20Concept%20of%20Security.pdf. Fecha de consulta el 5 de junio de 2018.

BEROES RIOS, M. A., «60% de las empresas que pierden información quiebran en seis meses», CIO América Latina, 2 de febrero de 2016. Disponible en http://www.cioal.com/2016/02/02/82195/. Última fecha de consulta el 5 de julio de 2018.

BIROT, Y., «La science au service de la foresterie en región méditerranéenne: les vois du futur», en *Forêt médoterranéene*, t. XXXII, nº. 4, diciembre 2011.

BRANDOM, R., «UK Hospitals hit with massive ransomwareattck», en The Verge, 12 mayo 2012, disponible en https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin, Última fecha de consulta el 21 de junio de 2018.

CERVERA, J., Assange contra Snowden: parecidos y diferencias, diario Turning, 6 de enero de 2014. Disponible en https://www.eldiario.es/turing/vigilancia_y_privacidad/Assange-Snowden-parecidos-diferencias_0_215228764.html, útlima fecha de consulta, 20 de junio de 2018.

CLAPPER, D. L., «Stolen data and fraud: The Hannaford Brothers Data Brach», en Journal of the International Academy for Case Studies, Vol. 16, Special Issue, nº. 1, 2010, pp. 121-130. Disponible en

http://www.alliedacademies.org/articles/jiacsvol16si12010.pdf#page=133. Última fecha de consulta el 5 de junio de 2018.

FERNÁNDEZ, R., Rusia prorroga a Snowden el permiso de residencia hasta 2020.

Foro Mundial de Solidaridad Digital. Disponible en https://www.itu.int/itunews/manager/display.asp?lang=es&year=2005&issue=03&ipage=global_digital&ext=html, última fecha de consulta 6 de julio de 2018.

GARRIGA DOMÍNGUEZ, A., *Tratamiento de datos personales y derechos fundamentales*, España, Dykinson, 2004.

GÓMEZ VIEITES, A., *Seguridad Informática*, 2ª. ed., Madrid, Ra-MA, 2014.

HEINZ, F., «Software vs. Copyright», en Argentina Copyleft. La crisis del modelo de derecho de autor y las prácticas para democratizar la cultura, Argentina, Fundación Henrich Böll Stiftung. Cono Sur, 2010.

http://documents.irevues.inist.fr/bitstream/handle/2042/47148/FM_XXXII-4_349-353.pdf?sequence=1&isAllowed=y. Fecha de consulta 5 de junio de 2018.

Internet Corporation for Assigned Names and Numbers está disponible en: https://www.icann.org/es. Última fecha de consulta el 5 de junio de 2018.

ISO/IEC 1779 Tecnología de la Información Técnicas de seguridad. Código de práctica de la gestión de la seguridad de la información. https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf. Última fecha de consulta el 20 de junio de 2018.

MATTEI, T. A., «Privacy, confidentiality, and security of health care information: Lessons from the recent Wannacry Cyberattack», en World Neurosurgery News, agust 2017, vol. 107.

Plan de Acción de Ginebra. Disponible en https://www.itu.int/net/wsis/outcome/booklet/plan_action_D-es.html, última fecha de consulta el 20 de junio de 2018.

Resolución aprobada por la Asamblea General 55/2. Declaración del milenio, disponible en http://www.un.org/spanish/milenio/ares552s.htm, última fecha de consulta el 20 de junio de 2018.

RIVERA, N., Cronología del caso Edward Snowden, el hombre más buscado del mundo, en el newsletter Hipertextual, sección cultura, 15 de marzo de 2016. Disponible en https://hipertextual.com/2016/03/cronologia-edward-snowden, Consultado el 20 de junio de 2016.