XXVI
TECMUN Jr.

Comisión de Ciencia y Tecnología para el Desarrollo

"Sobre todo, sean capaces de sentir en
lo más hondo cualquier injusticia
cometida contra cualquiera en
cualquier parte del mundo. Es la
realidad más linda de un revolucionario."
- *Ernesto Guevara*

Delegados,

Siempre creí que eso de ser presidente era para la gente que sabía debatir o que ganaba la Mención Honorífica o el Mejor Delegado. Sin embargo, aquí me encuentro. Quiero aprovechar este momento para desearles lo mejor durante estos tres días, días que no serán fáciles, días cansados, pero al final, días que te dejan con una gran satisfacción. Podrían creer que a estas alturas ya no estoy nervioso de abrir el foro, que ya no siento ese cosquilleo que recorre mi cuerpo durante las sesiones, que ya estoy seguro de mis palabras y que todo lo que salga de mi boca va a ser completamente acertado, pero a decir verdad, todavía no me siento así. Me siento como si fuera mi primera vez en TECMUN como si fuera mi primera vez siendo delegado y tuviera que hacer mi primera intervención, siento los mismos nervios que ustedes cuando alzan su placa y están preocupados por lo que tienen que decir. Sigo sintiendo ese cosquilleo por todo mi cuerpo cuando estoy parado frente a ustedes, siento esa alegría, esa emoción que me causa el debate, sigo sintiendo.

No considero que sentirme igual que la primera vez sea malo, todo lo contrario, me transporta a la persona que era antes y me hace reflexionar lo que soy ahora. Yo también fui un delegado, y con eso me refiero a que era un delegado que no aportaba ideas interesantes al debate, participaba cada que la mesa lo obligaba y nunca tenía algo interesante que decir. Siempre permanecí callado, ante las adversidades, ante las injusticias, ante los problemas, siempre estuve en silencio. No cometan los mismos errores que yo, alcen la voz, no se callen, hagan frente ante las injusticias, no dejen de luchar por lo que quieren. Confío en sus conocimientos, en sus esperanzas y en sus sueños para este modelo y sé que todo lo que hagan los hará llegar muy lejos porque, si yo siendo un delegado nervioso que no participaba y que siempre se callaba ante los problemas llegó a ser presidente, ustedes que alzan su voz y se hacen oír ¿Cuántas cosas no podrán hacer?

_____

Israel Sánchez Miranda

Presidente de la Comisión de Ciencia y Tecnología para el Desarrollo

XXVI TECMUN Jr.

Antecedentes de la Comisión de Ciencia y Tecnología para el Desarrollo

La Comisión de Ciencia y Tecnología para el Desarrollo (CCTD) es un órgano subsidiario del Consejo Económico y Social. Fundada en 1992 como consecuencia del anhelo de la ONU por mejorar la aplicación científica y tecnológica de sus estados miembros, la CCTD se encarga de examinar todos los asuntos referentes a ciencia y tecnología a nivel mundial. Su principal función es promover el uso de la tecnología y la innovación de diferentes campos científicos para impulsar el desarrollo de los estados que la conforman creando nuevas políticas relativas a los avances tecnológicos y científicos más recientes y generando inteligencia en países en vías de desarrollo, aunado a esto la comisión puede formular recomendaciones y brindar asesorías técnicas a los países miembros de las Naciones Unidas.

Tópico A

Políticas regulatorias para salvaguardar el uso responsable de la biotecnología y apoyar al desarrollo sostenible.

Por: Israel Sánchez Miranda
Abril Valenzuela Domínguez

Introducción a la problemática

Se denomina biotecnología a "toda aplicación tecnológica que utilice sistemas biológicos y organismos vivos o sus derivados para la creación o modificación de productos o procesos para usos específicos" (Naciones Unidas, 1992). Gracias a los avances en el campo de la biotecnología se ha logrado la creación de varios productos beneficiosos para el desarrollo y la sostenibilidad de las naciones, desde la creación de cultivos genéticamente modificados hasta su influencia en la industria farmacéutica, la biotecnología es una herramienta de suma eficacia para el avance socioeconómico de las delegaciones. Pese a los beneficios que ésta puede traer, el panorama biotecnológico teme por la posible amenaza del uso indeseable de esta tecnología, la creciente tendencia del *biohacking* (biólogos y/o biotecnólogos "caseros") o la creación de laboratorios comunitarios y clandestinos pueden significar una amenaza a nivel internacional, en un intento por reducir esta posible amenaza se han hecho varias regulaciones en el campo de la biotecnología, impidiendo el uso específico de ciertas áreas de la biotecnología en diferentes países. Esto ha desatado una polémica muy polarizada en donde se justifican las regulaciones con el fin de proteger a las naciones, sin embargo, al impedir el uso de la biotecnología en ciertas áreas se está afectando directamente el avance social y económico de los países.

Importancia del uso de la biotecnología para los Objetivos de Desarrollo Sostenible

La biotecnología provee muchas oportunidades para el desarrollo en varios sectores, una de éstas es la agricultura. En 2016, tras 20 años de investigación, un grupo de 20 de los mejores científicos de la Academia Nacional de Ciencia, Ingeniería y Medicina de los Estados Unidos demostró que los cultivos pueden ser mejor aprovechados y ser más compatibles con el medio ambiente, dañándolo menos y apoyando a la biodiversidad, "los agentes de protección de cultivos pueden ser utilizados [...] incrementando la diversidad de plantas y animales en el campo" (Little, s.f.), este mismo estudio no sólo logró demostrar los beneficios de los Organismos Genéticamente Modificados (GMOs por sus siglas en inglés) sino que también logró rebatir un artículo realizado por el biólogo francés Gilles-Éric Sérlain en 2012; dicha investigación empezó con el famoso pensamiento que afirmaba que los GMOs generaban cáncer, aseveración que resultó ser falsa y no se ha podido comprobar. Otro aspecto importante de la biotecnología es que mejora la calidad de los alimentos evitando reacciones alérgicas y aumentando la cantidad de vitaminas, de igual forma las plantas Genéticamente Modificadas

(GM) han demostrado ser más seguras que las convencionales. Con esta clase de avances se podrán lograr varios de los Objetivos de Desarrollo Sostenible (ODS), éstos son metas globales que, se espera, erradiquen problemas de índole internacional como la pobreza, acceso a la educación, protección ambiental, etc., propuestos por los miembros de las Naciones Unidas que deberán alcanzarse para el año 2030.

Otra área donde la biotecnología aporta varios beneficios es la medicina; conocida como biotecnología roja, ésta se encarga de mejorar la salud tanto de humanos como de animales, investigando diversas enfermedades y desarrollando nuevos medicamentos. Se han tenido avances reduciendo el número de pacientes con cáncer, rabia, sarampión o Virus de Inmunodeficiencia Humana (VIH) -con ayuda de la creación de vacunas recombinantes-, se espera que con los avances en el campo de la medicina se puedan utilizar este tipo de vacunas con el fin de crear inmunidad ante ciertas enfermedades y/o bacterias para evitar la proliferación de éstas alrededor del mundo, especialmente en los países en vías de desarrollo. De igual forma, los cultivos GM pueden servir de apoyo para acabar con enfermedades virales, se les conoce como vacunas comestibles, este tipo de plantas actúan para proteger el cuerpo produciendo defensas sumamente eficaces contra ciertas enfermedades.

El congreso Bio América 2016 se enfocó en hablar sobre la fuerte influencia que tiene la biotecnología en Iberoamérica, resaltando factores importantes como la biotecnología ambiental explicando los procesos que sirven para manejar aguas tratadas y lodo, de igual forma, se fomentó el apoyo de la nanotecnología para poder desarrollar tratamientos de agua para potabilizarla y facilitar el desarrollo de comunidades con dificultades para conseguir agua limpia, también se destacó que la biotecnología podría contrarrestar los daños que ha generado el cambio climático en los últimos años.

La importancia de la biotecnología en la actualidad se debe a varios factores, uno de los más importantes es su versatilidad en el apoyo al desarrollo sostenible en diversas áreas, por tal motivo es crucial cuidar y propiciar el desarrollo de la biotecnología para poder lograr los ODS y aprovechar sus beneficios para ayudar a países en vías de desarrollo a la par que se generan nuevas tecnologías para la sostenibilidad de las diferentes delegaciones.

Riesgos del uso irresponsable de la biotecnología

A pesar de los grandes beneficios que la biotecnología puede traer para el desarrollo, ésta puede representar una gran amenaza si no es usada de manera responsable y precavida. Las amenazas

que el uso irresponsable de la biotecnología trae se pueden dividir en cuatro grupos: los riesgos a la salud humana, los riesgos al medio ambiente, los riesgos económicos y los riesgos a la seguridad.

La creación de alimentos GM desde un inicio ha sufrido severas críticas debido a los riesgos que puede traer a la salud humana, aunque no haya evidencia, se teme que la concentración en exceso de ciertos compuestos pueda ocasionar alergias y enfermedades mortales a los consumidores. Por ello se han generado políticas y medidas de seguridad y salubridad que miden y controlan la calidad de estos productos con el fin de reducir la amenaza de repercusiones negativas a la salud humana.

Otro de los peligros que el mal uso de la biotecnología conlleva es el daño colateral que puede causar al medio ambiente, el uso excesivo de GMOs en cultivos genera mutaciones a los organismos dañinos que habitan en los alrededores, debido a la larga exposición que tienen ante estas plantas, organismos perniciosos como la maleza o insectos se pueden hacer resistentes no sólo ante las toxinas que tienen los GMOs sino también ante los pesticidas que se usen para erradicarlos. Todo esto puede ocasionar un severo desbalance en el ambiente, afectando a los seres vivos que lo habitan y al mismo ser humano.

En términos económicos, el impacto de la biotecnología a gran escala es preocupante. La biotecnología es difícil de desarrollar sin la infraestructura adecuada y no todos los países cuentan con los recursos económicos para poder generar ese tipo de equipamientos, por lo que, si países tecnológicamente desarrollados continúan avanzando en campos de la biotecnología, la brecha tecnológica que habrá entre éstos y los países en vías de desarrollo crecerá de manera exponencial. Esto puede traer problemas grandes a nivel económico, generando monopolios en la industria de la agricultura y segregando a países que no cuentan con este tipo de tecnología.

Aunado a lo previamente mencionado se encuentra el temor por ataques bioterroristas, la idea de que grupos extremistas utilicen virus modificados como el ébola, la erradicada viruela o incluso la gripe para conseguir sus propios fines se ha estado extendiendo principalmente en países de la Unión Europea como España y países de Occidente, se han estado tomando varias medidas pero el crecimiento desmedido de los avances biotecnológicos solamente incrementa el riesgo de estos ataques, poniendo en peligro la seguridad internacional en niveles de salud con el uso de bacterias y virus letales y alimentación gracias a la creación GMOs.

La tendencia del biohacking y la amenaza que puede representar

Con la creciente y desmedida expansión de la biotecnología, se ha generado una inmensidad de plataformas tecnológicas y comunidades que han dado origen a una de las tendencias más innovadoras de los últimos años, el *biohacking*, conocido también como *DIYBio* (*Do It Yourself Bio*) este movimiento consiste en el uso y aplicación de la biotecnología y tecnología en un nivel más cotidiano. Esta tendencia lleva los conocimientos del campo de la biotecnología a laboratorios caseros y/o clandestinos, facilitando la creación de cadenas de ADN e incluso nuevos microorganismos. El *biohacking* se puede dividir en dos grandes grupos: la manipulación y creación de organismos y medicamentos y la creación de *gadgets* que ayuden al ser humano.

La manipulación de organismos y creación de medicamentos es una de las aplicaciones más comunes del *biohacking*, ésta se encarga de crear diversos medicamentos y manipular e incluso crear nuevos organismos vivos como virus y/o bacterias. Su proliferación se debe a la expansión masiva de recetas, reactivos y equipamiento para la creación de medicamentos y organismos que se ha dado en internet; se pueden encontrar páginas y hasta comunidades en línea en donde se pueden conseguir infinidad de artefactos necesarios para esta área del *biohacking.* Un grupo de *biohackers* conocidos como *Four Thieves Vinegar* logró crear una inyección de epinefrina igual de eficaz y mucho más barata que una inyección convencional, la finalidad de estos *biohackers* es esparcir estos conocimientos para que cada persona pueda crear sus productos desde su propia casa.

Otra aplicación de la biotecnología es el uso de componentes electrónicos en organismos vivos para el mejoramiento de sus habilidades, un ejemplo de esto es el desarrollo de chips que monitoreen los signos vitales, lentillas que permiten ver en la oscuridad, sensores que sustituyan en su totalidad las contraseñas, entre otros artefactos. El uso de estos componentes permitiría un gran desarrollo y avance en la tecnología de la sociedad.

Pese a que el principal objetivo de los *biohackers* no es dañar a la sociedad, sino todo lo contrario, la expansión desmedida de esta tendencia puede significar varios riesgos no sólo a nivel nacional sino también a nivel internacional; entre los principales riesgos está la creación ya sea accidental o planeada de algún virus o bacteria que pueda causar una pandemia, de igual manera, se cree que grupos extremistas podrían aprovechar la poca regulación y seguridad que

hay en este ámbito y podrían usar el *biohacking* a su favor. Otro de los principales riesgos de la proliferación del *biohacking*, en específico el área de creación de *gadgets*, es el riesgo de acceder al funcionamiento de estos dispositivos de manera remota ya sea intencional o accidentalmente, tal y como ocurriría con un marcapasos y afectar directamente a la persona. Cuando se juntan la biotecnología química y la tecnológica se pueden generar productos beneficiosos como hebras de ADN que contengan información digital y se suprima por completo el uso de contraseñas, no obstante, esto puede representar un grave riesgo ya que se ha comprobado que se puede injertar algún virus informático con la capacidad de hackear sistemas en las hebras del ADN.

Los problemas relacionados con esta tendencia tienden a acrecentarse debido a que existen diversas inconsistencias en las leyes de las delegaciones sobre si debería penalizarse esta práctica o simplemente tomar precauciones para evitar daños colaterales, por ejemplo, en 2004 en los Estados Unidos de América el artista Steve Kurtz al estar trabajando con GMOs ocasionó la muerte súbita de su esposa, el FBI lo arrestó acusándolo de bioterrorismo, al investigar más sobre Kurtz se llegó a la conclusión de que no se le debía juzgar por estos cargos y se decidió aplicarle cargos federales por fraude postal, en 2008 éstos también fueron retirados ya que no hay ley en Estados Unidos que expresamente condene el trabajar con GMOs fuera de instalaciones no autorizadas. En cambio, en Europa, específicamente en Alemania, con el fin de evitar la expansión de esta tendencia se han aplicado penas de prisión y multas de hasta cincuenta mil euros a aquellos individuos que practican esta tendencia. Las inconsistencias penales al *biohacking* son una de las principales amenazas y una de las causas por las que éste puede representar un riesgo a nivel internacional.

Regulaciones de la biotecnología y sus consecuencias

La biotecnología utiliza un tipo de tecnología horizontal; es decir, que afecta a muchos sectores de la actividad humana como pueden ser la salud, minería, agricultura, elaboración de fármacos, producción de energía, etc. Al considerarse como una de las tecnologías con más peso económico y relevancia en la sociedad, es importante poder contar con regulaciones y reglas básicas para un buen uso y desarrollo. Tomando en cuenta que la biotecnología tiende a "operar" en organismos vivos ésta tiene suma relevancia, por lo que es coherente que las naciones más desarrolladas quieran avanzar en el desarrollo de la biotecnología y al mismo tiempo evitar daños al ambiente y a la sociedad.

Se denomina bioseguridad al conjunto de procedimientos y reglas que se utilizan con la finalidad de poder garantizar la protección humana, animal y ambiental en todas las aplicaciones de la biotecnología y diversos procesos químicos, la bioseguridad es la encargada de evaluar los productos y experimentos que se van generando. La evaluación de GMOs consiste en revisar el alimento modificado y se debe tomar como referencia el alimento no transgénico para así poder revisar a fondo sus diferencias, durante todo el proceso se debe llegar a la conclusión que el alimento modificado no ha tenido cambios que puedan afectar el valor nutricional o su inocuidad, de igual forma, la evaluación en el campo de la agricultura consiste en utilizar herbicidas para generar resistencia y verificar si éste genera una clase de inmunidad. Con este tipo de evaluaciones se puede garantizar que todos los productos ayuden al desarrollo y mejoren los productos realizados, es importante resaltar que con el apoyo de la bioseguridad los nuevos procedimientos de desarrollo en la agricultura podrían ser más seguros.

El Protocolo de Cartagena es un acuerdo internacional que tiene como objetivo la regulación del movimiento transfronterizo de los Organismos Genéticamente Modificados como consecuencia del avance de la biotecnología, este protocolo entró en vigor en el año 2003 como protocolo suplementario al Convenio de Diversidad Biológica (1993), convenio en el cual se establecieron regulaciones y procedimientos para mantener la diversidad ambiental. La principal función de este protocolo es la regulación, manipulación y utilización de forma segura de los organismos modificados que podrían generar adversidades en la diversidad biológica. Después de diversas reuniones con los países participantes, se tomó la decisión de crear un grupo de especialistas jurídicos y técnicos para que se pudieran realizar las normas y procedimientos internacionales sobre temas de biotecnología, años después surgió un nuevo protocolo conocido como: Protocolo de Nagoya–Kuala Lumpur sobre Responsabilidad y Compensación Suplementario al Protocolo de Cartagena sobre Seguridad de la Biotecnología (2010), con este nuevo protocolo se logró mantener la idea del uso seguro en todas las áreas donde la biotecnología pueda desarrollarse y tomar medidas de seguridad y restricciones con el fin de evitar un mal uso de esta tecnología.

La Comisión Europea (1958) es una de las comisiones que ha trabajado con el desarrollo de biotecnología y ha tratado de crear regulaciones pertinentes, esta comisión se ha centrado en el desarrollo de la relación entre la biotecnología y la sociedad tomando como base seis aspectos relevantes:

- Aspectos éticos relacionados con la vida humana en la práctica médica, el diagnóstico y consejo médico, la investigación en embriones humanos o la secuenciación del genoma humano;
- aspectos jurídicos relativos a los límites de los derechos de propiedad intelectual;
- cuestiones ambientales relacionadas con los posibles efectos de la difusión de GMOs;
- implicaciones a la seguridad y salud de los trabajadores de empresas biotecnológicas y de sus productos;
- valoración de las repercusiones socioeconómicas de las nuevas biotecnologías (sectores agrícola y ganadero, etc.) y,
- cuestiones relativas a la formación, información y participación ciudadana en la toma de decisiones y a la elección de alternativas relacionadas con la biotecnología.

Se deben ocupar las regulaciones necesarias para poder mejorar cada vez más el uso de la biotecnología en la vida diaria. Afortunadamente, las consecuencias del uso de las regulaciones han sido positivas y han sido un factor primordial para evitar desastres en el ambiente así como también en la sociedad. El bioterrorismo es la única área que no sigue este tipo de regulaciones pero ya se han tomado medidas y acciones necesarias para contrarrestar su proliferación alrededor del mundo. Tomando en cuenta los diversos protocolos y acuerdos a los que las naciones han llegado, se concluye que la biotecnología no busca generar daños a la sociedad sino todo lo contrario, generar oportunidades para aumentar el desarrollo sostenible en las diversas áreas donde se puede aplicar y que en las manos correctas puede generar beneficios muy grandes para las naciones, por lo que se debe evitar su mal uso y crear políticas y regulaciones que eviten los riesgos potenciales del uso indebido de la biotecnología a la par que se propicia el desarrollo de ésta en los diferentes países evitando un rezago tecnológico.

Referencias

1. Agro-Bio. (2016). *La biotecnología será muy importante para el desarrollo sostenible de Iberoamérica.* Recuperado el 5 de junio de 2018, de Asociación de Biotecnología Vegetal Agrícola. Web <http://www.agrobio.org/agricultura/biotecnologia-importante-desarrollo-sostenible-iberoamerica/>
2. Altieri, M. (2001). *Los impactos ecológicos de la Biotecnología Agrícola.* Recuperado el 6 de junio de 2018, de Actionbioscience. Web <http://www.actionbioscience.org/esp/biotecnologia/altieri.html>
3. Arias, J. (1992). *Los riesgos de la biotecnología.* Recuperado el 6 de junio de 2018, de El Tiempo. Web <http://www.eltiempo.com/archivo/documento/MAM-65612>
4. Baumgaertner, E. (2018). *El riesgo de los laboratorios genéticos caseros.* Recuperado el 15 de junio de 2018, de The New York Times. Web <https://www.nytimes.com/es/2018/05/16/genetica-edicion-laboratorios-virus/>
5. Bayer. (s.f.). *"Biotecnología - Una oportunidad para el desarrollo sustentable"* Eco-Forum organizado por Bayer y la Universidad Tecnológica de Varsovia. Recuperado el 5 de junio de 2018, de Bayer Argentina. Web <http://bayer.com.ar/centro-de-prensa/noticias/biotecnologia-una-oportunidad-para-el-desarrollo-sustentable.html>
6. BBC Mundo. (2016). *"Los cultivos transgénicos son seguros"*: las conclusiones de 20 años de investigaciones. Recuperado el 13 de junio de 2018, de BBC. Web <http://www.bbc.com/mundo/noticias/2016/05/160519_ciencia_alimentos_modificados_peligros_ninguno_gtg>
7. Biotecnología. (s.f.). *Organismos Reguladores en Biotecnología.* Recuperado el 15 de junio de 2018, de Biotecnología. Web <http://porquebiotecnologia.com.ar/index.php?action=cuaderno&opt=5&tipo=1&note=19>
8. BiotecPedia. (s.f.). *Biotecnología roja.* Recuperado el 5 de junio de 2018, de BiotecPedia. Web <https://biotecpedia.wordpress.com/biotecnologia-roja/>
9. Boehringer Ingelheim. (s.f.). *Vacunas recombinantes y su importancia actual.* Recuperado el 5 de junio de 2018, de Boehringer Ingelheim. Web

<http://www.conasamexico.org.mx/conasa/2011_docs_19a_reunion/201110_26-miercoles/salon_MONTEBELLO/PRODUCTOS_BIOLOGICOS/comite_18/CARLOS_GONZALEZ.pdf>

10. Cique, A. (2017). *"Biohacking" y "biohackers"*: amenazas y oportunidades. Recuperado el 15 de junio de 2018, de *Instituto Español de Estudios Estratégicos.* Web <http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO93-2017_Biohcking_CiqueMoya.pdf>

11. Domínguez, A. & Vázquez, M. (s.f.). Ensayo - *"Biotecnología para el desarrollo sustentable"*. Recuperado el 5 de junio de 2018, de Civilpedia. Web <https://civilpedia.wordpress.com/articulos-2/ensayo-biotecnologia-para-el-desarrollo-sustentable/>

12. Dumonteil, E. (2000). *Vacunas de DNA: el presente y el futuro.* Recuperado el 5 de junio de 2018, de Revista Biomédica. Web <http://www.revbiomed.uady.mx/pdf/rbs00113.pdf>

13. EITB. (2018). *Seguridad alimentaria: de listeria al bioterrorismo y detectar el glaucoma.* Recuperado el 6 de junio de 2018, de EITB. Web <http://www.eitb.eus/es/radio/radio-euskadi/programas/la-mecanica-del-caracol/detalle/5452715/seguridad-alimentariade-listeria-al-bioterrorismo-detectar-glaucoma/>

14. ExtraConfidencial. (2017). *España y Occidente temen un ataque bioterrorista con el virus de la viruela por parte de ISIS: el Gobierno dispone de un stock suficiente para afrontarlo*. Recuperado el 6 de junio de 2018, de ExtraConfidencial. Web <https://extraconfidencial.com/noticias/espana-y-occidente-temen-un-ataque-bioterrorista-con-el-virus-de-la-viruela-por-parte-del-isis/>

15. Fundación Antama. (2018). *La Biotecnología en los Objetivos de Desarrollo Sostenible de las Naciones Unidas.* Recuperado el 5 de junio de 2018, de Fundación Antama. Web <http://fundacion-antama.org/la-biotecnologia-en-los-objetivos-de-desarrollo-sostenible-de-las-naciones-unidas/>

16. Hidalgo, M. (2016). *Biohacking, el nuevo movimiento que hackea tu cuerpo y hace temblar la industria biotecnológica*. Recuperado el 15 de junio de 2018, de Muhimu Web <https://muhimu.es/ciencia-tecnologia/biohacking/>

17. Iáñez, E. & Moreno, M. (s.f.). *Promesas y conflictos de la Ingeniería Genética Vegetal*. Recuperado el 6 de junio de 2018, de UGR. Web <https://www.ugr.es/~eianez/Biotecnologia/vegetal.html#produc>

18. Luján, L. & Moreno, L. (s.f.). *BIOTECNOLOGÍA Y SOCIEDAD: CONFLICTO, DESARROLLO Y REGULACIÓN*. Recuperado el 15 de junio de 2018, de Instituto de Estudios Sociales Avanzados. Web <http://digital.csic.es/bitstream/10261/1992/1/dt-9305.pdf>

19. Martin, L. (2018). *Viruela, ébola y gripe, los tres virus más mortales.* Recuperado el 6 de junio de 2018, de Diario AS México. Web <https://as.com/deporteyvida/2018/05/18/portada/1526661432_144847.html>

20. Mendoza, V. (2015). *Vacunas Recombinantes.* Recuperado el 5 de junio de 2018, de Prezi. Web <https://prezi.com/gfgxdztbpzz7/vacunas-recombinantes/>

21. Ministerio para la Transición Ecológica. (s.f.). *Protocolo de Cartagena*. Recuperado el 15 de junio de 2018, de Gobierno de España. Web <http://www.mapama.gob.es/es/calidad-y-evaluacion-ambiental/temas/biotecnologia/organismos-modificados-geneticamente-omg-/protocolo-cartagena/>

22. Naciones Unidas. (1992). *Convenio sobre la diversidad biológica.* Recuperado el 15 de junio de 2018, de Naciones Unidas. Web <https://www.cbd.int/doc/legal/cbd-es.pdf>

23. Naciones Unidas. (2005). *Biotecnología para el uso sostenible de la biodiversidad: capacidades locales y mercados potenciales.* Recuperado el 5 de junio de 2018, de Comisión Económica para América Latina y el Caribe. Web <https://www.cepal.org/es/publicaciones/2813-biotecnologia-uso-sostenible-la-biodiversidad-capacidades-locales-mercados>

24. Naciones Unidas. (s.f.). *PROTOCOLO DE NAGOYA – KUALA LUMPUR SOBRE RESPONSABILIDAD Y COMPENSACIÓN SUPLEMENTARIO AL PROTOCOLO DE CARTAGENA SOBRE SEGURIDAD DE LA BIOTECNOLOGÍA.* Recuperado el 15 de junio de 2018, de Secretaría del convenio sobre la diversidad biológica Montreal. Web <http://www.wipo.int/edocs/trtdocs/es/cbd-sp/trt_cbd_sp.pdf>

25. Nadal, M. (2017). *"Biohacking", ¿el siguiente paso en la evolución del ser humano?*. Recuperado el 15 de junio de 2018, de Retina. Web <https://retina.elpais.com/retina/2017/09/09/tendencias/1504978992_564033.html>

26. Redacción PA. (2018). *¿Los transgénicos pueden causar cáncer?* Evidencias científicas han demostrado que no. Recuperado el 13 de junio de 2018, de Plumas Atómicas. Web <https://plumasatomicas.com/noticias/ciencia/transgenicos-cancer-evidencia-cientifica/>

27. Romero, G. (2008). *Biotecnología: generalidades, riesgos y beneficios.* Recuperado el 6 de junio de 2018, de Curso Experto Universitario en Biotecnología Aplicada a los Alimentos. Web <http://www2.uned.es/experto-biotecnologia-alimentos/TrabajosSelecc/GloriaRomero.pdf>

28. Ruiz, C. (2008). *Biotecnología y bioseguridad.* Recuperado el 15 de junio de 2018, de Alai. Web <https://www.alainet.org/es/active/27281>

29. Tait, J. (s.f.). *Riesgos medioambientales y regulación de la biotecnología*. Recuperado el 15 de junio de 2018, de Gobierno de España. Web <http://www.mapama.gob.es/ministerio/pags/Biblioteca/fondo/pdf/2687_11.pdf>

30. Threatpost. (2015). *Revisando las ventajas y desventajas del biohacking*. Recuperado el 15 de junio de 2018, de Universidad Nacional Autónoma de M*éxico.* Web <https://www.seguridad.unam.mx/historico/noticia/index.html-noti=2121>

31. Zwanenberg, P. (2013). *La regulación de la biotecnología agrícola y la política de selección de tecnología.* Recuperado el 15 de junio de 2018, de Steps America Latina. Web <http://stepsamericalatina.org/wp-content/uploads/sites/21/2014/12/PvZ_capitulo_La-regulaci%C3%B3n-de-la-biotecnolog%C3%ADa-agr%C3%ADcola_2013.pdf>

A

Aseveración: Asegurar, afirmar o confirmar lo que se dice.

B

Biohacking: Experimentación hecha con material biológico realizada como hobby, actividad lucrativa o criminal por personas que no son oficialmente un científicos y/o expertos.

Bioterrorismo: Forma del terrorismo que usa tecnología biológica para propagar virus o agentes patógenos en la población a manera de intimidación.

E

Embrión: Ser vivo en sus primeras etapas de desarrollo, abarcando desde la fecundación del mismo hasta que el organismo adquiere las características morfológicas correspondientes a su especie.

Epinefrina: Medicamento hecho con adrenalina (hormona segregada por el cuerpo humano) que se usa para tratar el asma, alergias agudas, reanimación cardiaca y como anestesia local.

Erradicar: Eliminar o suprimir una cosa, especialmente perjudicial o negativo, de manera completa y definitiva.

G

Gadget: Aparato o máquina pequeña que tiene un uso en particular.

Genoma: Secuencia de moléculas que constituyen al ADN de un individuo o de una especie.

H

Herbicida: Producto químico que impide el desarrollo de hierbas perjudiciales en un terreno.

I

Índole: Condición, naturaleza e inclinación propia de una persona o cosa.
Inocuidad: Cualidad de un objeto o persona que no hace daño.

M

Monopolio: Acuerdo en el cual una empresa obtiene derecho a aprovechar alguna industria o comercio para que en el mercado la oferta de cierto producto se reduzca a un solo vendedor.

N

Nanotecnología: Tecnología de los materiales que se mide en milímetros, tiene aplicaciones químicas, físicas y biólogas.

P

Pandemia: Epidemia que se esparce a varios países o que ataca a la mayoría de la población.

Pernicioso: Que daña o afecta.

Proliferación: Multiplicarse o reproducirse de manera abundante.

R

Rezago: Atraso o residuo de algo.

T

Transgénico: Organismo vivo que ha sido modificado por medio de genes exógenos para otorgarle nuevas propiedades y mejorarlo.

V

Vacuna recombinante: Vacunas que utilizan parte del genoma u organelos del germen, ofreciendo una respuesta inmunitaria muy fuerte y dirigida a zonas claves del virus.

Tópico B

Medidas de seguridad para la mejora de la Gobernanza de Internet debido a la creciente tendencia del Internet de las Cosas.

Por: Israel Sánchez Miranda
Abril Valenzuela Domínguez

Introducción a la problemática

Desde su creación, Internet ha sido una de las herramientas más beneficiosas para el desarrollo de la sociedad (Escudero, 2017), debido a su gran utilidad e influencia, se ha buscado llegar a un equilibrio entre el gobierno, el sector privado y la sociedad civil dentro de Internet para establecer políticas y medidas que hagan más seguro y efectivo el uso de la red. A este equilibrio se le conoce como Gobernanza de Internet, este objetivo se ha visto obstaculizado debido a lo extenso y diverso que es Internet. A principios de 2018 el *Centre for International Governance Innovation* (CIGI) organizó una encuesta referente al uso y manejo de datos en la red, aproximadamente un 61% de las respuestas expresaban una preocupación por el manejo de sus datos en la red. El creciente riesgo de ciberataques y la ascendente tendencia del Internet de las Cosas (IoT), principio que describe la interconexión de diversos objetos a Internet, ha acrecentando las preocupaciones de la sociedad a que objetos como sensores, cámaras de seguridad, dispositivos médicos, e incluso sus datos personales sean hackeados y utilizados de manera indeseable. Las problemáticas anteriormente mencionadas son los retos más complicados que se tienen que afrontar para poder llegar a una gobernanza más efectiva de Internet.

Antecedentes de ciberataques y manejo irresponsable de datos e información en Internet

Se conoce como ciberataque a los actos que provocan daño y perjudican a personas, instituciones y/o naciones por medio del uso de computadoras o de Internet (Frett, 2015), se debe aclarar que los agravios no son cometidos por los objetos tecnológicos, sino que los usuarios son los que cometen estos ataques a través de computadoras u otros dispositivos electrónicos. Un ciberataque puede tener diversas finalidades, como afectar los sistemas o equipos computacionales que operan una red a nivel nacional o mundial, enfocarse en la obtención de información que está almacenada en bases de datos, entre otras. Cuando un ciberataque se comete contra un sistema su propósito es anular el servicio que proveen ya sea de forma temporal o permanente utilizando *software* o virus informáticos que dificulten su funcionamiento normal, en cambio, cuando el ciberataque está dirigido hacia la información y datos personales del usuario, tiene como finalidad comercializarlos para usos militares o privados. Los ciberataques han adquirido mayor importancia debido a los grandes avances en la tecnología en los últimos años, éstos han aumentado y cada vez se vuelven más sofisticados, por lo que la ciberseguridad se ha vuelto una prioridad en muchas organizaciones que se

encargan de este tipo de situaciones como la Organización Internacional de Policía Criminal (INTERPOL), La Oficina Europea de Policía (EUROPOL), el Centro de Respuesta a Incidentes de Seguridad e Industria (CERTSI), entre otras.

En 2008 se registró un ciberataque hacia *Heartland Payment System*, empresa multinacional de pagos, este atraco estuvo a cargo del *hacker* Albert González, quien robó la información de un promedio de 130 millones de tarjetas de crédito y débito. El sitio de subastas, *eBay*, anunció públicamente en 2014 que había sido víctima de un ataque informático con el que tuvieron acceso a su base de datos donde se encontraba la información de las contraseñas de todos sus usuarios, este suceso afectó a un total de 145 millones de usuarios. En 2013 la empresa de edición *Adobe* sufrió un robo de cuentas bancarias, la empresa expresó que eran un promedio de 3 millones de personas que resultaron perjudicadas, posteriormente se estipuló que el número había aumentado a un total de 152 millones de usuarios afectados. En 2013 la empresa *Yahoo* fue víctima del *phishing* lo que afectó sólo a los usuarios que recibieron correos y al abrirlos sus cuentas fueron secuestradas. En 2016 fue cuando *Yahoo* declaró la mayor vulneración de seguridad sufrida hasta la fecha, según el director de Seguridad Informática de la empresa Bob Lord, los *hackers* obtuvieron "nombres, direcciones de correo electrónico, números de teléfono, fechas de nacimiento, contraseñas encriptadas y, en algunos casos, preguntas y respuestas de seguridad encriptadas o sin encriptar" (Condliffe, 2016). Los ciberataques no sólo han afectado a páginas y empresas que operan en Internet, sino que también han afectado a plataformas gubernamentales, de empresas bancarias, inmobiliarias, etc. y organizaciones internacionales, por eso se deben de tomar acciones pertinentes para poder reducir la frecuencia con la que estos ataques son realizados.

Con la llegada de las Tecnologías de la Información y la Comunicación (TIC), las herramientas que Internet ofrece han mejorado la comunicación y mantienen informada a la población, pero de igual forma puede convertirse en una herramienta perniciosa si no consta de regulaciones necesarias. El peligro de no controlar el uso responsable del Internet puede afectar a niños, adolescentes y adultos por igual pues en muchos sitios los ordenamientos no son los necesarios para evitar fraudes, contenido inapropiado y, en muchos casos, el robo de información.

Un estudio realizado en 7 países presentado por la EUROPOL en 2013 reveló que el 21.3% de los adolescentes podrían presentar indicios de conducta adictiva a Internet, debido al uso excesivo de este en actividades académicas, recreativas, etc. ocasionando daños a nivel

psicológico y físico. Aunado a esto la mayor parte de los adolescentes se ven amenazados por el *grooming*, ésta es una actividad que por medio de las redes sociales contacta adolescentes con fines sexuales para poder entrelazar una relación con la víctima y así poder obtener información de índole sexual; este método también es utilizado para la trata de personas, el *grooming* suele mantener comunicación con menores de edad, específicamente con mujeres adolescentes.

Importancia del equilibrio entre el sector privado y el gobierno en la red

La Gobernanza de Internet debe afianzar el acuerdo mutuo entre las múltiples partes interesadas (el sector privado, el gobierno y la sociedad) para formular políticas y medidas que ayuden a la gestión de Internet con el fin de preservar su existencia y beneficiar a sus usuarios. Tanto el sector privado como el gubernamental representan partes de suma importancia para poder llegar a un equilibrio que mejore la gobernanza en la red, ya que ambos afectan directamente al usuario.

El sector privado es de suma importancia para desarrollar y reforzar los derechos humanos del usuario (Lara, 2016), la participación de empresas privadas en la construcción de infraestructura, mantenimiento de servidores, creación de *hardware* o *software*, etc. influye directamente en los derechos del usuario haciendo que estos mejoren o empeoren. La participación correcta de las empresas, beneficiando a sus usuarios y protegiendo sus derechos humanos a la par que éstas consiguen sus intereses, puede suponer varios beneficios al consumidor y mejorar el futuro de Internet, corrigiendo graves problemas como la falta de libertad de expresión, falta de información, entre otros.

En el Informe del Relator Especial para la Libertad de Expresión del 2016 de la Organización de las Naciones Unidas se resaltan cuatro temas legales que son considerados de suma importancia para mejorar el equilibrio en Internet entre empresas privadas y el gobierno: la regulación de contenidos; la vigilancia y seguridad digital; la transparencia y los recursos legales para enfrentar atentados en contra de los derechos humanos. Sin embargo, no se cuenta con políticas o regulaciones legales que puedan sancionar o tener efectos jurídicos en Internet, a causa de lo poco que se ha explorado este panorama. En consecuencia, empresas como *Hacking Team* y *Gamma Group* han invertido en tecnología para la vigilancia en países latinoamericanos como México, Panamá y Paraguay, alarmando a la población por la posible

violación de su derecho a la privacidad. Otro caso es la intervención de Proveedores de servicios de Internet (ISP) que, junto con la creciente problemática de la neutralidad de la red, pueden deteriorar la calidad del medio digital limitando la innovación y la libertad de expresión a pesar de haber un aumento en la base de usuarios.

El gobierno forma una parte fundamental en la red ya que provee al usuario de políticas y medidas que aseguran el uso de su información y datos en Internet, sin embargo, la eficacia es mínima debido a la ineficiencia de algunos gobiernos, como el de Chile y Argentina en 2014 o Estados Unidos en el 2007, para tratar con plataformas digitales. Internet es un medio de comunicación que puede permitir una participación más activa de los ciudadanos en temas políticos, desde foros de debate hasta la toma de decisiones. A pesar de la gran influencia y relación que hay entre el gobierno, la sociedad y el Internet, la relación entre estos tres se ha visto mermada por el uso inadecuado de las plataformas digitales, la censura por parte de ciertos gobiernos, la falta de interés y el descontento de la población, etc.

Al llegar a un equilibrio entre el sector privado y el gobierno se asegura un ambiente sano y estable en la red, previniendo amenazas como el *hacking*, robo de datos, cibercrímenes, etc. El mayor reto a afrontar para llegar a una gobernanza efectiva de Internet es mantener a las empresas interesadas a la par que apoyan los derechos humanos y que el gobierno se involucre más en temas tecnológicos y digitales para poder crear políticas efectivas que prometan seguridad y estabilidad para el futuro del Internet.

Amenazas de los objetos hiperconectados o del Internet de las Cosas

El Internet de las Cosas es una de las tendencias de las TIC que han adquirido suma importancia en los últimos años, ésta tendencia se refiere a la conexión de toda clase de objetos de uso cotidiano entre sí (objetos hiperconectados) y a su vez a Internet. Aparatos como televisores, cámaras, *wearables*, monitores y controladores de inventarios (M2M), drones, automóviles, aparatos médicos y toda clase de objetos de uso cotidiano pueden estar conectados a Internet y ofrecer una experiencia mucho más cómoda para el usuario ya que simplifican el uso de estos objetos.

A pesar de ser de suma utilidad en la cotidianidad, los objetos conectados al IoT pueden verse amenazados por dos grandes factores: el desinterés de las empresas por implementar mayor seguridad en sus objetos hiperconectados y las pocas regulaciones con las que el gobierno cuenta para mantener un panorama seguro en el IoT. Los problemas relacionados con el IoT atentan contra la seguridad y privacidad de los usuarios amenazando sus derechos humanos.

La poca seguridad con la que los productos conectados al IoT son manufacturados es una de las principales causas por las que *hackers* realizan sus ataques contra objetos hiperconectados. Esto sugiere una grave amenaza no sólo a los empresarios causandoles pérdidas económicas, sino que también a los consumidores ya que se atenta contra sus datos personales, por ejemplo, el hackeo de *wearables,* accesorios como relojes, pulseras, lentes, etc. "inteligentes" o conectados a Internet, puede permitir el acceso a información personal como correos, cuentas bancarias, e incluso el ingreso a conversaciones privadas con el fin de conseguir información.

El hecho de que criminales puedan acceder con suma facilidad a datos personales y de suma importancia de empresas o usuarios hace que el IoT se vea sumamente amenazado. Pero, a pesar de los riesgos que el IoT puede representar, los empresarios no han decidido concentrarse en mejorar la seguridad tanto de *software* como de *hardware* de sus dispositivos y aunado a esto el gobierno a nivel internacional no ha creado políticas que se dirijan directamente a la regulación de productos conectados al IoT. Gracias a esto los *hackers* pueden tener acceso a una gran cantidad de dispositivos que les permiten controlar una amplia gama de sectores: el económico con los sistemas M2M, permitiendo manipular las ganancias de una empresa, el bélico con el control de drones o vehículos no tripulados, el social con el ataque directo a carros con sistemas conectados a Wi-fi o *wearables,* y muchos otros sectores igual de diversos.

El historial de ataques al IoT demuestra que un *hacker* puede acceder con facilidad a objetos remotos interconectados y usarlos para su propio beneficio. En 2009 en el medio oriente insurgentes lograron acceder a las señales del dron *Predator,* obteniendo información al usarlo como objeto de espionaje. Otro ejemplo de lo fácil que puede resultar acceder al IoT es que en los *DroneGames* de 2012 el ganador logró crear un virus que "contagiaba" a cualquier dron que se acercara al dron infectado.

La falta de seguridad en dispositivos hiperconectados y la poca intervención del gobierno hacen del IoT una herramienta que puede ayudar al progreso de comunidades pero también es objeto de amenaza para criminales con acceso a Internet y conocimientos básicos de informática. Por ello es necesario que tanto el sector privado como el gobierno intervengan y encuentren un equilibrio para no sólo mejorar la gobernanza de Internet sino también para implementar políticas y medidas que reduzcan las amenazas de ciberataques y evitar el mal uso del IoT para asegurar los derechos de los usuarios de esta plataforma.

Acciones tomadas en el panorama internacional para la mejora de la Gobernanza de Internet

La difusión de las innovaciones en las TIC ha protagonizado cambios muy significativos en el entretenimiento, la cultura y la economía de las sociedades avanzadas (Pérez, s.f.). A raíz del avance en el manejo del Internet se han convocado diversos debates sobre los cambios necesarios en la gestión del Sistema de Nombres de Dominio (DNS) y las asignación de direcciones IP, también se ha hablado sobre la desigualdad entre naciones ricas y pobres que existe en Internet, la seguridad en Internet, medios de comunicación y redes sociales, la piratería digital o distribución ilegal de diversos contenidos de multimedia, entre otros temas. Los debates tienen como finalidad promover la importancia del control en Internet así como la preocupación de algunos países por el mal uso del mismo. Durante varios años se han presentado varias iniciativas en diferentes foros nacionales e internacionales donde se propone un nuevo sistema para estudiar a fondo el fenómeno de la gobernanza en Internet, también se ha expresado la necesidad de normas de regulación a través de los mecanismos y organizaciones participantes como: la *Association for Computing Machinery* (ACM), la Asociación de Gestión de Derechos Intelectuales – Derechos de Propiedad Intelectual (AGEDI), el Consejo Económico y Social de Naciones Unidas (ECOSOC), el Institute of Electrical and Electronics Engineers (IEEE), la Transmission Control Protocol / Internet Protocol (TCP/IP), entre otras.

Los diferentes sistemas socioeconómicos y culturales, el sistema de compra-venta, las existentes regulaciones y la relevancia que ha alcanzado el Internet tiene como consecuencia diversos debates sobre el gobierno o “Gobernanza de Internet”. Existen dos tipos de modelos de gestión: el primero es un sistema tradicional que utilizan los servicios de telecomunicaciones y redes el cual usa mecanismos organizados por monopolios nacionales, el segundo surge como

consecuencia del manejo de internet y funciona con los nuevos panoramas de distintos mercados convergentes y las continuas competencias del mercado más liberalizado.

El tema de la Gobernanza de Internet fue de los puntos más relevantes a tratar en la Cumbre Mundial sobre Sociedad de la Información (*World Summit on Information Society*, WSIS), esta cumbre fue encabezada por la Organización de las Naciones Unidas (ONU) y la Unión Internacional de Telecomunicaciones (UIT). La ONU expresó su interés por continuar con las regulaciones necesarias; de igual forma se creó el Internet Governance Forum (IGF), un foro abierto para debatir y exponer las políticas y leyes necesarias para la sostenibilidad y eficacia de Internet. Este foro se compone por diversos gobiernos, el sector privado, los colectivos académicos y de investigación y la sociedad civil.

Lo complejo de la Gobernanza de Internet se debe a las grandes diferencias entre los mecanismos del gobierno de telecomunicaciones, tecnologías de la información, industrias de electrónica, etc. El integrar todo lo que el Internet desarrolla vuelve complejo el poder ejercer un gobierno eficaz que regule y mantenga estable este servicio. La UIT es de las organizaciones que más ha aportado y participado en los debates que este fenómeno ha generado como la *Voice over IP* (VoIP, grupo de tecnologías que permiten la transmisión de voz y multimedia a través de Internet), entre otros. Con este tipo de reuniones se ha generado que organizaciones de estandarización de Internet y la UIT mantengan una mejor comunicación, al igual que se confirmó que la UIT tiene un rol importante con respecto a cuestiones claves relacionadas con la evolución del sistema global de telecomunicaciones.

El Internet se ha convertido en uno de los mayores medios de comunicación y en una parte fundamental para las telecomunicaciones, pues ha generado e incorporado distintos elementos para el beneficio de las nuevas sociedades y, de alguna forma, se puede interpretar que Internet ha sido el último de una serie de cambios que han impactado el sector de las telecomunicaciones. (Pérez, s.f.). En este sector se han logrado objetivos como el crecimiento y nuevas oportunidades en industrias rentables y dinámicas; pero en el caso de Internet se considera que su desarrollo puede afectar la infraestructura de la industria de las telecomunicaciones causando cambios drásticos a nivel económico y técnico. (UIT, 1997).

Durante los últimos años se han establecido acuerdos internacionales para equilibrar la Gobernanza de Internet entre los países y entre el sector privado y gubernamental. A pesar de esto aún se han mantenido las cumbres y foros relacionadas a la gobernanza correcta de la red para que este fenómeno sea beneficioso para todas las naciones, así como para mantener su uso

de forma segura y evitar un monopolio que generaría el descontrol de este medio de comunicación que es de suma importancia en la actualidad.

Referencias

1. Acis. (s.f.). La vulnerabilidad del Internet de las Cosas (IoT), un riesgo para las empresas. Recuperado el 4 de julio de 2018, de *Acisi.* Web <http://acis.org.co/portal/content/la-vulnerabilidad-del-internet-de-las-cosas-iot-un-riesgo-para-las-empresas>
2. Adsuara, B. (2016). ¿Qué es la Gobernanza de Internet? Recuperado el 25 de mayo de 2018, de *ABC Tecnología.* Web <http://www.abc.es/tecnologia/redes/abci-gobernanza-internet-201611120159_noticia.html>
3. Albors, J. (2014). Amenazas en IoT y dispositivos que no imaginabas conectados. Recuperado el 4 de julio de 2018, de *Welivesecurity*. Web <https://www.welivesecurity.com/la-es/2014/09/12/amenazas-iot-dispositivos-no-imaginabas-conectados/>
4. Aspis, A. (2014). La gobernanza de Internet y la nueva agenda mundial de los recursos tecnológicos.Recuperado el 5 de julio de 2018, de *Simposio Argentino de Informática y Derecho.* Web <http://43jaiio.sadio.org.ar/proceedings/SID/2.pdf >
5. Cambronero, F. (2013). Gobernanza de internet, ¿cuál es el panorama? Recuperado el 5 de julio de 2018, de *SlideShare*. Web <https://es.slideshare.net/facambronero/gobernanza-de-internet-cul-es-el-panorama-actual-fatima-cambronero-26254345 >
6. Condliffe, J. (2016). La historia completa de los ciberataques masivos e interminables a Yahoo. Recuperado el 29 de junio de 2018, de *MIT Technology Review*. Web <https://www.technologyreview.es/s/6582/la-historia-completa-de-los-ciberataques-masivos-e-interminables-yahoo>
7. Computerworld. (2014). El Internet de las Cosas: Las cinco amenazas principales. Recuperado el 4 de julio de 2018, de *Computerworld*. Web <http://www.computerworld.es/tendencias/el-internet-de-las-cosas-las-cinco-amenazas-principales>
8. Del Cid, M. (2017). Libertad de expresión en Internet. Recuperado el 25 de mayo de 2018, de *FNPI.* Web <http://www.fnpi.org/es/etica-segura/libertad-de-expresion-en-internet>
9. Dominicas. (s.f.). INTERNET; RIESGOS Y CONSECUENCIAS DE UN USO INADECUADO. Recuperado el 29 de junio de 2018, de *Dominicas*. Web <http://www.dominicas.org/INTERNETRIESGOS.pdf>
10. El País. (2017). A los internautas les preocupa cada vez más la privacidad en la red. Recuperado el 25 de mayo de 2018, de *El País.* Web <https://www.elpais.com.uy/vida-actual/internautas-les-preocupa-vez-privacidad-red.html>
11. Escudero, F. (2017). Riesgos y peligros de las redes sociales en Internet. Recuperado el 29 de junio de 2018, de *About Español.* Web <https://www.aboutespanol.com/riesgos-y-peligros-de-las-redes-sociales-en-internet-2878956>

12. Frett, N. (2015). ¿Qué es un ciberataque?. Recuperado el 29 de junio de 2018, de *Auditool.* Web <https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque>

13. Gómez-Merelo, M. (2017). CIBERATAQUES. Amenazas globales, ensayos reales. Recuperado el 29 de junio de 2018, de *Tendencias21.* Web <https://www.tendencias21.net/seguridad/CIBERATAQUES-Amenazas-globales-ensayos-reales_a28.html >

14. Hernández, C. (2018). Libertad de expresión en Internet. Recuperado el 25 de mayo de 2018, de *Adelante.cu.* Web <http://www.adelante.cu/index.php/es/noticias/de-camagueey/13168-libertad-de-expresion-en-internet-noticia-en-construccion>

15. History. (s.f.). Los seis mayores ciberataques de la historia. Recuperado el 29 de junio de 2018, de *History*. Web <https://mx.tuhistory.com/noticias/los-seis-mayores-ciberataques-de-la-historia>

16. Internet Society. (2016). Informe de políticas: Gobernanza de Internet. Recuperado el 28 de junio de 2018, de *Internet Society.* Web <https://www.internetsociety.org/es/policybriefs/internetgovernance/>

17. La Nación. (2013). La democracia en la era de Internet. Recuperado el 28 de junio de 2018, de *La Nación.* Web <https://www.nacion.com/opinion/foros/la-democracia-en-la-era-de-internet/LNU4E46GVVDUTGKZPTILH2DPEM/story/>

18. Lara, J. (2016). ¿Cuál es el rol del sector privado sobre la libertad de expresión en internet?. Recuperado el 28 de junio de 2018, de *Derechos Digitales.* Web <https://www.derechosdigitales.org/10160/cual-es-el-rol-del-sector-privado-sobre-la-libertad-de-expresion-en-internet/>

19. Luján, J. (s.f.). ¿Qué es Wanna Cry?. Recuperado el 29 de junio de 2018, de *EDteam.* Web <https://ed.team/blog/que-es-wanna-cry >

20. MásQueNegocio. (2016). Riesgos y amenazas del Internet de las Cosas. Recuperado el 4 de julio de 2018, de *MásQueNegocio*. Web <https://www.masquenegocio.com/2016/02/02/amenazas-internet-cosas/>

21. McGuinness, D. (2017). Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. Recuperado el 29 de junio de 2018, de *BBC*. Web <http://www.bbc.com/mundo/noticias-39800133>

22. Milenio. (2014). eBay, víctima de ciberataque. Recuperado el 29 de junio de 2018, de *Milenio.* Web < http://www.milenio.com/estilo/ebay-victima-de-ciberataque>

23. Mundo Contact. (2014). Del Internet de las Cosas al Internet de las Amenazas. Recuperado el 4 de julio de 2018, de *Mundo Contact*. Web <https://mundocontact.com/del-internet-de-las-cosas-al-internet-de-las-amenazas/>

24. Narr, C. (2018). Opinión: Los peligros de los objetos hiperconectados. Recuperado el 25 de mayo de 2018, de *Zoom Tecnológico.* Web <https://www.zoomtecnologico.com/2018/03/07/objetos-hiperconectados/>

25. Noticias ONU. (2018). Las políticas de ciberseguridad, una amenaza contra la intimidad. Recuperado el 26 de mayo de 2018, de *Noticias ONU.* Web <https://news.un.org/es/story/2018/03/1428622>

26. Otero, J. (2017). Gobiernos necesitan impulsar el desarrollo de las TIC. Recuperado el 3 de julio de 2018, de *El Economista*. Web

<https://www.eleconomista.com.mx/opinion/Gobiernos-necesitan-impulsar-el-desarrollo-de-las-TIC-20171129-0185.html>

27. Paredes, A. (2015). Cómo influye internet en la política y comunicación de gobierno. Recuperado el 28 de junio de 2018, de *Forbes México.* Web <https://www.forbes.com.mx/como-influye-internet-en-la-politica-y-comunicacion-de-gobierno/>

28. Pérez, J. (s.f.). La gobernanza de Internet. Recuperado el 5 de junio de 2018, de *Escuela Técnica Superior de Ingenieros de Telecomunicación*. Web <http://www.isoc-es.org/files/downloads/LaGobernanzadeInternet.pdf >

29. Promoción y Educación de la Salud. (2013). Riesgos de un mal uso de Internet. Recuperado el 29 de junio de 2018, de *Promoción y Educación de la Salud.* Web <http://blogs.murciasalud.es/edusalud/2013/03/22/riesgos-de-un-mal-uso-de-internet/>

30. Rada, A. (2016). Internet de las Cosas: ¿Una amenaza real?. Recuperado el 4 de julio de 2018, de *B-secure* Web <https://www.b-secure.co/blog/internet-de-las-cosas-una-amenaza-real>

31. Rubén. (s.f.). Los ciberataques: tipos y previsiones para el 2018. Recuperado el 29 de junio de 2018, de *RCG Comunicaciones.* Web <http://rcg-comunicaciones.com/los-ciberataques-tipos-previsiones-2018/>

32. UNCTAD. (2018). Data privacy: new global survey reveals growing Internet anxiety. Recuperado el 26 de mayo de 2018, de *United Nations Conference on Trade and Development.* Web <http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1719>

33. UIT. (2017). El Foro de la Cumbre Mundial sobre la Sociedad dela Información de 2017 promueve el apoyo mundial a las TIC para los ODS. Recuperado el 31 de mayo de 2018, de *Unión Internacional de Telecomunicaciones.* Web. <https://www.itu.int/es/mediacentre/Pages/2017-PR28.aspx>

34. West, D. (2008). Mejorar la utilización de la tecnología en el gobierno electrónico alrededor del mundo, 2008. Recuperado el 3 de julio de 2018, de *Brookings.* Web <https://www.brookings.edu/es/research/mejorar-la-utilizacion-de-la-tecnologia-en-el-gobierno-electronico-alrededor-del-mundo-2008/>

E

Estipular: Convenir las condiciones de un acuerdo, concretar y/o acordar las condiciones de tal.

Encriptado: Poner información o señales electrónicas en un código secreto ya sea un sistema de letras, números o símbolos, para dificultar su entendimiento.

G

Gestionar: Realizar diligencias como administración u organización para la resolución o logro de algo en específico.

Grooming: Actividad que por medio de las redes sociales contacta adolescentes o niños con el fin de entrelazar una relación con la víctima y persuadirla para poder obtener información de índole sexual.

H

Hardware: Utensilios, instrumentos y aparatos especiales para un fin determinado, parte de un equipo electrónico, específicamente computadoras

Hiperconectado: El uso de múltiples sistemas y dispositivos para permanecer constantemente conectado a la red y/o fuentes de información.

I

Interconexión: Se define como relación o conexión entre dos o más elementos en la red.

M

Mermar: Disminuir o se consumir una parte de un todo.

Machine to Machine (M2M): Intercambio de información y transmisión de datos entre un dispositivo y otro inalámbircamente.

P

Phishing: Es un método para estafar por medio de la red, robando datos, información y dinero a través de comunicados falsos por Internet o correo electrónico.

S

Software: Es un programa o código diseñado para hacer que la computadora o el ordenador cumpla funciones específicas.

W

Wearable: Se traduce como aquellos dispositivos tecnológicos con los que se puede vestir o utilizar para complementar la vestimenta, éstos contienen tecnología computarizada o se pueden conectar a Internet.