La evolución tecnológica y la necesidad de crear nuevas metodologías para la seguridad digital en el siglo XXI

TECHNOLOGICAL EVOLUTION AND THE NEED TO CREATE NEW METHODOLOGIES FOR THE DIGITAL SECURITY IN THE 21ST CENTURY

Recibido: 06 / 11 / 2018 Aprobado: 26 / 11 / 2018

Dra. María Beatriz Juárez Escribano
España

La autora es Doctora Cum Laude por unanimidad en Publicidad y Relaciones Públicas, dentro del programa de Educación y Creatividad: Aplicaciones Tecnológicas, Sociales y Psicopedagógicas, por la Universidad Camilo José Cela. Es licenciada en Ciencias Ambientales por la universidad Alfonso X El Sabio de Madrid, España, y licenciada en Comunicación Audiovisual por la universidad Camilo José Cela de Madrid, España. Tiene una maestría en Prevención de Riesgos Laborales por el Instituto de Formación de Madrid, y un máster en Energías Renovables y Mercado Energético por la Escuela de Organización Industrial. Actualmente es profesora en el Máster de Tecnologías de la Información y Comunicación para la educación en la Universidad Antonio de Nebrija. mjuareze@nebrija.es

RESUMEN

Los riesgos tecnológicos son en gran parte desconocidos e inciertos. La revolución digital ha multiplicado de manera exponencial todos los datos que las distintas empresas, instituciones, centros educativos, organismos internaciones y administraciones públicas vuelcan a la red, lo que conlleva a que los diferentes usuarios de Internet puedan consultarlos a diario. Debido a esta generación de contenido ingente de información, se hace esencial que la ciberseguridad de los próximos años sea óptima en la era digital.

Palabras clave:

Ciberseguridad, educación, era digital, innovación, Internet, tecnología.

ABSTRACT

Technological risks are largely unknown and uncertain. The digital revolution has multiplied exponentially all the data that different companies, institutions, schools, international organizations and public administrations overturn into the network, which means that different Internet users can consult them daily. Due to this generation of huge information content, it is essential that the cybersecurity of the coming years will be optimal in the digital age.

Keywords:

Cybersecurity, digital era, education, innovation, Internet, technology.

Introducción

A mediados del siglo XX se produjo un acontecimiento denominado Revolución Digital que modificó la sociedad de manera radical, dando paso a la Era de la Información o Sociedad del Conocimiento (Hergueta, 2017). Pero no sólo modificó la estructura social, sino que también surgieron numerosos avances científicos, apareciendo ciertos procesos tecnológicos y unas redes de comunicación digitales a través de ordenadores, que cambiaron drásticamente el transcurso de la historia de la humanidad. Surge por tanto la necesidad de crear un sistema de seguridad para proteger tanto los datos personales de los múltiples usuarios de la Red, como la información de las distintas instituciones privadas, públicas y del Ejército.

¿Pero cuáles tres acontecimientos son la fuente de los orígenes del presente tecnológico en el que estamos? Según Rodríguez de las Heras, Catedrático de Humanidades y Director del Instituto de Cultura y Tecnología de la Universidad Carlos III de Madrid, son tres sucesos, todos ellos de carácter militar, los que marcan el comienzo de esta revolución tecnológica, y que aún está aconteciendo en nuestros días. El primero de ellos fue la creación de los misiles V-1 y V-2; en segundo lugar el desarrollo del Colossus, primer gran ordenador basado en un primitivo sistema binario, y en tercer lugar la detonación de la primera bomba nuclear en la base de misiles militar situada en Trinity Site, Álamo Gordo, Nuevo México.

Se hace necesario comprender el origen de estos sucesos, ya que el progreso de esas tecnologías provocó la creación, casi ineludible, de una tecnología específica creada para salvaguardar y proteger a la nueva sociedad digital que se estaba creando, y que hoy en día continúa desarrollándose.

Desarrollo

Para comenzar a explicar estos sucesos es necesario que nos situemos en tiempo y espacio. Nos encontramos en los últimos años de la Segunda Guerra Mundial, concretamente en Peenemunde, una pequeña región norteña germana, donde la pretensión del Ejército alemán era crear un arma poderosa que consiguiese alcanzar, con una carga explosiva, una trayectoria balística mucho más fuerte que un cañón. Este proyecto, diseñado por el ingeniero Von Braun, supuso un gran esfuerzo tecnológico en un breve espacio de tiempo. Los V-1 eran aviones a reacción no tripulados que se disparaban desde una rampa, atravesaban el Canal de la Mancha e impactaban contra los objetivos militares y civiles de Londres y otras ciudades de las islas. A los pocos meses los alemanes desarrollaron los V-2, cohetes que trazaban, hacia el mismo objetivo, una trayectoria balística de gran altura a más de 80 kilómetros de altitud, llegando al suelo a una velocidad imparable para cualquiera aviación o defensa antiaérea, algo que no sucedía con los V-1.

Figura 1: misil V-2.

Fuente: ecured.com.

Se convirtieron pues en un arma psicológica para la población. A pesar del increíble desarrollo tecnológico (tuvieron que buscar materiales resistentes a las altas presiones y temperaturas, motores poderosos para la propulsión, resolvieron con éxito problemas de aerodinámica, encontraron combustibles energéticos… en muy poco espacio de tiempo) este proyecto se desarrolló en los años tardíos de la Segunda Guerra Mundial, cuando prácticamente Alemania había caído y seguramente se perdieron más vidas de personas trabajando en condiciones infrahumanas en estos misiles, que víctimas se produjeron por los impactos de esos cohetes.

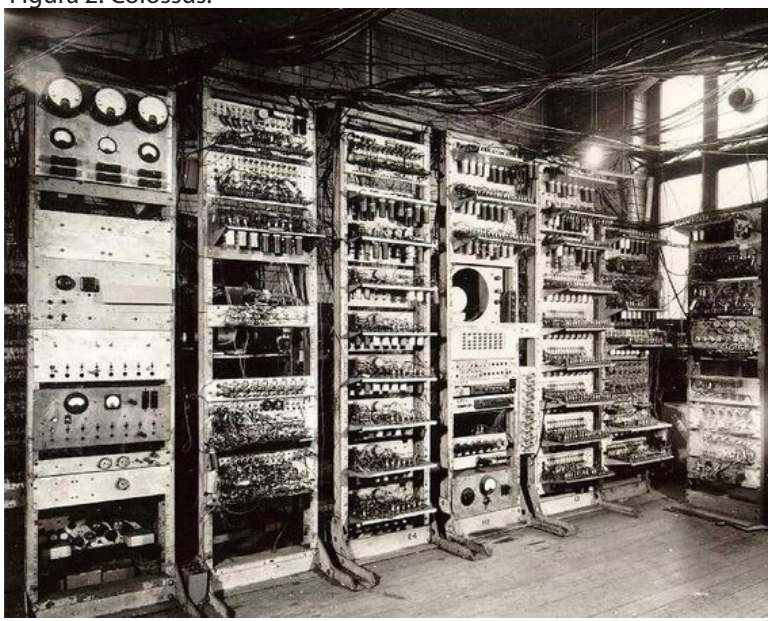
Todos estos avances contenidos en un arma se difundieron cuando, al terminar la guerra, sus artífices se separaron y marcharon, con sus conocimientos, a uno y otro de los bloques en los que se dividió el mundo.

Como señalábamos anteriormente el segundo gran avance tecnológico fue el Colossus, primer ordenador electrónico de válvulas utilizado por las fuerzas de inteligencia de los aliados. Fue desarrollado en Bletchley, Inglaterra, por Tommy Flowers. El Colussus dio resultados muy provechosos ya que en mayo del 44 lograron descodificar los mensajes del Ejército alemán, pudiendo acabar la guerra dos años antes de lo previsto.

Destacar a Alan Turing, matemático profesor de Cambridge, predecesor del código binario base de nuestra sociedad digital, y que el servicio británico contrató para trabajar en el proyecto.

Pasados los años, después de la Segunda Guerra Mundial, concretamente en el año 1954, Turing se suicidó comiendo una manzana impregnada en cianuro. El motivo de ese suicidio fue porque unos días antes un juez le había condenado a un tratamiento hormonal para curar su homosexualidad. De este trágico suceso tiene su origen el logotipo de Apple, o al menos es una de las diversas teorías que existen sobre el dibujo de la marca de Steve Jobs (Ibáñez, 2011).

Figura 2: Colossus.



Fuente:sites.googles.com.

Se empieza a crear pues una sociedad tecnológica, base de la sociedad del conocimiento. Con este ordenador se inicia todo el desarrollo de estos casi 75 años de lo que se ha constituido como sociedad tecnológica y digital.

Por último, es necesario desarrollar el inicio del tercer gran avance tecnológico, no por ello exento de polémica. Nos encontramos en agosto de 1939, donde la situación del mundo era inquietante. En ese verano tuvo lugar una reunión entre Leo Szilard (físico judío americano) y Albert Einstein, donde Szilard le planteó el riesgo de que los alemanes, a partir de un artículo puramente científico escrito en una revista, pudieran llegar a desarrollar una bomba nuclear. Szilard trasladó a Einstein esa inquietud, y pudo convencerle para que redactara una carta al presidente Roosevelt donde se le planteó ese posible escenario. La respuesta de Roosevelt fue inmediata y concluyó que había que adelantarse a esa posibilidad. Como resultado, surgió el conocidísimo e impresionante Proyecto Manhattan en el que participaron 100.000 personas, entre ellas ingenieros, científicos, empresas muy variadas (desde la Westinghouse a la Du Pont) y varias universidades como la de Chicago. En seis años se consiguió que desde ese artículo que comentó Szilard a Einstein hasta la explosión en julio de 1945 en Nuevo México, se diese una zancada tecnológica impresionante.

Para detonar la bomba de manera controlada se construyó un tubo de contención, el tubo Jumbo, que se utilizó como precaución para que en caso de que fallara la explosión, estuviera contenida y evitar que el material radioactivo se extendiera. El cuerpo militar intentó años más tarde destruir ese tubo, pero debido a su dureza fue imposible. Ahora mismo, en Trinity Site se mide una radioactividad 10 veces superior respecto a otros lugares del mundo y este recinto solo se puede visitar dos veces al año (WSMR Army, 2018).

Cabe destacar varios detalles del Proyecto Manhattan, ya que propició que la tecnología se desarrollara de forma mucho más rápida. Entre esos detalles nos gustaría mencionar a Vaneevar Bush quien en 1945 redactó un artícu-

lo para presentar una posible máquina para resolver un problema que él mismo había detectado al participar en el Proyecto Manhattan. La cantidad de información que se generó en un proyecto de estas características fue ingente, por lo que fue necesario idear una máquina que con aquellos medios tecnológicos de la época, pudiera imitar de alguna forma el funcionamiento de nuestra memoria asociativa (es decir, almacenamiento y recuperación de información por asociación con otras informaciones.) Es decir, había que crear una máquina que funcionara como un Internet a muy pequeña escala, a la que denominó Memex (Montero, 2012).

Otros de los detalles importantes que queremos mencionar fue la intervención de la empresa privada por primera vez en un proyecto de estas características, así como el inmenso salto tecnológico en tan poco tiempo que supuso al conseguir controlar una reacción en cadena de la bomba nuclear, es decir, se había conseguido una planta nuclear controlada.

Llegados a este punto, es necesario preguntarse si las guerras son necesarias para que el hombre progrese tecnológicamente. Las guerras traen unas necesidades urgentes y graves que hacen que las invenciones, los avances se hagan mucho más rápidamente. Por la gravedad de la situación se aportan unos esfuerzos y unos recursos que aceleran los cambios.No obstante, por muchas veces que se haya producido esta asociación no tiene que aceptarse el determinismo de que es el único camino para el futuro (Rodríguez de las Heras, 2018). De no ser así apostaríamos por provocar guerras para conseguir avances tecnológicos continuamente. Recordemos que las necesidades de tipo militar no llevan a la invención en muchos de los casos pero sí al desarrollo acelerado de la tecnología (Braun y Mc Donald, 1984), es decir, el proyecto puede surgir del mundo civil pero su desarrollo posterior se ve acelerado y mejorado por las necesidades y los presupuestos del ámbito militar, migrando posteriormente al mercado civil de manera más perfeccionada como ocurrió con la tecnología microelectrónica (Ortega, 2010).

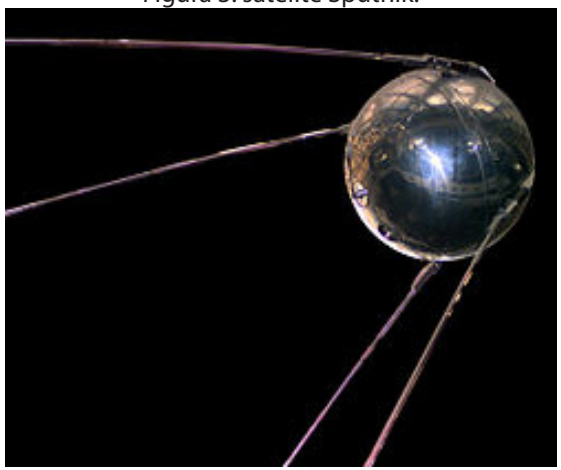
Así pues, "la importancia que tuvo el desarrollo de la tecnología militar en la victoria de los aliados en la Segunda Guerra Mundial lleva a la preponderancia de esta tecnología sobre la civil, situación que continúa durante la Guerra Fría" (Ortega, 2010, p.4). Jordi Molas afirma que "el sistema de innovación militar que se desarrolló durante la Guerra Fría tendió a cerrarse sobre sí mismo, definiendo un sistema de innovación protagonizado por un número de actores relativamente pequeño y definido (ministerios de defensa, laboratorios militares, industrias de defensa) los cuales desarrollaron sus propias dinámicas de generación y selección de nuevas tecnologías. Era un sistema jerárquico, cerrado y estable"(Molas, 2008). Todo ello tuvo como resultado lo que se conoce como el complejo militar-industrial, lo que provocó que a principios de los años 90 comenzara a aumentar el desarrollo de la tecnología más enfocada al ámbito civil.

Por un lado, se produce una fuerte disminución de los presupuestos de defensa en los países occidentales, lo que lleva a buscar componentes y subsistemas de coste más bajo. Por otro lado, hay un cambio en la percepción del concepto clásico de guerra y el surgimiento de nuevas amenazas a la seguridad nacional y la naturaleza del conflicto armado: nuevas guerras, nuevo terrorismo, estados fallidos, etc., y cobra importancia el nuevo concepto de seguridad en el

que confluyen tareas propias de la seguridad doméstica o interior de los países con las de defensa militar, con fronteras muy poco definidas.

Para averiguar cómo surge entonces el nuevo modelo de comunicación que implica la búsqueda de nuevas tecnologías para la seguridad y defensa en el mundo virtual, partiremos de los orígenes de Internet, ya que su desarrollo fue el principal motor impulsor de la actual era digital.

Figura 3: satélite Sputnik.



Fuente: Nationalgeographic.org.

Estos orígenes hay que situarlos en ARPANET, una red de ordenadores establecida por ARPA (Advanced Research Proyects Agency) en septiembre de 1969. El Departamento de Defensa de Estados Unidos fundó esta Agencia de Proyectos de Investigación Avanzada en 1958 para movilizar recursos procedentes principalmente del mundo universitario, con el objetivo de alcanzar la superioridad tecnológica militar sobre la Unión Soviética, que acababa de lanzar su primer satélite Sputnik en 1957 (CASTELLS, 2003, p.26).

El objeto de este Departamento, según definió su primer director Joseph Licklider (CASTELLS, 2003, p.33), psicólogo convertido en informático, era estimular la investigación en el campo de la informática interactiva. El proyecto ARPANET se justificó como un medio de compartir el tiempo online de los ordenadores entre varios centros de informática y grupos de la agencia. El siguiente paso consistió en conectar ARPANET con otras redes de ordenadores ajenos a la agencia y así surgió el nuevo concepto World Wide Web, término acuñado en 1992 por Tim Berners Lee (ORSI, 2008, p.11) y actualmente denominada Web 1.0. Los contenidos de esta Web eran fundamentalmente información estática sobre las actividades o características de empresas o particulares, ofrecidas por ellos mismos con fines habitualmente publicitarios, profesionales o comerciales.

Los administradores, o webmasters, tenían el control absoluto sobre toda la información volcada en su sitio web. Así, Internet no era más que un conjunto de sitios web de lectura, sin apenas interacción con los usuarios finales (ORSI, 2008). En este período el internauta era un simple consumidor pasivo de información.

Paralelamente se fue desarrollando un subgrupo minoritario, en su mayoría hackers cercanos a los movimientos contraculturales y modos de vida alternativos, que crearon comunidades virtuales (término popularizado por el crítico y ensayista Howard Rheingold (1993)), y éstas poco a poco se fueron convirtiendo en fuente de valores que determinaban el comportamiento y la organización social (CASTELLS, 2003, p.77). Los implicados en esta nueva interacción social desarrollaron así los primeros chats, las BBS (Bulletin Board System o Sistema de Tablón de Anun-

cios donde los usuarios descargaban software y datos) foros y juegos online, iniciándose con ellos un modo nuevo de comunicación interpersonal.

Mientras tanto, la cultura comunitaria iba configurando sus formas, procesos y usos sociales. A medida que las comunidades virtuales aumentaban de tamaño y se multiplicaban sus temáticas, la conexión entre los primeros usuarios y la contracultura se fue debilitando. La Web se popularizaba. Conforme pasaba el tiempo, iban surgiendo toda clase de valores e intereses en las redes informáticas. Cuando la World Wide Web terminó de eclosionar en los años noventa, millones de usuarios volcaron en la Red sus propias innovaciones sociales, creando nuevos contenidos y páginas digitales. Surge la Web 2.0 donde el usuario ya no es pasivo, sino que interactúa con el nuevo entorno y es considerado como un creador de contenidos y, en definitiva, el centro de la información que se produce y se comparte.

Como ya hemos mencionado, esto conllevó a que en muy pocos años el número de usuarios se multiplicara de manera exponencial en la Red. Más de 4.000 millones de personas en el mundo cuentan con acceso a Internet, es decir, más de la mitad mundial, concretamente el 54%, tiene capacidad para conectarse a la Red (Europa Press, 2018). Cada individuo y organización vuelca a la nube información sensible cada día, por lo que se considera esencial que se lleve a cabo una actividad de investigación de la seguridad online de manera constante, desarrollando a partir de la detección de nuevas situaciones de riesgo, nuevas herramientas capaces de reconocerlas y, en su caso, controlarlas (INTECO, 2009).

El Instituto Nacional de Tecnologías de la Comunicación de España (INTECO), propone una serie de propuestas y recomendaciones dirigidas a los agentes intervinientes en la ciberseguridad. Entre ellas se recoge la recomendación para los fabricantes y proveedores de servicios de seguridad, donde se indica que deben tener en cuenta dos aspectos clave para lograr el máximo nivel de seguridad: por un lado la prevención del fraude online, tales como: phishing, pharming; suplantación de la identidad de usuarios; spam y difusión de contenidos inapropiados. Y por otro la investigación y desarrollo en materia de seguridad tecnológica. (INTECO, 2009).

Este aspecto también lo recoge el Decreto No. 230-18 de República Dominicana, sobre la Estrategia Nacional de Ciberseguridad 2018-2021, que dispone establecer los mecanismos de ciberseguridad adecuados para la protección del Estado, sus habitantes y en general, del desarrollo y la seguridad nacional. De hecho, República Dominicana es uno de los 10 países de la región que cuenta con una estrategia de ciberseguridad (Diario Libre, 2018).

A continuación estudiaremos qué principales propuestas y recomendaciones sobre seguridad tecnológica propone el INTENCO para los fabricantes de soluciones y servicios de seguridad.

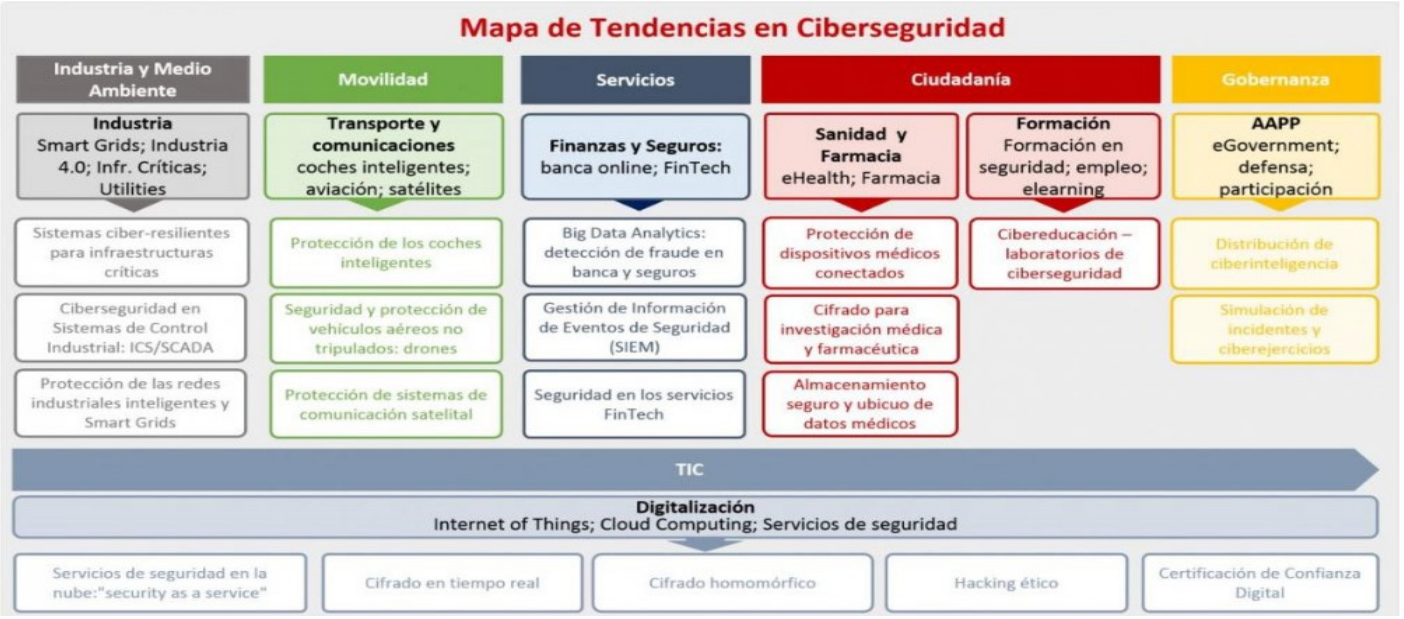
Según el INTECO se recomienda a las empresas de seguridad fomentar la interoperabilidad de sus sistemas de protección, y que colaboren directamente con las Fuerzas y Cuerpos del Estado en la investigación de nuevas situaciones de riesgo. Además se les pide que "sean proactivos en la detección de códigos maliciosos de programación que permitan agujeros de seguridad en las plataformas, así como la elaboración de listados (Black Listed), en los que sean

incluidos todos los nombres de dominio que cuenten con contenidos no autorizados, o en su caso, que no superen los criterios de seguridad previamente establecidos" (INTECO, 2009, p.134).

A los prestadores de servicios de acceso a Internet (ISP) el INTECO recomienda la creación de plataformas de comunicación fidedigna y segura con las Fuerzas y Cuerpos de Seguridad del Estado, Ministerio Fiscal y Autoridades Judiciales. Además se insta a apoyar y dar asistencia plena a estos organismos, e indica como esencial "dotar a las brigadas tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado, tanto estatales y autonómicas, como internacionales, de herramientas tecnológicas que les permitan investigar, mantener la cadena de custodia de las pruebas electrónicas y bloquear situaciones que pudieran ser susceptibles de delitos y/o perjudiciales para los usuarios de redes sociales y plataformas colaborativas" (INTECO, 2009, p.141).

Tras haber identificado las principales recomendaciones del INTECO, y para finalizar, pasaremos a estudiar las tendencias entecnologías de la información y comunicación (TIC) en el sector de la ciberseguridad, con el objetivo de identificar los potenciales segmentos en esa área. Hay que tener en cuenta que en el año 2015, según Gartner, el sector de la ciberseguridad facturaba 62.5 40 millones de euros a nivel mundial (INCIBE, 2016), y en 2018 se espera que esté cerca de los 80.000 millones de euros (a la espera de los resultados definitivos). En la siguiente tabla se resumen de manera esquemática las principales tendencias en ciberseguridad según el Instituto Nacional de Ciberseguridad (INCIBE).

Tabla 1: tendencias en ciberseguridad.

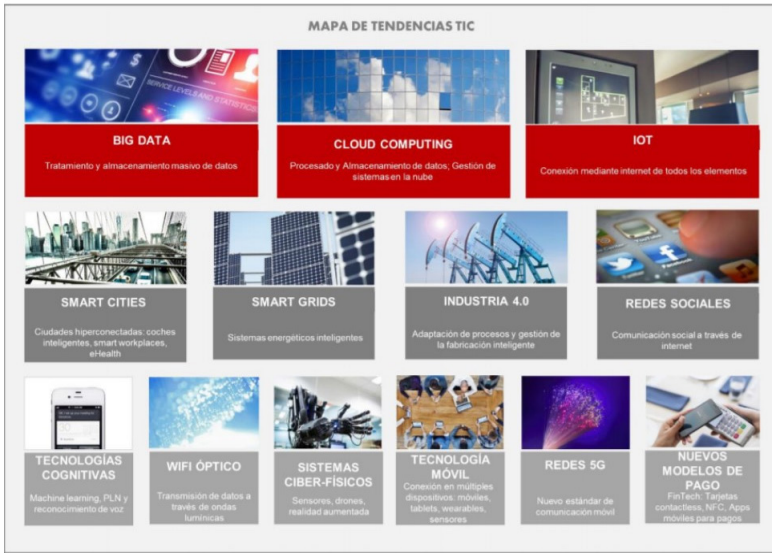


Fuente: INCIBE, 2016.

Como punto de inicio para el análisis se establece el significativo auge de la digitalización en todos los sectores, lo que conlleva al incremento del uso de las TIC. Las tendencias de estas tecnologías conviven con el Programa Europeo Horizonte 2020, "cuyos Programas de Trabajo recogen entre sus secciones temáticas a las Tecnologías de la Información y las Comunicaciones. Concretamente, el Programa de Trabajo TIC posee 6 actividades principales", (INCIBE, 2016, p.18):

- Una nueva generación de componentes y sistemas: dentro de esta actividad se contemplan los sistemas ciberfísicos así como el Smart Anything (implementación de tecnologías digitales altamente conectadas e integradas en una gran variedad de sistemas físicos cada vez más autónomos con numerosas dinámicas (Horizon2020, 2016)).
- Sistematización avanzada y Cloud Computing: focalizada a una automatización de baja energía y computación en la nube.
- Internet del Futuro: referente también al Internet of Everything, dirigida especialmente a las redes 5G y a las tecnologías software para sistemas complejos y altamente conectados.
- Contenido: referente al acceso, creación, gestión, uso e intercambio de grandes cantidades de datos, a través de la puesta en marcha de tecnologías Big Data. Asimismo se orienta hacia la convergencia de la industria de los contenidos y los nuevos medios de comunicación y, al desarrollo de tecnologías para el aprendizaje e interfaces para la accesibilidad.
- Robótica y sistemas autónomos: para su estudio en la industria avanzada de los automóviles, la salud, la logística, etc.
- Tecnologías clave habilitadoras: investigación e innovación en fotónica así como micro y nano-electrónica y su aplicación en la industria.

Para concluir añadir que estas actividades están alineadas a su vez con las macrotendencias TIC detalladas a continuación.



Fuente: INCIBE, 2016

Conclusión

Observamos cómo los ejércitos y los sistemas de armas han jugado un papel importante tanto en la invención como en el desarrollo de tecnologías, siendo puestos posteriormente al servicio de aplicaciones civiles, como por ejemplo ocu-

rrió con el radar o el desarrollo ulterior de las tecnologías de microondas, e incluso dando un gran impulso a Internet (Ortega, 2010).

Hemos construido un mundo totalmente distinto al que conocemos de hace 100 años, pero estamos intentando manejarlo a partir de una cultura de hace siglos o milenios. El resultado es una disfunción insostenible. Así que nuestro reto es aceptar que se necesita de una revolución cultural donde las competencias tecnológicas y sobre todo mediáticas, se hacen totalmente imprescindible para proteger nuestros datos e identidad en la Red.

Podemos crear nuevos métodos y procesos que nos defiendan de los ataques externos, pero si no hay una correcta usabilidad de esas tecnologías, o no se dispone de los suficientes conocimientos para que nos ofrezcan su máxima capacidad, de nada nos sirve la ciencia. El sector público requiere soluciones de seguridad integral, basadas en ciberinteligencia y ciberdefensa, que contribuyan a la protección de los organismos públicos locales, regionales, nacionales e internacionales (INCIBE, 2016), siempre y cuando esté en manos de profesionales que sepan manejarlas de forma correcta.

Referencias Bibliográficas

Braun, E. y Mc Donald, S. (1984) R*evolución en miniatura: La historia y el impacto de la electrónica del semiconductor.* Madrid: Fundescos/Tecnos.

Castells, M. (2003). *La Galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*. Barcelona: Edición De Bolsillo.

República Dominicana es uno de los 10 países de la región con una estrategia de ciberseguridad. (21 de junio de 2018). Santo Domingo: *Diario Libre*. Recuperado de https://bit.ly/2qurQbh

Europa Press. (2018). ¿Cuáles son los países más adictos a Internet? Madrid: *Vozpopuli*. Recuperado de https://bit.ly/2F1pOcO

Hergueta, E. (2017). *La sociedad del conocimiento*. Madrid: Universidad Antonio de Nebrija.

Horizon 2020. (2016). Sistemas ciber físicos. España: 2020 *Horizon*. Recuperado de http://www.2020horizon.es/Sistemas-ciber-fisicos-i2363.html

Ibañez, A. (2011). Leyenda y realidad tras el logo de la manzana mordida de Apple. España: *Rtve noticias*. Recuperado de https://bit.ly/19EZ89I

INCIBE. (2016). *Tendencias en el mercado de la ciberseguridad*. Recuperado de https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf

INTECO. (2009). *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Recuperado de https://www.uv.es/limprot/boletin9/inteco.pdf

Molas, J. (2008). *El vínculo entre innovación militar y civil: Hacia un nuevo marco de relación*. Ciencia, Pensamiento y Cultura, (84).

Montero, M. (2012) Memex. El invento que pudo haber cambiado el mundo. Galicia: *Xombit*. Recuperado de https://bit.ly/2h5XRBw

ORSI. (2008). *Estudio Castilla y León 2.0: Hacia una Sociedad de la Colaboración*. Consejería de Fomento de la Junta de Castilla y León, Observatorio Regional de la Sociedad de la Información.

Ortega, V. (2010). *La innovación tecnológica en el sector de la Defensa y la Seguridad en España*. En IV Congreso Internacional de Seguridad y Defensa. Madrid.

Rheingold, H. (1993). The Virtual Community: Homesteading on the Electronic Frontier. New York: *Addison-Wesley*. Recuperado de http://www.rheingold.com/vc/book/

Rodríguez de las Heras, A. (2018). *EdX: Utopedia*: Educación para una Sociedad del Conocimiento. Recuperado de https://bit.ly/2zuqbXc

WSMR (2018). Radiactividad. New México. White Sands Missile Range. Recuperado de https://bit.ly/2yTuAns