Capítulo primero

Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0)

Luis Joyanes Aguilar
Presidente de la Fundación I+D del Software Libre (Fidesol)
Catedrático de Lenguajes y Sistemas Informáticos
Universidad Pontificia de Salamanca

Resumen

Industria 4.0 *ha sido un término acuñado por el Gobierno alemán con el soporte de industrias alemanas para describir la digitalización de sistemas y procesos industriales, y su interconexión mediante* ***Internet de las cosas*** *para conseguir llegar a una nueva visión de la fábrica del futuro o fábrica inteligente.* La transformación digital de la industria y las empresas con la integración de las nuevas tecnologías disruptivas como ***Big Data***, ***Cloud Computing*** (la ***nube***), **Internet de las Cosas** y ***Ciberseguridad***, todo ello, enmarcado en las **Ciudades Inteligentes (*Smart Cities*),** está produciendo el advenimiento y despliegue de la **cuarta revolución industrial**. Las sofisticadas amenazas a la propiedad intelectual y a la privacidad, a los sistemas y los productos conectados, requieren estrategias y herramientas de ciberseguridad que garanticen en el marco de la Industria 4.0, ciberseguridad de calidad industrial y habilitados para la tendencia dominante de Internet de las Cosas.

Palabras clave

Industria 4.0, *Big Data*, computación en la nube, Internet de las Cosas, cadena de bloques, tecnologías financieras, aprendizaje automático, aprendizaje profundo, privacidad, robots conversacionales, robots virtuales, robots conversacionales, ciudades inteligentes, web profunda.

Abstract

Industry 4.0 has been a term coined by the German Government with the support of German industries, to describe the digitization of systems and industrial processes, and their interconnection via the Internet of things to get reach a new vision of the factory of the future or intelligent factory. The digital transformation of the industry and companies with the integration of new disruptive technologies like **Big Data, Cloud Computing (Cloud), Internet of Things** and **Cybersecurity**, all framed in the Smart Cities is producing the advent and deployment of the **fourth industrial revolution.** The sophisticated threats to intellectual property and privacy, systems and connected products require strategies and tools cybersecurity to ensure within the framework of the Industry 4.0, cybersecurity industrial quality and enabled the dominant trend of Internet of Things.

Keywords

Industry 4.0, Big Data, cloud computing, Internet of Things, blockchain, fintech, machine learning, deep learning, privacy, cobots, bots, chatbots, smart cities, deep web.

La ciberseguridad en tiempo real

Las noticias de impacto relativas a ciberseguridad se suceden casi sin solución de continuidad y, con frecuencia, la última noticia hace palidecer la anterior. En el mes de septiembre de 2015, Apple sufrió el mayor ataque informático de su historia y tuvo que retirar más de cincuenta aplicaciones que contenían un *software* malicioso (*malware*) que pretendía robar datos de los dispositivos de los usuarios. Unos meses antes, Sony Pictures Entertainment quedó paralizada por la intrusión de unos *hackers* que robaron más de 33.000 documentos con información comprometedora de la compañía y sus empleados. El propio Pentágono de Estados Unidos ha sufrido ciberataques de diferentes índoles.

El viernes 21 de octubre de 2016 se produjo una oleada de ciberataques masivos que inutilizaron las páginas web de grandes compañías[1]. La prensa mundial calificó a estos ciberataques como los más graves de la última década. Los ciberataques se produjeron contra uno de los mayores proveedores de internet, la empresa Dyn, que controla los servicios de páginas web de grandes compañías y medios de comunicación como Twitter, Spotify, Reddit, Airbnb, Netflix, Paypal, eBay... y medios de comunicación como *The New York Times, Financial Times, The Guardian*... Los ataques fueron de denegación de servicios, DDoS y estimaciones publicadas hablaban de haber afectado a más de 1.000 millones de usuarios.

Durante el encuentro anual de 2015 del Foro Económico Mundial (*WEF*, World Economic Forum), celebrado en Davos (Suiza), John Chambers, *CEO* de Cisco, definió muy claramente la situación actual de la ciberseguridad como objetivo preferente de las empresas con la siguiente frase lapidaria, lanzada durante su intervención en el evento: «Las empresas se dividen en dos categorías: las que han sido *hackeadas* y las que no lo saben». Viniendo del máximo responsable de la empresa fabricante número 1 del mundo de las comunicaciones, es para hacernos pensar. En este mismo foro, la ciberseguridad estuvo en primer plano y en posición preferente como objetivo de las empresas. Entre las conclusiones de los expertos del Foro se anunció con gran resonancia que el sector tecnológico, en el que se engloba el análisis masivo de datos (*Big Data*) y el almacenamiento en la nube, podría producir unos beneficios globales de entre 9,6 y 21,6 billones de dólares, por lo que alertaron sobre la seguridad informática y advertían que si la sofisticación de los ataques superaba las capacidades defensivas de los equipos los altercados provocarían pérdidas y daños más graves.

Las empresas necesitan fondos para investigar sobre nuevos tipos de *malware* y desarrollar nuevos métodos para prevenir ciberdelitos. El citado

[1] Guillén, Beatriz; Faus Joan y Jiménez, Rosa. «Varios ciberataques masivos inutilizan las webs de grandes compañías». *El País*, 22 de octubre de 2016. http://tecnologia.elpais.com/tecnologia/2016/10/21/actualidad/1477059125_058324.html

Chambers concluyó su intervención en el Foro expresando su temor por lo que puede estar al caer: «las cuestiones relacionadas con la ciberseguridad empeoraron en 2014 y, lamentablemente, en 2015 va a ser mucho peor»[2].

Otra fuente solvente, IBM[3], una de las grandes empresas especializadas en la actualidad en ciberseguridad, considera que una organización recibe un promedio de 1.400 ciberataques por semana y a nivel mundial estima que el cibercrimen genera anualmente 440.000 millones de dólares en ganancia, y cada día se generan nuevas amenazas a las que las empresas no tienen capacidad de enfrentarse con éxito, a menos que dispongan de una buena estrategia de ciberseguridad, así como las herramientas y programas adecuados.

¿Así pues, *cómo está España en ciberseguridad con indicadores y referencias internacionales?*

El índice mundial de ciberseguridad de la UIT (*ITU*)

El **Índice Mundial de Ciberseguridad** [IMC**,** en inglés**,** *GCI* (*Global Cybersecurity Index*][4] surge de la asociación de colaboración entre el sector privado y una organización internacional, la UIT, con el fin de impulsar la cuestión de la ciberseguridad hasta el primer plano de las agendas nacionales.

El IMC es un proyecto conjunto emprendido por ABI Research y la Unión Internacional de Telecomunicaciones (*ITU*, International Telecommunications Union), que contribuye a una mejor comprensión del compromiso de los Estados soberanos con la ciberseguridad. Tiene sus raíces en la Agenda sobre Ciberseguridad Global de la UIT y considera el nivel de compromiso en cinco ámbitos o indicadores: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional.

---

[2] Noticias de Panda Security: www.pandasecurity.com/spain/mediacenter/malware/la-ciberseguridad-objetivo-preferente-de-las-empresas [consultado, 30 de julio de 2016].

[3] Antonio Becerra, «El reto actual de la ciberseguridad», en *El Economista*, México, 29 de agosto de 2015. www.eleconomista.com.mx/tecnociencia/2015/08/29/reto-actual-ciberseguridad [consultado, 7 de agosto de 2016].

[4] La última edición publicada como informe «Índice Mundial de Ciberseguridad y perfiles de ciberbienestar» fue en abril de 2015 [en línea y descarga gratuita: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf]. La edición de 2016 está en construcción, aunque la última visita [5 de octubre de 2016] realizada a su página oficial en el sitio oficial, de la *ITU* [www.itu.int] y en la página oficial del índice GCI 2016 [en línea: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx] se anuncia que el índice está en elaboración y que la próxima edición del GCI tiene previsto un índice mejorado, más consultas abiertas y más *partners*. *ITU* manifiesta que se ha formulado el nuevo índice con un enfoque *multistakeholder* que potencia la experiencia de diferentes organizaciones, con los objetivos de mejorar la calidad del GCI, promoviendo la cooperación internacional y el intercambio de conocimiento en este tema [http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2016.aspx, consultado 14 de octubre de 2016].

El resultado es un índice a nivel de país y una clasificación mundial de la preparación para la ciberseguridad. El IMC no pretende determinar la eficacia ni el éxito de una medida particular, sino simplemente la existencia de estructuras nacionales para implementar y promover la ciberseguridad.

La UIT reconoce que no es posible que una sola publicación trate adecuadamente todos los aspectos de la ciberseguridad con la profundidad necesaria. Sin embargo, esperan que el perfil de ciberseguridad sea de utilidad para los debates y las investigaciones en curso ya que proporciona datos reales sobre los retos y oportunidades actuales en materia de ciberseguridad. En el anexo 3 de la publicación del IMC[5] figura una recopilación de los perfiles de ciberseguridad de todos los Estados miembros de la UIT, actualizados en el momento de imprimir de la citada publicación.

Clasificación mundial (índice IMC)

Muchos países tienen la misma clasificación en el índice, lo que indica que se encuentran en el mismo nivel de preparación. Este índice tiene un bajo nivel de detalle, ya que su objetivo es presentar la preparación de los países para la ciberseguridad o su compromiso con esta y no el detalle de sus capacidades ni sus posibles vulnerabilidades (fuente: *ITU*).

Cuadro 1: Clasificación de los países por índice

País	Índice	Clasificación mundial
Estados Unidos de América*	0,824	1
Canadá*	0,794	2
Australia*	0,765	3
Malasia	0,765	3
Omán	0,765	3
Nueva Zelandia*	0,735	4
Noruega*	0,735	4
Brasil	0,706	5
Estonia*	0,706	5
Alemania*	0,706	5
India*	0,706	5
Japón*	0,706	5

Figura 1.1.
Fuente: ITU. http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf

En la clasificación mundial España ocupa el grupo 9, pero por índice numérico figuramos en el puesto 33. Destacar que en Europa los países con mayor índice (por encima de España) son: Noruega, Estonia, Alemania, Reino Unido, Austria, Hungría, Países Bajos, Letonia, Suecia, Letonia, Eslovaquia y Francia; a continuación España y nos sigue Italia. Resaltar que en el caso

[5] Véase: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf

de Latinoamérica están delante de España: Brasil, Uruguay y Colombia, por este orden.

Índice mundial de ciberseguridad y perfiles de ciberbienestar

País	Índice	Clasificación mundial
República de Corea	0,706	5
Reino Unido	0,706	5
Austria*	0,676	6
Hungría*	0,676	6
Israel*	0,676	6
Países Bajos*	0,676	6
Singapur	0,676	6
Letonia*	0,647	7
Suecia*	0,647	7
Turquía	0,647	7
Hong Kong	0,618	8
Finlandia	0,618	8
Qatar	0,618	8
Eslovaquia	0,618	8
Uruguay	0,618	8
Colombia	0,588	9
Dinamarca*	0,588	9
Egipto	0,588	9
Francia*	0,588	9
Mauricio	0,588	9
España*	0,588	9
Italia	0,559	10
Marruecos	0,559	10
Uganda	0,559	10

Figura 1.2.
Fuente: ITU. http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdfFig

La cuarta revolución industrial

La cuarta revolución industrial (origen del término Industria 4.0) hace referencia a las cuatro fases de la revolución industrial.

- *Primera revolución industrial*. Máquinas de vapor y ferrocarril en el siglo XIX.
- *Segunda revolución industrial*. Motores eléctricos y producción en masa a principios del siglo XX. Aparece el motor de combustión, se desarrolla el aeroplano y el automóvil, y como grandes inventos aparece el teléfono y la radio.
- *Tercera revolución industrial.* Automatización y la informática en los años 70 del siglo XX.
- *Cuarta revolución industrial.* Los actuales «sistemas ciberfísicos» que recopilan y procesan información, toman decisiones inteligentes y ejecutan tareas en entornos cambiantes.

La Industria 4.0 es el producto más tangible de la cuarta revolución industrial y está favoreciendo la fabricación inteligente en un marco revoluciona-

rio para diseñar, implantar y gestionar ecosistemas complejos que proporcionan información en tiempo real y posibilitan las interacciones autónomas entre máquinas, sistemas, objetos y cosas. Este modelo permite sacar el máximo partido y rendimiento del **Internet de las Cosas** (**IoT**), la nube, los *Big Data* y la analítica de datos, las aplicaciones de última generación y la ciberseguridad.

Industria 4.0: origen, evolución y futuro

Industria 4.0 ha sido un término acuñado por el Gobierno alemán para describir la digitalización de sistemas y procesos industriales y su interconexión mediante el Internet de las Cosas; en otras palabras, conseguir la transformación digital de la industria. Pese a todo el esfuerzo de propagación del término, en el caso alemán, como origen del mismo, todavía muchas empresas de ese país —en el año 2015— no sabían bien qué hacer con ese nuevo paradigma industrial y cómo posicionarse[6]. «Uno de cada dos directivos de la industria alemana, austriaca y suiza desconocen el término Industria 4.0, solo una cuarta parte sí dice conocer el término, sin saber bien qué entender del mismo y solo la cuarta parte restante conoce bien los cambios que traerá consigo la Industria 4.0».

En España, el País Vasco ha sido pionero y el Gobierno vasco lanzó una iniciativa para impulsar la Industria 4.0 haciendo propio el concepto y poniéndose un objetivo: «que la industria vasca vuelva a alcanzar el 25 % del PIB[7]». Más tarde comentaremos la iniciativa a nivel nacional conocida como «Industria Conectada 4.0».

El término Industria 4.0 ha hecho fortuna y, tanto en Europa como en Asia y América, ya existen iniciativas sobre el mismo. En realidad, el significado inherente al término es la creación del concepto de **fábrica inteligente** que ha sido impulsada, principalmente por las empresas industriales alemanas Siemens y Bosch.

Industria 4.0 viene asociado con el nacimiento de la cuarta revolución industrial y se corresponde con una nueva manera de organizar los medios de producción utilizando las tecnologías digitales y la información inteligente de datos a partir del *Big Data* (los grandes volúmenes de datos que se podrán transmitir entre objetos inteligentes a través del Internet de las Cosas).

---

[6] Resultados de la encuesta realizada por el proveedor de servidos informáticos CSC entre novecientos altos directivos de empresas en Alemania, Austria y Suiza. Ver «Industria 4.0: hacia el futuro de la producción industrial» en *Economía Hispano-Alemana*, n.º 2, 2015, pp. 7-8.

[7] Eneko Ruiz Jiménez, «La cuarta revolución industrial llega desde Alemania», *El País*, 2 de julio de 2015. http://www.elpais.con/ccaa/2014/10/15/paisvasco/1413383975:967198.html [consultado 2 de octubre de 2015].

El concepto fue utilizado por primera vez en 2011 en la Feria de Hannover (Salón de Tecnología Industrial). Posteriormente, en 2013, el Gobierno alemán encargó a una comisión de trabajo e investigación de la National Academy of Science and Engineering (ACATECH) un informe que detallara el significado y el posible poder del término.

Las tecnologías disruptivas tales como *Cloud Computing* (la nube), Computación Ubicua, Internet de las Cosas *(IoT, Internet of Things), Big Data* y *Analytics*... o las tendencias de consumo como ***BYOD*** (Bring Your Own Device) están revolucionando la forma de entender la tecnología y el modo en que interactuamos las personas con ella. A la industria están llegando las tecnologías anteriores unidas a otras que ya se apoyan en el campo de los sensores, las redes inalámbricas, los objetos inteligentes... Así, tecnologías ya clásicas como ***M2M*** (*Machine to Machine*), soporte de la comunicación entre máquinas y dispositivos; redes inalámbricas de sensores ***WSN*** (Wireless Sensor Networks) y la evolución del Internet de las Cosas en el Internet Industrial de las Cosas, ***IIoT*** (*Industrial Internet of Things*) o internet de todo, ***IoE*** (*Internet of Everything*), como prefiere denominarlo Cisco —el gigante mundial de las telecomunicaciones—.

Industria conectada 4.0

La iniciativa «Industria Conectada 4.0» es la extensión del concepto Industria 4.0 a la realidad nacional española y se lanzó a finales de julio de 2015, habiéndose presentado ya el programa oficial y todo el proyecto el 8 de octubre del mismo año. El proyecto busca impulsar la transformación digital de la industria española mediante la actuación conjunta y coordinada del sector público y privado. Por parte oficial, el antiguo Ministerio de Industria, Energía y Turismo y, por parte privada, las empresas multinacionales españolas, Banco de Santander, Telefónica e Indra, en una primera presentación.

El proyecto Industria Conectada 4.0 contempla los denominados «habilitadores digitales» que son el conjunto de tecnologías que hacen posible esta nueva industria que explota el potencial del Internet de las Cosas. Estos habilitadores se agrupan en tres grandes categorías[8] (figura 3 del Proyecto Oficial).

– **Hibridación del mundo físico y digital** que permiten poner en relación el mundo físico con el digital mediante sistemas de captación de información o de materialización de la información digital en el mundo físico. Los habilitadores de mayor relieve en la actualidad según el informe:

  • Impresión 3D (impresión o fabricación aditiva).
  • Robótica avanzada.
  • Sensores y sistemas embebidos.

[8] Informe «Industria Conectada 4.0. La transformación digital de la industria española».

Figura 1.3. Marco conceptual de habilitadores digitales.Fuente: Informe original «Industria Conectada 4.0». Ministerio de Industria, Energía y Turismo (8 de octubre de 2015).http://www.industriaconectada40.gob.es/Paginas/Index.aspx#inicio

– **Comunicaciones y tratamiento de datos.** La información anterior se canaliza y procesa. Son las tecnologías que permiten trasladar la información de forma segura desde los habilitadores de hibridación del mundo físico y digital hasta el siguiente grupo. Esos habilitadores —indispensables para que todos los restantes puedan funcionar adecuadamente— son, fundamentalmente:

  • Computación y *cloud* (computación en la nube).
  • Conectividad (hiperconectividad) y movilidad.
  • Ciberseguridad.

– **Aplicaciones de gestión intraempresa/interempresa**. La información alimenta a la tercera capa de habilitadores aplicando la inteligencia y los datos recibidos en aplicaciones de gestión. Conforman la capa de inteligencia o procesamiento de la información obtenida de los dos primeros bloques. Se consideran:

  • Soluciones de negocio.
  • Soluciones de inteligencia (*Big Data* y *Analytics)* y control.
  • Plataformas colaborativas.

En el citado informe oficial, presentado el 8 de octubre de 2015, se insistía en la necesidad de la digitalización para mantener posiciones competitivas y hacía hincapié en la hiperconectividad y las nuevas tecnologías ya implantadas: la computación en la nube, el Internet de las Cosas, el *Big Data* y la sensorización (sensores, contadores inteligentes...) que permitirían que la industria pueda alcanzar la cuarta revolución industrial.

La Industria 4.0 está soportada en cuatro grandes pilares, los tres citados del Internet de las Cosas, la nube y *Big Data* y un cuarto, la ciberseguridad.

Son numerosos los estudios publicados durante 2015 y 2016 —probablemente continuarán— sobre las tecnologías disruptivas de la Industria 4.0. Deseamos resaltar uno, en especial, que ha tenido gran impacto en el mundo de la empresa e industria. Ha sido realizado por la consultora multinacional The Boston Consulting Group. Este estudio define nueve pilares o parámetros de la Industria 4.0. A los cuatro citados anteriormente añade:

- Robots autónomos (colaborativos, inteligentes...).
- Los drones con énfasis en los drones programables y autónomos que, por una parte, están llamados a revolucionar a la industria y, por otra, a traer grandes riesgos a la ciberseguridad pública y privada.
- Simulación 3D.
- Sistemas integrados.
- Realidad aumentada (geolocalización).
- Fabricación aditiva (impresión en 3D).

Las tecnologías disruptivas pilares en la Industria 4.0 y en la ciberseguridad

The Boston Consulting Group, en el estudio[9] citado anteriormente —publicado en abril de 2015—, identifica nueve áreas básicas (pilares del avance tecnológico) de la Industria 4.0.

Traducción de la figura original en sentido de las agujas del reloj

Robots autónomos.

Simulación.

Sistemas de integración horizontal y vertical.

Internet industrial de las cosas.

Ciberseguridad.

La nube (*Cloud*).

Fabricación aditiva (impresión 3D).

Realidad aumentada.

Big Data & Analytics.

El pie del recuadro.

Industria 4.0 es la visión de la producción industrial del tuturo.

Fuente: BCG.

[9] Michael Rüßmann, Markus Lorenz, Philipp Gerbert, Manuela Waldner, Jan Justus, Pascal Engel, y Michael Harnisch. The Boston Consulting Group. *Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries*. Capítulo 1. *The Nine Pillars of Technological Advancement,* 9 de abril de 2015.
https://www.bcgperspectives.com/content/articles/engineered_products_project_business_industry_40_future_productivity_growth_manufacturing_industries/#chapter1

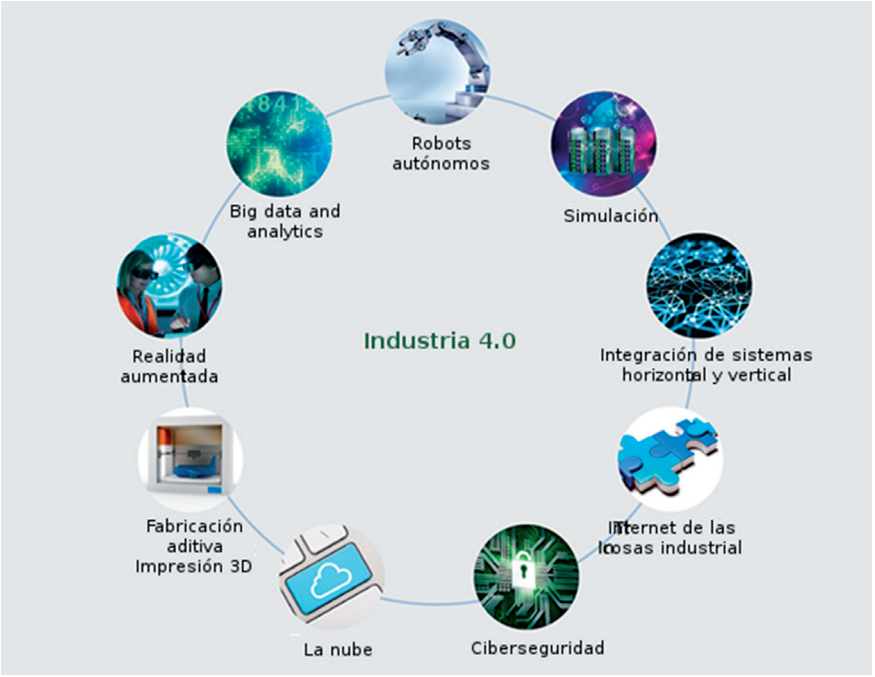

Figura 1.4. Nueve pilares del avance tecnológico en la Industria 4.0: la visión de la producción industrial del futuro. Fuente: The Boston Consulting Group.

La mayoría de estas nueve tecnologías ya se usan actualmente en las fábricas, sin embargo, es en la Industria 4.0 donde estas tecnologías transformarán la producción: células aisladas y optimizadas se unirán conjuntamente para formar flujos de producción totalmente integrados, automatizados y optimizados, lo que conllevará mayor eficiencia y un cambio en las relaciones tradicionales de producción entre distribuidores, productores y clientes, así como entre máquinas y humanos. Un extracto en traducción libre del estudio se describe a continuación.

«Muchas industrias han usado robots desde hace mucho tiempo para abordar tareas complejas, pero es ahora cuando los robots industriales están evolucionando para alcanzar una mayor utilidad. Cada vez son más autónomos, flexibles (colaborativos) y cooperativos, hasta tal punto que interactuarán con otros robots y trabajarán lado a lado con humanos de forma segura, aprendiendo de ellos. Estos robots costarán menos y tendrán más capacidades que los usados actualmente en la fabricación».

«En la fase de ingeniería ya se usan hoy día simulaciones 3D de productos, materiales y procesos de producción. Pero en el futuro las simulaciones se usarán también más extensivamente en operaciones de planta. Estas simulaciones explotarán datos en tiempo real que reflejarán el mundo físico en

un modelo virtual, el cual incluirá máquinas, productos y humanos. Esto permitirá a los operadores realizar pruebas y optimizar las configuraciones de las máquinas para el producto siguiente en la línea de producción virtual antes de cualquier cambio en el mundo físico, reduciendo así los tiempos de configuración de las máquinas y aumentando la calidad».

«La mayoría de los sistemas TI (tecnologías de la información) no están plenamente integrados actualmente. Las compañías, los distribuidores y los clientes no suelen estar estrechamente vinculados; tampoco los departamentos como los de ingeniería, producción o servicio. Las funciones desde la empresa hasta el nivel de planta no están totalmente integradas. Incluso el departamento de ingeniería en sí (producto-planta-automatización) carece de completa integración. Sin embargo, con la Industria 4.0 las compañías, los departamentos, las funciones y las capacidades estarán mucho más cohesionadas. Redes universales de integración de datos evolucionarán y permitirán cadenas de valor verdaderamente automatizadas».

«A día de hoy, solo algunos sensores y máquinas trabajan en red y hacen uso de computación empotrada (embebida). Típicamente están organizados en una pirámide de automatización vertical en la cual los sensores, los dispositivos de campo con inteligencia limitada y los controladores de automatización están gobernados por un sistema de control global. Con el Internet Industrial de las Cosas un mayor número de dispositivos (a veces, incluso productos no terminados) se enriquecerán de la computación empotrada y se conectarán a través de estándares tecnológicos. Esto permitirá a los dispositivos de campo comunicarse e interactuar, tanto con otros iguales a ellos como con controladores más centralizados, según sea necesario. También descentraliza el análisis y la toma de decisiones, lo que permitirá respuestas en tiempo real».

«Muchas compañías todavía dependen de sistemas de gestión y producción desconectados o cerrados, pero con la creciente conectividad y uso de protocolos de comunicación estándar que conlleva la Industria 4.0, la necesidad de proteger los sistemas industriales críticos y líneas de fabricación de las amenazas de ciberseguridad aumentan dramáticamente. Como resultado, son esenciales tanto comunicaciones seguras y fiables, como sofisticados sistemas de gestión de identidad y acceso de máquinas y usuarios».

«Las compañías ya usan *software* basado en la nube para algunas aplicaciones de empresa y de análisis, pero con la Industria 4.0 un mayor número de tareas relacionadas con la producción requerirán mayor intercambio de datos entre lugares y compañías. Al mismo tiempo, el rendimiento de las tecnologías en la nube mejorará, alcanzando tiempos de reacción de solo unos milisegundos. Como resultado, los datos y la funcionalidad de las máquinas irán poco a poco haciendo uso cada vez más de la computación en la nube, permitiendo más servicios basados en datos para los sistemas de producción. Incluso los sistemas de monitorización y control de procesos podrán estar basados en la nube».

«Las compañías acaban de empezar a adoptar la fabricación aditiva como, por ejemplo, la impresión 3D, la cual es usada, principalmente, para crear prototipos y producir componentes individuales. Con la Industria 4.0 estos métodos de fabricación aditiva serán ampliamente usados para producir pequeños lotes de productos personalizados que ofrecen ventajas de construcción, como son los diseños ligeros y complejos. Los sistemas de fabricación aditiva descentralizados, de alto rendimiento, reducirán las distancias de transporte y el *stock* de productos».

«Los sistemas basados en realidad aumentada soportan una gran variedad de servicios, como por ejemplo la selección de piezas en un almacén y el envío de instrucciones de reparación a través de dispositivos móviles. Estos sistemas se encuentran aún en sus primeros pasos, pero en el futuro las compañías harán un uso mucho más amplio de la realidad aumentada para proporcionar a los trabajadores información en tiempo real con el objetivo de mejorar la toma de decisiones y los procedimientos de trabajo. Por ejemplo, los trabajadores podrían recibir instrucciones de cómo sustituir una pieza en particular mientras están mirando el propio sistema bajo reparación a través de unas gafas de realidad aumentada, por ejemplo. Otra aplicación podría ser la formación de trabajadores de forma virtual».

«El análisis de grandes cantidades de datos ha surgido recientemente en el mundo industrial, permitiendo optimizar la calidad de la producción, ahorrar energía y mejorar el equipamiento. En la Industria 4.0, la obtención y exhaustiva evaluación de datos procedente de numerosas fuentes distintas (equipos y sistemas de producción, sistemas de gestión de clientes...) se convertirá en norma para el apoyo de toma de decisiones en tiempo real».

Tendencias en ciberseguridad: un primer avance (2015-2016)

El *Informe Anual de Seguridad Nacional 2015*[10] del Gobierno de España, publicado por el Departamento de Seguridad Nacional en mayo de 2016, dedica la parte 3 de la sección «Ámbitos de la Seguridad Nacional» a la ciberseguridad (pp. 53-64). En este último informe se destaca «la importancia de la colaboración público-privada que resulta clave en un ámbito como la ciberseguridad». Asimismo, resalta la realización de varios eventos, entre ellos la realización en 2015 del Foro Nacional para la Confianza Digital dentro del enfoque de colaboración público-privada, con veintiuna instituciones participantes y otros eventos de gran impactos.

Otras iniciativas notables y muy destacadas en el citado *Informe Anual 2015* son:

[10] http://www.lamoncloa.gob.es/presidente/actividades/Paginas/2016/270516rajoycsn.aspx http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/INFORME %20ANUAL %20DE %20SEGURIDAD %20NACIONAL %202015.pdf [consultados 30 de septiembre, 2016].

– Promoción de la capacitación de profesionales en ciberseguridad e impulso a la industria española a través de un Plan de I+D+i.
– Implantación de una cultura de ciberseguridad sólida.
– Intensificación de la colaboración internacional.

En el anterior *Informe Anual de Seguridad Nacional de 2014*[11], publicado el mes de abril de 2015 por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, con la participación de otros organismos públicos, se incluyó por primera vez un apartado único sobre ciberseguridad (pp. 64-75). El Informe destaca cuatro tipos de ataques a los sistemas de información:

– El **ciberespionaje**: una de las mayores preocupaciones durante el año 2014 para los gobiernos occidentales.
– La **ciberdelincuencia**: durante 2013 los criminales han aumentado la frecuencia, variedad y amplitud de ataques a cambio de una recompensa.
– El **ciberterrorismo**: en sus dos vertientes, bien como instrumento facilitador de sus actividades, o bien como objeto de su acción para la comisión de actividades terroristas.
– El ***hacktivismo****:* aunque con menor representación, engloba aquellos ataques dirigidos por grupos movidos por una determinada ideología y que tienden a atacar la seguridad de los sistemas y la información.
– **La ciberguerra**, que engloba operaciones militares y aquellas otras orientadas a negar, modificar, llevar a engaño o destruir las capacidades propias residentes en los sistemas de información y telecomunicaciones que afecten a la defensa nacional.

Informe de seguridad de la información de Cisco

Entre los numerosos estudios de tendencias de ciberseguridad, citar los de Intel, Karspesky, Panda, McKinsey... aunque hemos decidido quedarnos con el de Cisco[12], publicado en agosto de 2015, en el que destaca las tendencias hacia fuentes de ciberinteligencia.

Analiza las principales tendencias de ciberseguridad durante la primera mitad del citado año y desvela cómo la evolución hacia el Internet de Todo (*Internet of Everything*, *IoE*) y la transformación digital están generando nuevos vectores de ataque y nuevas oportunidades de lucro para los cibercriminales.

Cisco señalaba en el estudio que: «restaurar la confianza en el año 2015 requerirá una mayor colaboración por parte de la industria y la creación de nuevos estándares para hacer frente a este panorama de amenazas y con mejores estrategias de seguridad que reduzcan el tiempo de detección, haciendo un mayor y mejor uso de todas las fuentes de ciberinteligencia. Sería necesario

[11] http://www.dsn.gob.es/sites/dsn/files/Informe_Seguridad_Nacional %202014.pdf
[12] Cisco, *Informe Semestral de Seguridad de Cisco 2015*, 6 de agosto de 2015.

llegar a un modelo donde la seguridad sea un elemento crítico desde el proceso mismo de diseño y desarrollo de cada dispositivo y de cada aplicación».

«Amenazas asociadas con Flash y explotadas por kits como Angler, la evolución de *ransomware* o campañas de *malware* mutante como Dridex requieren imperiosamente reducir los tiempos de detección. Estos se sitúan hoy entre los cien y doscientos días, según las estimaciones de la industria, frente a las cuarenta y seis horas —según Cisco— de media que ofrecen las soluciones de nueva generación, tales como Cisco Advanced Malware Protection (***AMP***) que incluye seguridad retrospectiva».

Recomendaciones de Cisco

La batalla entre cibercriminales y proveedores de seguridad —marcada principalmente por la rápida innovación en técnicas de ataque y defensa— se está acelerando, generando un mayor riesgo para empresas y usuarios. Los proveedores deben así centrarse en el diseño de soluciones de seguridad integradas que ayuden a las organizaciones a ser más proactivas y a establecer políticas alineadas con los usuarios, los procesos y la tecnología. Cisco ofrece algunas recomendaciones al respecto:

Defensa integrada. Las organizaciones demandan soluciones de seguridad integradas en lugar de puntuales, que permitan incluir la seguridad en todas partes y reforzarla en cualquier punto, desde el centro de datos (*data center)* hasta los terminales, las oficinas remotas y la nube (C*loud*).

Servicios profesionales. La proliferación de amenazas avanzadas, dinámicas y persistentes, la creciente carencia de expertos en ciberseguridad y la fragmentación de la industria requiere que las organizaciones se apoyen en servicios profesionales efectivos.

Marco regulatorio global de ciberseguridad. Es necesario establecer un marco regulatorio global y cohesionado en el que participen múltiples Gobiernos y empresas para evitar problemas jurisdiccionales a la hora de hacer frente a las ciberamenazas, resolver los problemas geopolíticos y sostener el crecimiento económico.

Proveedores contrastados. Para que un proveedor tecnológico pueda considerarse contrastado y fiable debe integrar la seguridad desde el principio, en todas sus soluciones y a través de todo su ciclo de vida, desde el proceso de desarrollo y test hasta la cadena de suministro y soporte.

Los ciberriesgos

Las amenazas (ciberamenazas o ciberriesgos) son cada vez más frecuentes y avanzadas, por lo que gestionar una crisis cibernética es algo más que probable: los ataques de denegación de servicio distribuidos (***DDoS***), el robo

de credenciales mediante técnicas de *phishing* o *malware*, la fuga masiva de información digital, el *ransomware*[13] (programas que impiden el acceso a la información mediante técnicas de cifrado, pidiendo un rescate para el descifrado) o las amenazas avanzadas persistentes (*APT*, *Advanced Persistent Threats*).

Los *hackers, sin* ninguna duda, nunca descansan. Uno muy sonado realizado en agosto de 2015 fue el robo de datos de clientes de la página web de contactos Ashley Madison, que durante las siguientes semanas trajo de cabeza no solo a la compañía, sino también a sus 37 millones de usuarios.

La web profunda, la web invisible (Deep Web)

Existe una creciente dificultad para detectar y erradicar las redes de robots *(botnets*) que se siguen utilizando para la diseminación de *spam*, para la ejecución de ataques *DDoS, spear-phishing, click-fraud, keylogging,* así como la difusión de *ransomware* o la sustracción de dinero digital. Los datos de 2014 señalaban, por aquel entonces, un descenso en el número de *botnets* detectadas, aunque no su eficacia y su peligrosidad. De hecho, los atacantes ahora utilizan la red **TOR** para ocultar *botnets* y/o servidores de mando y control (C & C), lo que dificulta enormemente su detección y erradicación [CCN-CERT 2015, 14-15]. Recordemos que el CCN-CERT define *TOR*[14] como:

> *«**TOR** (abreviatura de The Onion Router) es un software diseñado para permitir el acceso anónimo a internet. Aunque durante muchos años ha sido utilizado principalmente por expertos y aficionados, el uso de la red TOR se ha disparado en los últimos tiempos, debido principalmente a los problemas de privacidad de internet. Correlativamente, TOR se ha convertido en una herramienta muy útil para aquellos que, por cualquier razón, legal o ilegal, no desean estar sometidos a vigilancia o no desean revelar información confidencial».*

La razón de todo ello podemos encontrarla en la cada vez mayor sencillez para desarrollar ataques *DDoS* y la facilidad para acceder a determinadas herramientas (adquiridas en el mercado negro de la *hidden-wiki*[15], por ejemplo).

---

13 Véase Informe «*Ciberamenazas 2014. Tendencias 2015*» del CCN-CERT IA-09/15.

14 CCN-CERT IA-09/15. *Ciberamenazas 2014. Tendencias 2015*. Resumen ejecutivo, p. 15. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html

15 Es una enciclopedia que se encuentra alojada en la web oculta (*Hidden web* llamada también *invisible web* o *deep web*) y funciona como índice para acceder a páginas de dominio (.onion) que indica una dirección IP anónima accesible por medio de la red *TOR* (*The Onion Route*) (CCN-CERT 2015, p. 15).

La necesidad de un seguro de ciberriesgos en la empresa

Los ciberriesgos han dejado de ser una amenaza esporádica para las empresas y se constituyen ya como un problema importante en todos los sectores. La Administración, la banca, organizaciones y empresas de todo tipo, la industria, deben estar alertas ante su peligrosidad. El Instituto Nacional de Ciberseguridad (INCIBE) publicó un informe a finales de septiembre de 2015[16] donde alertaba de un importante aumento de ciberataques durante ese año y, en concreto, cincuenta y dos ciberataques a infraestructuras críticas y servicios básicos del país, la mitad dirigidos a operadores de suministro eléctrico; en cuanto a ataques contra empresas, el INCIBE advierte que se han doblado en 2016, hasta llegar a los 36.000 en el mes de agosto de ese año.

Por estas razones, los ciberriesgos han pasado a ser uno de los principales focos de atención de los gerentes de riesgos de las empresas, de cualquier tamaño y sector. Ello ha obligado al «estudio y posible implantación de un seguro de ciberriesgos» al igual que cualesquiera otros riesgos relevantes en las empresas y en cualquier industria.

Un informe de Allianz Global[17] sobre ciberseguridad, dado a conocer el 8 de septiembre de 2015, señalaba que las primas mundiales de seguros cibernéticos superarán los 20.000 millones de dólares en la próxima década frente a los 2.000 millones que captan en la actualidad. El aumento de este negocio se producirá por una mayor concienciación sobre estos riesgos y por los cambios normativos que propician la contratación de esta cobertura asegurada por parte de las empresas, señala el citado estudio. «En la actualidad menos del 10 % de las empresas suscriben una póliza para cubrirse de los riesgos cibernéticos». La «ciberdelincuencia» cuesta 445.000 millones de dólares anuales a la economía mundial y la mitad de este importe recae en las diez principales economías mundiales (Estados Unidos con 108.000 millones lidera la clasificación, seguida de China con 60.000 millones y Alemania con 59.000 millones).

Los expertos recomiendan a las compañías que, además de ser innovadoras en tecnología y atención al cliente, deberían hacer una inversión especial en ciberseguridad, tanto en protección como en la respuesta a los ataques de los *hackers*, ya que los datos que manejan a diario son un material sensible por contener información personal de sus clientes.

---

[16] Anuncio realizado en León el 24 de septiembre de 2015, por el Instituto Nacional de Ciberseguridad (INCIBE), a través del CERT de Seguridad e Industria. Véase *La Vanguardia*: http://www.lavanguardia.com/tecnologia/20150924/54436823384/espana-ha-sufrido-52-ciberataques-a-infraestructuras-criticas-en-2015.html

[17] Citado por Marimar Jiménez en «El negocio de la ciberseguridad se dispara ante las nuevas amenazas», *Cinco Días*, 30 de noviembre de 2015 [en línea]. http://cincodias.com/cincodias/2015/11/29/tecnologia/1448814144_530160.html

«Los usuarios deben estar seguros y tranquilos con los datos personales que ceden a las empresas. Con la revolución tecnológica existe el "ciberriesgo", pero para responder a estos ataques nos reinventamos constantemente para crear barreras de contención», afirmaba un directivo de Axa en un foro empresarial, organizado por el periódico *Expansión*[18] y la consultora Cap Gemini.

La ciberseguridad en la empresa y la empresa ante la ciberseguridad

La naturaleza de los ciberriesgos existentes requiere la definición de una estrategia en materia de seguridad, alineada con los objetivos de la empresa. ¿Cómo definir esta estrategia? Para ello será necesario determinar cuál es el punto de partida de la empresa, en qué situación se encuentra en ese momento en materia de seguridad y cuál debería ser el nivel de seguridad de la organización, en función de una serie de factores, como el sector de negocio al que pertenecemos, los objetivos estratégicos o los requisitos que define el mercado, entre otros. El camino entre nuestro punto de partida y nuestro objetivo de seguridad determinarán cuál es nuestra hoja de ruta hacia la ciberseguridad.

Para ayudar a definir la hoja de ruta de su empresa, INCIBE ha creado el decálogo hacia la ciberseguridad: un conjunto de diez pasos orientados a mejorar el nivel de seguridad de su empresa y, por tanto, proteger su negocio. El *Decálogo de Ciberseguridad*[19] es el siguiente:

1. Analizar los riesgos.
2. Los responsables de seguridad.
3. Seguridad en el proyecto de trabajo.
4. La protección de la información.
5. Movilidad con seguridad.
6. Protección *antimalware.*
7. Actualización y parcheo.
8. La seguridad de la red.
9. Monitorización.
10. Seguridad gestionada.

Como casos de estudio a considerar queremos destacar el caso de Bankia[20], que en septiembre de 2015 creó un «Comité de respuesta a incidentes de ciberseguridad» y otro «Comité de gestión del fraude tecnológico».

---

[18] Carmen Alaba, 14 de septiembre de 2015. www.expansion.com/empresas/banca/2015/06/22

[19] INCIBE. «*Decálogo de Ciberseguridad: «El camino hacia la ciberseguridad en su empresa. Diez pasos para garantizar la ciberseguridad en su empresa*». 2015. https://www.incibe.es/protege-tu-empresa/blog/decalogo-ciberseguridad-empresas , 30 de octubre de 2014 [consultado, 1 de septiembre de 2016].

[20] Junta general de accionistas 2015 de Bankia**.** *Expansi**ó**n*, 22 de septiembre de 2015.

También, y por seguir con el sector bancario y en este caso a nivel europeo, mencionar al Banco Central Europeo (BCE) que en el *Informe de Estabilidad Financiera*, publicado en 2015, advirtió de que el riesgo de ciberataques es creciente dado que las amenazas cada vez son más complejas e intensas y recomendaba a las ciento veintitrés principales entidades de la Eurozona bajo su vigilancia, activar medidas de seguridad contra el cibercrimen e instaba a dichas entidades a revisar los sistemas y protocolos de protección frente a los ciberataques para impedirlos y garantizar así la continuidad del negocio y el buen servicio a los clientes.

El negocio de la ciberseguridad

Como muestra del negocio que ofrece la ciberseguridad, en España, Telefónica ha alcanzado ya un volumen de negocio global en el ámbito de la ciberseguridad de 400 millones de euros[21]. Solo en España las ventas de productos y servicios de Telefónica a empresas superan los 100 millones con un crecimiento anual del 30 %.

A nivel global, un informe publicado a mediados de septiembre de 2015 por la consultora Gartner evaluaba en 75.000 millones de dólares la cifra que gastarán las organizaciones de todo el mundo en materia de ciberseguridad durante ese año 2015.

La ciberseguridad en la industria eléctrica: necesidad de estándares

La industria eléctrica, según INCIBE, requerirá como infraestructura crítica:

- Identificar y conocer los conceptos de ciberseguridad en Sistemas de Control Industrial y Protección de Infraestructuras Críticas, sus definiciones y relaciones.
- Descubrir y analizar el estado del arte de la Protección de Infraestructuras Críticas a nivel internacional.
- Detectar y analizar la situación actual de la seguridad en el sector industrial y las amenazas y vulnerabilidades de los Sistemas de Control Industrial reconociendo su riesgo asociado.

Y además será necesario identificar, describir y adoptar marcos y estándares aplicables en estos entornos: **ISA/IEC 62443, ISO 27001, BS 25999, NIST SP 800-82,** etcétera**;** establecer, implementar y adoptar un *Programa de Seguridad de los Sistemas de Control Industrial* y *Diseñar un Plan de Seguridad y Protección de la Infraestructura Crítica*.

[21] Santiago Millán. «Telefónica supera los 400 millones de dólares en su negocio global de ciberseguridad», *Cinco Días*, 9 de octubre de 2015, p. 6.

De un modo sectorial las redes inteligentes (*Smart Grid*), fiel reflejo de la fábrica inteligente y estandarte de la Industria 4.0, unido a las nuevas normativas legales y a la creciente implantación de los contadores inteligentes junto con la infinidad de objetos inteligentes que utilizan, inundarán las infraestructuras críticas del suministro eléctrico y conducirán, sin ninguna duda, a la necesidad de actualización de las estrategias de ciberseguridad existentes para hacerlas más fiables y eficientes y que deberán desplegar las operadoras eléctricas.

Para afrontar con las debidas garantías de éxito las estrategias de ciberseguridad en las redes inteligentes se requiere del uso de estándares de obligado cumplimiento por las operadoras eléctricas (INCIBE 2015) y deberán implementar estos estándares tanto en los dispositivos como en el proceso. Los estándares que nuestras operadoras, nos consta, ya utilizan, y aprobados por el organismo de estandarización CENELEC/ETSI, son los siguientes[22]:

- *Estándares específicos del sector eléctrico.* Se desarrollan para asegurar los mecanismos eléctricos en términos de seguridad lógica y ciberseguridad: estándares **ISO/IEC TR 27019:2013** y el estándar clásico de seguridad de la información **ISO 27002.**
  A estos estándares que recomienda INCIBE consideramos sería preciso añadir el cumplimiento del estándar **ISO/IEC 27032** «para la ciberseguridad» con el que la organización ISO pretende garantizar la seguridad en los intercambios de información en la Red que puede ayudar a combatir el cibercrimen con cooperación y coordinación, así como luchar contra ataques de ingeniería social, *hackers, malware, spyware y* otros tipos de *software* no deseado.
- *Estándares de seguridad lógica provenientes del campo de las TIC***.** Pueden servir (total o parcialmente) para guiar la seguridad de las redes inteligentes. Estándar **ISO/IEC 15408.**
- *Estándares provenientes del campo de automatización industrial***.** En general y sin excepciones es el campo de la ciberseguridad. Son más cercanos a la operativa real de las redes inteligentes al proyecto del sector industrial. Estándar **ISA/IEC 62443.**

Otros temas importantes a considerar por las empresas: la monitorización de los Centros de Datos (*Data Centers*), la reciente Ley de Protección de Infraestructuras Críticas, la ciberseguridad en el sector eléctrico, el papel de la ética y de la situación de la industria de la seguridad informática en diferentes regiones geográficas del planeta.

[22] INCIBE (2015). *Estándares de ciberseguridad en las redes inteligentes*, 3 de septiembre de 2015. https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Estandares_ciberseguridad_redes_inteligentes

Las operadoras eléctricas disponen de Sistemas de Gestión de la Ciberseguridad Industrial (**SGCI**) que contemplan los riesgos relacionados con la ciberseguridad que se han de centrar en la indisponibilidad de los sistemas y en el acceso indebido a determinadas aplicaciones así como la gestión de:

- *Firewalls* y sistemas antintrusión.
- Sistemas antivirus.
- Mejora del sistema de seguridad de los requisitos de acceso.
- Mecanismos de detección de incidencias.
- Actualización de *software*.
- Simulacros de ataques.
- ...

La ciberseguridad en la banca y en el sector financiero (tecnologías financieras de impacto)

El informe «Financial Services Technnology 2020 and Beyond: Embracing disruption», elaborado por la consultora PwC[23] y publicado en julio de 2016, analiza las grandes tendencias relacionadas con la tecnología que van a transformar el sector financiero en los próximos cuatro años y que, por consiguiente, tendrán gran impacto en la ciberseguridad de la información en este campo:

> «**FinTech,** *la economía colaborativa;* **Blockchain***, la inteligencia artificial y la robótica; la nube; la ciberseguridad; el empuje de Asia como centro tecnológico y de innovación; la inteligencia de cliente; la tecnología aplicada en el ámbito de la regulación y la digitalización de todos los procesos y actividades»*[24].

En lo relativo a la ciberseguridad, el informe destaca que: «la ciberseguridad ya es una de las principales preocupaciones de los máximos ejecutivos de las entidades financieras y esa situación no hará sino continuar en los próximos años como consecuencia, entre otros factores, del rápido crecimiento del Internet de las Cosas, especialmente las áreas de pagos, seguros y banca comercial» (Nacenta, 2016)[25]. Sin embargo, son las otras dos tecnologías, ***fintech*** y ***blockchain,*** esencialmente «financieras», a las que dedicaremos nuestra atención, reiterando, claro está, el impacto que prevé el informe de la nube, la robótica y la inteligencia artificial, que trataremos en otro momento en este capítulo.

---

[23] http://www.pwc.es/es/publicaciones/tecnologia/assets/informe-financial-services-tecnology %202020.pdf

[24] Nota de prensa, de la filial española, elaborada por Salvador Nacenta, socio del Sector Financiero de PwC: http://www.pwc.es/es/sala-prensa/notas-prensa/2016/informe-financial-services-tecnology-2020.html.

[25] Ibíd.

Tecnologías y empresas Fintech

Fintech, contracción de las palabras *Finance* y *Technology*, aglutina y define a todas aquellas empresas que se sirven de las últimas novedades tecnológicas para brindar productos y servicios financieros innovadores, incluyendo aquellos que facilitan la vida cotidiana gracias a la disrupción tecnológica, englobando prestaciones como: la banca digital, los créditos y pagos *online* o el cambio de divisas a través de la Red. De información extraída —esencialmente de la prensa económica y los portales de los grandes bancos españoles, BBVA y Santander, entre otros— las empresas Fintech aglutinan a todas aquellas que desarrollan y ofrecen servicios financieros que utilizan la última tecnología existente para poder ofrecer productos innovadores. Así aparecen los nuevos productos financieros basados en innovación tecnológica tales como: negociación de mercados, financiación colectiva, desarrollo de sistemas de seguridad financiera, asesoramiento en línea, dinero digital, criptomonedas, monederos digitales (*wallets*), etcétera. Estas empresas y tecnologías asociadas implicarán políticas de seguridad de la información (ciberseguridad) en el ámbito de las instituciones financieras, retos normativos y técnicos de la seguridad, de cooperación internacional, de protección de datos, etcétera.

Una definición más académica, del IEBS, considera que: *Fintech* es un concepto que aglutina a aquellas empresas financieras tecnológicas que tratan de aportar nuevas ideas y que reformulan, gracias a las nuevas tecnologías de la información, las aplicaciones móviles o el *Big Data*, la forma de entender y prestar los servicios financieros. Las *Fintech* producen y producirán una transformación radical del sector financiero (IEBS, 2016)[26]. La escuela de negocios IEBS enumera un gran número de áreas y sectores sobre los que actuará IEBS (de ahí, los retos y oportunidades que supondrán las *fintech* y los riesgos y necesidad de políticas claras y eficaces en ciberseguridad en las empresas y en la banca que adopten dichas tecnologías):

- Banca móvil.
- *Big Data* y modelos predictivos.
- *Crowdfunding* y *crowdlending*.
- Criptomonedas y monedas alternativas.
- Mercado de divisas.
- Gestión automatizada de procesos y digitalización.
- Gestión de riesgos.
- Pagos y transferencias.
- Préstamos P2P.
- Seguros.

[26] Raúl Jaime Maestre. *¿Qué es el Fintech, definición, sectores y ejemplos de* startups*?* http://comunidad.iebschool.com/iebs/finanzas-2-0-y-control/que-es-fintech/. Diciembre de 2015.

– Seguridad y privacidad.
– Servicios de asesoramiento financiero.
– *Trading*.
– ...

Blockchain

El *World Economic Forum*, en el informe publicado en junio de 2016 relativo a las «10 tecnologías emergentes de 2016»[27], en colaboración con la prestigiosa revista *Scientific American*, destaca de modo muy especial las tecnologías *blockchain*. ¿Qué es *blockchain*? Es una tecnología de transferencia de información, soporte de las monedas digitales, en particular del *bitcoin.* Técnicamente *blockchain* (cadena de bloques) es una base de datos descentralizada donde las transacciones electrónicas se registran de forma segura y verificada. La cadena de bloques conforma una gigantesca base de datos abierta al público y a través de la cual se envía información de un emisor a un receptor. Por el camino los datos de ese intercambio se verifican por distintos actores independientes conectados a la misma red, que otorgan veracidad a esta transmisión. Al decir de grandes expertos, la futura economía mundial se basará en transacciones en cadenas de bloques y las organizaciones de terceros pueden no ser necesarias.

El *blockchain*, asociado a *bitcoin*, es público aunque las personas que intervienen en la base de datos son anónimas a ojos del usuario. De hecho, la historia del término considera que esta tecnología de transferencia de información nació para posibilitar la aparición del *bitcoin.*

¿Por qué su impacto en la economía mundial y en la economía de la ciberseguridad? Visa, Microsoft, Accenture, la banca (en España, una iniciativa liderada por el Banco de Santander)... se están subiendo al carro de este protocolo de transferencia segura de datos. Algunos bancos comienzan a utilizarlo como alternativa a su sistema propio *SWIFT*. Grandes empresas tecnológicas como IBM[28] cuentan también con su propio sistema de *blockchain*; Microsoft, a mediados de septiembre de 2016, ha lanzado su proyecto de *blockchain: Microsoft's Blectchley Blockchain Project*[29].

El Banco de Santander, según noticias de *El Confidencial*[30], estima que la adopción de esta tecnología le permitirá ahorrar alrededor de 20.000 millo-

[27] weforum.org/es/agenda/2016/06/las-10-tecnologias-emergentes-de-2016
[28] Sitio de *blockchain* de IBM: www.ibm.com/blockchain
[29] Christine Avanessians Senior Program Manager, Microsoft Azure. 20 de septiembre de 2016. https://azure.microsoft.com/en-us/blog/project-bletchley-blockchain-infrastructure-made-easy/.
[30] Jaume Esteve. «Avalancha Blockchain: la tecnología que está reinventando el negocio de la banca». *El Confidencial*, 22 de septiembre de 2016. http://www.elconfidencial.com/tecnologia/2016-09-22/blockchain-fintech-banca-online_1263534/

nes de dólares al año. El propio Banco de Santander está promoviendo el uso de dinero digital entre bancos utilizando la tecnología.

El diario *Expansión*[31], en un detallado artículo, explica cómo el Grupo del Santander se ha aliado con UBS, BNY Mellon, Deutsche Bank, el operador de mercado ICAP y la *start-up* Clearmatics para desarrollar la moneda digital *Utility Settlement Com* (***USC***). Se trata de un sistema que utiliza la tecnología *blockchain* para facilitar los pagos y liquidaciones de forma eficiente, rápida y segura. La tecnología *blockchain*, sobre la que se basan criptomonedas como el *bitcoin*, permite la «transaccionalidad» de activos reales como euros o dólares. Así, un *USC* sería una «moneda» que existe en un registro contable distribuido, es decir, en un *blockchain*.

La nueva divisa digital podría ponerse en funcionamiento a comienzos de 2018. Según las fuentes de *Expansión* se considera que «además de mejorar los servicios para los clientes, Santander estima que el uso de esta nueva divisa digital genera al sector un ahorro de costes de 20.000 millones de dólares (cerca de 17.750 millones de euros), según se incluye en *The Fintech 2.0 Paper*, un estudio realizado por el propio Santander con Oliver Wyman»[32].

La ciberseguridad y la inteligencia artificial

La inteligencia artificial desde el advenimiento de *Big Data* está llegando a numerosos sectores que hasta hace unos años prácticamente era impredecible y que en la actualidad están impactando en la ciberseguridad de las organizaciones y empresas.

El conocimiento en la inteligencia artificial integrada con *Big Data* está ayudando y ayudará a los delitos informáticos. Una nueva generación de plataformas de negocio está surgiendo en la convergencia del **aprendizaje automático** (*machine learning*) —recientemente el **aprendizaje profundo** (*deep learning*)— y B*ig Data* que generarán un gran cambio en materia de ciberseguridad. Los algoritmos de aprendizaje automático y la ciberinteligencia asociada están potenciando las predicciones de ataques cibernéticos que mejorarán las tasas de detección y pueden ser la clave para revertir la tendencia actual en cuanto a crecimiento de delitos cibernéticos y potenciar la ciberseguridad.

[31] *Expansión*, «Santander promueve el uso de dinero digital entre bancos**»**, 26 de julio de 2016. http://www.expansion.com/empresas/banca/2016/08/26/57bf44d8e5fdea8b4c8b464a.html. El artículo, además de comentar todo el proyecto, incluye una ilustración muy significativa del funcionamiento del *blockchain* como sistema de pago.

[32] *The Fintech 2.0 Paper: rebooting financial services.* http://santanderinnoventures.com/fintech2/

IBM Watson

IBM decidió hace varios años cambiar su modelo de negocio principal y centrarse en las tecnologías cognitivas a través de su supercomputador *Watson*, la referencia central del fabricante.

Watson se hizo famoso al competir en 2011 en un famoso concurso de televisión estadounidense de preguntas, «Jeopardy¡», al derrotar a sus dos oponentes humanos, como ya lo hiciera en el año 1977 el supercomputador *DeepBlu*e que ganó a Gary Kasparov —campeón mundial— jugando al ajedrez.

IBM *Watson* es el primer sistema cognitivo diseñado de forma que los computadores no se programan sino que son capaces de entender el lenguaje natural de las personas y aprender. Se ha convertido, desde aquel año 2011, en una tecnología comercial accesible a través de la nube y que cuenta con clientes en numerosos sectores y países del mundo, entre ellos España, donde, gracias a la colaboración con CaixaBank ha aprendido, además de técnicas financieras, el lenguaje español.

IBM *Watson* es un sistema informático de inteligencia artificial diseñado para realizar labores de computación cognitiva (entre ellas el procesamiento de lenguajes naturales y el razonamiento y el aprendizaje automático), desarrollado sobre la tecnología DeepQA de IBM. Una plataforma tecnológica que utiliza el procesamiento del lenguaje natural y el aprendizaje automático para analizar y revelar información clave de las grandes cantidades de datos no estructurados.

En la práctica *Watson* analiza datos no estructurados (artículos, reportes de investigación, datos empresariales, datos de redes sociales, datos de sensores...) utilizando procesos de lenguaje natural para entender la gramática y el contexto, entiende preguntas complejas –evaluando los posibles significados y determinando qué es lo que se está preguntando–, contesta a la preguntas más exigentes de sus clientes, extrae –casi en tiempo real– información clave de documentos y descubre y presenta información, patrones y relaciones entre datos. *Watson* aprende sobre un nuevo tema antes de contestar preguntas relacionadas. Utiliza algoritmos de aprendizaje automático investigando en grandes volúmenes de datos (*Big Data*) para encontrar las muchas respuestas posibles.

Watson se utiliza hoy día en un gran número de aplicaciones en todo tipo de sectores, desde empresariales e industriales hasta la Administración, la universidad y la investigación. Las más recientes inauguraciones relacionadas con IBM *Watson* ha sido el Centro de IBM *Watson* para Internet de las Cosas[33]

[33] El centro inaugurado por IBM, según el propio IBM, es su mayor inversión en Europa en las dos últimas décadas. Contará con mil expertos en Internet de las Cosas y en Industria 4.0. Integrará las tecnologías cognitivas de IBM con *IoT*, Industria 4.0 en la nube de IBM a través de la plataforma *IBM Watson IoT Cloud* [en línea: https://www-03.ibm.com/press/es/es/pressrelease/48491.wss].

—un centro de referencia mundial con sede en Múnich (Alemania), inaugurado el 15 de diciembre de 2015— y la plataforma expresa para ciberseguridad inaugurada a finales de mayo de 2016 y disponible comercialmente que comentamos a continuación.

Watson for Cyber Security

IBM Security[34] anunció en mayo de 2016 que va a dedicar a la ciberseguridad una nueva versión basada en la nube (*Cloud*) de la tecnología cognitiva de la empresa, entrenada en el lenguaje de seguridad como parte de un proyecto de investigación a largo plazo. *Watson* va a ser entrenado con la ayuda de varias universidades estadounidenses en el lenguaje de la ciberseguridad. IBM pretende optimizar las capacidades de los analistas en seguridad utilizando sistemas cognitivos que automaticen la búsqueda de conexiones entre los datos, las amenazas emergentes y las distintas estrategias de protección. IBM ha denominado a este nuevo modelo de seguridad como «seguridad cognitiva» que generará hipótesis, razonamientos basados en evidencias y recomendaciones para mejorar la toma de decisiones en tiempo real.

Plataforma de Ciber-Inteligencia de Accenture

La consultora Accenture, una de las «cuatro grandes» (*big four*) compañías a nivel mundial (junto con PwC, KPMG y EY) lanzó a primeros de marzo de 2016 una «plataforma de Ciber-Inteligencia»[35] que hace uso de los avances en tecnología y permite identificar ciberamenazas en tiempo real, monitorizando en tiempo real comportamientos sospechosos.

Según Accenture es la primera solución del mercado que combina servicios de seguridad gestionada, inteligencia artificial, *cloud* y *analytics;* es una plataforma que permite a la compañía identificar amenazas en tiempo real. «Hace uso de los avances en tecnología de procesadores (chips) con una combinación patentada de inteligencia artificial, aprendizaje automático y análisis de datos constante que permite a las organizaciones identificar ciberamenazas en tiempo real. La plataforma examina la actividad en las redes para aprender, determinar y reportar comportamientos sospechosos atribuibles a ciberataques»[36]. Es de resaltar, según Accenture, que la plataforma se puede implementar en una semana y una vez instalada la plataforma empieza a aprender «automáticamente» —lo que es normal— y ella misma mejorará continuamente.

[34] www-03.ibm.com/press/us/en/pressrelease/49683.wss#feeds
[35] www,accenture.com/es-es/company-news-release-new-cybersecurity-platform
[36] Ibíd.

Robótica y ciberseguridad: *cobots*, *bots* y *chatbots*

El informe del *World Economic Forum* (*WEF*), «The future of Jobs and Skills» presentando en Davos en enero de 2016, y que ha tenido una gran repercusión mundial, predecía para los próximos años la desaparición de 7,1 millones de empleos debido a la implantación de las tecnologías disruptivas que traería la cuarta revolución industrial y, especialmente, la robótica unida a la inteligencia artificial, *Big Data* y el Internet de las Cosas. Por suerte, también consideraba la creación en el mismo periodo de 2 millones de empleos que traerían las nuevas profesiones y oficios para cubrir los nuevos puestos de trabajo derivados de las mismas tecnologías.

En este apartado queremos destacar, por su innegable presencia en la ciberseguridad —y su impacto fundamental en la privacidad y protección de datos—, a los nuevos modelos de robots colaborativos (*cobots*), así como los robots virtuales o asistentes virtuales (*bots* y *chatbots*).

*Robots colaborativos (*cobots*)*

Una nueva generación de robots está llegando a las fábricas y cadenas de producción, así como a muchos otros sectores como el turismo, la medicina, los centros comerciales o los aeropuertos, son los robots colaborativos que, a su vez, están originando una nueva tendencia en ingeniería: la **cobótica.**

Los robots colaborativos (*cobots*) son una nueva generación de robots, que aprovechando la integración de la inteligencia artificial y el inmenso caudal de datos que proporcionan los *Big Data* y el Internet de las Cosas, se están integrando con los humanos[37], permitiendo trabajar de una manera estrecha a robots y personas humanas, sin restricciones de seguridad como las requeridas en aplicaciones típicas de robótica industrial. Los *cobots* son unas nuevas generaciones de robots que están llegando a las fábricas y otros sectores de la industria y la empresa para colaborar de forma segura con los trabajadores gracias a los avances ya citados y además las tecnologías visuales —realidad virtual y realidad aumentada— y la innumerable presencia de los sensores.

Los robots colaborativos están diseñados para trabajar con seguridad e interactuar con los humanos en una fábrica, un taller, un hotel... haciendo que los trabajadores sean más productivos ya que ayudan a reducir algunas o muchas de las tareas repetitivas que hacen esos trabajadores a lo largo de su jornada laboral.

Los *cobots* están permitiendo el nacimiento de una nueva era en la automatización industrial y en las cadenas de producción. Los robots colaborativos,

[37] También se les suele conocer en algunos ámbitos académicos e industriales como «robots humanoides».

al decir de los grandes expertos en robotización y cobotización, compiten con los robots industriales por la sencillez, flexibilidad y facilidad de programación. Se verán cada vez más en los procesos de producción y en sectores diferentes a los procesos industriales.

Un caso de estudio muy implantado es el sector de la hostelería y el turismo. Hosteltur —la organización profesional de turismo— en su revista oficial[38] (el número de julio-agosto de 2016) describe varias aplicaciones prácticas ya en funcionamiento que están trabajando en el diseño de robots sociales para ferias, museos y hoteles. Algunas de ellas son las siguientes:

«Incorporación de robots a la plantilla de nuevos hoteles. 1. El hotel "Ghent Marriot", en Bélgica, cuenta desde finales de 2015 con *Mario*, un robot que ayuda a los recepcionistas a efectuar el *check-in*, habla diecinueve idiomas e incluso entretiene a los clientes con sus bailes». Cita la revista un caso excepcional: el hotel "Henn-na", situado en Nagasaki, «es el primero del mundo en atender a sus clientes exclusivamente con robots. Cuenta con dos robots en recepción, dos en conserjería, uno en cada habitación que realiza las tareas usuales del servicio añadiendo pronósticos del tiempo, turismo y varios robots para transportar equipaje».

Los asistentes virtuales: bots *y* chatbots

Un ***bot*** (también llamado asistente virtual personal) es un programa informático basado en inteligencia artificial que imita el comportamiento humano para realizar diferentes tareas o funciones por su cuenta y sin la ayuda de un ser humano. El *bot* es capaz de comunicarse con los seres humanos (a través de texto, voz, emociones...) manteniendo una conversación con una persona utilizando el lenguaje natural en dicha conversación. Un ***chatbot*** *(chatter bot)* o *bot conversacional* es el modelo de *bot* más popular, capaz de simular una conversación con una persona y se ha integrado en las aplicaciones de mensajería, tipo *chat*.

Los asistentes virtuales más populares son: *Siri* de Apple (para sistemas operativos iOS y Mac) es el más conocido, dado que también es uno de los más populares desde su incorporación a los teléfonos móviles iPhone; *Cortana* de Microsoft incorporado al sistema operativo Windows 10 y *Google Now* para el sistema operativo móvil Android. Sin embargo, muchos de los grandes fabricantes de computación, tanto de *hardware* como de *software*, así como empresas pequeñas innovadoras, están creando plataformas comerciales de *bots* a las que empresas clientes o particulares pueden conectarse y también desarrollar sus propios asistentes virtuales. Estos son los casos

[38] Xavier Canalis *et al*. «La próxima revolución del turismo. Los robots toman el mando». Madrid: *Hosteltur,* julio-agosto de 2016, pp. 7-19 [en línea: www.hosteltur.com/edicion-impresa/robots-y-turismo-la-proxima-revolucion] [consultada 24 de septiembre de 2016].

del ya mencionado *Watson* de IBM, Amazon con su plataforma *Echo* y asistente virtual *Alexa*, Google que ha convertido su *Google Now* en una nueva plataforma denominada *Google Assistant, Facebook Messenger* con su plataforma *M* para *bots* presentada en abril de 2016 que facilitará las *API (Application Programming Interterface,* interfaz de programación de aplicaciones) para el desarrollo de sus propios *chatbots* por empresas y particulares que los podrán integrar en su propia red social. Samsung ha comprado en 2016 el asistente virtual *Viv* y tiene el proyecto de incluirlo en todos sus productos (aparatos de televisión, teléfonos...). Además de estas plataformas de las grandes empresas de computación, han nacido empresas que han creado sus propias plataformas de *bots* y que tienen también cientos de millones de usuarios, como es el caso de *Kik* y *Slack*, diseñadas especialmente para clientes empresariales y profesionales.

Aplicaciones de los bots

Algunas aplicaciones de asistentes citados anteriormente son:

El asistente virtual *Cortana* de Microsoft, *Siri* de Apple o *Alexa* de Amazon con su altavoz *Echo* —por citar algunos ejemplos— pueden actuar como agentes inteligentes y son capaces de interactuar con *bots* para la ejecución de aplicaciones de comercio electrónico o soluciones de atención al cliente, bien con programas de gestión de relaciones con los clientes (CRM) o con *call centers.*

WeChat —una aplicación de mensajería instantánea muy popular— ha desarrollado sus propios *bots* que permiten, por ejemplo, realizar reservas de hotel, confirmar citas médicas o comprar entradas para el cine a través de mensajes de texto que son interpretados por *bots*.

Google Assistant apoyado por el servicio de mensajería **Allo**, lanzado en septiembre de 2016 y basado en aprendizaje profundo (*deep learning*), pretende dar respuestas predictivas de modo instantáneo y tiene la capacidad de aprender sobre el usuario y las personas con las que se relaciona habitualmente para hacer sugerencias u ofrecer información. La revista *Hosteltur*[39], en el número ya citado (julio-agosto de 2016), describe numerosas aplicaciones de *bots* en la industria del turismo y, en particular, comenta diferentes aplicaciones presentadas en la feria «Fiturtech 2016». Así, en el caso de *Google Assistant* cita algunas aplicaciones de interés: «por ejemplo, si una persona habla con un contacto sobre una cita para cenar, el asistente virtual de Google le ofrecerá restaurantes y la posibilidad de realizar la reserva sin salir de la aplicación *Allo* (lanzada oficialmente en septiembre de 2016) y teniendo en cuenta sus preferencias culinarias permitirá acceder a recorridos virtuales de hoteles, restaurantes u otros recursos turísticos basa-

[39] Ibíd., pp. 11-12.

dos en tecnología "StreetView" (la aplicación de Google Maps) que estarán integrados».

Elies Campo (2016)[40], en un artículo de referencia sobre el tema de *chatbots* publicado en *El País*, considera que «empresas y Gobiernos serán los primeros en beneficiarse de esta tendencia de aplicaciones conversacionales, ya que por fin se podrán comunicar de manera privada de la misma forma en que lo hacen sus clientes y ciudadanos». También en el mismo artículo destaca, en su opinión, los «tres principales tipos de aplicaciones y oportunidades de los *chatbots*»:

- «Las aplicaciones conversacionales para el usuario final, que ofrecen un servicio y experiencia única y resuelven un problema concreto. Asistentes virtuales, asesores financieros, entrenadores personales, etcétera.
- *Software* de *backend* y herramientas para poder gestionar conversaciones de atención al cliente. Compañías, organizaciones y gobiernos se comunicarán e interactuarán con sus clientes y ciudadanos a través de mensajería.
- Los medios de comunicación y periodistas tendrán una nueva manera de comunicarse con su audiencia, distribuir su contenido y facilitar la participación de la audiencia. Para una creciente mayoría de medios de comunicación la mensajería ya es su principal distribución de contenidos».

Asistentes virtuales en páginas web de organizaciones y empresas

Algunos asistentes virtuales ya en uso en numerosas páginas web de organizaciones y empresas que hemos seleccionado:

- ***Elvira*,** asistente de la Universidad de Granada, con una interfaz elaborada con apariencia de ser humano y que trata de dar respuestas acerca de información del sitio web (https://www.ugr.es; http://tueris.ugr.es/elvira).
- ***Irene*.** Ayuda en la compra de billetes de tren en Renfe (http://consulta.renfe.com/renfeO/index.jsp).
- ***Anna***. Asistente al usuario en la compra de muebles en IKEA —cadena de almacenes— (www.ikea.com/es/es).

Los bots*: ¿las nuevas aplicaciones móviles?*

Existe una tendencia creciente de sustitución de aplicaciones móviles por *bots*. Esta es la opinión de Satya Nadella, presidente de Microsoft, que en la

[40] Elies Campo Cid ha sido responsable del crecimiento y negocio de WhatsApp para España, Portugal y América Latina, *El País*, 11 de abril de 2016 [en línea: http://tecnologia.elpais.com/tecnologia/2016/04/11/actualidad/1460348403_483191.html] [consultado 2 de agosto de 2016].

presentación de su plataforma de *bots* planteaba que en lugar de tener que utilizar multitud de aplicaciones móviles los usuarios podrán interactuar con los *bots* de una manera mucho más natural utilizando su propio lenguaje. Con este motivo, Microsoft —y muchos de los gigantes tecnológicos o empresas especializadas— facilitará el desarrollo de *bots* compatibles con su plataforma por parte de empresas y usuarios finales.

En Facebook, en tan solo algo más de seis meses, desde su presentación en abril de 2016 de su plataforma M (Messenger) de *bots*, se han abierto más de 30.000 *chatbots* para ofrecer servicios personalizados. El cometido principal de estos *chatbots* es facilitar la relación entre el cliente y la marca y desde la propia red social de la empresa. Facebook permite de esta manera que la red social de la empresa pueda ser el canal de comunicación con clientes, proveedores, socios... utilizando un *chatbot* propio de la empresa como complemento a las funcionalidades propias de su red social.

La seguridad y los riesgos de los bots

Hemos visto las grandes ventajas que aportan los *bots.* Pero los *bots* también representan grandes riesgos para la seguridad de la información, ya que pueden ser utilizados para realizar tareas maliciosas, como, por ejemplo, promover ciberataques, fraudes, robos, envío de *spam* y propagación de virus, entre muchas otras tareas delictivas. Por eso, el uso de *bots* impone la necesidad de establecer ciertos límites éticos en lo referente a su programación y sus funciones, asumiendo los riesgos que para las estrategias de ciberseguridad de las empresas deben contemplarse.

El nuevo reglamento de protección de datos de la Unión Europea (25 de mayo de 2016)

El 27 de abril de 2016 fue aprobado en Bruselas el Reglamento General de Protección de Datos (UE 2016/679) por el Parlamento y el Consejo Europeo. El Reglamento aprobado se centra en el tratamiento de datos personales y la libre circulación de estos datos. Este Reglamento deroga la Directiva 95/46/EC que ejercía como anterior reglamento.

El Reglamento ha entrado en vigor el 25 de mayo del citado año pero no comenzará a aplicarse hasta dos años después, el 25 de mayo de 2018. Hasta entonces tanto la Directiva 85/46 como las normas nacionales que la trasponen, entre ellas la española, siguen siendo plenamente válidas y aplicables.

La Agencia Española de Protección de Datos (www.agpd.es) ha publicado un amplio documento en el que con un formato «pregunta-respuesta» trata de facilitar la compresión del nuevo marco normativo a los ciudadanos y ayudar a las organizaciones a adaptarse a los cambios que incorpora y cumplir así con sus obligaciones.

Novedades del nuevo reglamento

Estrella Barrionuevo, abogada de la Asesoría Jurídica de Telefónica España, se adelantó a la entrada en vigor del Reglamento y publicó un artículo en el blog *aunclicdelastic* del también blog de Telefónica, blogthinkbig.com, con las novedades más sobresalientes —en su opinión— del nuevo Reglamento de Protección de Datos de la Unión Europea. Un resumen de estas novedades es el siguiente[41]:

- «Introducción del concepto "pseudoanonimización" como categoría intermedia entre los datos personales y los datos anónimos.
- En cuanto al consentimiento, se concreta de forma específica que será necesario que el usuario realice una acción afirmativa para consentir, de manera que las casillas "premarcadas" o la inactividad del usuario no constituirá un consentimiento válido, lo que elimina la posibilidad del conocimiento tácito.
- Se modifica la edad por defecto para que los menores puedan consentir por sí mismos y no a través de quien ostente su patria potestad que pasa de los 14 años que establece actualmente la Ley Orgánica de Protección de Datos (LOPD) a 16, aunque este límite podrá reducirse por parte de los Estados miembros sin bajar de los 13 años.
- Nuevos derechos para el usuario.
  - Derecho al olvido.
  - Derecho a la portabilidad de los datos personales.
- Se crea el nuevo rol profesional de ***DPO*** (*Data Protection Office*), delegado o director de Protección de Datos para Administraciones públicas y entidades que traten datos personales a gran escala.
- Se establece la obligación de realizar análisis de riesgos y evaluaciones de impacto para determinar el cumplimiento normativo.
- Se amplía la obligación de comunicar las brechas o incidentes de seguridad, tanto a los afectados como a la AEPD, a todos los operadores del mercado que traten datos de carácter personal, en un plazo de setenta y dos horas».

Recomendaciones de la AEPD sobre el nuevo reglamento

La AEPD ha elaborado y publicado un documento simplificado —como ya se comentó anteriormente— con el objeto de intentar resolver las posibles dudas de los ciudadanos, organizaciones y empresas, relativas a la puesta en marcha del mencionado Reglamento de la Unión Europea. El modo elegido para redactar el documento ha sido el de «pregunta-respuesta» y para ello ha seleccionado un conjunto de doce preguntas clave con doce respuestas a

[41] aunclicdelastic.blogthinkbig.com/nuevo-reglamento-europeo-de-proteccion-de-datos- [consultado el 27 de julio de 2016].

las mismas y cuya lectura y consulta recomendamos, precisamente, basadas en la procedencia de la fuente, AEPD[42]. Estas preguntas son:

1. La entrada en vigor del Reglamento ¿supone que ya no se aplica la Ley Orgánica de Protección de Datos española?
2. ¿Cuál es, entonces, el significado de que el Reglamento haya entrado en vigor?
3. ¿A qué empresas u organizaciones se aplica?
4. ¿Qué implica para los ciudadanos que el Reglamento amplíe el ámbito de aplicación territorial?
5. ¿Qué nuevas herramientas de control de sus datos poseen los ciudadanos?
6. ¿A qué edad pueden los menores prestar su consentimiento para el tratamiento de sus datos personales?
7. ¿Qué implica la responsabilidad activa recogida en el Reglamento?
8. Entonces, ¿supone una mayor carga de obligaciones para las empresas?
9. ¿Cambia la forma en la que hay que obtener el consentimiento?
10. ¿Deben las empresas revisar sus avisos de privacidad?
11. ¿En qué consiste el sistema de «ventanilla única»?
12. ¿Tienen las empresas que empezar a aplicar ya las medidas contempladas en el Reglamento? No, el Reglamento está en vigor, pero no será aplicable hasta 2018.

Proyecto de colaboración público-privada de la Unión Europea (5 de julio de 2016)

La expansión del Internet de las Cosas y el aumento exponencial de las comunicaciones de datos entre personas y objetos de todo tipo aumenta también la preocupación de los ciudadanos, organizaciones y empresas, por la posibilidad de que se produzca un ataque contra sus datos personales y corporativos.

El inmenso valor de los datos relevantes de la vida de la gente que se vuelcan en la Red crece de igual modo que el auge del citado Internet de las Cosas y restantes tecnologías disruptivas presentes en la actual sociedad. Como señala el suplemento «Negocios» del diario *El País*, todas estas circunstancias harán: «redoblar la importancia de la ciberseguridad para la economía del continente europeo, no solo para la defensa del consumidor y empresas sino como un mercado de 75.000 millones de dólares del que Europa necesita participar»[43].

El 5 de julio de 2016, la Comisión Europea, anunció un **acuerdo de colaboración público-privada** por valor de 1.800 millones de euros hasta 2020, de los que Bruselas pone 450 millones a través del programa «Horizonte 2020» y el

[42] www.agpd.es

[43] NEGOCIOS. «Hacia un mercado común en la Red». Periódico *El País*, suplemento NEGOCIOS, 28 de agosto de 2016, p. 12.

resto tiene previsto venir de la industria concertada a través del convenio de colaboración con la European Cyber Security Organization (*ECSO*, en sus siglas en inglés)[44]. La Comisión Europea, a la hora de definir la estrategia de I+D de los próximos años en el ámbito de la ciberseguridad, «tendrá en cuenta la opinión del sector empresarial de la ciberseguridad», teniendo como interlocutor a la citada asociación *ECSO*. La Comisión ha firmado a este efecto un contrato ***cPPP*** (contractual Public-Private Partnership) de colaboración público-privada con *ECSO*, «el plan de acción tiene su origen en la *Estrategia de Mercado Único Digital*[45] de 2015, en la *Estrategia de Ciberseguridad de la Unión Europea*[46] y en la directiva sobre Seguridad de Redes y Sistemas de Información *"The Directive on security of network and information systems"*» (*NIS* Directive)[47].

Directiva de ciberseguridad (*NIS*) de la Unión Europea (6 de julio de 2016)

El 6 de julio de 2016 —el siguiente día a la firma del acuerdo de la Unión Europea sobre colaboración público-privada en materia de ciberseguridad— se publicó la Directiva *Network and Information Sistems* (*NIS*) que obliga a los «prestadores de servicios esenciales» a tomar las medidas necesarias para garantizar la seguridad de sus instalaciones. El objetivo final es el mercado común digital: «Europa tiene que estar preparada para parar amenazas digitales cada vez más sofisticadas y que no reconocen frontera alguna»[48].

La directiva (UE) 2016/1148[49] del Parlamento Europeo y del Consejo de la Unión Europea de 6 de julio de 2016 es la primera directiva europea en ciberseguridad y la primera norma relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea. La directiva sobre Seguridad de Redes y Sistemas de Información «The Directive on security of Network and Information Sistems» (*NIS* Directive) constituye un paso decisivo para hacer frente al reto que suponen las amenazas de ciberseguridad. La norma establece un enfoque común para evitar ataques a empresas y servicios clave.

---

[44] Ibíd. La empresa española S2 Grupo ha sido una de las participantes en la firma del contrato que se celebró el 5 de julio de 2016 en la sede del Parlamento Europeo de Estrasburgo, en el que han colaborado cincuenta organizaciones europeas. S2 será una de las empresas que liderará la estrategia de I+D de ciberseguridad europea en los próximos años. Representando a la empresa española, como socio de *ECSO*, asistió Miguel A. Juan, *CEO* de S2 Grupo.

[45] Digital Single Market. ec.europa.eu/priorities/digital-single-market_en

[46] https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-open-safe-and-secure-cyberspace

[47] https://ec.europa.eu/digital-single-market/eu)news/directive-security-network-and-information-systems-nis.directive

[48] Andrus Ansip, Comisario Encargado de Seguridad de la Unión Europea, ibíd. «Negocios», *El País*, p. 12.

[49] https://www.boe.es/doue/2016/194/L00001-00030.pdf

El objetivo es acabar con la fragmentación de los sistemas de seguridad cibernética entre los países para actuar de forma cohesionada en el seno de la Unión Europea y exige a las empresas de servicios críticos cumplir con nuevos requisitos. En la práctica busca producir un aumento del nivel general de ciberseguridad en la Unión Europea y es esencial para asegurar la ciberseguridad en Europa.

La citada directiva en ciberseguridad entró en vigor en agosto de 2016 y los Estados miembro tendrán veintiún meses para transponerla y seis meses más para identificar a los operadores de servicios esenciales. Para conseguir sus objetivos establece la obligación, para todos los Estados miembros, de adoptar una estrategia nacional de seguridad de las redes y sistemas de información:

- Crea un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos.
- Crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo «red de *CSIRT*», por sus siglas en inglés de *computer security incident response teams*) con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz.
- Establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales.
- Establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y *CSIRT* con funciones relacionadas con la seguridad de las redes y sistemas de información.

El escudo de privacidad Unión Europea-Estados Unidos (12 de julio de 2016)

La Comisión Europea adopta y pone en marcha el Escudo de la Privacidad (*Privacy Shield*) Unión Europea-Estados Unidos[50]: «más protección para los flujos de datos transatlánticos», el día 23 de julio de 2016.

Este nuevo marco protege los derechos fundamentales de cualquier persona de la Unión Europea cuyos datos personales se transfieran a Estados Unidos y aporta claridad jurídica para las empresas que dependen de transferencias transatlánticas de datos.

El Escudo de la Privacidad Unión Europea-Estados Unidos se basa en los siguientes principios:

[50] europea.eu/rapid/press-release_IP_16_2461_es.htm

- Obligaciones rigurosas para las empresas que trabajan con datos.
- Obligaciones en materia de transparencia y salvaguardias claras para el acceso de la Administración estadounidense: Estados Unidos han dado a la Unión Europea garantías de que el acceso de las autoridades públicas a efectos de aplicación de la ley y de seguridad nacional está sujeto a limitaciones, salvaguardias y mecanismos de supervisión claros.
- Protección eficaz de los derechos individuales.
- Mecanismo de revisión conjunta anual.

La formación en ciberseguridad y en sus tecnogías disruptivas

Empresas de todo tipo, desde multinacionales a pequeñas y medianas empresas, requieren y buscan expertos en seguridad informática y, en especial, en ciberseguridad. Diferentes son los campos de la ciberseguridad más demandados. Entre ellos podríamos destacar:

- Ciberinteligencia.
- Análisis forense.
- *Hacking* ético.
- Desarrollo de *hardware* y *software* seguro.
- Ciberespionaje.
- Encriptación.
- Seguridad en la nube.

En España, América Latina y Caribe existe una amplia oferta de másteres *(*maestrías*),* especializaciones, diplomaturas y expertos, cursos profesionales y de posgrado especializados en ciberseguridad e impartidos por universidades y escuelas de negocio con el apoyo de las grandes empresas informáticas, de seguridad informática y de las grandes consultoras. Estas ofertas hoy día son tanto presenciales como *online* (virtuales) o híbridos.

Los perfiles demandados son muy variados. Desde analistas y consultores de ciberseguridad a expertos en ciberinteligencia, análisis forense, seguridad en la nube... Y cada día más se comienzan a solicitar analistas de *Big Data* para aplicaciones de ciberseguridad, así como desarrolladores de Internet de las Cosas y de Ciudades Inteligentes para gestión de objetos inteligentes de todo tipo (ingenieros de objetos inteligentes).

Asimismo, y dado que la nube (*cloud computing*) es la espina dorsal de la transformación digital de las organizaciones y empresas, soporte de la Industria 4.0 y base de la cuarta revolución industrial, las empresas requieren especialistas y profesionales de la nube, apareciendo nuevos perfiles profesionales tales como «Diseñador de "nubes"» y «Gestores de seguridad en la nube».

Como nota de interés, comentar que los **científicos de datos** (*Data Scientist*)**,** una de las profesiones emergentes más demandada en la actualidad —re-

lacionada directamente con los analistas y desarrolladores *de Big Data*—, comienza a ser ya solicitada para roles en ciberseguridad, especialmente para análisis de datos y ayuda en la toma de decisiones en las estrategias de ciberseguridad fundamentalmente de las grandes empresas para asesoramiento en los grandes volúmenes de datos que hoy día maneja. Por eso se han puesto en boga cursos especializados de Análisis de Datos y de Estadística Computacional, así como de **Aprendizaje Máquina** (*Machine Learning*) y **Aprendizaje Profundo** (*Deep Learning*), programación y desarrollo de lenguajes de programación especializados en análisis de datos, como **R** y **Python,** además, claro, de posgrados (máster y especializaciones) en **Ciencia de Datos** (*Data Science*).

Los nuevos roles profesionales

El sector de las tecnologías de la información tiene en la actualidad un carácter transversal y cada día reclama además de las formaciones clásicas de ingeniería informática, de telecomunicaciones, industriales, electrónica, matemáticas, estadística... otras disciplinas. Asimismo, recomienda formación en empresa, *marketing*, recursos humanos... y, con la creciente preocupación por la privacidad y la protección de datos, también perfiles jurídicos para afrontar las nuevas competencias profesionales hoy demandadas en las empresas y que, a continuación, comentamos.

Las empresas y la Administración requieren ya no solo los departamentos de seguridad de la información y ciberseguridad, sino también de departamentos —independientes o relacionados con los anteriores— de privacidad y protección de datos junto a la concienciación de los riesgos y oportunidades de la ciberseguridad en todos los niveles profesionales de la empresas a nivel personal de directivo o simple empleado.

Así a los perfiles o roles profesionales ya implantados de director de Tecnología (*CTO*, *Chief Technology Officer*) con unas competencias muy abiertas y transversales en toda la organización y empresa, el director de Informática o de Sistemas de Información (*CIO*, *Chief Information Officer*), director de Seguridad de la Información (*CISO*, *Chief Information Security Officer*), hay que sumar dos perfiles profesionales que cada día serán muy demandados en la Administración, organizaciones y en empresas de todo tipo:

– *Chief Data Officer* (*CDO*) (director de Datos). Es un cargo dependiente del máximo ejecutivo de la empresa, a quien reporta directamente. Une las dos disciplinas hoy imperantes en la transformación digital: *Big Data* y *Ciberseguridad.* Su misión es impulsar el crecimiento de la organización y la empresa mediante la transformación digital de la misma. Ha de tener una amplia visión de la gestión de la empresa y del mundo digital, de análisis de datos y de seguridad de la información con el objeto de diseñar estrategias y políticas de ciberseguridad. Requiere una formación

multidisciplinar de ingeniería, estadística, analista digital, especialista en ciberseguridad, además de una amplia visión y conocimiento de la empresa.
– *Data Protection Officer* (*DPO*). Es un perfil jurídico pero con formación informática y de seguridad de la información y ciberseguridad, aunque también podría ser un tecnólogo con formación jurídica en protección de datos y privacidad. Este perfil va a ser exigible en la Administración y en determinadas empresas a partir de 2018, en el que entre en vigor con todas sus consecuencias la nueva Ley de Protección de Datos y Privacidad de la Unión Europea, aprobada en mayo de 2016.

Además de las acreditaciones anteriores, las organizaciones y empresas valorarán cada día con mayor intensidad a los demandantes de empleo y a los propios empleados, las certificaciones internacionales en seguridad como CISA, CISSP, CISM... o certificaciones propias de los grandes fabricantes y proveedores de soluciones de seguridad de la información, *hardware* y *software* propietario o de código abierto, con estándares como OpenStack y otros.

Además y conforme se despliegan las nuevas tecnologías y tendencias tecnológicas como: inteligencia artificial (*machine learning* y *deep learning*), robótica, tecnologías cognitivas (robots, *bots, cobots* y *chatbots, Watson* de IBM), drones, fabricación aditiva (impresión 3D), tecnologías ponibles (*wearables*), aplicaciones de la banca digital, especialmente *fintech* (aplicaciones financieras), tecnologías *blockchain* (cadenas de bloques encriptadoras*)*, aplicaciones de cartografía, GIS, geodesia y ciencias de la tierra... es preciso constatar que aunque las oportunidades que traerán estas tecnologías son innumerables, los incidentes cibernéticos irán en aumento si les unimos los riesgos del «Internet Industrial de las Cosas o Internet de Todo» y el crecimiento exponencial de los datos (*Big Data*) alojados en grandes centros de datos, desplegados a lo largo y ancho del mundo en la nube (*cloud computing*), junto con los enormes riesgos a la privacidad y protección, por parte de los innumerables *hackers* y de *empresas* del «cibercrimen como servicio». Los retos en formación e investigación serán innumerables y una gran oportunidad para el sector.

Por estas razones continuarán emergiendo nuevos perfiles o profesiones que como los grandes sociólogos, especialistas en recursos humanos, nos recuerdan todavía no han nacido y son difíciles de imaginar. Un listado de nuevas profesiones —algunas ya citadas— es la siguiente:

– *Growth Hacker* (responsable de la imagen digital que combina conocimientos de *marketing*, *SEO*, *Community Manager, Social Media Manager*, programación web... Twitter, Facebook, Uber, Airbnb... han potenciado esta nueva profesión).
– Analista de *Big Data*.
– Ingeniero de *Big Data*.

- Científico de datos.
- Ingeniero de Internet de las Cosas.
- Consultor de *hacking ético* (analista de los peligros informáticos y de su prevención y corrección).
- Gestor de robots colaborativos.
- Desarrollador de APIs para *bots, chatbots*...
- Diseñador de «nubes».
- Gestor de seguridad en la nube.
- Expertos en impresoras 3D y fabricación aditiva.
- Ingenieros de robótica y de inteligencia artificial.
- Ingenieros de objetos inteligentes.
- ...

Todos los roles y profesiones citados guardarán una estrecha relación con la nube, la ciberseguridad, Internet de las Cosas y *Big Data*, los cuatro pilares de la transformación digital de las organizaciones y empresas del final de esta década y de la próxima.

Los datos: presente y futuro de la ciberseguridad

En 2020, según estima Cisco, habrá 50.000 millones de objetos conectados (computadores, teléfonos inteligentes, tabletas, sensores, electrodomésticos, etcétera). Por esas fechas, las tecnologías móviles 5G es previsible se comercialicen con velocidades de transmisión de datos doscientas cincuenta veces mayor que la actual 4G (LTE y LTE-Advanced). Estos datos significan que el Internet de las Cosas, Internet de Todo o el Internet Industrial de las Cosas se habrá implantado a lo largo y ancho del mundo, por lo que «el futuro del Internet de la cosas estará en manos de la ciberseguridad». Esta situación significa que se requiere, desde ya, una alta inversión en ciberseguridad, dado que la falta de inversión producirá grandes problemas en organizaciones y empresas.

Los datos se alojarán preferentemente en la nube, por lo que el análisis de los grandes volúmenes de datos será una práctica diaria, de tal forma que *Big Data*, Internet de las Cosas y ciberseguridad serán la piedra angular de la sociedad de la tercera década de nuestro siglo.

Las grandes carreras tecnológicas del futuro —además de las relacionadas con inteligencia artificial y robótica— serán los citados anteriormente: **científicos de datos, desarrolladores del Internet de las Cosas** junto a los **arquitectos y especialistas de ciberseguridad.**

La ciberseguridad en América Latina y Caribe

Existen varios informes sobre el estado del arte y el impacto de la ciberseguridad en la región y tras analizar y estudiar una extensa documentación dispo-

nible en internet de grandes empresas consultoras, empresas especializadas en seguridad informática y organizaciones internacionales de la región hemos decidido seleccionar dos informes, ambos respaldados por organizaciones internacionales como el Banco Internacional de Desarrollo (BID) y la Organización de Estados Americanos (OEA), que han contado con la colaboración, en un primer caso, de una empresa multinacional de seguridad, Symantec, presentado en junio de 2014 y, en un segundo caso, por una institución docente de gran prestigio como la Universidad de Oxford, presentado en marzo de 2016.

- *Tendencias de Seguridad Cibernética en América Latina y el Caribe*[51], realizado por Symantec, la Organización de Estados Americanos (OEA), la Secretaría de Seguridad Multidimensional (SMS) y el Comité Interamericano contra el Terrorismo. Presentado en junio de 2014.
- *Informe Ciberseguridad 2016. ¿Estamos preparados en América Latina y el Caribe?*[52], realizado por el BID (Banco Iberoamericano de Desarrollo), la OEA y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford. Presentado el 14 de marzo de 2016.

Tendencias de seguridad cibernética en América Latina y el Caribe (junio 2014)

Symantec, la Organización de Estados Americanos (OEA), la Secretaría de Seguridad Multidimensional (SMS) y el Comité Interamericano contra el Terrorismo (CICTE) presentaron un informe[53] que analiza el panorama de amenazas, las tendencias de ciberseguridad e incluye información sobre las acciones de los Gobiernos en América Latina y el Caribe frente a estos temas.

El informe (reporte) desarrollado en conjunto explora diferentes aspectos relacionados con la seguridad cibernética, incluyendo el incremento exponencial de las fugas de datos y tendencias como:

- «Crecimiento del *Ransomware* y *Cryptolocker*.
- *Malware* en cajeros automáticos.
- Estafas en redes sociales.
- Vulnerabilidades y riesgos en cómputo móvil.
- Código malicioso (*malware)*.
- *Spam*.
- *Spear phishing*».

A diferencia de otros reportes de amenazas sobre vulnerabilidades cibernéticas que existen en el mercado este informe es único, ya que está enfocado en la región e incluye las perspectivas de los Gobiernos de los Estados miembros de la OEA, así como información detallada sobre el panorama de

[51] https://www.symantec.com/es/mx/page.jsp?id=cybersecurity-trends
[52] https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/
[53] https://www.symantec.com/es/mx/page.jsp?id=cybersecurity-trends

amenazas cibernéticas actual obtenida de la Red Global de Inteligencia de Symantec.

Ciberseguridad 2016 en América Latina y Caribe (marzo 2016)

El Informe *Ciberseguridad 2016. ¿Estamos preparados en América Latina y el Caribe?*[54] fue presentado el 14 de marzo de 2016 en la sede del Centro de Estudios Estratégicos e Internacionales (CSIS) en Washington DC. En el evento participaron, entre otros, el presidente del BID, Luis Alberto Moreno; el secretario general de la OEA, Luis Almagro, y el presidente del CSIS, John Hamre, entre otras autoridades. El informe fue presentado posteriormente en varios países de la región y su recomendación principal ha sido el mensaje de «considerar "urgente" que América Latina y Caribe actúen para proteger su ciberespacio».

El informe analiza el estado de preparación de treinta y dos países basado en cuarenta y nueve indicadores y en la nota de prensa de la presentación oficial se consideró que era la primera radiografía profunda del nivel de preparación de América Latina y el Caribe ante la creciente amenaza del cibercrimen. El informe presenta una imagen completa y actualizada sobre el estado de la seguridad cibernética (riesgos, retos y oportunidades) de los países de América Latina y el Caribe, y consta de dos secciones principales.

La primera sección incluye una serie de ensayos sobre las tendencias de la seguridad cibernética en la región, aportados por reconocidos expertos internacionales en el tema.

La segunda sección examina la «madurez cibernética» de cada país mediante la aplicación del Modelo de Madurez de Capacidad de Seguridad Cibernética (*CMM*, por sus siglas en inglés) que toma en cuenta las consideraciones de seguridad cibernética a través de cinco dimensiones y las evalúa en cinco niveles de madurez para cada uno de sus cuarenta y nueve indicadores. El *CMM* es el primero de su tipo en términos de extensión y profundidad en cada aspecto de capacidad de la seguridad cibernética. Está construido sobre una base de consulta de múltiples partes interesadas y el respeto de los derechos humanos, equilibrando cuidadosamente la necesidad que se tiene de seguridad para permitir el crecimiento económico y la sostenibilidad, al tiempo que se respetan el derecho a la libertad de expresión y el derecho a la privacidad.

Las conclusiones más destacadas en la presentación[55] fueron:

---

[54] Vídeo presentación informe OEA–BID: *Cybersecurity Report 2016: Are We Ready in Latin America and the Caribbean?*
https://www.csis.org/events/cybersecurity-report-2016-are-we-ready-latin-america-and-caribbean

[55] www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina,11420html

- El informe demuestra que la región presenta vulnerabilidades «potencialmente devastadoras».
- Cuatro de cada cinco países de la región carecen de estrategias de ciberseguridad o planes de protección de infraestructuras críticas.
- Dos de cada tres países no cuentan con un centro de comando y control de seguridad cibernética.
- La gran mayoría de las fiscalías carecen de capacidad para perseguir los delitos cibernéticos, entre otras carencias.

El informe destaca que —en el primer trimestre de 2016— solo seis países de América Latina y el Caribe, Brasil, Colombia, Jamaica, Trinidad y Tobago, Panamá y Uruguay tienen estrategias de seguridad cibernética, mientras que Argentina, Antigua y Barbuda, Bahamas, Costa Rica, Dominica, El Salvador, Haití, México, Paraguay, Perú y Surinam están en proceso de articular una estrategia.

El secretario general de la OEA, Luis Almagro, enfatizó en su presentación que: «los riesgos de abusos aumentan a medida que América Latina y el Caribe se incorporan a la revolución digital. La región es el cuarto mayor mercado móvil del mundo. La mitad de la población usa internet. Hay países en América Latina que procesan el 100 % de sus compras gubernamentales por vía electrónica. Los riesgos se multiplicarán con el advenimiento de la "Internet de las Cosas", donde ya no solo estarán interconectadas las computadoras sino un universo de máquinas y sensores inteligentes, controlando virtualmente todo lo que usamos a diario»[56]. En lo relativo a formación en ciberseguridad, Almagro considera que «apenas seis países de la región cuentan con un programa estructurado de educación en seguridad cibernética, que incluye estabilidad presupuestaria así como mecanismos de investigación y transferencia de conocimiento».

Conclusiones: tendencias en ciberseguridad

En la sección de bibliografía se incluyen los informes considerados de mayor impacto, publicados a lo largo del bienio 2015-2016 en España, y algunos a nivel internacional y queremos destacar las recomendaciones de dos de ellos, INCIBE y Telefónica, como conclusión del capítulo, dado que la mayoría de las tendencias TIC publicadas en ambos informe han sido recogidas en el mismo.

Tendencias TIC de INCIBE (2016). Julio 2016

INCIBE resalta la conexión y ubicuidad de los datos basados en Internet de las Cosas, *Cloud Computing*, dando lugar a la creación de redes y ciudades

[56] Ibíd.

inteligentes donde el *Big Data* es un elemento esencial y las tendencias TIC que recomienda son:

- *Big Data, Cloud Computing* e Internet de las Cosas (*IoT*).
- *Smart Cities* y *Smart Grids*.
- Industria 4.0.
- Redes sociales.
- Tecnologías cognitivas (incluyendo aprendizaje automático, procesamiento en lenguaje natural «NLP» y reconocimiento de voz).
- Sistemas ciberfísicos (incluyendo el uso de *drones*, redes de sensores y realidad aumentada).
- Tecnologías móviles, WiFi óptico y Redes 5G.
- Nuevos modelos de pago.

INCIBE recomienda también tendencias específicas en ciberseguridad, agrupándolas en veinte tendencias globales catalogadas en torno a seis sectores de actividad.

Nuevos escenarios y desafíos de la seguridad. Telefónica (septiembre de 2016)

Telefónica publicó en septiembre de 2016, en coedición con Ariel, el informe «Ciberseguridad, la protección de la información en un mundo digital». En un extenso capítulo 4, los autores del informe consideran los nuevos escenarios y desafíos de la seguridad y hacen una clasificación de las principales tendencias actuales e identifican sus principales vulnerabilidades, así como sus necesidades de seguridad:

- *Cloud Computing, Big Data* e Internet de las Cosas.
- BYOD (trae tu propio dispositivo al trabajo y empresa).
- Internet industrial (Industria 4.0).
- *Apps* móviles.
- Múltiples identidades digitales.
- Desafíos legales a la ciberseguridad.

Otras tecnologías de impacto en el futuro de la ciberseguridad analizadas

En este capítulo 1 también hemos considerado otras tecnologías de gran impacto en el ámbito de la ciberseguridad:

- Tecnologías financieras: *Fintech* y *Blockchain,*
- Robots colaborativos (*cotbots*), *bots* y *chatbots* (*bots* conversacionales),
- Aprendizaje profundo (*Deep Learning*). Una tecnología cognitiva de inteligencia artificial y un tipo específico de gran impacto del aprendizaje automático (*machine learning*).

En un mundo actual donde la transformación digital de las organizaciones y empresas es una necesidad ineludible, estas han de contemplar una estrategia de ciberseguridad actualizada y como Miguel Rego (director de INCIBE) manifestó en Santander en el Encuentro de Telecomunicaciones y Economía de la Universidad Menéndez Pelayo: «Sin ciberseguridad no se puede construir una España digital... y la razón es sencilla, los usuarios no recurrirán a servicios *online* si no se sienten seguros»[57].

[57] Encuentro de Telecomunicaciones y Economía Digital, Universidad Menéndez Pelayo, Santander, 9 de septiembre de 2016 [en línea. http://www.ciospain.es/seguridad/sin-ciberseguridad-no-se-puede-construir-una-espana-digital-asegura-el-incibe]

Estudios de ciberseguridad

BANKINTER (2016). *Ciberseguridad. Un desafío mundial*, mayo de 2016. www.fundacionbankinter.org

INCIBE (2016a). *Tendencias en el mercado de la Ciberseguridad*. León, julio de 2016. www.incibe.es

INCIBE/OSI/AEPD (2016b). *Guía de privacidad y seguridad en Internet*. León, octubre de 2016. www.incibe.es

INCIBE (2016c). *Punto de partida al modelo de gestión y seguimiento del TALENTO en ciberseguridad en España*. *Visión conjunta de la industria, sector académico e investigador y profesionales del sector* https://www.incibe.es/sites/default/files/contenidos/notasprensa/doc/modelo_gestion_talento_incibe.pdf

INCIBE (2015). *Decálogo de ciberseguridad. El camino hacia la ciberseguridad en su empresa.* https://www.incibe.es/extfrontinteco/img/File/empresas/blog/2014Octubre/decalogo_ciberseguridad_empresas.pdf

McAfee Labs (2016a). *Predicciones sobre amenazas para 2016*. Intel Security/McAfee. Agosto de 2016. http://www.mcafee.com/es/resources/reports/rp-threats-predictions-2016.pdf.

McAfee *Labs* (2016b). *Informe de McAfee Labs sobre amenazas. Septiembre 2016*. Intel Security/McAfee. Septiembre de 2016. http://www.mcafee.com/es/resources/reports/rp-quarterly-threats-sep-2016.pdf

MINISTERIO DE LA PRESIDENCIA (2015). *Informe anual de Seguridad Nacional 2014*. Madrid: Gobierno de España. http://www.dsn.gob.es/sites/dsn/files/Informe_Seguridad_Nacional%202014.pdf

MINISTERIO DE LA PRESIDENCIA (2016). *Informe anual de Seguridad Nacional 2015.* Madrid: Gobierno de España. http://www.lamoncloa.gob.es/presidente/actividades/Paginas/2016/270516rajoycsn.aspx

http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/INFORME%20ANUAL%20DE%20SEGURIDAD%20NACIONAL%202015.pdf

OEA-BID (2016). *Ciberseguridad 2016. ¿Estamos preparados en América Latina y el Caribe*? Marzo de 2016. https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/

ONTSI (2016). *Estudio sobre la ciberseguridad y confianza en los hogares españoles*. Junio de 2016. http://www.ontsi.red.es/ontsi/es/estudios-informes/ciberseguridad-y-confianza-en-los-hogares-espa%C3%B1oles-junio-2016

TELEFÓNICA (2016). *Ciberseguridad. La protección de la información en un mundo digital.* Madrid: Ariel/Fundación Telefónica. Septiembre de 2016. http://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/531/

Bibliografía de consulta

AYALA, Luis (2016). Cyber-Physical Attack REcovery Procedures. A Step-by-Step Preparation and Response Guide. New York: Apress.

DONALDSON, Scott E., et al. (2015). Enterprise Cibersecurity. How to Build a Successful Cyberdefense Program Against Advanced Threads. New York: Apress.

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (2011). Ciberseguridad. Retos y amenazas a la seguridad nacional en el Ciberespacio. Cuadernos de Estrategia, no. 149. JOYANES, Luis (Coord). Madrid: Ministerio de Defensa.

JOYANES AGUILAR, Luis (2015). Sistemas de información en la empresa. El impacto de la nube, la movilidad y los medios sociales. Barcelona: Marcombo; México DF: Alfaomega.

JOYANES AGUILAR, Luis (2014). Big Data. Análisis de grandes volúmenes de datos en organizaciones. Barcelona: Marcombo;: México DF; Alfaomega.

JOYANES AGUILAR, Luis (2013). Computación en la nube. El imacto del cloud computing en las empresas. Barcelona: Marcombo; México DF: Alfaomega.

MEDINA, Manel y MOLIST, Mercè (2015). Cibercrimen. Barcelona: Tibidabo Ediciones

SEGURA, Antonio y GORDO, Fernando (Coords). Ciberseguridad global. Oportunidades y compromisos en el uso del ciberesepacio. Granada. Universidad de Granada/Mando de Adiestramiento y Doctrina.

SIKORSKI, Michael y HONIG, Andrew (2012). Practical Malware Analysis. The Hands-On Guide to Dissecting Malicious Software. San Francisco: No Starch Press.

TOUHIL, Gregory J. y TOUHILL, C. Joseph (2014). Cibersecurity for Executives. A Practical Guide. New Jersey: Wiley.

ULSCH, MacDonnell. Cyber Threat! How to Manage the Growing Risk of Cyber Attacks. New Jersey: Wiley