Tendencias en el mercado de la Ciberseguridad

Julio de 2016

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Julio 2016

INCIBE_PT_TendenciasCS_2015-v1

INDICE

RESUMEN EJECUTIVO

El objetivo principal del Estudio es **identificar** las grandes **tendencias del mercado de la ciberseguridad** y describir su potencial **oportunidad de negocio** para las empresas de la **Industria Nacional en Ciberseguridad**, configurándose para los integrantes como:

- Mecanismo para la **toma de decisiones sobre el modelo de negocio y la estrategia de desarrollo de productos y servicios** de ciberseguridad.
- Elemento de **promoción de nuevos segmentos y oportunidades de inversión** para las empresas.
- Método de estudio sobre la **colaboración entre distintos agentes del mercado** favoreciendo el establecimiento de sinergias.

Para la elaboración del Estudio de tendencias en el mercado de la ciberseguridad se ha aplicado la siguiente metodología:

- **Identificación de tendencias** a través de un conjunto representativo de referencias bibliográficas, con documentación procedente de entidades tanto públicas como privadas con prestigio nacional e internacional:
  - **Estudios de mercado de entidades de referencia**, como: Forrester, Gartner, Deloitte, PWC, Forbes, Markets and Markets, Technavio, EY y DONALD W. DUNPHY.
  - **Catálogos de productos de grandes empresas en ciberseguridad**, como: MCAFEE, KASPERSKY, CISCO, AON, SYMANTEC, PANDA, SOPHOS, Trend Micro, BT, IBM, Thales e-Security, Intel Security, ISACA y VERIZON.
  - **Informes de incidentes y amenazas de organismos públicos de referencia**, como: ENISA, la OCDE, CNI, IEC (International Electrotechnical Commission), Consejo Nacional de Ciberseguridad, Comisión Europea, CCN CERT, UTAD, US CERT, Parlamento Europeo, Consejo Europeo, Gobierno de Luxemburgo, Bank of England, Marca España, Instituto de Estudios Bursátiles (IEB) y Presidencia del Gobierno.

- **Selección y sectorización de tendencias** con la **participación** de un grupo de trabajo conformado por diferentes agentes de la **Industria Nacional en Ciberseguridad** (ICEX, Netxtel, I4S, Thales España, Everis, Leet Security, CITIC, PESI, SCASSI, Telefónica, Enigmedia, ISDEFE, Gradiant, CSIC, Innotec System, Softcom, Deloitte, Syneidis, S.L.).

- **Análisis de las tendencias** a través de: **experiencias de éxito** de empresas y casos reales de aplicaciones de la tendencia; **previsiones de demanda** y acogida del mercado en la comercialización de productos y/o servicios aplicados; **principales empresas**, usuarios y sectores beneficiarios del impulso de la tendencia; etc.

En la selección de tendencias en ciberseguridad se ha seguido un proceso de **análisis top-bottom**, en el que se han definido primero las **grandes tendencias socio-económicas**, para posteriormente fijar las tendencias del sector TIC y llegar, en última instancia, a las vinculadas con la industria de la ciberseguridad.

Macro Tendencias socio-económicas

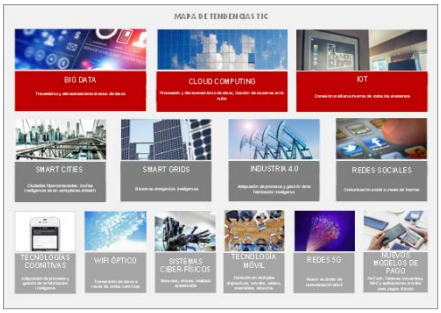
Según las macro tendencias identificadas, en **el futuro de la sociedad**, las **megaciudades** jugarán un papel fundamental impulsando la adopción de la tecnología**, que constituirá un factor clave en la mejora de vida de las personas**, y el **crecimiento de la economía**, a través de la **innovación** y la **generación masiva de datos** que mantendrán hiperconectados a los ciudadanos. Así pues, el auge de la tecnología y su poder para aumentar significativamente la **calidad de vida** de los ciudadanos marcará la nueva concepción de sociedad.

- Auge de las megaciudades.
- Desequilibrio en la conectividad.
- Mejor nivel de vida por medio de la tecnología.
- Economía sustentada por multinacionales y pequeñas empresas.
- Necesidad de talento.
- Innovación disruptiva.
- Generación masiva de datos.
- Nuevos modelos de pago.

Tendencias TIC

El análisis de las tendencias TIC identificadas pone de manifiesto la especial relevancia de la **conexión y ubicuidad de los datos** basados en IoT y Cloud Computing, dando lugar a la creación de **redes y ciudades inteligentes**, donde el **Big Data** es un elemento esencial. Dichas ciudades inteligentes se configuran principalmente sobre nuevas redes y **tecnologías móviles** que fomentan un cambio alternativo en el modelo de vida tradicional de sus ciudadanos.

- Big Data.
- Cloud Computing.
- IoT.
- Smart Cities.
- Smart Grids.
- Industria 4.0.



- Redes sociales.
- Tecnologías cognitivas.
- Wifi óptico.
- Sistemas ciber-físicos.
- Tecnología móvil.
- Redes 5G.
- Nuevos modelos de pago.

Previo a la presentación y definición de las tendencias en ciberseguridad se procede a caracterizar el **mercado de la ciberseguridad.**

- A **nivel global**, según **Gartner**, el sector de la ciberseguridad presenta una facturación mundial de **62.540 millones de euros en 2015** y una previsión de **aumento de la demanda** (partiendo de un gasto en ciberseguridad de 54.082 millones de euros en 2014) que alcanzará los 79.292 millones de euros en 2018.
- A **nivel nacional**, la **facturación total** del sector de la ciberseguridad en 2014 fue de **598,2 millones de euros**, según datos del ONTSI.

Tendencias de Ciberseguridad

Teniendo en cuenta la cadena de valor de la ciberseguridad y su impacto en ciudadanos, empresas y Administraciones Públicas, se ha diseñado un **mapa de tendencias de demanda** en el que se identifican **20 tendencias** globales en ciberseguridad catalogadas en torno a **6 sectores** de actividad.

- **Sector Industrial y Medio Ambiente**.

  - **Sistemas ciber-resilientes para Infraestructuras Críticas**. La destrucción o perturbación de infraestructuras estratégicas cuyo funcionamiento es indispensable tendría **graves consecuencias** sobre servicios esenciales, por lo que requieren de **sistemas diseñados** para hacer frente a una crisis de seguridad sin que su actividad se vea afectada.
  - **Ciberseguridad en Sistemas de Control Industrial: ICS/SCADA**. La complejidad de los sistemas ICS/SCADA radica principalmente en su **naturaleza multidisciplinar** y aplicable a multitud de sectores. Ello justifica la necesidad de implantar altos niveles de ciberseguridad en los sistemas SCADA.
  - **Protección de las redes industriales inteligentes y Smart Grids**. La necesidad de protección de las redes de sensores industriales radica en **medidas de seguridad** tales como protocolos de autenticación, cifrado de conexiones M2M y eliminación de redundancias.

- **Sector Movilidad**
  - **Protección de vehículos inteligentes**. La protección de vehículos inteligentes hace referencia a la seguridad de los **sistemas de control** de vehículos interconectados y de vehículos terrestres autónomos, así como de los **sistemas inteligentes** que interaccionan con ellos por medio de redes de comunicaciones específicas. Estas redes deben estar protegidas contra **bloqueos de la señal**, ataques de denegación de servicio y transmisión de datos falsos a los vehículos terrestres conectados y a sus conductores.

  - **Seguridad y protección de vehículos aéreos no tripulados: drones**. El desarrollo y uso de drones supone un gran reto para la seguridad. Desde el punto de vista de la ciberseguridad, estos dispositivos están expuestos a riesgos de **pérdida de confidencialidad, integridad y disponibilidad** de los datos.
  - **Protección de sistemas de comunicación vía satélite**. Las Comunicaciones por Satélite juegan un papel vital en el sistema de telecomunicaciones global. Estos sistemas presentan distintas vulnerabilidades que podrían permitir a **atacantes remotos** inutilizar por completo los dispositivos. Entre los sistemas afectados se podrían encontrar múltiples **sistemas y servicios críticos**, como: servicios de emergencia, militares, aviones, barcos, sistemas industriales, etc.

- **Sector Economía**
  - **Big Data Analytics: detección de fraude en banca y seguros**. El uso de Big Data Analytics en el sector bancario y de seguros, permite entre otras la detección y prevención del fraude en tiempo real, reduciendo los costes de monitorización e investigación de incidentes y por tanto reduciendo las pérdidas derivadas de actividades fraudulentas.

  - **Gestión de Información de Eventos de Seguridad (SIEM)**. Se basa en la detección de amenazas y respuesta a incidentes de seguridad a través de la obtención en **tiempo real** de eventos de seguridad y su **análisis histórico**, a partir de una amplia variedad de fuentes de eventos y datos contextuales.
  - **Seguridad en los servicios Fintech**. La seguridad en servicios Fintech se basa en el desarrollo de nuevas soluciones de protección de sistemas o aplicaciones de pago online, sistemas de m-commerce o comercio móvil, dispositivos de tecnología NFC, lectores de tarjetas para móviles, etc., basadas en la **autenticación de usuario** y soluciones de prevención de fraude.

- **Sector Ciudadanía**
  - **Protección de dispositivos médicos conectados**. Estos dispositivos pueden exponer a los pacientes y a las organizaciones de atención de la salud, a los riesgos de la seguridad y la protección. Todos estos dispositivos interconectados en una red necesitan asegurar la **confidencialidad, integridad y control** de los mismos, especialmente, en aquellos cuyo software no está personalizado para su uso.
  - **Cifrado para investigación médica y farmacéutica**. La tendencia de seguridad de datos médicos avanza hacia un **cifrado apto** para hacer coincidir las fuentes de información de múltiples centros médicos, que están **cifrados con claves diferentes**, sin descifrado de la información, salvaguardando la **confidencialidad** en la información de los pacientes.
  - **Almacenamiento seguro y ubicuo de datos médicos**. La sensibilidad de la información de los pacientes requiere no sólo de un sistema de almacenamiento cifrado, sino de un mecanismo de transferencia seguro, garantizando que la **ubicuidad de los datos personales y clínicos** de los pacientes no pone en peligro su confidencialidad.
  - **Cibereducación – Laboratorios de seguridad**. La integración de la educación con la tecnología y la ciberseguridad converge en lo que se reconoce como cibereducación. Se trata de una **modalidad educativa** que formula la enseñanza a partir de diferentes competencias y disciplinas, tales como: interactuación, retroalimentación, gamificación, simulación, etc. aplicadas a la formación en ciberseguridad.

- **Sector Gobernanza**
  - **Distribución de ciberinteligencia**. Se trata de un modelo basado en el intercambio de información entre organismos, públicos y privados, proveniente del **análisis de ciberamenazas** con el objetivo de mejorar y agilizar la detección y actuación ante las amenazas en ciberseguridad.
  - **Simulación de incidentes y ciberejercicios**. Los sistemas de simulación de escenarios e incidentes se basan en la utilización de **entornos de entrenamiento**, que ponen a prueba la capacidad tecnológica y de reacción de las herramientas y recursos de una organización. Los **ciberejercicios**, por su parte, permiten evaluar el estado de preparación de los participantes frente a **crisis de origen cibernético**.

- **Sector TIC**

  - **Servicios de seguridad en la nube: "security as a service"**. Estos servicios son generalmente **modelos de outsourcing** de la administración de la seguridad, que se aprovechan de la escalabilidad del modelo de Cloud Computing permitiendo a las organizaciones dimensionar los esfuerzos a su capacidad actual.
  - **Cifrado en tiempo real**. Se trata de un mecanismo de **protección de la seguridad de los datos** en las transacciones electrónicas en el que los datos se cifran antes de ser almacenados y se descifran al descargarse, previamente a su utilización. Este tipo de cifrado permanece en segundo plano ante el usuario.
  - **Cifrado homomórfico**. Esta tendencia de cifrado permite que la información que se codifique pueda ser compartida con **terceras partes** y ser utilizada en cálculos y procesos computacionales, sin que los sistemas implicados puedan interpretar dicha información pero sí ofrecer un resultado no cifrado a esos cálculos y procesos.
  - **Hacking ético**. Se basa en la búsqueda de vulnerabilidades mediante la utilización de **pruebas de penetración o "pentest"** en las redes de una organización con el objetivo de prevenir posibles fallos de seguridad, mitigar el impacto provocado por cualquier incidente de seguridad, priorizar riesgos y verificar el cumplimiento normativo.
  - **Certificado de confianza digital**. Consiste en comprobar, materializar y dar visibilidad el **nivel de ciberseguridad** que implementa un proveedor en un servicio determinado, es decir, la emisión de **sellos de confianza digital** que valoran objetivamente las medidas de seguridad integradas por el proveedor de servicios.

1. INTRODUCCIÓN

La evolución de las Tecnologías de la Información y las Comunicaciones, vinculadas a una incipiente necesidad de protección y seguridad del entorno de conectividad, generan un sustancial impacto en la Economía y la Sociedad Digital.

La creación de un clima de confianza digital que permita reforzar la protección de los organismos y estimule la implicación de los ciudadanos en el entorno digital, resulta vital para impulsar el pleno desarrollo de la sociedad conectada; para lo cual, **el sector de la ciberseguridad se configura como un elemento habilitador clave.**

En esta línea, la Agenda Digital para España pone especial énfasis en ello y concretamente, a través del Plan de Confianza en el ámbito Digital se planteaba realizar un estudio de viabilidad en colaboración con los principales agentes de referencia y con el Foro Nacional para la Confianza Digital, con el objetivo de desarrollar una propuesta integradora para **la puesta en marcha de un Polo Tecnológico Nacional en Ciberseguridad**.

El **Polo Tecnológico Nacional en Ciberseguridad** contará, entre otros, con un objetivo estratégico clave basado en **incrementar la actividad productiva competitiva a nivel internacional de los participantes en materia de ciberseguridad.**

Una vez aprobada la idoneidad y oportunidad de desarrollar y potenciar dicho Polo Tecnológico Nacional en Ciberseguridad, competitivo a nivel internacional y sostenible en el tiempo, **INCIBE** como entidad de referencia y actor neutral en el ámbito de la ciberseguridad nacional, dentro de un marco de colaboración público-privada, **pone en marcha una primera fase de medidas encaminadas a aumentar la competitividad del sector, potenciar el mercado interior y promover la internacionalización de la Industria** de ciberseguridad española para su desarrollo.

En este sentido, como parte de la puesta en marcha de una primera fase del desarrollo e implementación, se van a desarrollar distintas medidas transversales para todo el sector dirigidas a acelerar el desarrollo de éste, cuyo **primer objetivo está enfocado a potenciar el mercado interior de ciberseguridad.**

Concretamente, enmarcada entre las medidas para la potenciación del mercado interior de la ciberseguridad, se encuentra la **realización del presente Estudio de tendencias en el mercado y nuevos segmentos en ciberseguridad.**

2. OBJETIVOS Y METODOLOGÍA

2.1. Objetivos del Estudio

El objetivo principal del estudio de tendencias y nuevos segmentos se basa en la **identificación y descripción de las tendencias del mercado de la ciberseguridad, sus productos y servicios,** adaptándolas como nuevas oportunidades de negocio para las empresas de la **Industria Nacional en Ciberseguridad.**

El estudio pretende **adelantar la evolución del mercado de la ciberseguridad,** proporcionando información actualizada y un mayor conocimiento sobre el mismo, permitiendo así orientar las estrategias empresariales de los integrantes de la Industria.

Además, dicho estudio pretende servir a los distintos agentes que conforman la Industria como:

- Mecanismo para la **toma de decisiones en relación a su modelo de negocio y a su estrategia** de desarrollo de productos y servicios.
- Elemento de **promoción de nuevos segmentos y oportunidades de inversión** para las empresas.
- Método de estudio sobre la posibilidad de **colaboración entre los distintos agentes del mercado** favoreciendo así, el establecimiento de sinergias.
- **Orientación a la Red de Excelencia en I+D+i en ciberseguridad hacia objetivos de investigación** de cuyos resultados se pueda beneficiar a la **Industria Nacional en Ciberseguridad** debido a su potencial claro en el mercado.

Para ello, el estudio de tendencias se encuentra estructurado en torno a los siguientes bloques de análisis:

En primer lugar, comprende un breve **análisis en el que se estudian las macro tendencias globales socio-económicas,** tanto a nivel nacional como internacional, que tendrán un importante impacto en la sociedad y en la economía en los próximos años.

Posteriormente, en base a dichas macro tendencias socio-económicas y a la consulta de diversas fuentes de información, dado el importante papel que juega la digitalización en el contexto global, **se extraen las principales tendencias TIC y su nexo con la ciberseguridad,** a fin de contextualizar la evolución del sector.

Finalmente, teniendo en cuenta la cadena de valor de la ciberseguridad y su impacto en los ciudadanos, las empresas y las Administraciones Públicas, **se presentan las principales tendencias detectadas en el campo de la ciberseguridad** como una oportunidad empresarial, relacionándose también con mercados verticales concretos (sectores económicos).

La clasificación de dichas tendencias en ciberseguridad, en función del tipo de oportunidad que representan, se articula de acuerdo a los distintos agentes de la cadena de valor de la ciberseguridad definida por el catálogo de ciberseguridad de INCIBE:

- **Desarrollo software y hardware de ciberseguridad,** es decir, de productos, en torno a las siguientes categorías:

- **Servicios** de: consultoría, integración o gestión de seguridad (MSSP) / externalización de servicios, en torno a las siguiente categorías:

2.2. Metodología

El estudio de tendencias ha sido elaborado por el equipo del área de INCIBE de **Talento, Industria y Apoyo a la I+D+i.**

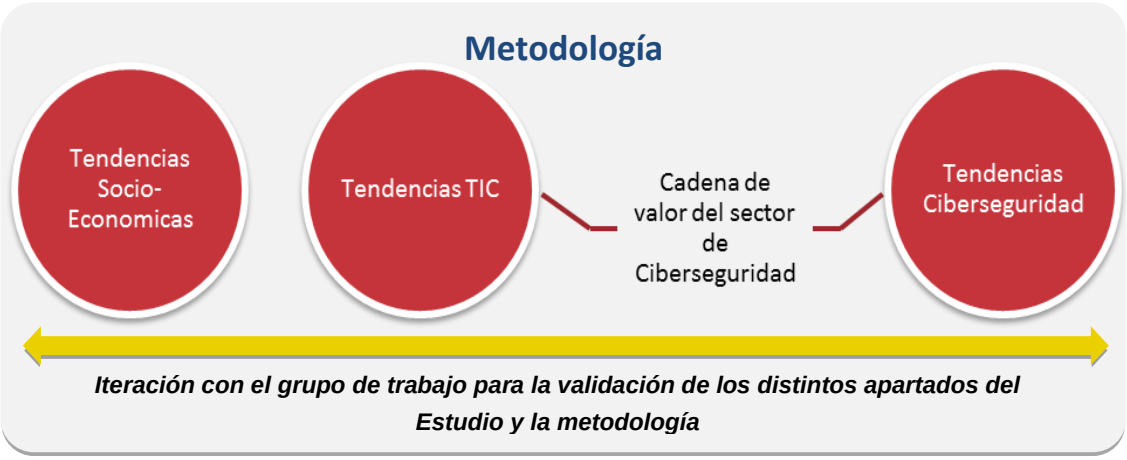
Este equipo ha tomado como punto de partida en la detección de tendencias una selección representativa de **referencias bibliográficas** procedentes de las entidades, nacionales e internacionales, **más representativas en los diferentes ámbitos de actividad del sector de la ciberseguridad** *(véase el Anexo I).*

Además, el estudio ha contado con la participación de un **grupo de trabajo entre diferentes agentes de la Industria de la Ciberseguridad Nacional** (empresas, agentes de la Red de Excelencia, Institutos de Investigación y otros organismos relacionados), cuya colaboración y asistencia empresarial ha sido esencial en el proceso de validación de criterios y selección de tendencias correspondientes a las distintas partes que componen el estudio.

En particular, el sistema de participación llevado a cabo con los integrantes del grupo de trabajo, para la confección del estudio de tendencias, ha seguido el procedimiento descrito a continuación:

- Para el lanzamiento del estudio se remitió un correo informativo e introductorio de presentación a todos los integrantes seleccionados.
- A lo largo de la elaboración del estudio se ha mantenido una **interacción dinámica con el grupo de agentes** para la presentación de avances y el seguimiento e inclusión de sugerencias y modificaciones.
- Para concluir, se ha celebrado una **reunión con el grupo de agentes con el objetivo de validar** la selección de tendencias y criterios finales aplicados y por ende, **el estudio**.
- Finalmente, se ha enviado el estudio de tendencias a todos los agentes de la industria, incluyendo a aquellos que no formaron parte del grupo de trabajo, para incorporar sugerencias y modificaciones propuestas por los mismos, de manera que la participación de todos los agentes en el estudio fuera efectiva.

Por tanto, en línea con el procedimiento de participación descrito anteriormente y teniendo en cuenta la estructura del estudio definida en el apartado previo, la **metodología seguida para la realización de éste** se articula atendiendo al siguiente proceso:



Iteración con el grupo de trabajo para la validación de los distintos apartados del Estudio y la metodología

3. MACROTENDENCIAS Y LA CIBERSEGURIDAD

En el marco de una sociedad globalizada, cada vez más digital y conectada, y en la que la información y por consiguiente, la generación masiva de datos marcan el paradigma de sociedad actual, las principales tendencias socio-económicas se cimentan en el impacto que las TIC tienen en la sociedad actual.

Por ello, en este capítulo del estudio se identifican, en primer lugar, las principales **macrotendencias que marcarán la evolución socioeconómica** de la sociedad durante los próximos años. Seguidamente, se **identificarán las tendencias TIC y su vínculo con el ámbito de la ciberseguridad.**

3.1. Macrotendencias Socio-Económicas

Como primer paso en la caracterización del sector de la ciberseguridad, se proponen las siguientes macro tendencias socio-económicas que cambiarán el contexto global e impactarán en la sociedad y la economía en los próximos años:

Auge de las megaciudades

La rápida urbanización y la expansión de los límites de las ciudades están derivando hacia la aparición de megaciudades, **grandes aglomeraciones urbanas que se convierten,** en buena parte, **en ciudades autosuficientes y sedes del talento, inversión, creación de riqueza y crecimiento económico.**

A pesar de su relevancia, todavía existen límites significativos en su capacidad para hacer frente a los problemas universales como el cambio climático o para perseguir otros objetivos nacionales o mundiales. Sin embargo, dada su escalabilidad, lo que suceda en una megaciudad puede convertirse rápidamente en un **estándar global** que afecte a gran número de personas.

Desequilibrio en la conectividad

En el futuro **la mayoría de población estará conectada a la red** a través de numerosas plataformas, tanto físicas como digitales. No obstante, **una parte significativa de la población** (predominantemente ciudadanos sin recursos económicos, personas mayores o personas que vivan en áreas con conectividad limitada) **apenas tendrá conexión.**

Esta brecha en la conexión plantea desafíos continuos en cuanto a la prestación de servicios públicos se refiere, dado que se deberán emplear tecnologías versátiles para satisfacer las expectativas tanto de los ciudadanos hiper-conectados como de aquellos que permanezcan *offline*.

Mejora del nivel de vida por medio de tecnología

La sociedad está entrando en un período de transformación radical en el que el uso de diversas tecnologías, tendrá el poder para aumentar significativamente el nivel de vida de la población.

Avances sin precedentes en la asistencia sanitaria, la neurociencia, la tecnología, la informática, la nanotecnología y el aprendizaje comienzan a permitir que los seres humanos amplíen sus facultades físicas y mentales, aumentando la longevidad, la mejora del coeficiente intelectual y la capacidad de aprendizaje o recuperación de la audición y la visión.

Economía sustentada por multinacionales y pequeñas empresas por medio de tecnología

La economía se concentra en un reducido número de grandes multinacionales, por un lado y un gran grupo de pequeñas empresas y microempresas, por el otro.

Existe una creciente diferenciación que se abre entre aquellas empresas que actúan como plataformas frente a otras que son proveedoras de productos y servicios de nicho.

Sin embargo, son las pequeñas empresas aquellas que encuentran mayores áreas de desarrollo intactas por las grandes multinacionales, que les permiten crecer y prosperar.

Estas áreas se convierten, a menudo, en importantes fuentes de innovación.

Necesidad de talento

La capacidad de **fomentar, desarrollar y mantener generaciones de empleados cualificados** se ha convertido en una prioridad global. Muchos países trabajan para disminuir el envejecimiento de la población trabajadora y cubrir la falta de talento técnico cualificado.

Estos esfuerzos se basan en **impulsar la "economía independiente"** (*freelance*), en la cual los trabajadores se mueven entre distintos puestos de trabajo de manera fluida, provocando importantes cambios en las políticas de inmigración, educación y formación.

Los gobiernos, empresas privadas y organizaciones educativas se unen para hacer frente a la creciente brecha de conocimiento y a un cambio de paradigma educativo basado en el aprendizaje permanente como potencial fuerza laboral.

Innovación disruptiva

El núcleo de la tecnología (potencia de los ordenadores, almacenamiento y ancho de banda) **continúa mejorando e incrementándose**. Esto conlleva la progresiva adopción de las tecnologías por todo tipo de industrias, funciones y disciplinas.

El impacto de la innovación se acentúa aún más cuando las tecnologías se unen en plataformas abiertas y ecosistemas, permitiendo a las personas y a las tecnologías construir y cimentarse rápidamente sobre olas anteriores de innovación.

Por ello, el centro de la innovación exponencial se encuentra fundamentado en la continua mejora tecnológica.

Generación masiva de datos

En un **mundo hiperconectado y sensorizado**, se generará progresivamente mayor cantidad de información. Ésta, en su mayoría será de carácter personal y, en el futuro, los consumidores recopilarán y venderán sus datos, convirtiéndolos en una "moneda" en sentido literal.

Asimismo, esto provocará la **transformación de las fuentes de datos abiertos en soluciones y aplicaciones, y el análisis de éstos para la toma de decisiones y generación de estrategias**. A la larga, las personas estarán dispuestas a sacrificar su privacidad para una mayor comodidad.

Por otro lado, la tendencia hacia la **transparencia radical** provocará que la mayoría de las industrias expongan sus datos, a petición de los consumidores, así como los gobiernos a sus ciudadanos.

Sin embargo, esta transparencia radical provocará una creciente preocupación por la privacidad y el libre acceso a la información, en un contexto en el que ésta constituye un elemento fundamental en la propuesta de valor de la empresa.

Nuevos modelos de pago

Las **alternativas al dinero en efectivo y los sistemas financieros tradicionales** ganan ya un importante impulso en la economía actual basada en una convergencia progresiva entre pagos, financiación y riesgo.

Los sucesores de Bitcoin, Ripple y otros sistemas basados en criptomonedas o monedas virtuales se incrementarán sobre la base de la economía digital, dando paso a nuevos modelos de pago.

De igual manera, **los pagos por móvil llegarán a ser algo habitual dentro de un estilo de vida digital**, mientras que la protección contra el robo digital se convertirá en un asunto a regular y en un imperativo a tener en cuenta por las agencias reguladoras y organizaciones en todo el mundo.

En definitiva, las *megaciudades* jugarán un papel fundamental en el futuro de la sociedad impulsando la adopción de la tecnología, que constituirá un factor clave en la mejora de vida de las personas, y en el crecimiento de la economía, a través de la innovación y la generación masiva de datos que mantienen hiperconectados a sus ciudadanos. El auge de la tecnología y su poder para mejorar la calidad de vida de los ciudadanos, marcarán la nueva concepción de sociedad.

3.2. Tendencias TIC

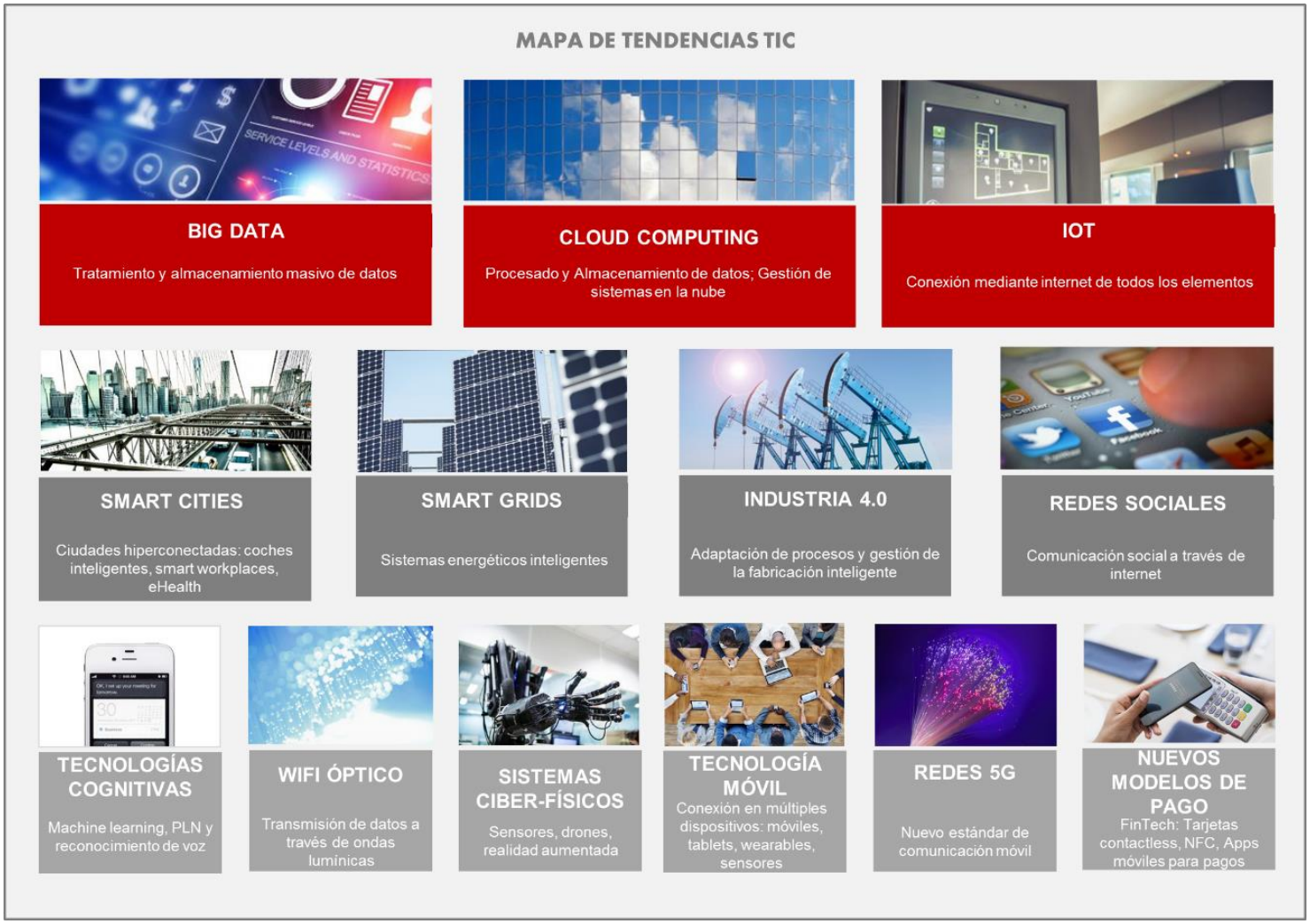
Tras haber identificado las principales tendencias socioeconómicas y con el objetivo final de caracterizar e identificar las tendencias propias y los potenciales segmentos del sector de la ciberseguridad, se establece un punto de análisis intermedio basado en el importante auge de la digitalización de cualquier ámbito o sector de actividad y por ende, el auge de las TIC.

Las tendencias TIC identificadas van en línea con el **Programa Europeo Horizonte 2020**, cuyos Programas de Trabajo recogen entre sus secciones temáticas a las Tecnologías de la Información y las Comunicaciones.

Concretamente, el **Programa de Trabajo TIC** posee **6 actividades principales**:

- **Una nueva generación de componentes y sistemas**: dentro de esta actividad se contemplan los sistemas ciberfísicos así como el "Smart Anything".
- **Computación avanzada y Cloud Computing**: se enfoca a computación de baja energía y computación en la nube.
- **Internet del Futuro**: relativa también al "Internet of Everything", se focaliza especialmente en las redes 5G y las tecnologías software para sistemas complejos y altamente conectados.
- **Contenido**: referido al acceso, creación, gestión, uso e intercambio de grandes cantidades de datos, a través de la puesta en marcha de tecnologías Big Data. También se enfoca hacia convergencia de la industria de los contenidos y los nuevos medios de comunicación y, al desarrollo de tecnologías para el aprendizaje e interfaces para la accesibilidad.
- **Robótica y sistemas autónomos**: para su aplicación en la industria avanzada de los automóviles, la salud, la logística, etc.
- **Tecnologías clave habilitadoras**: investigación e innovación en fotónica así como micro y nano-electrónica y su aplicación en la industria.

Estas actividades están alineadas con las macrotendencias TIC detalladas a continuación.



Big Data

Las grandes cantidades de datos se consideran la próxima vía de la innovación TIC.

Según Gartner, se estima que el gasto TIC en Big Data a nivel mundial alcanzará los 55.000 millones de dólares (42.652 millones de euros) en 2016.

El Big Data comienza a cobrar cada vez más importancia gracias a la proliferación de páginas web, aplicaciones de imagen y vídeo, redes sociales, dispositivos móviles, apps, sensores, internet de las cosas, etc. capaces de generar más de 2.5 quintillones de bytes al día.

Las vastas cantidades sin precedentes de nueva información que se crean y se comparten cada segundo, así como el análisis de dichos datos, se convierten en un activo transformador de gigabytes de información en conocimiento tanto para ciudadanos, empresas o gobiernos.

Estos **grandes datos no estructurados**, en un principio no relacionados, **contextualizados pueden proporcionar importantes conclusiones** que formen parte de otros productos o servicios. Como tal, las grandes cantidades de datos pueden ser usados para sintetizar la información de seguridad, confidencial, personal, etc.

Cloud Computing

El **Cloud Computing** o computación en la nube adquiere un importante protagonismo, convirtiéndose en un **componente esencial en las arquitecturas de aplicaciones modernas**, lo que provoca un incremento en las capacidades de las tecnologías, principalmente aquellas basadas en la tecnología móvil, la analítica y el procesado de datos.

Los servicios de computación en la nube o a distancia permiten la colaboración masiva alrededor de enormes conjuntos de datos, ofreciendo soluciones escalables y asequibles para la resolución de problemas computacionales.

Así pues, por medio del Cloud Computing se fomenta la **disminución de la brecha digital entre grandes y pequeñas empresas** al posibilitar una colaboración a distancia más rápida y asequible a través de varias disciplinas.

Muchas organizaciones públicas y empresas ya han apostado por este modelo; los últimos datos publicados del Internacional Data Center (IDC) revelan que en España, el Cloud Computing es una opción tecnológica conocida por el **81% de compañías y organizaciones** públicas del país y utilizada por un **41% del tejido empresarial e institucional** español.

Internet de las cosas

Internet de las Cosas (IoT), es decir, **dispositivos interconectados que forman redes ad hoc** como parte de alguna aplicación, es un área que cuenta con un creciente potencial de desarrollo e innovación.

A medida que el tamaño y el coste de los sensores y tecnologías de la comunicación siguen disminuyendo, Internet de las cosas (IoT) **crece a pasos agigantados.**

A corto plazo, según los datos de la firma de análisis de mercado Gartner, este 2016 se sobrepasarán los **6.400 millones** de dispositivos. **A cinco años**, las previsiones apuntan a que habrá más de **50.000 millones dispositivos conectados** a internet. Además, se estima que esta tendencia generará **12.000 millones de euros** solo en Europa de aquí a 2020.

Las cifras resaltan el atractivo del negocio que gira en torno al IoT. Es por ello que las empresas y los gobiernos se esfuerzan por integrar dicha tecnología, aún en desarrollo, haciendo uso del análisis de los datos generados para investigar y diseñar nuevos modelos de prestación de atención de la salud, transporte, seguridad y defensa, gestión de infraestructuras y muchas otras áreas.

Smart Cities

Smart City o Ciudad Inteligente se define como la **visión holística de una ciudad que aplica las TIC para la mejora de la calidad de vida y la accesibilidad de sus habitantes** y asegura un desarrollo sostenible económico, social y ambiental en mejora permanente.

Una ciudad inteligente permite a los ciudadanos interactuar con ella de forma multidisciplinar y se adapta en tiempo real a sus necesidades, de forma eficiente en calidad y costes, ofreciendo datos abiertos, soluciones y servicios orientados a los ciudadanos para resolver los efectos del crecimiento de las ciudades, en ámbitos públicos y privados, a través de la integración innovadora de infraestructuras con sistemas de gestión inteligente.

Las iniciativas marcadas dentro de una Smart City tienen como pilar básico el uso de las TIC, permitiendo optimizar la gestión de las infraestructuras y los servicios públicos.

Una Smart City desarrolla su actividad focalizada principalmente en torno a distintos ámbitos de actuación, tales como:

- el desarrollo del medio ambiente, cuyas actividades se centran en la gestión energética eficiente o de residuos, o el desarrollo del medio ambiente urbano sostenible;
- el fomento de la movilidad en la ciudad, basado en la mejora de la accesibilidad, de la conectividad (coches conectados), del tráfico o del estacionamiento;
- la gobernanza pública y las soluciones enfocadas hacia la administración electrónica (e-government), la transparencia o la participación ciudadana;
- el desarrollo de la economía, cuyas actividades se basan en impulsar el turismo inteligente, el consumo, el comercio, o el empleo y el emprendimiento;
- la mejora de la inclusión digital y la colaboración ciudadana vinculadas al uso de las TIC y entre las que destaca la creación de “smart workplaces”;
- la mejora de los servicios públicos, tales como la educación apoyada en los programas de e-learning o más concretamente, el fomento de la cibereducación; salud vinculada a e-health; cultura; seguridad o asuntos sociales, entre otros.

Existen distintas estimaciones del volumen de negocio que puede generar el concepto de Smart City, pero en ningún caso se pone en duda que se trata de un mercado en explosión, favorecido por el **crecimiento de las urbes** y el porcentaje creciente de población que reside en las ciudades, el cual según Naciones Unidas, alcanzará el **66% para el 2050.**

Smart Grids

Las **Smart Grids o redes eléctricas inteligentes** se pueden definir como la **integración dinámica de los desarrollos en ingeniería eléctrica y los avances de las TIC** permitiendo que las áreas de: coordinación de protección, control, instrumentación, medida, calidad y administración de energía, etc. sean concatenadas en un solo sistema de gestión inteligente.

Estas redes tienen el objetivo primordial de realizar un **uso eficiente y racional de la energía.**

Según Spain Technology for Life, se estima que las **inversiones en redes inteligentes, alcanzarán los 10.000 millones de euros** durante los próximos diez años y generarán un valor de entre 2 y 3,5 veces esta inversión.

Sus aplicaciones respaldadas por tecnologías avanzadas de monitorización, control, y comunicación, aportarán beneficios tanto al medio ambiente como a los clientes, dado que: aumentan el nivel de fiabilidad y calidad en el suministro de energía eléctrica; facilitan a los clientes instrumentos que les permiten optimizar su propio consumo eléctrico y mejorar el funcionamiento del sistema global; contribuyen a mantener la sostenibilidad ambiental; o mejoran la eficiencia en la distribución de los flujos de energía y aportan la flexibilidad en la gestión de los picos de demanda.

Los expertos estiman que la **mejora de la eficiencia del sistema eléctrico** aportará un beneficio de entre 1.100 y 1.800 millones de euros. Esa mejor eficiencia, impactará también en la **dependencia energética de España**, reduciéndose 5,3 puntos porcentuales en 2020.

Industria 4.0

El concepto de Industria 4.0 es relativamente reciente y se refiere a la **cuarta revolución industrial que consiste en la introducción de las tecnologías digitales en la industria.** También es conocido como la Industria Inteligente o la Industria del futuro.

Esta cuarta revolución industrial supone una significativa **transformación de las empresas** en cuanto a lo que se refiere al uso integrado de datos, algo que requiere una gran inversión sobre todo en TIC, equipos, sistemas logísticos (CPS) y formación.

PWC estima que **Alemania invertirá 40 mil millones de euros** al año hasta 2020 en Industria 4.0. Además, para ese mismo año, calcula que más del **80% de las empresas habrán digitalizado su cadena de valor,** con aumento de la eficiencia del 20%. .

Industria 4.0 conlleva muchos significados, pero los primeros avances en este ámbito han implicado la incorporación de una **mayor flexibilidad e individualización de los procesos de fabricación**.

Se espera que, junto con los fabricantes de electrónica, la industria alimentaria sea pionera en la adopción de procesos de fabricación flexibles e individualizados. Asimismo, es probable que la Industria 4.0 encuentre una rápida aceptación de este enfoque en la industria automotriz.

Redes sociales

Las redes sociales se adentran en todos los ámbitos de la vida a medida que los ciudadanos y los gobiernos exploran nuevas maneras de aprovechar el poder de la multitud.

Las **redes sociales proporcionan un flujo vital** de los datos utilizados por los gobiernos y las organizaciones para poder aplicar **analítica avanzada de sentimientos**.

Por un lado, las redes sociales de nicho o centradas en áreas de interés o aplicación específicas, permiten personalizar y filtrar el contenido y combinar dicha información con geolocalización, proporcionando **hiperplataformas sociales conectadas**.

Tecnología móvil

Sin embargo, por otro lado, los crecientes problemas de privacidad conducen al auge de **plataformas de medios sociales temporales**. Estas plataformas, incrementan el **sentido de control** sobre las condiciones de la exposición, representando el primer paso hacia un nuevo tipo de comunicación digital.

Los **dispositivos móviles de todas las formas y tamaños**, incluyendo *wearables* como relojes y gafas, **mantienen a millones de personas en todo el mundo constantemente conectadas, entretenidas e informadas.**

Las herramientas móviles revolucionan el cuidado de la salud y la educación, mientras que los pagos móviles se convierten en el patrón más habitual.

Algunos de los ejemplos más representativos en el auge de la tendencia basada en la tecnología móvil son los siguientes:

Sistemas de **traducción de voz en tiempo real** en los dispositivos móviles que permiten eliminar numerosas barreras del idioma.

La **tecnología *wearable*** en forma de relojes y gafas, que permite a los usuarios navegar por Internet, ver fotos, o adquirir experiencias de realidad aumentada.

Los **monederos móviles**, aprovechando el avance en la comunicación de campo cercano (NFC en sus siglas en inglés) y que permiten a los usuarios realizar pagos directos.

Los expertos señalan que los consumidores pronto comenzarán a decantarse por los pagos a través de sus teléfonos móviles como demuestra el hecho de que Apple Pay admite tarjetas que representan el **90% del volumen de compras con tarjetas de crédito en EEUU** y pueden utilizarse en un total de 220.000 puntos de venta.

Tecnologías Cognitivas

Multitud de tecnologías cognitivas, incluyendo la robótica, los sistemas basados en reglas, la visión por ordenador, optimización, planificación y programación, resultarán especialmente relevantes para las organizaciones.

Sin embargo, las tecnologías cognitivas más importantes en el mercado de software empresarial serán:

- El **aprendizaje automático** como la capacidad de los sistemas informáticos para mejorar su rendimiento gracias a la explotación de los datos pero sin la necesidad de seguir las instrucciones explícitamente programadas.
- El **Procesamiento del lenguaje natural (NLP)** en el que los sistemas puedan procesar textos de la misma manera que los seres humanos a partir del análisis de textos no estructurados.
- El **reconocimiento de voz** como la capacidad para transcribir automáticamente y con precisión el lenguaje humano.

El rápido progreso en el campo de la inteligencia artificial ha provocado un importante debate sobre las implicaciones de las tecnologías cognitivas en la sociedad. De hecho, los cambios son tan rápidos que se pronostica que entre los próximos tres a cinco años las tecnologías cognitivas tendrán un gran **impacto en el empleo, los profesionales y las compañías.**

Muchas empresas ya han descubierto el potencial de las tecnologías cognitivas para mejorar la funcionalidad principal de sus productos, genera nuevas y valiosas ideas para los clientes, y mejorar las operaciones de negocio a través de la automatización mediante tecnologías cognitivas.

Actualmente, IBM está invirtiendo 1.000 millones de dólares en el desarrollo de **aplicaciones cognitivas** y ya cuenta con una primera oleada de aplicaciones desarrolladas por socios y emprendedores, preparadas para ser **lanzadas al mercado y especializadas** en los sectores de turismo, distribución, servicios TIC, salud y de organizaciones sin ánimo de lucro.

WiFi óptico

LiFi, el equivalente óptico al WiFi y que hace referencia al término *Light Fidelity,* es la comunicación de datos mediante la luz. El LiFi **significa comunicación a través de impulsos de luz visible** mediante los que se transfiere información.

Su principal ventaja es la **transmisión de datos a alta velocidad** al mismo tiempo que se ilumina una habitación.

LiFi es, por tanto, una interesante tecnología con mucho potencial de futuro, más barata y rápida que el WiFi. Además, esta tecnología no satura el espectro electromagnético habitual y promete altas velocidades de transmisión con poco consumo de batería.

Algunos de los expertos en telecomunicaciones se han atrevido a llamar a esta nueva invención como "**el WiFi del futuro**" debido a su rápida interacción de datos; LiFi supera las expectativas que se vive en el día a día con las diferentes conexiones a Internet.

LiFi ha probado ser mucho más rápido que otros sistemas de transmisión de datos que se conocen hoy en día, aparte de ser una **idea ecológica**, por lo que no contamina con radiofrecuencias, y lo hace más seguro para la aplicación de esta tecnología en lugares que generalmente no es posible la implementación de redes WiFi.

Sistemas ciber-físicos

Un sistema ciber-físico (CPS) es todo **aquel dispositivo que integra capacidades de computación, almacenamiento y comunicación para controlar e interactuar con un proceso físico**. Los sistemas ciber-físicos están normalmente conectados entre sí y a su vez conectados con el mundo virtual y las redes digitales globales. Entre los sistemas ciber-físicos con más auge se encuentran los siguientes:

- **Redes de sensores** de medida y registro de todo tipo desde temperatura, luz y movimiento hasta de riesgos biológicos e indicadores físicos del cuerpo.

  La disminución de los costes y de los avances en la tecnología de sensores hacen que sea accesible, ampliamente utilizado y una parte integral del ecosistema digital.

- Los **drones**, aviones no tripulados y manejados por control remoto, inundarán el cielo con diversas tipologías: drones de aprendizaje autónomo, micro-drones, drones impresos en 3D o drones de energía solar.

  - Estos vehículos colaboran ya con la actividad de la Policía Nacional, las encuestas geográficas, las patrullas marítimas o en la entrega de productos, entre otras múltiples aplicaciones comerciales y militares.

  - El estudio de mercado de Teal Group estima que el gasto de **Vehículos Aéreos No Tripulados** (UAVs) se duplicará en la próxima década alcanzando a nivel mundial la cifra de **91.000 millones de dólares**.

  - Según cálculos de la Comisión Europea, en 2050 habrá generado **150.000 empleos** y generará alrededor de 15.000 millones de euros al año de beneficios.

- Sistemas de **realidad aumentada** que permiten a los usuarios experimentar el mundo físico real complementado con elementos sensoriales generados por ordenador, como: sonido, vídeo, gráficos, o datos de localización.

  - El futuro promete mejoras radicales en esta tecnología con la introducción de las interfaces gestuales y retroalimentación sensorial que fusiona el mundo físico con la información digital.

Redes 5G

5G representa la siguiente fase de los sistemas de telecomunicaciones móviles y arquitecturas de red más allá de los actuales estándares 4G.

Su objetivo es la banda ancha extrema y ultra-resistente con baja latencia de conectividad y se encuentra orientada a la conectividad de Internet de las Cosas.

A pesar del debate significativo sobre las especificaciones técnicas y la madurez tecnológica de 5G, que son objeto de debate en diversos foros, se espera que 5G pueda afectar positiva y significativamente a varios sectores de la industria que van desde las TIC a los sectores de la industria tales como automóviles y otras industrias manufactureras, la salud y la agricultura.

Nuevos modelos de pago

El despegue de las redes 5G vendrá impulsado por el IoT y la necesidad de conexión de más de **50.000 millones dispositivos para el año 2020**, según las previsiones de los analistas del sector, con soluciones hardware y software de última generación (como los beacons o balizas) para utilizar los sistemas móviles en cualquier entorno y aplicación, con el **sector retail** como principal impulsor para ofrecer en los puntos de venta una **experiencia integral al cliente** en promociones, medio de pago, comunicación y servicios de valor

Las alternativas al dinero en efectivo y los sistemas financieros tradicionales ya tienen una especial relevancia en la economía digital actual.

El desarrollo de servicios financieros basados en innovación tecnológica: **FinTech**, entre los que destacan los servicios de pago online como Paypal, la tecnología NFC (Near Field Communications), las tarjetas *contactless* o las aplicaciones móviles, se encuentra ya en pleno auge.

Según Deloitte, los pagos a través del teléfono móvil han crecido un **7% en el último año**. En 2014, PayPal procesó un volumen total de pagos de **218.000 millones de euros** con 1.100 millones de transacciones, un 27% más que el año anterior. Además, generó unos ingresos de más de 7.400 millones de euros.

La revolución digital, la creciente proliferación de los pagos a través de Internet y sobre todo, la telefonía móvil, están **cambiando la fisonomía de la industria de los medios de pago en todo el mundo.**

FinTech supone para las empresas la posibilidad de abrir nuevas líneas de negocio para adaptarse a las necesidades de los usuarios. Asimismo, entre los nuevos medios de pago destaca el uso de **bitcoin, la criptomoneda virtual que permite transacciones a través de Internet, nacional e internacionalmente, respetando el anonimato.**

Además, los nuevos medios de pago permiten en muchos casos la utilización del Big Data, es decir, la posibilidad de utilizar datos de los usuarios para desarrollar nuevos productos como por ejemplo, planes de ahorro adaptados a su situación.

En definitiva, el estudio de las tendencias TIC pone de manifiesto la especial relevancia de la conexión y ubicuidad de los datos basados en IoT y Cloud Computing y que dan lugar a la creación de redes y ciudades inteligentes, donde el Big Data es un elemento esencial. Dichas ciudades inteligentes se configuran, principalmente, sobre nuevas redes y tecnologías móviles que fomentan un cambio alternativo en el modelo de vida tradicional de sus ciudadanos

3.3. La importancia de la ciberseguridad y su relación con las TIC

La evolución de las TIC ha provocado un gran cambio de paradigma en la sociedad. El uso intensivo de éstas por parte de los ciudadanos, empresas, gobiernos y organizaciones sociales lleva consigo una serie de riesgos y por lo tanto, la **puesta en marcha de medidas de protección y seguridad de los datos intercambiados y los sistemas y redes conectados**, que hacen que la ciberseguridad deba ser tenida en cuenta formando parte integral del progreso tecnológico.

La **creación de un clima de seguridad y confianza digital**, que permita reforzar la protección de los organismos públicos y privados y estimule la implicación de los usuarios en el entorno digital, es vital para el pleno desarrollo de la Sociedad y Economía en un contexto en el que los incidentes son cada vez más frecuentes, complejos y de mayor magnitud.

Este objetivo se ve reforzado a través del **Programa Horizonte 2020**, centrado, a través del apartado de **Desafíos de la Sociedad**, en la generación de sociedades seguras, por medio de apertura de convocatorias para la puesta en marcha de proyectos destinados a la protección de las infraestructuras críticas, el aseguramiento en privacidad de los datos, o la ciberseguridad en pymes, administraciones locales y ciudadanos.

Así pues, según la Unión Internacional de Telecomunicaciones (UIT), la ciberseguridad se define como:

"el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad."

Por lo tanto, la **ciberseguridad está definida como un conjunto de directrices, políticas y herramientas que tienen como objetivo crear ese clima de confianza digital, por medio de la protección de los activos de organizaciones y particulares, que tengan soporte TIC**.

Además, la necesidad de disponer de una red y entornos seguros está cada vez más presente en las empresas y las Administraciones Públicas, a la hora de definir sus prioridades en relación al entorno TIC.

Dado que la ciberseguridad se encuentra estrechamente ligada al uso de la tecnología, las tendencias TIC hallan vulnerabilidades o respuestas a dichas vulnerabilidades en numerosas soluciones de ciberseguridad.

Por ejemplo, **Cloud Computing**, al ser un componente importante en las arquitecturas de aplicaciones modernas, se considera dentro de las tecnologías emergentes **como principal objetivo de las ciberamenazas**. Esto se debe, principalmente, a **la gran cantidad de información potencialmente valiosa almacenada y/o procesada**. Al igual que las empresas, los ciberdelincuentes reconocen las ventajas de la computación en la nube por cuestiones de costes, un mejor camuflaje de actividades maliciosas en sitios legítimos o por razones de rendimiento.

En consecuencia, es de esperar que los proveedores de servicios en la nube tengan que proporcionar controles de seguridad y guiar a sus clientes a desarrollar sus propias estrategias de ciberseguridad.

Por otro lado, IoT dado que es una implementación ubicua de sistemas y múltiples elementos interconectados, lleva asociado un perímetro borroso de seguridad que obligará a desarrollar nuevos enfoques para asegurar las funciones de la red y los datos. **Los principales riesgos asociados a la seguridad de IoT estarán relacionados con la complejidad resultante de la convergencia de múltiples plataformas y aplicaciones en sistemas embebidos.**

Además, IoT se considera un importante productor de grandes volúmenes de datos en bruto a muy altas velocidades. Como tal, **estos datos (Big Data) pueden ser usados para sintetizar la información que es relevante en materia de seguridad, confidencialidad, personal, etc**.

Sin embargo, es evidente que la falta de seguridad en el apoyo o el suministro de tecnologías y sistemas tienen el potencial de afectar negativamente a estos grandes sistemas de datos.

Por otro lado, se prevé que aumente el uso en la seguridad de los dispositivos móviles respecto a todo el ecosistema móvil, incluyendo almacenamiento en la nube, las API de aplicaciones, componentes internos de aplicaciones, procesos de investigación, ataques sigilosos, etc. **La tendencia se basará en migrar todas las técnicas maliciosas del PC al móvil, por lo que proliferarán los ataques especialmente diseñados para dichos dispositivos.**

Finalmente, el impacto del uso de las TIC en la sociedad y su extensión en los distintos sectores del panorama empresarial brindan protagonismo a la **ciberseguridad aplicada**, que adecua los productos de ciberseguridad a las distintas necesidades y demanda de los sectores. De esta manera, recientemente han surgido **soluciones de ciberseguridad adaptadas** a los sistemas de conectividad del sector automoción, e-health, Smart Grids e Industria 4.0, drones, realidad aumentada y virtual o banca online, entre otros ámbitos.

En resumen, el campo de estudio de la ciberseguridad se encuentra íntimamente ligado a la evolución de las tendencias TIC identificadas, dado que como se ha ejemplificado brevemente, **el auge en la conectividad, la ubicuidad de los datos o la saturación de los sistemas, entre otros, llevan asociados consigo una serie de vulnerabilidades y riesgos en ciberseguridad que deberán ser estudiados y abordados.**

4. CARACTERIZACIÓN DEL MERCADO GLOBAL DE LA CIBERSEGURIDAD

La creciente demanda de productos y soluciones que garanticen la protección de las infraestructuras TIC y las comunicaciones e información online, tanto de los particulares como de las empresas y administraciones públicas, han dado lugar a la configuración del sector de la ciberseguridad.

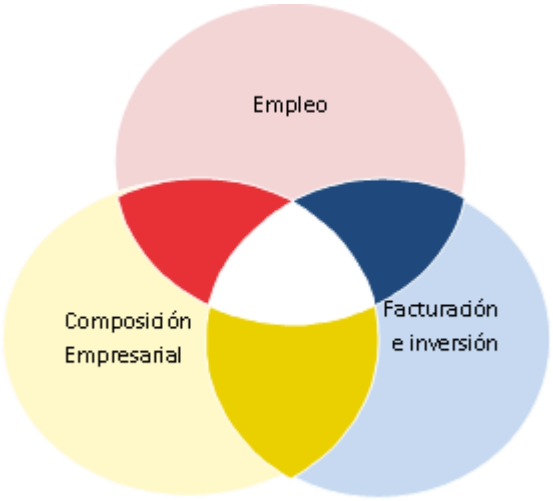
Por ello, con el objetivo de profundizar en la actividad del sector, este capítulo se encuentra dedicado a la caracterización de éste, para lo cual se presentan tanto los datos más relevantes que avalan el potencial del sector de la ciberseguridad, como la repercusión que éste tiene en diversos agentes y áreas de actividad.

4.1. El mercado de la ciberseguridad en cifras

Como primer punto de análisis de caracterización del mercado de la ciberseguridad y su potencial grado de desarrollo, conviene valorar cuantitativamente los datos del sector desde diversas perspectivas tanto nacionales como internacionales.

En primer lugar, **a nivel global,** según Gartner, **el sector de la ciberseguridad** se presenta como una actividad económica en auge, con una **facturación mundial de 62.540 millones de euros en 2015** y con una previsión de aumento de la demanda (partiendo de un gasto en ciberseguridad de 54.082 millones de euros en 2014) que alcanzará **79.292 millones de euros en 2018.**

De manera específica, para la caracterización del **mercado a nivel nacional**, se estudian los datos más relevantes del sector de la ciberseguridad en 2014 del ONTSI a través del análisis de las siguientes tres variables:



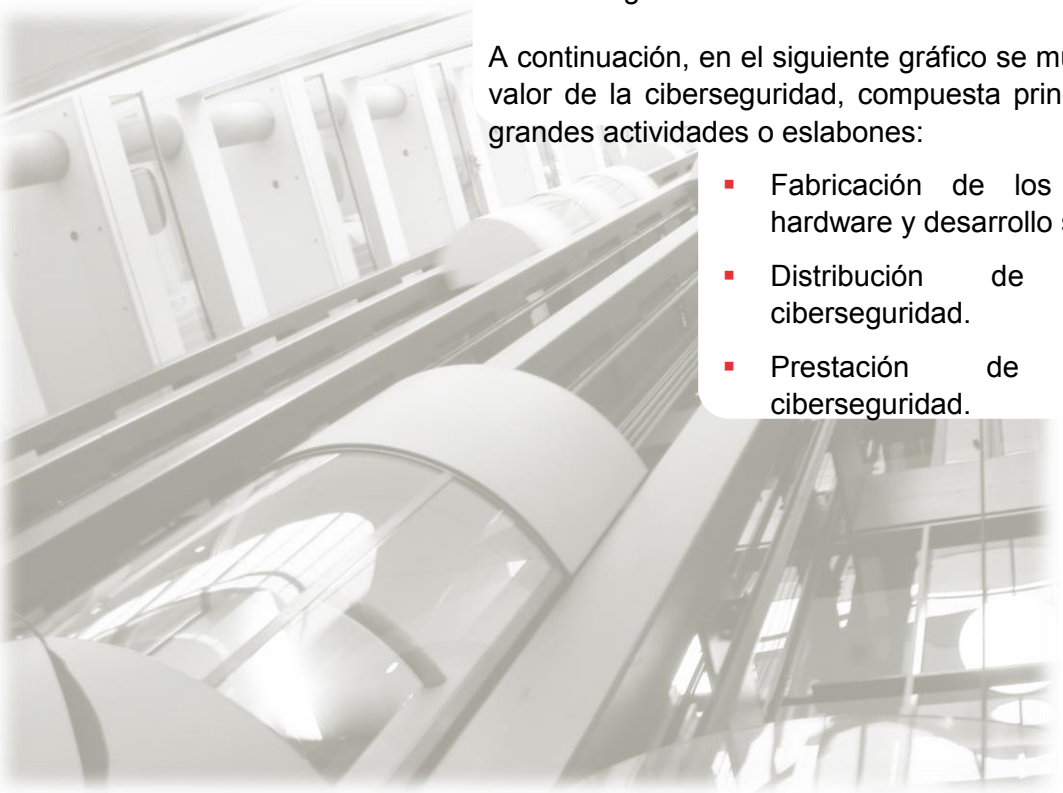
Por un lado, **el sector de la ciberseguridad en España** en 2014 estuvo compuesto por un total de **533 empresas**, *pure players* y empresas TIC, las cuales proporcionaban **empleo a 5.808 personas**. Prácticamente la totalidad de este empleo, el 99,5%, se concentraba en empresas pertenecientes al sector TIC. Además, 2.143 personas, es decir, un **37% de los empleados del sector, se dedicaban exclusivamente al negocio de la ciberseguridad**.

Por otro lado, la facturación total del sector de la ciberseguridad en 2014 fue de 598,2 millones de euros. **Las empresas dedicadas exclusivamente al sector de la ciberseguridad**, un 14,8% del total de las 533 empresas, contribuyeron a más del **50% de la facturación total del sector**.

Por último, la **inversión realizada por las empresas del sector durante ese año supuso 79 millones de euros**. La distribución de la inversión realizada situaba a las empresas pertenecientes al sector de Servicios TIC como las que mayor inversión habían llevado a cabo, con 77,8 millones de euros y un peso sobre el total del 98,5%. Concretamente, la inversión realizada en ciberseguridad por las empresas que se dedican exclusivamente a este negocio ascendía a 30,8 millones de euros en 2014.

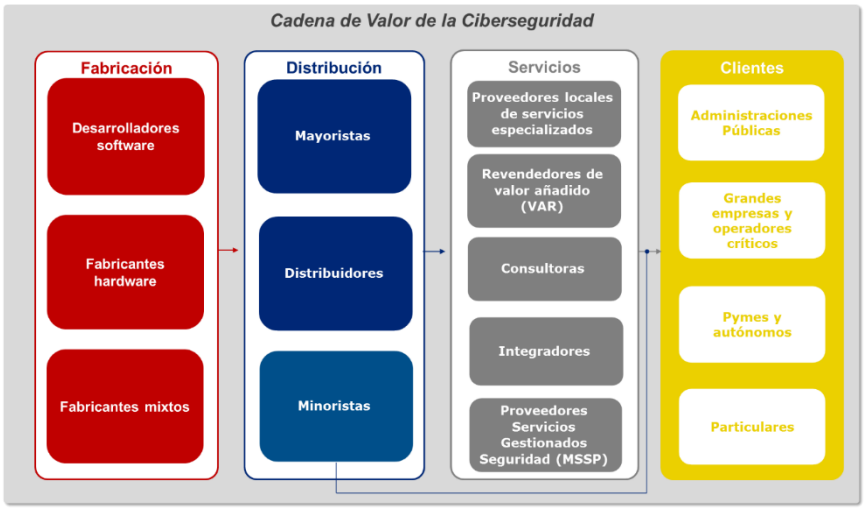
4.2. La cadena de valor de la ciberseguridad

La cadena de valor de la ciberseguridad es el modelo en el que se encuentran diseñadas las principales actividades y los vínculos de relación entre los distintos eslabones de la cadena para la creación de productos o prestación de servicios de ciberseguridad.

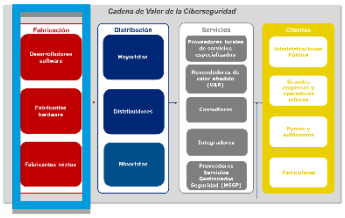


A continuación, en el siguiente gráfico se muestra la cadena de valor de la ciberseguridad, compuesta principalmente por tres grandes actividades o eslabones:

- Fabricación de los componentes de hardware y desarrollo software.
- Distribución de productos de ciberseguridad.
- Prestación de servicios de ciberseguridad.



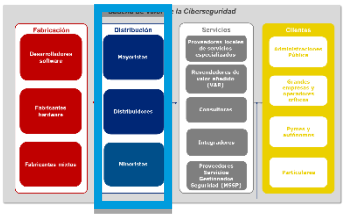
No obstante, algunos de estos agentes pueden intervenir en los tres eslabones, como es el caso de fabricantes de software especialistas y generalistas que, o bien venden a minoristas, o al cliente final.



En el **primer eslabón de la cadena de valor, fabricación,** se enmarcan los siguientes elementos o agentes de fabricación y desarrollo de soluciones de ciberseguridad:

- **Desarrolladores de software.** Suministran soluciones y aplicaciones (no físicas) para garantizar la seguridad en la red y contribuir a la gestión y control de acceso web e identidad de los usuarios.
- **Fabricantes de hardware.** Desarrollan soluciones y herramientas físicas de cifrado, así como sistemas y aplicaciones para garantizar la seguridad en la movilidad y en las redes corporativas.
- **Fabricantes mixtos.** Suministran productos hardware y soluciones software, diseñados para proteger las redes y proporcionar una conexión segura a las mismas.

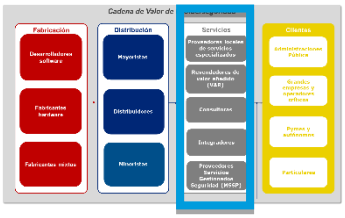
El modelo genérico de relación de los agentes de la cadena en esta fase, funciona de manera que los agentes involucrados en la actividad de fabricación se comunican principalmente con los distribuidores y mayoristas que forman parte del siguiente eslabón de la cadena de valor para la comercialización de sus productos.



Por su parte, el **segundo eslabón de la cadena de valor, distribución,** está compuesto por empresas que hacen de nexo de conexión entre las actividades de fabricación y prestación de servicios. En esta actividad operan los siguientes agentes:

- **Mayoristas.** Compran y venden productos de ciberseguridad a consultoras, a los integradores y a los proveedores de servicios gestionados de seguridad. Los mayoristas pueden estar especializados en seguridad TIC o bien, dedicarse a una actividad más genérica (informática, electrónica, etc.).
- **Distribuidores.** Venden directamente a empresas de ciberseguridad o a clientes finales los productos de ciberseguridad. En ocasiones, tanto mayoristas como distribuidores comercializan sus productos a los revendedores de valor añadido (VAR, Value Added Reseller).
- **Minoristas.** De manera frecuente, son puntos de venta constituidos por tiendas físicas de informática, grandes superficies e incluso pequeñas consultoras enfocadas a Pymes y particulares.

En el modelo de relación, los elementos que conforman este eslabón de distribución en la cadena de valor hacen de vínculo de comunicación entre los fabricantes y los prestadores de servicios de dichos productos en ciberseguridad. No obstante, estos agentes de distribución (minoristas, especialmente) pueden, en algunas ocasiones, mantener relación directa con los clientes.



Por último, **en el eslabón de servicios** se enmarcan los siguientes agentes:

- **Proveedores locales.** Ofrecen servicios especializados mediante el desarrollo de productos propios y la oferta de soluciones de nicho.
- **Revendedores de valor añadido (VAR).** Agregan valor a productos de software y hardware fabricados por otros agentes, a través de la incorporación de complementos para el diseño y elaboración de una solución o servicio completo.
- **Consultoras.** Prestan servicios especializados en ciberseguridad en torno a dos campos de actividad: negocio y tecnología.
  Las **consultoras de negocio** se dedican a la consultoría y asesoría orientada a los asuntos legales y organizativos de la seguridad de la información.

Sin embargo, las **consultoras tecnológicas** se encuentran especializadas en servicios de asesoramiento, respuesta y soporte relativos a las tecnologías de seguridad.

- **Integradores**. Crean soluciones complejas de seguridad TIC, adaptándose a las necesidades de los usuarios. Utilizan, con frecuencia, productos de diversos fabricantes y los complementan con soluciones propias.

- **Proveedores de servicios gestionados de seguridad** (MSSP, Managed Security Service Providers). Proporcionan servicios externalizados de seguridad al cliente con un enfoque integral y multidisciplinar de la seguridad corporativa que abarca tanto las áreas que afectan a la organización como a los aspectos tecnológicos.

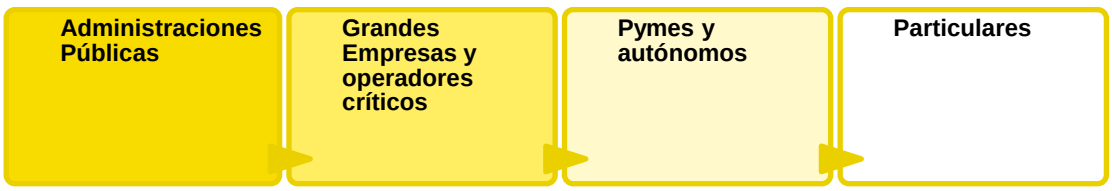
El modelo genérico de relación de los agentes de la cadena, en esta fase, funciona de forma que, exceptuando los proveedores locales, los agentes del eslabón comercializan sus bienes y servicios al cliente final, entre los que destacan la Administración Pública, las empresas y los particulares.

4.3. Destinatarios del sector

Por último, se describen los **principales destinatarios de los productos y servicios de ciberseguridad del sector**, es decir, se desglosa el último eslabón de la cadena de valor de la ciberseguridad.

Para ello, se clasifica cada uno de los grandes demandantes de ciberseguridad desde dos perspectivas: desde el punto de vista de las grandes amenazas sufridas y de los principales servicios o soluciones demandados, en función de su actividad.

Los clientes finales o demandantes de ciberseguridad se clasifican en cuatro grandes grupos:



En función del grado de complejidad de los sistemas empleados por los clientes, éstos demandarán distintos tipos de servicios y soluciones, quedando estructurados de la siguiente manera.

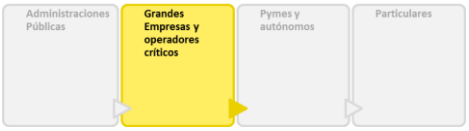
Administraciones Públicas

Las Administraciones Públicas son demandantes de seguridad para la protección de la información gestionada por la propia administración o bien, demandantes de soluciones de protección y seguridad en el ámbito de la defensa y de la inteligencia nacional.

Las **principales amenazas que pueden sufrir el gobierno y las administraciones públicas son el ciberespionaje y la sustracción de información**, que como resultado pueden provocar la publicación y venta de información sensible a través de Internet.

En base a ello, **el sector público requiere soluciones de seguridad integral, basadas en ciberinteligencia y ciberdefensa**, que contribuyan a la protección de los organismos públicos locales, regionales y nacionales.

Concretamente, las administraciones públicas o gobiernos demandan **servicios de gestión de ciberseguridad**, ofrecidos con el fin de dotar de seguridad a los procesos de trabajo; **servicios de ciberseguridad reactivos**, destinados a controlar y responder a una amenaza o incidente que pueda haber sufrido un sistema de información, minimizando su impacto; o **servicios de seguridad proactivos**, destinados a reducir los riesgos de seguridad a través de información e implantación de sistemas de protección y detección.



Grandes empresas y operadores críticos

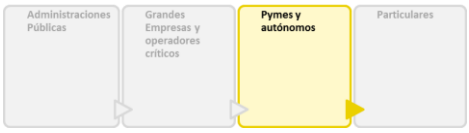
La demanda de soluciones de ciberseguridad del sector privado atiende al sector en el que opera la empresa, diferenciándose específicamente aquellos denominados como infraestructuras críticas, que son las infraestructuras estratégicas que proporcionan servicios esenciales y cuyo funcionamiento es indispensable, por lo que su interrupción o destrucción acarrea un grave impacto sobre los servicios.

Los principales **servicios de seguridad demandados por las infraestructuras críticas son soluciones industriales,** con una alta especialización en el sector, en la región o en la tecnología; y **soluciones de seguridad integral**.

El resto de las grandes empresas, por su parte, son también **susceptibles de ataques de ciberespionaje industrial, de control e interrupción de sistemas y de sustracción y venta de información confidencial.**

Por lo tanto, las soluciones y servicios que demandan son de todo tipo, desde auditorías técnicas, gestión de incidentes, soluciones de seguridad integral hasta seguridad en la nube.

Pymes y autónomos



Para el grupo de destinatarios conformado tanto por pymes como por trabajadores autónomos, las **principales amenazas se basan en el uso/abuso o reventa de información privada** que proporcionan los clientes a organizaciones privadas y, los ataques apoyados en ciberdelincuencia.

Con base en dichas amenazas, los principales productos orientados a estos clientes **son soluciones o herramientas estándar, desarrolladas de manera genérica por proveedores de ciberseguridad y enfocadas a empresas o usuarios a pequeña escala,** cuya utilización deriva del uso de entornos de trabajo *online*.

Por otro lado, la distribución se realiza mediante la concesión de licencias, o bien la entrega de un producto físico. Es también frecuente la existencia de un modelo *freemium* y otro gratuito de este tipo de soluciones.

Particulares

Los usuarios particulares o consumidores de ciberseguridad fuera del ámbito profesional son usuarios cuya seguridad versa en la necesidad de protegerse y prevenir los ataques, principalmente, hacia dispositivos móviles u ordenadores con acceso a Internet.

Al igual que para el caso de pymes y trabajadores autónomos, las principales amenazas **se basan en el uso/abuso o reventa de información privada, derivado de la digitalización de la ciudadanía** dado el inminente crecimiento del comercio electrónico para consumidores y, la puesta en marcha de las iniciativas de dinero electrónico para la inclusión económica.

Los principales productos orientados a estos clientes **son soluciones o herramientas genéricas y esenciales de ciberseguridad enfocadas a cualquier destinatario y cuya utilización deriva**, fundamentalmente, de un uso asiduo de Internet.

Además, en este caso, resulta fundamental promover el **desarrollo de conocimientos básicos de seguridad informática en el usuario** con el objetivo de generar conciencia del riesgo representado por utilizar software de dudosa procedencia, así como antivirus u otro software desactualizado.

5. TENDENCIAS DE MERCADO EN CIBERSEGURIDAD

El **sector de la ciberseguridad se presenta como un motor de desarrollo de la Economía Digital**. La seguridad y la protección de la información adquieren una gran relevancia en la era actual de la digitalización y la *hiperconectividad.*

El aumento en el número de vulnerabilidades y riesgos que las empresas, administraciones públicas o los ciudadanos pueden sufrir, requieren de un mayor grado de especialización y capacitación del sector y, más concretamente, de su respuesta ante ellos.

Es por ello que, **en este capítulo se definen las tendencias globales en ciberseguridad, sectorizadas en torno a los principales ámbitos de actividad.**

5.1. El Horizonte 2020 y su influencia en la evolución del sector de la ciberseguridad

Al igual que en la selección de tendencias TIC, **el análisis llevado a cabo para la extracción de tendencias en el sector de la ciberseguridad** se basa en los objetivos marcados por el **Programa Europeo Horizonte 2020**, que establece varios aspectos transversales a tener en cuenta, como son la **inclusión de la perspectiva de la Ciberseguridad o el Internet de las Cosas**, así como el desarrollo de Sociedades Seguras, protegiendo la libertad y la seguridad de Europa y su ciudadanía.

De manera particular, dentro del **Programa de Sociedades Seguras para el periodo 2016-2017** (*Secure Societies: Protecting freedom and security of Europe and its citizens*) se presentan una serie de convocatorias concretas para el desarrollo de proyectos de ciberseguridad enmarcados en los siguientes ámbitos:

- Protección de las **Infraestructuras Críticas**.
- **Seguros y certificaciones** para unos sistemas, servicios y componentes TIC más confiables y fiables.
- Servicios y soluciones de **ciberseguridad aplicables a pymes**, **administraciones públicas locales y particulares**.
- **Seguridad** digital de **datos médicos**.
- **Cooperación e intercambio de información** entre los miembros de la Unión Europea y otros países sobre investigación, desarrollo e innovación en ciberseguridad.
- **Criptografía**.

- **Ciberinteligencia** (Advanced Cybersecurity Threat) y actores implicados.
- **Privacidad**, protección de los datos e identidades digitales.

Las convocatorias relacionadas con proyectos de ciberseguridad tienen como fin incrementar la seguridad de las aplicaciones actuales, los servicios y las infraestructuras, y apoyar la creación de mercados líderes en Europa, siempre persiguiendo un enfoque de destinatario final, e incluyendo a organismos competentes en el cumplimiento de la ley, operadores de infraestructuras críticas, proveedores de servicios TIC, distribuidores TIC, operadores de mercado y ciudadanos.

En este sentido, este Programa trata de implicar a todas las **partes interesadas**: industria, incluyendo a las pymes; entidades de investigación; Universidades; así como organismos públicos, organizaciones no gubernamentales y organizaciones público privadas en el ámbito de la seguridad.

El **Programa específico de Tecnologías de la Información y las Comunicaciones para el periodo 2016-2017**, se centra en convocatorias concretas relacionadas con los siguientes ámbitos:

- Una **nueva generación de componentes y sistemas**. En este ámbito, cobra especial importancia la seguridad de sistemas ciber-físicos y sistemas smart.
- **Computación avanzada y Cloud Computing**. Donde se hace hincapié en la protección de sistemas en la nube.
- **Internet del Futuro**. Incluyéndose especificaciones para la seguridad en dispositivos móviles y el desarrollo de tecnologías de software seguras (seguridad desde el diseño).
- **Contenido.** En el que se llama a la creación de tecnologías Big Data que intrínsecamente contemplen la privacidad de los datos.
- **Robótica y sistemas autónomos.**
- **Tecnologías clave habilitadoras.**

Finalmente, en el documento de Visión Estratégica elaborado a partir de los grupos de trabajo para desarrollar los **Programas de Trabajo** del Horizonte 2020 **para el próximo periodo 2018-2020**, se han identificado 12 ejes impulsores de cambio, entre ellos, el relativo a la Revolución digital. En él, se plantea que la creciente dependencia de los sistemas TIC puede provocar el inicio de ciberguerras, y consecuentemente, la necesidad de poner en marcha **mecanismos de vigilancia integral**.

Con el auge del Big Data y el IoT, la **prevención del cibercrimen se convertirá en una de las principales preocupaciones de los gobiernos**. La posesión de gran cantidad de información por parte de los gobiernos y grandes empresas provocará que estas organizaciones se perciban como potenciales objetivos de ciberataques.

A este respecto, la Unión Europea ha implementado normativa y respalda la cooperación operativa, como parte de la Estrategia de Ciberseguridad de la Unión:

- Por un lado, se ha desarrollado **normativa para la protección frente al cibercrimen** como la Directiva 2013 relativa a Ataques contra Sistemas de Información, o la Directiva sobre Privacidad y Comunicaciones Electrónicas del año 2002.
- Por otro, la Comisión Europea ha jugado un papel clave en el desarrollo del **Centro Europeo del Cibercrimen (EC3),** en el que se ponen en común los conocimientos de ciberdelincuencia para apoyar las investigaciones de delitos de los Estados miembros.

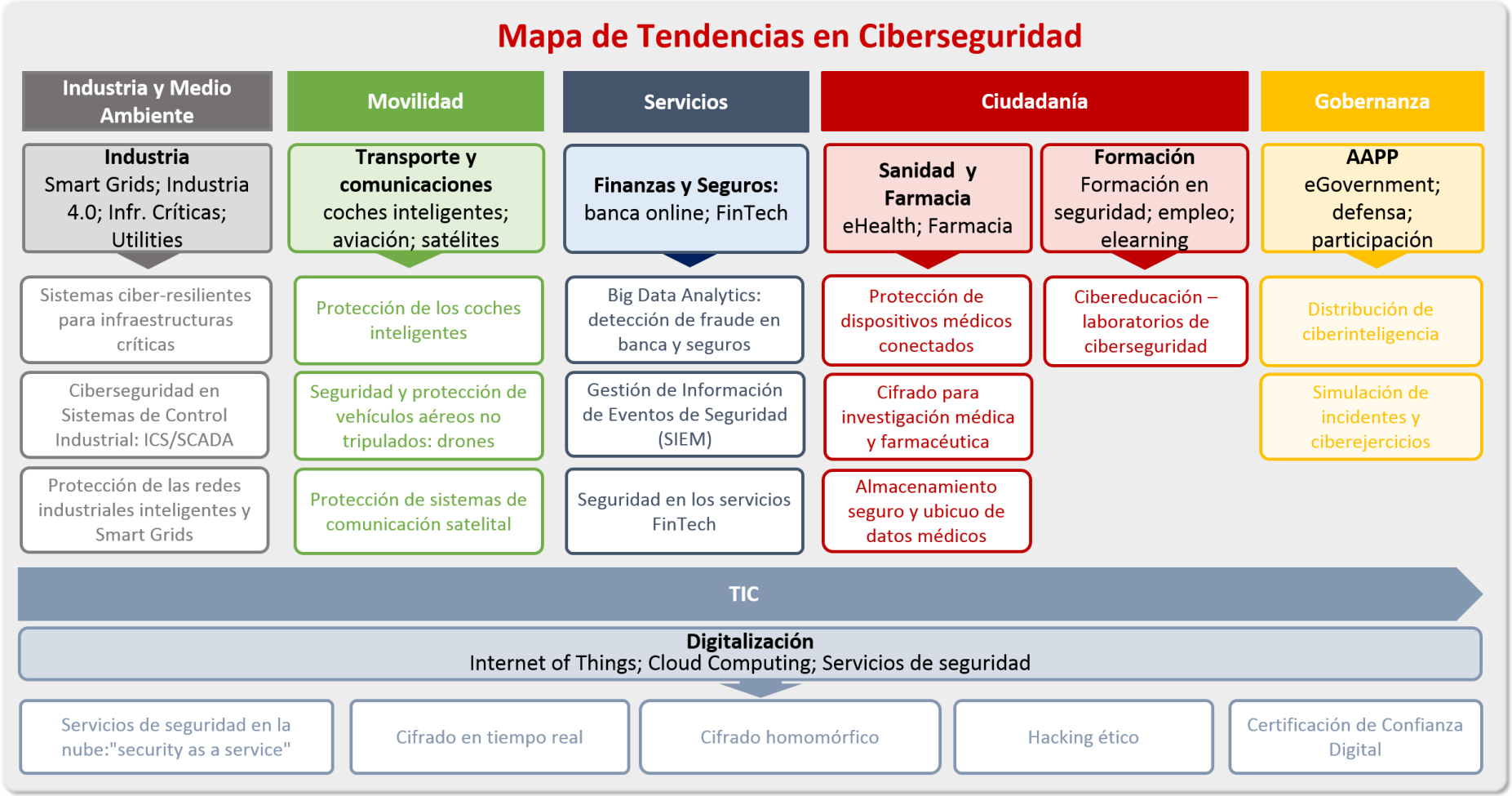
5.2. Mapa de tendencias y selección final

De manera integral, se presenta una selección de tendencias de mercado en ciberseguridad, adaptadas a oportunidades concretas de negocio empresarial.

Esta selección final de tendencias es fruto de un proceso de recopilación y clasificación llevado a cabo con base en diferentes *inputs*.

- El punto de partida en el análisis y selección de tendencias ha estado basado en un proceso de documentación procedente de las principales entidades de referencia, tanto nacionales como mundiales. Para ello, se han tomado diferentes fuentes documentales procedentes de:
  - Catálogo de productos de grandes *players* del sector.
  - Estudios e informes de diversas entidades de referencia, públicas y privadas.
  - Informes de incidentes y principales amenazas de ciberseguridad.
- En el proceso posterior de categorización y clasificación de las tendencias finalmente seleccionadas han intervenido diferentes agentes de la industria pertenecientes al grupo de trabajo de este Estudio de Tendencias en el mercado de la Ciberseguridad.

Con todo ello, a continuación, en el siguiente gráfico, se encuentra diseñado el **Mapa de Tendencias en Ciberseguridad**, que incluye el conjunto final de tendencias catalogadas en torno a siete sectores de actividad.


Mapa de Tendencias en Ciberseguridad
Industria y Medio Ambiente
Movilidad
Servicios
Ciudadanía
Gobernanza
Industria
Smart Grids; Industria 4.0; Infr. Críticas; Utilities
Transporte y comunicaciones
coches inteligentes; aviación; satélites
Finanzas y Seguros:
banca online; FinTech
Sanidad y Farmacia
eHealth; Farmacia
Formación
Formación en seguridad; empleo; elearning
AAPP
eGovernment; defensa; participación
Sistemas ciber-resilientes para infraestructuras críticas
Protección de los coches inteligentes
Big Data Analytics: detección de fraude en banca y seguros
Protección de dispositivos médicos conectados
Cibereducación – laboratorios de ciberseguridad
Distribución de ciberinteligencia
Ciberseguridad en Sistemas de Control Industrial: ICS/SCADA
Seguridad y protección de vehículos aéreos no tripulados: drones
Gestión de Información de Eventos de Seguridad (SIEM)
Cifrado para investigación médica y farmacéutica
Simulación de incidentes y ciberejercicios
Protección de las redes industriales inteligentes y Smart Grids
Protección de sistemas de comunicación satelital
Seguridad en los servicios FinTech
Almacenamiento seguro y ubicuo de datos médicos
TIC
Digitalización
Internet of Things; Cloud Computing; Servicios de seguridad
Servicios de seguridad en la nube:"security as a service"
Cifrado en tiempo real
Cifrado homomórfico
Hacking ético
Certificación de Confianza Digital

La clasificación de tendencias se asienta en torno a los siguientes siete sectores o ámbitos de actividad:

Sector Industrial y Medio Ambiente, cuyas necesidades de ciberseguridad se orientan hacia la protección y seguridad de los diferentes dispositivos y redes que conforman las Smart Grids, Infraestructuras Críticas, Industria 4.0 y demás servicios que tengan cabida en el sector industrial y, fundamentalmente, energético.

Sector Movilidad, principalmente enfocado en el transporte y las comunicaciones, y cuyos objetivos de ciberseguridad se fundamentan en la protección de medios de transporte aéreo o terrestre, tales como los vehículos autónomos o conectados, o dispositivos móviles que requieran de comunicación satelital.

Sector Servicios, en el cual quedaría incluida la división financiera y de seguros, cuya finalidad en ciberseguridad se asienta principalmente en la defensa y protección contra incidentes derivados de la digitalización de sus servicios, tales como la banca online o los servicios y aplicaciones *Fintech*.

Sector Ciudadanía, que incluye los servicios públicos básicos de sanidad y educación, cuenta con necesidades en ciberseguridad, por un lado, orientadas hacia la protección de dispositivos médicos interconectados, patentes o información sensible de pacientes utilizadas en el ámbito sanitario y farmacéutico y por otro lado, en la necesidad de formación y capacitación profesional especializada en ciberseguridad.

Sector Gobernanza, basado en los organismos públicos y Administraciones Públicas y sus correspondientes vulnerabilidades en ciberseguridad derivadas del control y gestión de información y servicios públicos ciudadanos electrónicos, fundamentalmente.

Sector TIC, o basado en la digitalización, es un sector transversal a los anteriores que recopila las necesidades y prácticas más habituales en materia de ciberseguridad, ofrecidas desde un entorno como la nube, y las cuales pueden ser aplicadas al resto de sectores definidos.

ANEXO I. REFERENCIAS

- AON. *Exploring the Latest Cyber Risk Trends in EMEA.*
- BANK OF ENGLAND. *Cyber resilience: a financial stability perspective.*
- BT. *Ethical Hacking and vulnerability assessment.*
- CAPITAL. CAPITAL. *Deliverable: D 2.4 List of Existing Solutions.*
- CAPITAL. CAPITAL. *Deliverable: D 3.1 Initial set of research activities listed to meet gaps.*
- CCN CERT. *Ciberamenazas 2014 y Tendencias 2015.*
- CISCO. *Informe Anual de Seguridad de Cisco 2015.*
- CNI. *Ciberseguridad, Retos y Amenazas a la seguridad Nacional en el ciberespacio*.
- COMISIÓN EUROPEA. *Horizon 2020. Work Programm 2014-2015 y 2016-2017.*
- COMISIÓN EUROPEA. *TOPIC: Increasing digital security of health related data on a systemic level.*
- COMISIÓN EUROPEA. *Towards a European strategy for cyberspace.*
- CONSEJO EUROPEO. *Improving cyber security across the EU.*
- CONSEJO NACIONAL DE CIBERSEGURIDAD. *Plan Nacional de Ciberseguridad.*
- DELOITTE. *Changing the game on cyber risk.*
- DELOITTE. *Cyber & Insider Risk: The Pharmaceutical Industry Tightening up safeguards against IP theft.*
- DELOITTE. *Cyber crime fighting.*
- DELOITTE. *Cyber Threat Intelligence. Move to an intelligence driven cybersecurity model.*
- DELOITTE. *Gov2020*.
- DELOITTE. *Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives.*
- DELOITTE. *State goverment at Risk: Time to Move forward.*
- DELOITTE. TMT *Predictions 2016.*
- DONALD W. DUNPHY. *Car Hacking. Preparing for the future now.*
- EDISON ELECTRIC INSTITUTE. *Frequently Asked Questions About Cybersecurity and The Electric Power Industry.*
- ENISA. *ENISA Threat Taxonomy*.
- ENISA. *La agencia de ciberseguridad de la UE, apuesta por una mayor protección de los sistemas SCADA.*
- ENISA. *Recomendaciones de ENISA para la certificación de profesionales de sistemas ICS/SCADA.*
- ENISA. *Secure Use of Cloud Computing in the Finance Sector.*
- ENISA. *Threat Landscape 2014.*
- ENISA. *Threat Landscape 2015.*
- ERNSY & YOUNG. *Big Data en el sector financiero español. Resultados de la encuesta sectorial sobre Big Data.*
- FEDERACIÓN ESPAÑOLA DE EMPRESAS DE TECNOLOGÍA SANITARIA. *Memoria 2014*
- FORBES. *Tendencias en ciberseguridad para 2015.*
- FORRESTER. *European Online Retail Forecast, 2012 To 2017.*
- GARTNER. *Innovation Insight for SIEM as a Service.*
- GARTNER. *Predicts 2016: Security Solutions.*
- GARTNER. *Secure M-Commerce Through Three Categories of Mobile User Authentication and Fraud Prevention.*
- GARTNER. *SIEM Technology, Market and Vendor Assessment.*
- GOBIERNO DE LUXEMBURGO. *National Cybersecurity Strategy II.*
- IBM. *Analytics: el uso de Big Data en el mundo real. Cómo las empresas más innovadoras extraen valor de datos inciertos.*

- IEC. *Internet of Things: Wireless Sensor Networks.*
- IEC. *Internet of Things: Wireless Sensor Networks.*
- INSTITUTO DE ESTUDIO BURSÁTILES. *II Ranking Anual Competidores del Sector Financiero.*
- ISACA. *2015 Global Cybersecurity Status Report.*
- ISACA. *State of Cybersecurity: Implications for 2015.*
- KASPERSKY. *Global IT Security Risks Survey.*
- KASPERSKY. *Kaspersky Security Bulletin 2015.*
- KASPERSKY. *Las predicciones de Kaspersky Lab en ciberseguridad para 2016.*
- MARCA ESPAÑA. *Los nuevos satélites españoles.*
- MARKETS AND MARKETS. *Managed Security Services Market by Services (Managed IDS/IPS, DDOS Protection, Managed SWG, SIEM, MICS, Log Management & Analytics), by Deployment Type (Hosted, On-Premise), & by Organization Size (SME, Enterprise) - Global Forecast (2014 - 2019).*
- MCAFEE. *Automotive Security Best Practices.*
- MCAFEE. *McAfee Labs Report 2016 Threats Predictions.*
- MCAFEE. *Threats Report August 2015.*
- MCAFEE. *Threats Report November 2014.*
- PANDA. *Informe Anual Pandalabs 2014.*
- PARLAMENTO EUROPEO. *Cibersegurity in the European Union and Beyond: Exploring the Threats and Policy Responses, Directorate-General for Internal Policies.*
- PONEMON INSTITUTE. *2015 Global Encryption & Key management Trends Study.*
- PRESIDENCIA DEL GOBIERNO. *Estrategia de Ciberseguridad Nacional 2013.*
- PRESIDENCIA DEL GOBIERNO. *Informe Anual de Seguridad Nacional 2014.*
- PWC. *Temas candentes de la Ciberseguridad, un nuevo espacio lleno de incógnitas.*
- RUBEN SANTAMARTA, IOACTIVE. *A Wake-up Call for SATCOM Security.*
- SOPHOS. *Tendencias amenazas de seguridad 2015.*
- SYMANTEC. *The Cyber Resilience Blueprint: A New Perspective on Security.*
- TECHNAVIO. *Top Trends in Aviation Cyber Security.*
- THE INSTITUTION OF ENGINEERING & TECHNOLOGY. *Automotive Cyber Security: An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles.*
- TREND MICRO. *Predicciones de seguridad para 2016 de Trend Micro: la delgada línea.*
- U.S FOOD AND DRUG ADMINISTRATION. *Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software.*
- US CERT. *Cyber Resilience Review (CRR).*
- UTAD. *Estado de la Ciberseguridad 2015.*
- VERIZON. *Data Breach Investigations report 2015.*


incibe_
2006-2016
TRABAJANDO POR
LA CONFIANZA DIGITAL