SEGURIDAD Y PRIVACIDAD EN BIG DATA: Retos y oportunidades (GDPR)

Madrid, 17 de enero, 2017

Luis Joyanes Aguilar (Fidesol)

ÍNDICE TEMÁTICO

- Tecnologías emergentes en el H2020 y en el entorno de Big Data: Tendencias tecnológicas para 2018
- Innovaciones tecnológicas presentadas en la feria de electrónica CES 2018 de Las Vegas (9-12 enero, 2018).
- El ciclo de vida de los datos: El caso de Big Data
- Calidad y seguridad de los datos: Gobernanza de datos
- Código de Buenas Prácticas en protección de datos de BIG DATA (AEPD/ISM Forum).
- El reglamento GDPR (RGPD) y *ePrivacy* de la UE.
- Novedades del GDPR. Entrada en vigor y ética de *big data*: Retos y oportunidades
- Conclusiones de Seguridad y Privacidad en el GDPR

Principales líneas tecnológicas: H2020*

Principales líneas tecnológicas:

- ❑ Una nueva generación de componentes y sistemas
- ❑ Computación avanzada y tecnologías *cloud*
- ❑ Internet del futuro
- ❑ Tecnologías de los contenidos y gestión de la información
- ❑ Robótica y sistemas autónomos
- ❑ Microelectrónica, nanoelectrónica y fotónica
- ❑ *Internet de las Cosas (IoT)*
- ❑ *Ciberseguridad*

cPPP: 5G, Photonic, Robotics y **Big Data**

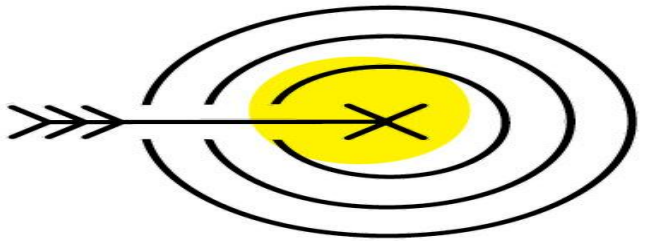
*http://eshorizonte2020.cdti.es/index.asp?MP=88&MS=709&MN=2

TECNOLOGÍAS DISRUPTIVAS

- *Big Data*
- Internet de las Cosas (Drones y Ciudades Inteligentes)
- Inteligencia Artificial Aplicada(*Machine Learning y Deep Learning*)
- *Blockchain* (Cadenas de bloques)
- Ciberseguridad
- 5G

https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/ ... octubre 2017

Top 10 Strategic Technology Trends for 2018



Intelligent

- AI Foundations
- Intelligent Apps and Analytics
- Intelligent Things

Digital

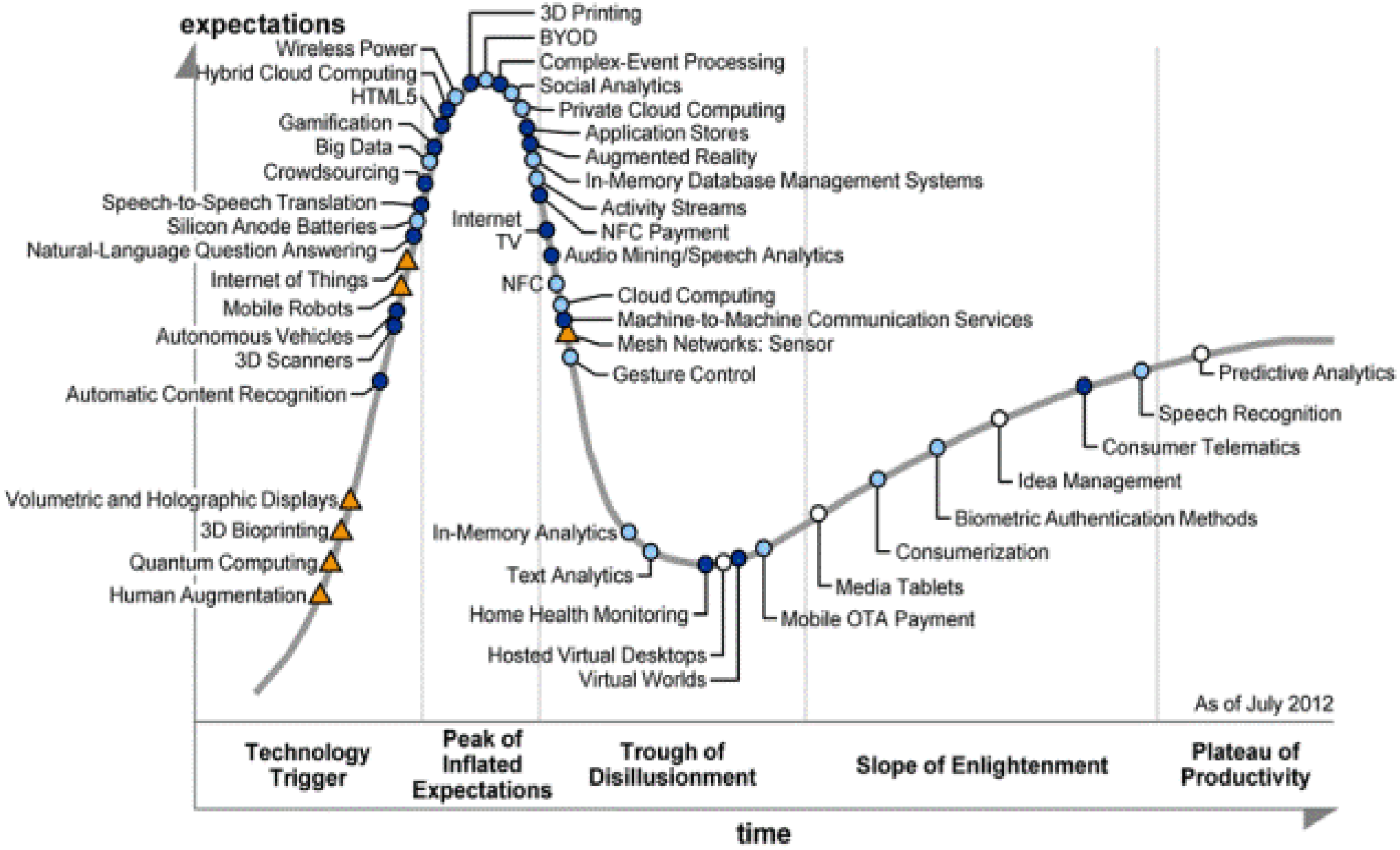
- Digital Twins
- Cloud to the Edge
- Conversational Platform
- Immersive Experience

Mesh

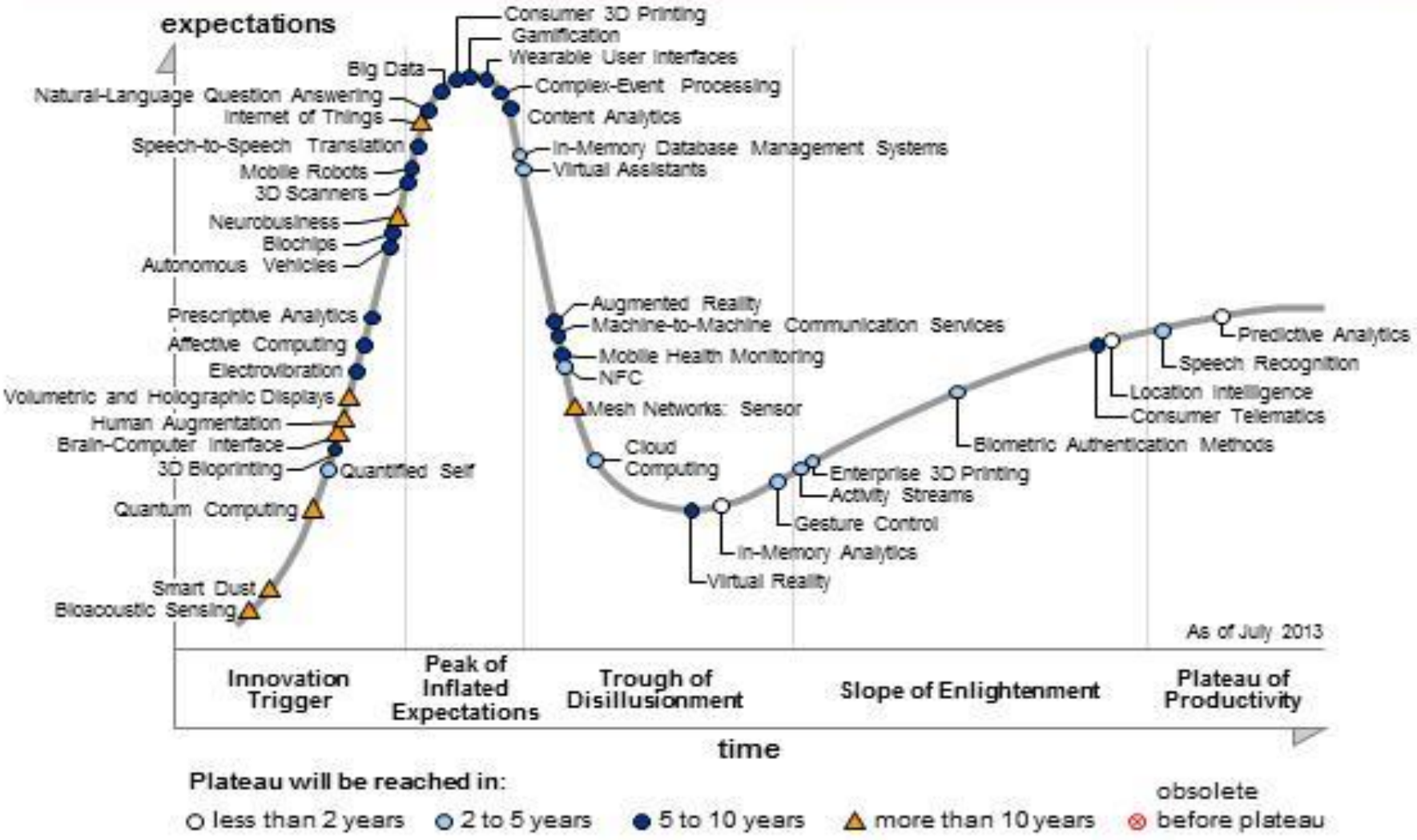
- Blockchain
- Event-Driven
- Continuous Adaptive Risk and Trust

gartner.com/SmarterWithGartner

Gartner

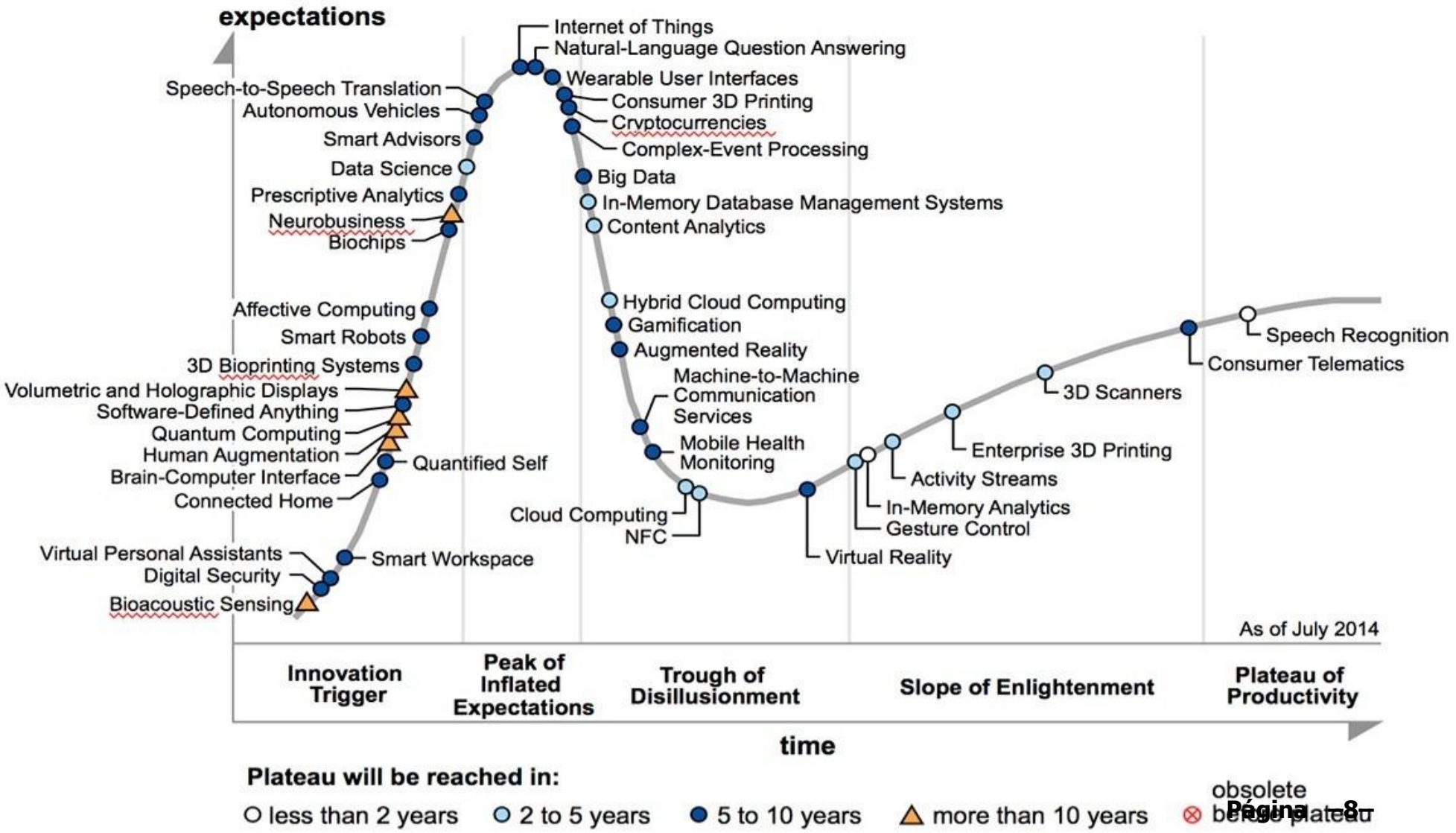

expectations
3D Printing
BYOD
Complex-Event Processing
Social Analytics
Private Cloud Computing
Application Stores
Augmented Reality
In-Memory Database Management Systems
Activity Streams
NFC Payment
Audio Mining/Speech Analytics
Cloud Computing
Machine-to-Machine Communication Services
Mesh Networks: Sensor
Gesture Control
Wireless Power
Hybrid Cloud Computing
HTML5
Gamification
Big Data
Crowdsourcing
Speech-to-Speech Translation
Silicon Anode Batteries
Natural-Language Question Answering
Internet of Things
Mobile Robots
Autonomous Vehicles
3D Scanners
Automatic Content Recognition
Internet TV
NFC
Volumetric and Holographic Displays
3D Bioprinting
Quantum Computing
Human Augmentation
In-Memory Analytics
Text Analytics
Home Health Monitoring
Hosted Virtual Desktops
Virtual Worlds
Predictive Analytics
Speech Recognition
Consumer Telematics
Idea Management
Biometric Authentication Methods
Consumerization
Media Tablets
Mobile OTA Payment
As of July 2012
Technology Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time
Plateau will be reached in:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
obsolete before plateau

Emerging Technologies Hype Cycle, 2013

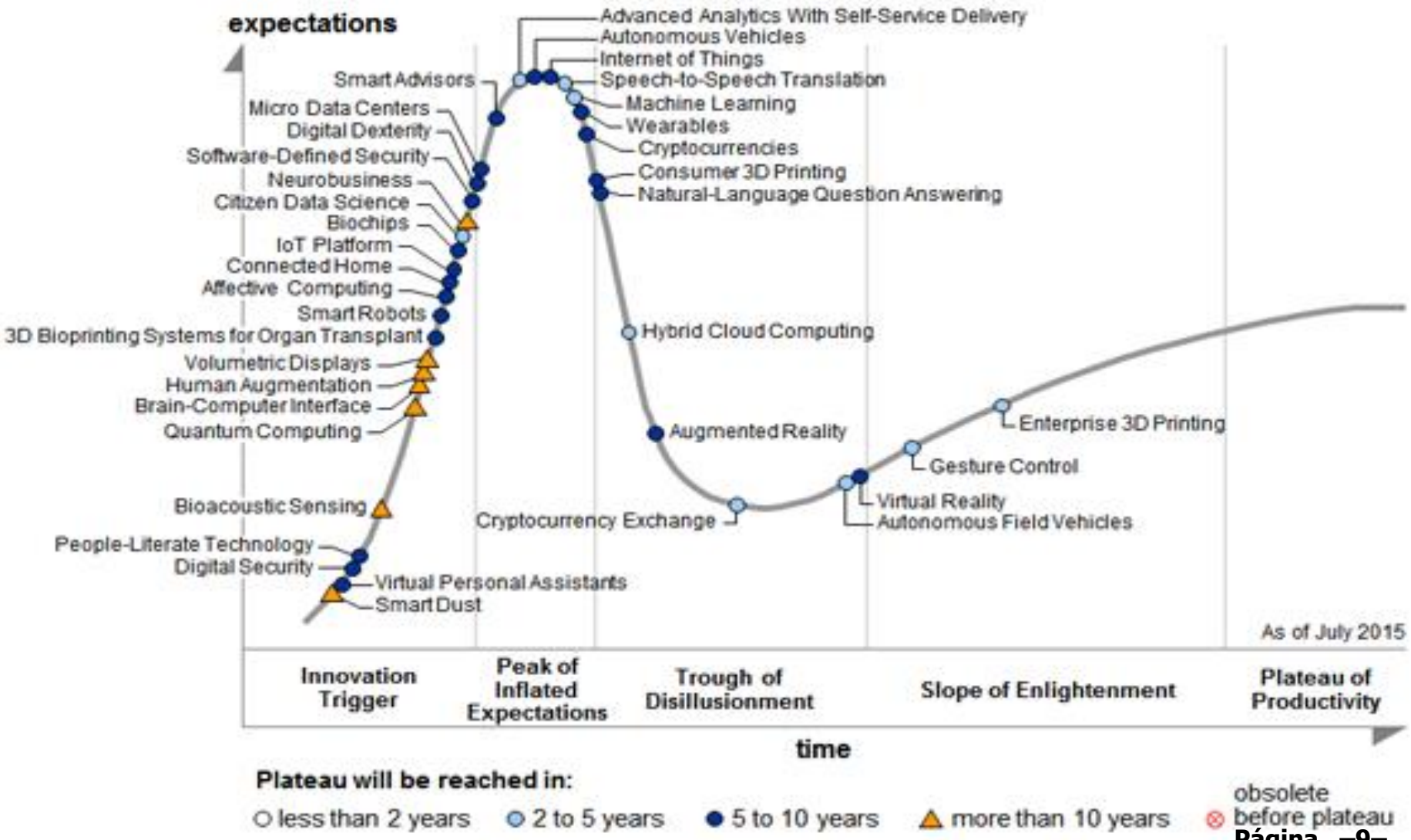


Gartner

Hype Cycle for Emerging Technologies, 2014



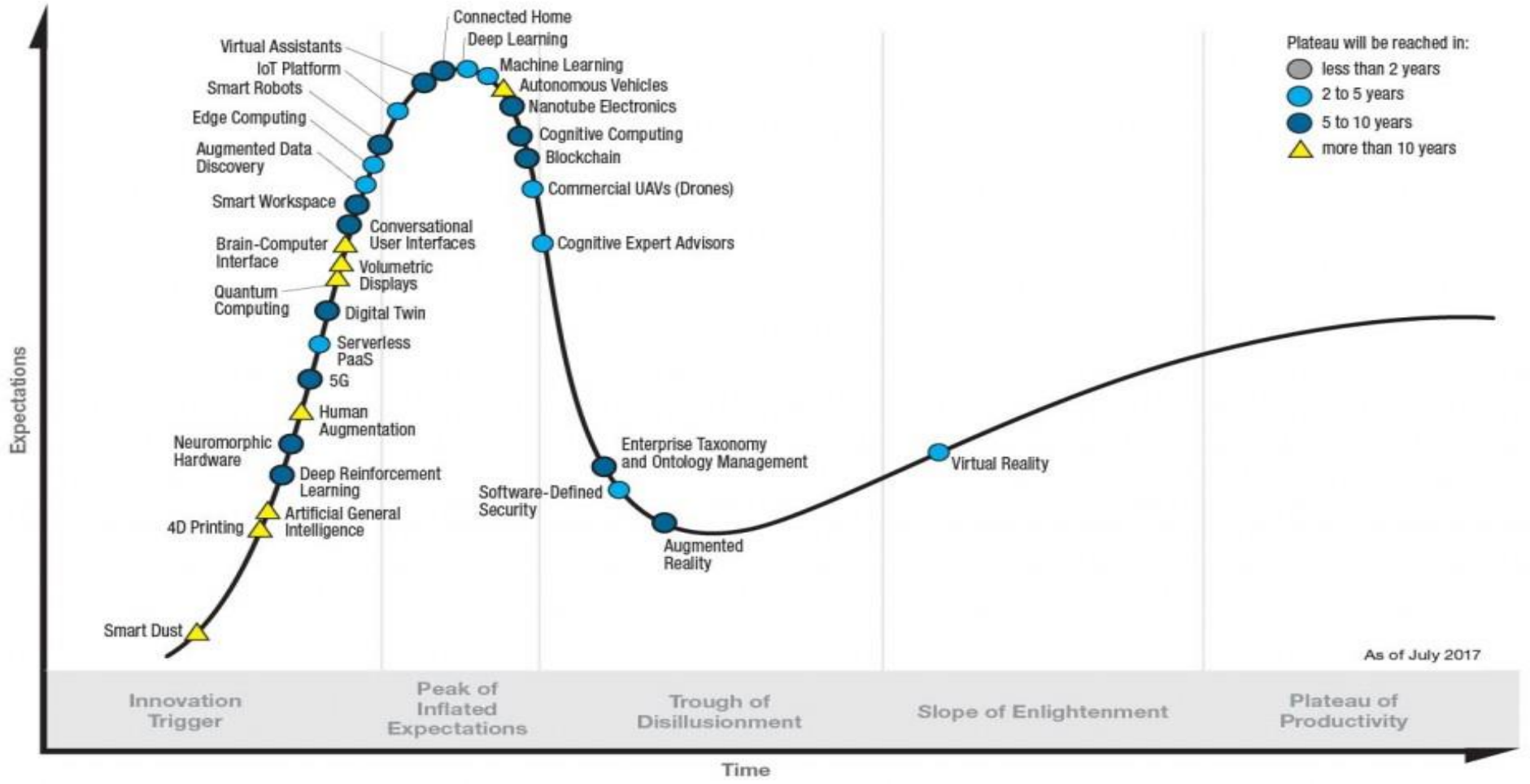
Hype Cycle for Emerging Technologies, 2015



Hype Cycle for Emerging Technologies, 2016

Source: Gartner (July 2016)

Gartner Hype Cycle for Emerging Technologies, 2017



gartner.com/SmarterWithGartner

Source: Gartner (July 2017)

Gartner

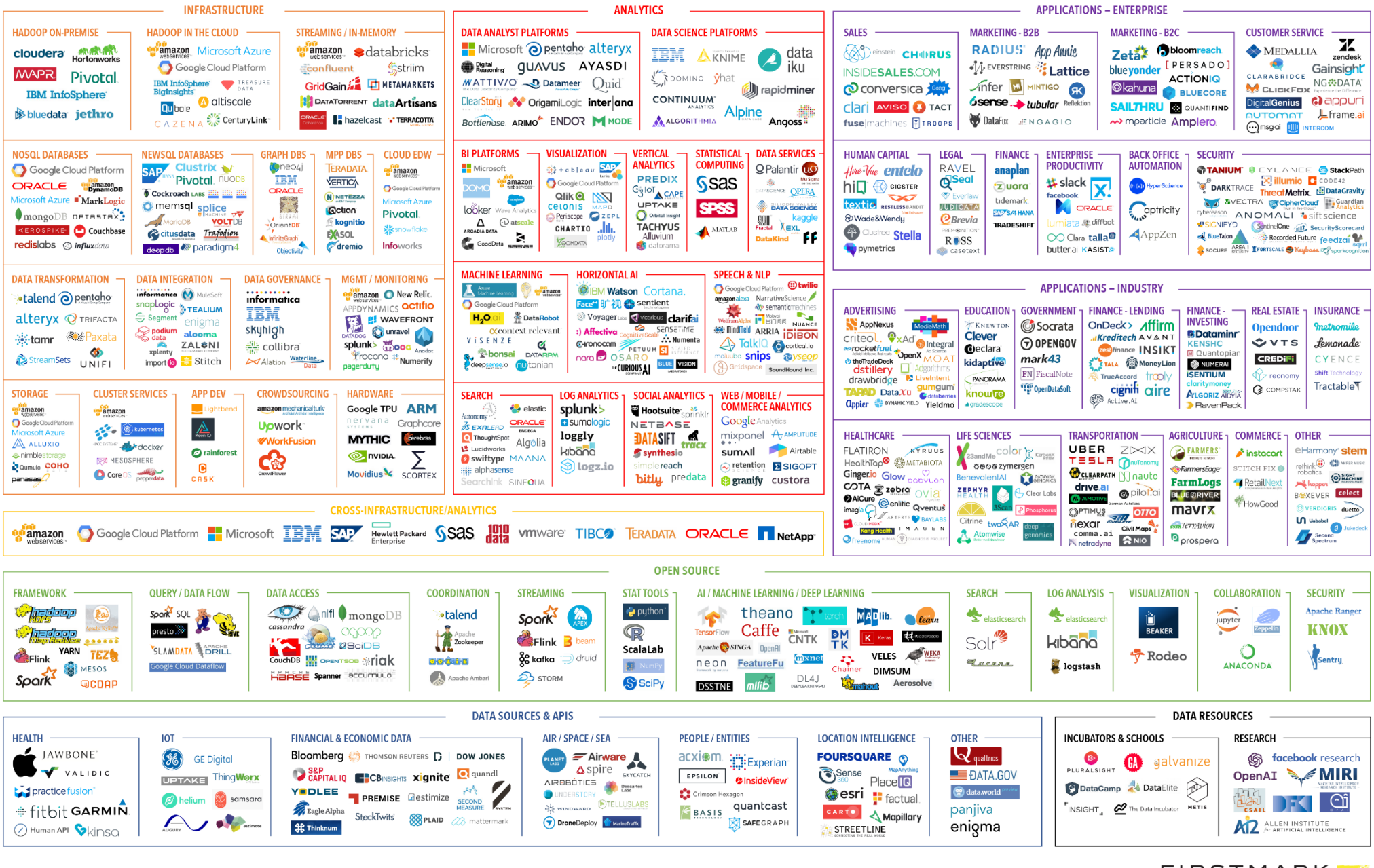
Innovaciones tecnológicas feria CES 2018 de Las Vegas (9-12 enero, 2018).

"TODO GIRA EN TORNO A LOS DATOS"

(*Data Driven*)

- **Inteligencia Artificial Aplicada**… Plataforma DeepThinQ de LG…
- **Asistentes de voz** y **Altavoces inteligentes** (Google, LG,
- **Vehículos autónomos** (Ford, Nissan, Volkswagen, Volvo.. ***Android Auto***)
- **Soluciones de IoT** (Samsung)
- **Aplicaciones de ciudades inteligentes** (Bosch)

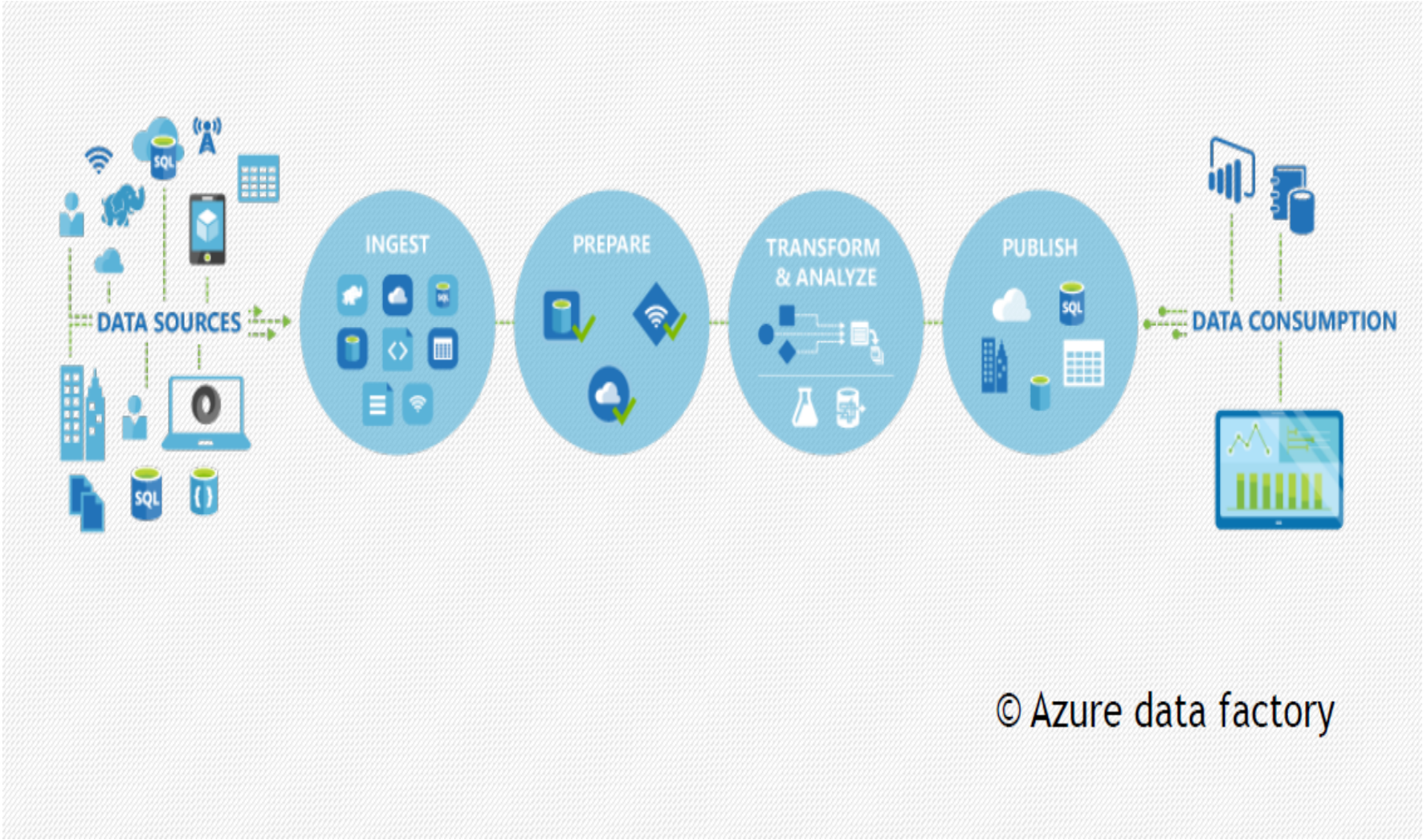
BIG DATA LANDSCAPE 2017



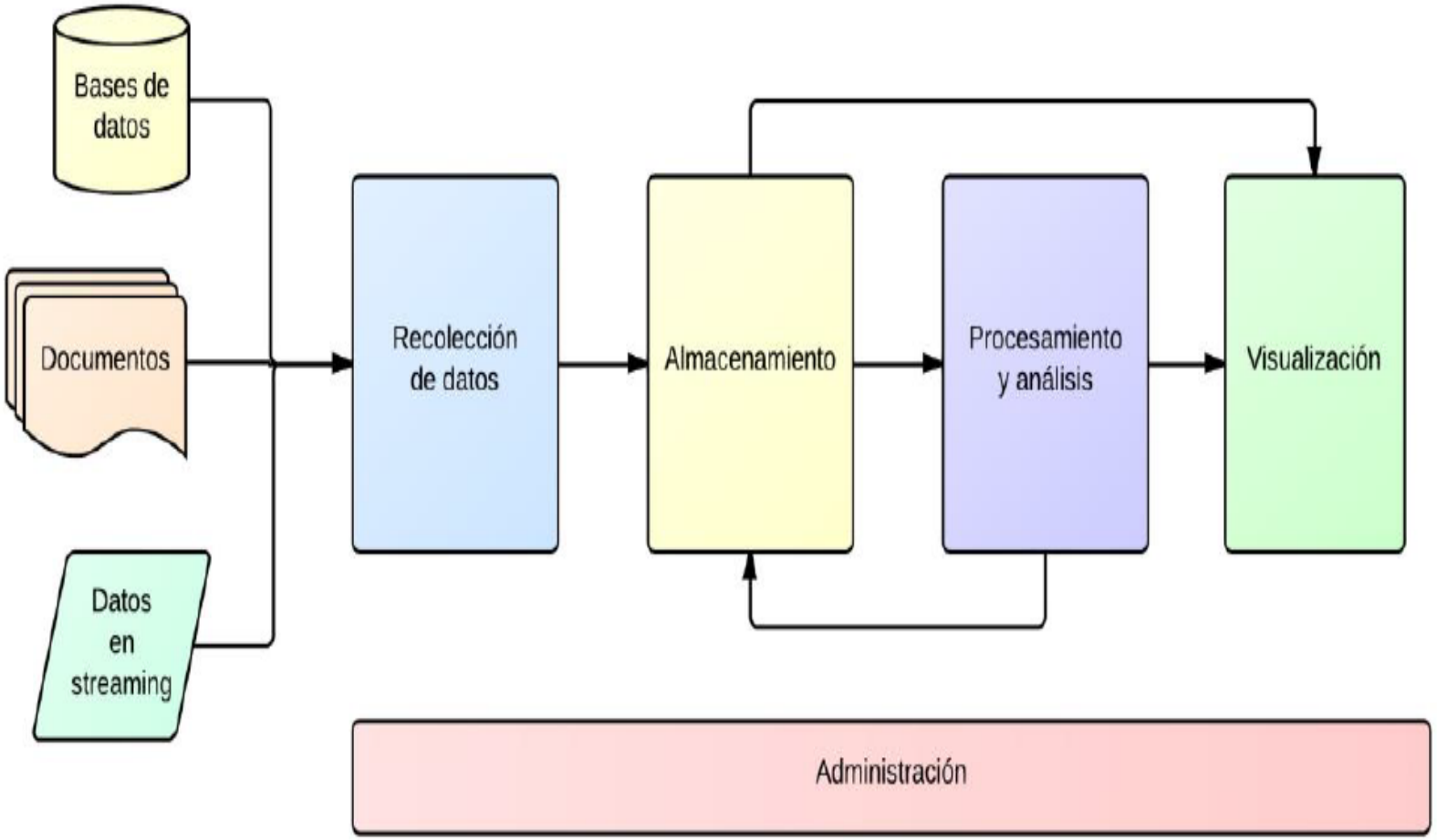
El ciclo de vida de los datos: El caso de *Big Data*

- Las empresas procesan cada vez más datos e información de los usuarios, haciéndose necesaria la regulación del tratamiento de este *Big Data.*
- *Las organizaciones deben asegurarse de que todos los requisitos de seguridad y privacidad* que se aplican a los conjuntos originales de datos sean monitorizados y mantenidos en los procesos de *Big Data* a lo largo del ciclo de vida de la información, desde la recopilación de los datos hasta su divulgación o destrucción.
- **Mantener los requisitos originales de privacidad y seguridad a lo largo del ciclo de vida de los datos.**

ARQUITECTURA DE BIG DATA



ARQUITECTURA DE BIG DATA



Calidad y Seguridad de los datos: Gobernanza de datos

Mantener los requisitos originales de privacidad y seguridad a lo largo del ciclo de vida de la información

- ❑ Calidad de los datos
- ❑ Seguridad de los datos
- ❑ Gestión de datos maestros
- ❑ Gobernanza de los datos
- ❑ Datos personales
- ❑ Protección de datos
- ❑ Privacidad de los datos

Big Data, privacidad y seguridad

- **La Agencia Española de Protección de Datos** y la **Asociación Española para el Fomento de la Seguridad de la Información** han publicado un *Código de Buenas Prácticas para la protección de datos en proyectos Big Data.* referencia práctica para asesorar a las entidades que estén desarrollando o tengan previsto implementar proyectos de este tipo **(basado en GDPR)**
- Apuesta por la explotación de grandes volúmenes de datos *"introduciendo conceptos como* ***gestión del riesgo*** *en los repositorios de datos para analizarlo y diseñar planes de contingencia"* y conseguir *"que las empresas que explotan datos logren recabar* ***el consentimiento*** *informado del usuario, y que éste sepa exactamente para qué se van a utilizar",*

Código de Buenas Prácticas en protección de datos de BIG DATA (AEPD/ISM Forum)*

- *http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf

¿QUÉ ES EL BIG DATA?

- SIGNIFICADO, USOS Y TECNOLOGÍAS DEL BIG DATA.
- *RIESGOS LEGALES, AMENAZAS Y OPORTUNIDADES*.
- *ÉTICA DIGITAL, PRIVACIDAD Y BIG DATA*.
- MARCO DE LA GOBERNANZA.
- PRÁCTICAS HABITUALES EN LOS TRATAMIENTOS.

Código de Buenas Prácticas en protección de datos de BIG DAT (GDPR)

❑ NORMAS Y PRINCIPALES OBLIGACIONES LEGALES EN MATERIA DE PRIVACIDAD.

- RÉGIMEN JURÍDICO APLICABLE.
- RESPONSABLE Y ENCARGADO DEL TRATAMIENTO.
- PRINCIPALES IMPLICACIONES DE LOS TRATAMIENTOS BIG DATA EN PRIVACIDAD.

1. Origen de los datos.
2. Transparencia en la información
3. Calidad de los datos y conservación.
4. Derechos de los interesados.
5. Decisiones individuales automatizadas.

Código de Buenas Prácticas en protección de datos de BIG DATA (GDPR)

❑ PRINCIPIOS Y ASPECTOS PROCEDIMIENTALES.

- PRIVACIDAD DESDE EL DISEÑO.
- "*ACCOUNTABILITY*".
- EVALUACIÓN DE IMPACTO (**EIPD**).
- REUTILIZACIÓN DE DATOS DISOCIADOS.
- RELACIONES CON LA AUTORIDAD DE CONTROL.

❑ MEDIDAS TECNOLÓGICAS PARA LA MEJORA DE LA PRIVACIDAD, SEGURIDAD Y CONFIANZA.

- ESTRATEGIAS DE PRIVACIDAD.
- MEDIDAS TÉCNICAS.
- MEDIDAS PARA MEJORAR LA CONFIANZA.
- BUENAS PRÁCTICAS.

El reglamento GDPR (RGPD) y *ePrivacy* de la UE

- El GDPR reemplaza a la Directiva de Protección de Datos 95/46/EC y se ha diseñado para armonizar las leyes de privacidad de datos en Europa, proteger y habilitar la privacidad de datos a todos los ciudadanos de la UE y remodelar el modo en que las organizaciones de la Región deben enfocar la privacidad de datos.
- www.eugdpr.org

Normativa GDPR*

- El GDPR es una normativa que comenzó a desarrollarse en 2012. Aprobado el **GDPR (General Data Protection Regulation)** por el Parlamento Europeo el 14 de abril de 2016.
- Se publicó en el DOUE el 4 de mayo de 2016 y entró en vigor 20 días después. **Comienza a aplicarse el 25 de mayo de 2018.**
- Hasta esta fecha, la Directiva 95/46 así como las normas nacionales que la trasponen –entre ellas la española- siguen en vigor plenamente válidas y aplicables. *173 consideraciones previas y 99 artículos. 88 páginas*
- *https://www.boe.es/doue/2016/119/L00001-00088.pdf

GDPR *Key Changes* (eugdpr.org)

- **El objetivo del GDPR es proteger a todos los ciudadanos de la UE de la privacidad y las violaciones de datos en un mundo controlado por datos (*data driven*) muy diferente del 1995 en que se estableció la Directiva.**
- **Además de los principios clave de privacidad de datos se han propuesto muchos cambios en las políticas regulatorias.**

GDPR *Key Changes* (eugdpr.org)

- Ámbito territorial ampliado (UE y países relacionados)
- Sanciones
- Consentimiento
- Derechos de los sujetos de datos
- Notificación de brechas o violaciones (en 72 horas)
- Derecho al acceso
- Derecho al olvido
- Portabilidad de datos
- Privacidad por diseño
- DPO (*Data Protection Officer*)
- https://www.eugdpr.org/key-changes.html

GDPR FAQ (eugdpr.org)

1. Cuando entra en vigor el GDPR
2. A quienes afecta el GDPR
3. ¿Cuáles son las sanciones por el no cumplimiento (*non-compliance*)
4. ¿Qué constituyen los datos personales? *Data Subject*
5. ¿Cuál es la diferencia entre un procesador de datos y un controlador de datos?
6. Los procesadores de datos necesitan un consentimiento del sujeto de datos "explícito" o "no ambiguo" y cual es la diferencia.

GDPR FAQ (eugdpr.org)

7. ¿Qué pasa con los sujetos de datos menores de 16 años?

8. ¿Cuál es la diferencia entre un Reglamento (*Regulation*) y una Directiva.

9. Obligatoriedad de un Delegado de Protección de Datos (DPO).

10. ¿Cómo afecta el GDPR a las políticas relacionadas con las violaciones de datos?

11. GDPR establecerá una ventanilla única para la regulación de privacidad de datos

https://www.eugdpr.org/gdpr-faqs.html

ESTRUCTURA DEL GDPR

88 págs. : 173 consideraciones previas; 9 Capítulos y 99 artos.

- **4. Definiciones de términos**
- **17. Derecho de supresión (El derecho al olvido)**
- **20. Derecho a la portabilidad de los datos**
- **25. *Protección de datos desde el diseño y por defecto***
- **32. Seguridad del tratamiento: *Seudonimización* y cifrado de datos personales.**

SELECCIÓN DE ARTs GDPR

- 33. Violación de la seguridad de los datos
- 35. Evaluación de impacto relativa a protección de datos
- 37. Designación del DPO
- 39. Funciones del DPD
- 42. Certificación
- 43. Organismos de certificación
- 68. Creación del Comité Europeo de Protección de Datos

¿a quién se aplica el GDPR?

- Los "controladores" y los "procesadores" de datos deben atenerse al GDPR.
- **Un controlador de datos indica cómo y por qué se procesan los datos personales, mientras que un procesador es la parte que realiza el procesamiento real de los datos.**
- *El controlador podría ser cualquier organización, desde una empresa con fines de lucro hasta una organización benéfica o un gobierno. Un procesador podría ser una empresa de TI que realice el procesamiento de datos real.*

IBM. https:// www-01.ibm.com/events/wwe/grp/grp309.nsf/vLookupPDFs/IBM%20Evento%20GDPR%20Julia%20Urio/$file/IBM%20Evento%20GDPR%20Julia%20Urio.pdf [https://ibm.co/2Dv8I2v]

GDPR Preparación Técnica
Áreas de actuación

IBM

Desde el Diseño y por Defecto

- Los responsables en el tratamiento deben asegurar medidas técnicas y organizativas que demuestren el cumplimiento con los principios principales de GDPR
- Tener en cuenta el derecho a la protección de datos cuando se desarrollan y diseñan productos, servicios y aplicaciones basados en el tratamiento de datos personales

IBM InfoSphere | IBM StoredIQ

Derechos de los ciudadanos Europeos

- Más derechos sobre los datos personales incluyendo: información, acceso, rectificación o borrado de datos personales, el derecho a la portabilidad de los datos y el derecho de oposición
- La limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos

IBM InfoSphere | IBM Optim Archiving, TDM | IBM StoredIQ

Responsabilidad de Cumplimiento

IBM InfoSphere

- Necesidad de demostrar cumplimiento en el tratamiento de los datos personales con el presente reglamento GDPR.
- Asegurar que los datos son tratados de forma legal, transparente, de forma compatible y que son adecuados, pertinentes y limitados en relación con los fines que son tratados

IBM StoredIQ | IBM Optim Archiving, TDM

Security of Personal Data

IBM Optim Archiving, TDMOP

- Obligación de implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo
- Incluye notificación en 72H a la autoridad de control competente y sin dilación indebida al interesado en escenarios de alto riesgo para sus derechos y libertades

Legalidad y Consentimiento

IBM InfoSphere MDM for Individual | IBM Case Manager | IBM Stewardhip Centre

- Procesamiento legal si: consentimiento, necessario para ejecutar contrato con el interesado, obligación legal, protección, interes público o legítimo o autoridad oficial
- El consentimiento debe ser una manifestación explícita, con voluntad libre, específica, informada e inequívoca

VOCABULARIO (eudgrp.org). Art. 4

- **«consentimiento del interesado»:** toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;
- **«violación de la seguridad de los datos personales»:** toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

¿Qué son datos personales bajo el GDPR?

❑«datos personales»:

- ❑ toda información sobre una persona física identificada o identificable **(«el interesado»);** se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, direcciones IP, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, **información económica, cultural o de salud mental**

Nuevas obligaciones para organizaciones, empresas y administraciones

- Será obligatorio designar un **Delegado de Protección de Datos (DPO),** interno o externo, que asista a las organizaciones en el proceso de cumplimiento normativo.
- Realizar **EVALUACIONES DE IMPACTO SOBRE LA PRIVACIDAD**
- Las empresas multinacionales tendrán como interlocutora a una sola autoridad de control nacional. Establecimiento principal de la entidad: **VENTANILLA ÚNICA**.
- Las **VIOLACIONES DE SEGURIDAD** deberán ser comunicadas a las autoridades de control y, en casos graves, a los afectados, tan pronto sean conocidas, estableciéndose el **plazo máximo de 72 horas.**

Nuevas obligaciones para organizaciones, empresas y administraciones

- **DATOS SENSIBLES:** Se amplían los datos especialmente protegidos, incluyendo ahora los **datos genéticos y biométricos.**
- La **SELECCIÓN de un encargado del tratamiento** se endurece, puesto que habrá que elegir uno que aporte suficientes garantías de cumplimiento normativo.
- **GARANTÍAS ADICIONALES PARA LAS TRANSFERENCIAS INTERNACIONALES DE DATOS:** Establecimiento de garantías más estrictas y mecanismos de seguimiento en relación con las transferencias internacionales de datos fuera de la Unión Europea.

Nuevas obligaciones para empresas, organizaciones y administraciones

- **SELLOS Y CERTIFICACIONES:** Se crean sellos y certificaciones de cumplimiento que permiten acreditar la ***Accountability*** por parte de las organizaciones.
- **DESAPARECE LA OBLIGACIÓN DE INSCRIBIR LOS FICHEROS**, que se sustituye por un control interno y, en su caso, un inventario de las operaciones de tratamiento de datos que se realicen.
- **SANCIONES:** Las cuantías de las sanciones por incumplimiento de la norma crecen, ***pudiendo llegar a los 20 millones de euros o el 4% de la facturación global anual***

Derechos de los ciudadanos europeos

- **TRANSPARENCIA e INFORMACIÓN.** Las organizaciones, al tratar datos personales, deben proporcionar mayor información y de un modo más inteligible, completo y sencillo, lo que favorecerá la toma de decisiones por el ciudadano. Se tiene una especial consideración con los menores de edad en este punto.

- **CONSENTIMIENTO. El consentimiento para poder tratar datos de carácter personal ha de ser inequívoco, libre y revocable y deberá darse mediante un acto afirmativo claro (no sirve por defecto). No se admite consentimiento tácito. En caso de silencio se entiende que no se ha prestado el consentimiento**

Derechos de los ciudadanos europeos

- **DERECHO AL OLVIDO.** Se podrá revocar el consentimiento prestado para el tratamiento de datos personales en cualquier momento, pudiendo exigir la supresión y eliminación de los datos en redes sociales o buscadores de internet.
- **DERECHO A LA LIMITACIÓN DEL TRATAMIENTO.** Permite al ciudadano solicitar el bloqueo temporal del tratamiento de sus datos cuando existan controversias sobre su licitud.
- **PORTABILIDAD DE LOS DATOS.** Se permitirá al ciudadano solicitar la transferencia de los datos personales de un proveedor de servicios en Internet a otro.

Derechos de los ciudadanos europeos

- **INDEMNIZACIONES.** Se reconoce la posibilidad de exigir indemnización de daños y perjuicios derivados del tratamiento ilícito de los datos personales.
- El responsable del fichero podrá establecer un **CANON** a la contestación de los ejercicios del derecho de acceso, teniendo en cuentas los costes administrativos que ello le suponga.
- **DENUNCIAS.** Se podrán presentar denuncias a través de asociaciones de usuarios.

PROTEGER LA PRIVACIDADAD DEL USUARIO

- Una vez que los datos han sido identificados, **es importante comenzar a evaluar los datos, incluyendo cómo se están produciendo y protegiendo**.
- **Con cualquier dato o aplicación, la primera prioridad debe ser proteger la privacidad del usuario**

PROTEGER LA PRIVACIDADAD DEL USUARIO

- **Las empresas deben completar una Evaluación de Impacto de la Privacidad (PIA) y la Evaluación de Impacto de la Protección de Datos (DPIA) de todas las políticas de seguridad, evaluando los ciclos de vida de los datos desde el origen hasta su destrucción.**

CONTROLADORES Y PROCESADORES

- El nuevo Reglamento distingue entre los controladores de datos y los procesadores de datos (tal como lo hace la directiva actual). **El controlador de datos** es la organización que determina los propósitos y medios del procesamiento de datos personales, mientras que un **procesador** es alguien que procesa los datos en nombre de otros.
- ***La mayoría de las organizaciones modernas caen bajo la definición de controlador***.
- Los procesadores también tendrán obligaciones como las que se oponen hoy en día cuando el controlador tiene la plena responsabilidad. Como ejemplo, los procesadores tendrán que informar de las infracciones de datos a partir de mayo de 2018 y tienen la obligación de informar al controlador de datos si sospechan que una instrucción de procesamiento de datos no se ha realizado de forma correcta.

Expansión, Economía Digital 9 enero, 2018

- "*Hasta ahora, las normativas sobre protección de datos habían sido responsabilidad en gran parte de "**los controladores de datos",** que determinan por qué y cómo se recopila la información personal, en lugar de los "**procesadores de datos",** que albergan la información. Sin embargo, el reglamento hará que los procesadores se encarguen de ceder o eliminar los datos que se exijan. Este cambio reestructura fundamentalmente las normas de empresas de servicios en la nube como **Microsoft, IBM, Amazon y Google**, que almacenan la información de pymes de todo el mundo. Muchas empresas subcontratan a terceros, lo que complicaría aún más que una persona pidiese que se eliminaran sus datos*".

DATA PROTECTION OFFICER

- El DPO no implementa soluciones. Verifica la efectividad de las soluciones implantadas según la normativa.
- **El DPO debe tener una formación y experiencia multidisciplinar con conocimientos jurídicos, técnicos, tecnológicos**.
- Se están implantando certificaciones del DPO. Se estudia la certificación internacional o por país.
- **En España, la AEPD en colaboración con la ENAC (Entidad Nacional de Acreditación) han elaborado un Esquema de Certificación para la figura de Delegado de Protección de Datos (DPO)**
- http://tecnologia.elderecho.com/tecnologia/privacidad/Protection-Officer-DPO-Reglamento-Proteccion-Datos-UE_11_945055002.html

DATA PROTECTION OFFICER

- **Organizaciones y empresas pueden solicitar la acreditación de ENAC para la certificación del DPD.**
- Todas las entidades que quieran certificar en el esquema de certificación deben estar acreditadas por ENAC conforme a la **norma UNE-EN ISO/IEC 17024:2012** (certificación de personas acreditadas por ENAC conforme a la norma ISO 17024)

PROTECCIÓN Y PRIVACIDAD DE DATOS EN ASISTENTES DE VOZ . CHATBOTS

- **Google Assistant … integrado en LG, Sony…**
- **Siri de Apple, Alexa de Amazon, altavoz Echo, Bixby de Samsung, Cortana de Microsoft**
- **Chatbots de empresas…**
- **¿Cómo son de seguros?**
- Estos dispositivos inteligentes manejan determinadas funciones del hogar, lugar de trabajo.. y tienen capacidad para escuchar y grabar conversaciones.

ANONIMIZACIÓN

- **Anonimizar (DRAE).** ***Expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad.***
- Disociar los datos de manera tal que no se permita la identificación de un afectado o interesado
- La anonimización implica el tratamiento de datos con carácter personal de modo tal que no sea posible volver a identificarlos.
- Datos personales (están sujetos a las normas de protección de datos). Datos anonimizados (conjunto de datos que no pueden identificar a un sujeto de derecho), la normativa de protección de datos no se aplica.
- ***Seudonimita.*** No existe en el DRAE

Consideraciones previas GDPR

- (28) La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.

Consideraciones previas GDPR

- (29) Para incentivar la aplicación de la ***seudonimización*** en el tratamiento de datos personales, debe ser posible establecer medidas de **seudonimización**, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas. 4.5.2016 L 119/5 Diario Oficial de la Unión Europea ES

Seudonimización (GDPR)

- El **Reglamento General de Protección de Datos**, introduce explícitamente en su artículo 32, relativo a la seguridad en el tratamiento de los datos personales, la **seudonimización** como una medida apropiada para garantizar un nivel de seguridad adecuado al riesgo.

Seudonimización (GDPR)

«seudonimización»:

el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

¿Es lo mismo *seudonimización* que *anonimización*?

- **No.** ***Un dato es anonimizado cuando en ningún caso sea posible la vinculación del dato con la persona a la que hubiese identificado. Es decir, cuando sea imposible volver a identificar a la persona a través de ese dato.***
- **Por el contrario, la *seudonimizacion* se reduce a limitar la trazabilidad entre el conjunto de datos tratados y la persona física cuya identidad queda asociada a estos.**
- **La vigente LOPD contempla anonimización pero no seudonimización. Según expertos en tratamiento de datos personales la anonimización es un proceso más integro.**

¿Cuáles serían las técnicas de seudonimización más habituales?

- **Dictamen 05/2014 del Grupo de Trabajo sobre Protección de Datos de Carácter del artículo 29,** de 10 de abril de 2014, las técnicas más relevantes serían:

- **Cifrado con clave secreta.**
- **Función hash:**
- **Función con clave almacenada:**
- **Cifrado determinista o función hash con clave de borrado de clave:**
- **Descomposición en tokens:**

PRIVACIDAD - ePrivacy

- ***ePrivacy*. Nuevo Reglamento de Privacidad de la UE. Previsible entrada en vigor el mismo día que EL GDPR. Primer borrador aprobado el 10-01-2017.**
- **ePrivacy establecerá una normativa conjunta para velar por la confidencialidad, seguridad y privacidad de los ciudadanos europeos. Sustituye a la actual Directiva 2000/58/CE y necesita ser adaptada para alinearla con las nuevas reglas del GDPR.**
- *Reglamento, en lugar de una directiva, crea un marco normativo europeo idéntico que otorgue la misma protección a empresas y consumidores, con independencia del país de procedencia de éstos*

PRIVACIDAD - ePrivacy

- https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation
- europa.eu/rapid/press-release_IP-17-16_es.pdf
- **New players**: privacy rules will in the future also **apply to new players providing electronic communications services such as WhatsApp, Facebook Messenger and Skype**. *This will ensure that these popular services guarantee the same level of confidentiality of communications as traditional telecoms operators.*

Reglas más sencillas sobre cookies

- Se racionalizará la denominada «disposición sobre cookies», que ha dado lugar a un exceso de solicitudes de autorización a los usuarios de internet.
- Simplificación sobre las políticas de cookies, debiendo ofrecer al usuario final un método sencillo y transparente de aceptación de cookies, utilizando los ajustes adecuados de un navegador u otra aplicación y **dando la posibilidad a los usuarios de aceptar o no las *cookies* que deseen**, eligiendo, por ejemplo, si aceptan *cookies* de terceros o propias.

Protección contra *Spam*

- **Comunicaciones electrónicas no deseadas (*Spam*). La propuesta prohíbe las comunicaciones electrónicas no solicitadas por cualquier medio (correo electrónico, mensajes de texto, llamadas telefónicas), si los usuarios no han dado previamente su consentimiento.**
- Quienes realicen llamadas comerciales deberán indicar su número de teléfono o utilizar un prefijo especial que indique que se trata de una llamada de este tipo

Metadatos

- El contenido de las comunicaciones electrónicas puede revelar información altamente sensible sobre las personas físicas involucradas en la comunicación.
- Igualmente, los **metadatos** derivados de las comunicaciones electrónicas (número de teléfono, páginas web visitas, geolocalización, etc.) también pueden revelar información muy sensible y personal, por lo que se deberá garantizar su confidencialidad.
- Las normas de privacidad también tendrán por objeto los nuevos proveedores de servicios de comunicaciones electrónicas, como WhatsApp, Facebook Messenger, Skype, Gmail, etc.

Metadatos

- **Contenido y metadatos de las comunicaciones**: La privacidad estará garantizada para el contenido y los metadatos derivados de las comunicaciones electrónicas (por ejemplo, hora y lugar en que se efectúa una llamada).

- Ambos tienen un alto componente de privacidad y, en virtud de las normas propuestas, deberán anonimizarse o suprimirse si los usuarios no han dado su consentimiento, salvo que se necesiten los datos, por ejemplo, para la facturación

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- **Incluir la protección de datos desde el inicio del diseño de nuevos productos o servicios.**
- Se ha de adoptar la **privacidad desde el diseño** que supone asumir un compromiso con la seguridad punto a punto, desde la creación y almacenamientos de los datos hasta que se eliminan o quedan obsoletos.
- **Privacidad por defecto**. Las opciones de protección de datos deben ser las máximas por defecto y es opcional para el interesado la posibilidad de rebajarlas.

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- Este derecho implicará que los controladores de protección de datos deberán trabajar estrechamente con diseñadores y desarrolladores desde el principio de cualquier proyecto tecnológico que implique tratamiento de datos. Es obligatorio establecer medidas de protección de datos y considerar la privacidad desde la fase inicial de diseño. Será obligatorio desde la entrada en vigor de GRPD.
- **El derecho por defecto** garantiza el máximo grado de privacidad ya que solo se podrán recoger los datos personales específicos para un proyecto determinado. Incluso si un servicio permite compartir datos con terceros, esta opción ha de ser activada por el usuario.

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- El responsable de tratamiento de datos deberá adoptar políticas internas y aplicar medidas técnicas y operativas para poder cumplir con los principios de protección de datos desde el diseño y por defecto.
- Se debe regular la privacidad desde el diseño como elemento fundamental antes de acometer cualquier proyecto tecnológico que implique tratamiento de datos.
- **Los especialistas en protección de datos se han de involucrar con los desarrolladores y otros profesionales en la fase de diseño de los proyectos**.
- **Los proyectos de privacidad se deben realizar desde el principio**

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- La novedad que afecta más directamente al ámbito de las seguridad consiste en la introducción del principio de protección de datos desde el diseño y por defecto..
- **La ciberseguridad y la protección de datos se debe tener presente mediante un modelo que combine tecnología, procesos y personas** y es necesario incorporar al núcleo del negocio la seguridad y privacidad por defecto desde el diseño e involucrar a todos los departamentos desde los primeros momentos, y en particular, a la dirección.

APROBACIÒN nueva LOPD -10 Nov 2017

- Consejo de Ministros
- **El Gobierno aprueba el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal**
- **Aprobado el proyecto de ley orgánica de protección de datos de carácter personal**
- *Viernes 10 de noviembre de 2017*
- Tiene como objetivos aumentar la seguridad jurídica y adaptar la normativa a la evolución tecnológica.
- Regula la potestad de los herederos sobre la información de personas fallecidas.
- Se aplicará a partir del próximo 25 de mayo de 2018.

NUEVAS FRONTERAS DE LA ÉTICA Y LA PRIVACIDAD

Luis Joyanes Aguilar

NUEVAS FRONTERAS DE LA ÉTICA

- ¿Qué hacer? ¿Nos fiamos del asesoramiento del algoritmo?
- Los algoritmos refuerzan las nuevas fronteras de la ética.
- Protección de datos. ***Multa (11 de septiembre, 2017) de la AEPD a Facebook 1,2 milones de €*** por no respetar la privacidad y protección de datos de los usuarios de la red social. **La Agencia ha detectado dos infracciones graves y una muy grave en el tratamiento de los datos**

ÉTICA EN LA NUBE y en BIG DATA

- **Big Data, Inteligencia Artificial, Robótica, Internet de las Cosas:**
- La inteligencia artificial (IA) y la robótica - especialmente los **robots humanoides, robots colaborativos "cobots" y los asistentes virtuales "bots" y "chatbots"**- apoyados en la expansión de ***big data***, plantean un desafío ético en el uso de los robots y los límites en el caso de la inteligencia artificial. Otra tendencia imparable es el **uso de algoritmos** como herramientas de control de todo tipo de máquinas y aplicaciones de software de IA.

ÉTICA Y GOBIERNO DE LOS ALGORITMOS

- La sociedad está "gobernada" por los algoritmos.
- Se requiere un análisis ético y control de las múltiples formas con las que un algoritmo puede impactar en la sociedad.
- CAMPOS DE ESTUDIO
  - Ética de la Inteligencia Artificial
  - Ética de los datos (Big Data e Internet de las Cosas)
  - Ética algorítmica (ética de los algoritmos)

Yucal Noah Harari (Autor de Sapiens)

Harari (autor de Sapiens y de Homo Deus)

- **El mundo va a cambiar radicalmente gracias a los algoritmos, el big data y la inteligencia artificial**, y de ahí podremos extraer las mejores soluciones.
- El mundo no se dividirá entre ricos y pobres, sino en superhumanos mejorados, humanos que les resultan útiles y una enorme masa prescindible
- Según Harari, la ciencia converge en un dogma universal que afirma que los organismos, incluido el ser humano, no son más que algoritmos y que la vida es procesamiento de datos. Pronto **los algoritmos nos conocerán mejor que nosotros mismos**. ¿Tiene sentido, entonces, que dejemos en sus manos nuestro futuro? ¿Deben tomar ellos nuestras decisiones? **La respuesta de Harari es afirmativa**

Algoritmos, robots, chatbots…

- Muchas de las decisiones cotidianas las toma un modelo matemático basado en un algoritmo
- **¿Se requiere una ética especial de los algoritmos?**
- ¿Se requiere una ética especial para los robots humanoides, robots colaborativos, robots virtuales? (asistentes virtuales como Siri, Alexa de Amazon…)
- **¿Deben pagar impuestos los robots igual que las personas a las que pueden sustituir?**
- **¿Cómo controlar la toma de decisiones de los algoritmos?**
- **Los dilemas éticos del Big Data**

DECLARACIÓN DE BARCELONA DE IA

- **Encuentro "Inteligencia Artificial, sueños, riesgos y realidad".**
- **Un grupo de científicos internacionales aprobó (9 y 10 de marzo, 2017) el MANIFIESTO "Declaración de Barcelona"*, las primeras recomendaciones sobre un uso "adecuado y ético" de la inteligencia artificial (IA), que propone medidas para evitar los posibles usos maliciosos de los sistemas basados en IA en Europa.**

DECLARACIÓN DE BARCELONA DE IA

- Los expertos mostraron los **beneficios y la importancia que la IA** tiene para el futuro de la economía y del funcionamiento de la sociedad europea, **pero reclamaron prudencia y la implementación de requisitos al usar las aplicaciones de IA para garantizar su fiabilidad y seguridad**

- *http://www.lavanguardia.com/vida/20170311/42782031262/cientificos-alertan-de-los-usos-maliciosos-de-la-inteligencia-artificial.html

LEYES SOBRE ROBÓTICA (UE) 13/06/2017

- El **Parlamento Europeo** ha aprobado una resolución para que la **Comisión Europea** empiece a estudiar **leyes** sobre **robótica**. El informe insta a la Unión Europea a sentar las bases de una legislación sobre inteligencia artificial y robótica.
- Creación a largo plazo de un "estatus jurídico específico" de **"persona electrónica" con "derechos y obligaciones"** que se aplique al menos a los robots más sofisticados. Entre esas obligaciones se incluiría la *posibilidad de pagar cotizaciones a la Seguridad Social, pensiones*. Asimismo, quiere que estén equipados con un **"botón de la muerte"** que permita desconectarlos si amenazan la vida de un ser humano.

Conclusiones de Seguridad y Privacidad en BIG DATA

Entrada en vigor del GDPR (25 mayo, 2018)

- **BIG DATA** seguirá ofreciendo grandes beneficios que compensarán los riesgos que entraña su implantación.
- **GDPR** es una nueva norma sobre seguridad y privacidad de los datos (big data)
- La entrada en vigor en toda la UE del nuevo **GRPD (RGPD)** ofrece grandes retos pero numerosas oportunidades para organizaciones y empresas.
- La entrada en vigor (en paralelo con el GRPD) del reglamento **ePrivacy** ofrecerá plenas garantías de privacidad en la Unión Europea

MUCHAS GRACIAS

ljoyanes@fidesol.org

joyanes@gmail.com

www.facebook.com/joyanesluis

¿PREGUNTAS?

[FIDESOL]
CalT Centro de apoyo a la Innovación Tecnológica
10° ANIVERSARIO 2006 - 2016

Prof. Luis Joyanes Aguilar

BIBLIOGRAFÍA

- **DOUE (UE).** *Reglamento (UE) 2016/79 del Parlamento Europeo y del Consejo, 27 de abril de 2016. Publicado el 4/05/2016.*

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

- **UE. eugdpr.org.** Sitio Web oficial de GDPR de la UE.
- **SAÍZ,** (coord.). *Código de buenas prácticas en protección de datos para proyectos de Big Data*. AEPD/isms Forum, mayo 2017.
  http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf

BIBLIOGRAFÍA

- **KAELBLE,** Steve. GDPR *Compliance for dummies. Wiley, 2018.* Edición especial de Informatica. 2018.
- **AEPD.** *Guía del Reglamento General de Protección de Datos para responsables de Tratamiento*. AEPD/apdcat/Agencia Vasca de Protección de Datos, 2016.
- **FPF**. Future of Privacy Forum / NSF/ RCN. htpps://rcn.fpf.org
- **AEPD.** *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. 2016

BIBLIOGRAFÍA

- **AEPD/INCIBE. (2016)** *Guía de Privacidad y Seguridad en Internet.* Madrid: León, 2016. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Privacidad_y_Seguridad_en_Internet.pdf.

- **APARICIO, J. P y BATUECAS, A.** (2015). *En torno a la privacidad y la protección de datos en la sociedad de la información*. Granada: Editorial Comares.

- **GIL, ELENA.** (2016) *Big data, privacidad y protección de datos*. Madrid: AEPD/Agencia Estatal BOE, 2016.

BIBLIOGRAFÍA

- JOYANES, Luis (2013). Computación en la nube. Estrategias de cloud computing en las empresas. Barcelona: Marcombo; México DF: Alfaomega
- JOYANES, Luis (2014). *Big Data. El análisis de los grandes volúmenes de datos*. Barcelona: Marcombo; México DF: Alfaomega.
- JOYANES, Luis (2016). *Sistemas de Información. Un enfoque dirigido a la empresa.* Barcelona: Marcombo; México DF: Alfaomega
- JOYANES, Luis (2017). *INDUSTRIA 4.0: La Cuarta Revolución Industrial.* Barcelona: Marcombo y Alfaomega: CDMX

BIBLIOGRAFÍA

- **HARARI,** Yuval Noah (2016). *Homo Deus*. *Breve historia del mañana*. Barcelona: Debate.
- **O´NEIL, Cathy (**2016). *Weapons of Math Destruction. How Big Data increases ineguality and threatens democracy*. Crown Random House. [en línea] https://weaponsofmathdestructionbook.com/
- **SADIN,** Éric (2017). *La humanidad aumentada. La administración digital del mundo*. Traducción de Javier Blanco y Cecilia Paccazochi. Caja Negra, 2017.
- **SCHWAB, Klaus** (2016). *La cuarta revolución industrial*. Barcelona: DEBATE.

NTICS

tecnología

Industria 4.0

LA CUARTA REVOLUCIÓN INDUSTRIAL

Big Data (grandes volúmenes de datos o macrodatos) supone la confluencia de una multitud de tendencias tecnológicas que venían madurando desde la primera década del siglo cuando han explosionado e irrumpido con gran fuerza en organizaciones y empresas, en particular, y en la sociedad, en general. Muchas veces estos datos no están estructurados, esta tecnología viene a iluminarlos. El libro se divide en 3 partes principales, se introduce el tema, se descubre la infraestructura y la analítica del Big Data. Tiene en sus manos la referencia necesaria para introducirse en Big Data.

Aprenda:

- ¿Qué es Big Data?
- Analítica de datos, analítica Web y analítica social
- Sectores estratégicos de Big Data y Open Data

Conozca:

- La revolución de la gestión, la analítica y los científicos de datos.
- Las mejores herramientas informáticas para procesar sus datos.
- Las nuevas tendencias tecnológicas y sociales que traen la nube y los Big Data.

el autor

Luis Joyanes Aguilar es Doctor Ingeniero en Informática y Doctor en Sociología, Catedrático de Lenguajes y Sistemas Informáticos de la Universidad Pontificia de Salamanca en el campus de Madrid y profesor invitado en diferentes universidades del mundo. Conferenciante en congresos, seminarios, jornadas y talleres a nivel mundial. Ha escrito numerosos libros y artículos relativos a Tecnologías de la Información.
Patrono de la Fundación de I+D Software Libre, miembro del Instituto Universitario "Agustín Millares" de la Universidad Carlos III de Madrid y presidente de SISOFT.

Más información.

www.alfaomega.com.mx

ÁREA: Informática — SUBÁREA: Nuevas Tecnologías y Temas de Actualidad

ISBN 978-607-707-089-6

"Te acerca al conocimiento"

Alfaomega Grupo Editor

JOYANES

Industria 4.0

Industria 4.0

LA CUARTA REVOLUCIÓN INDUSTRIAL

Luis Joyanes Aguilar

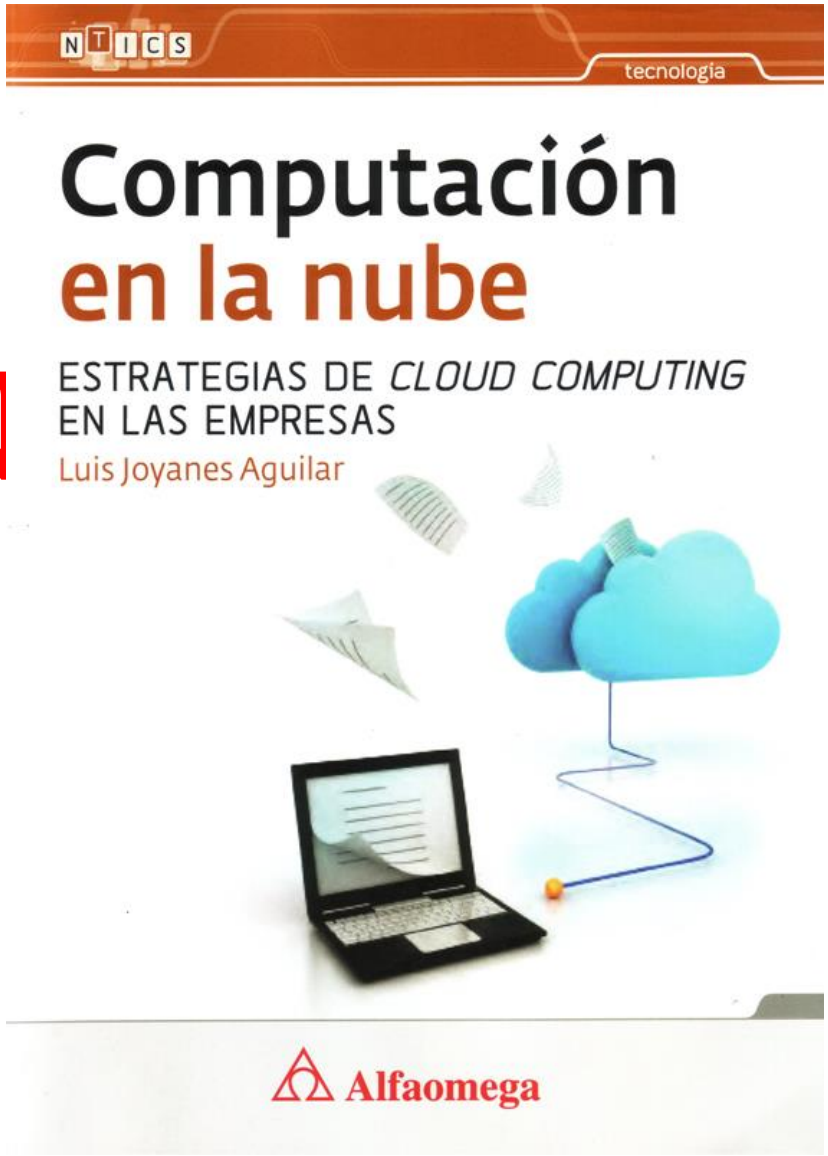
Alfaomega

ESTADO DEL ARTE DE *CLOUD COMPUTING*

COMPUTACIÓN EN LA NUBE

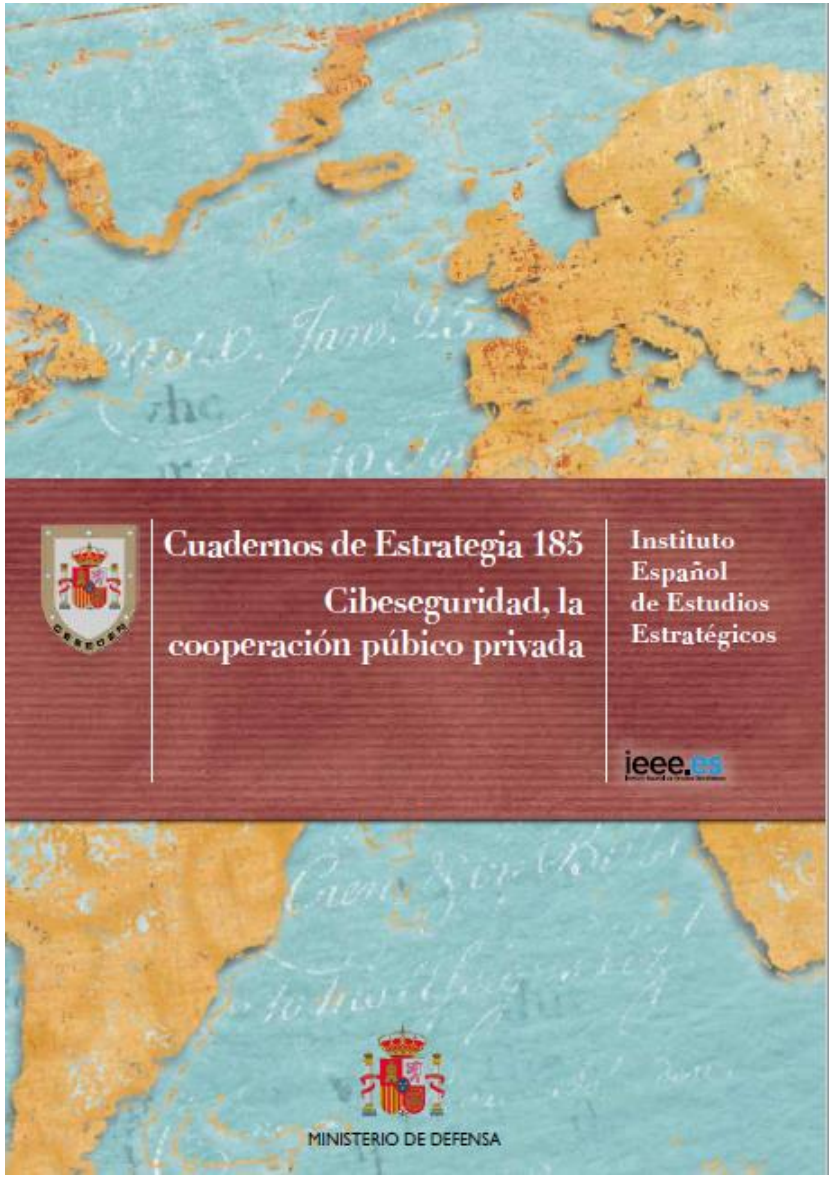
La nueva era de la computación

Prof. Luis Joyanes Aguilar




tecnología
Big Data
ANÁLISIS DE GRANDES VOLÚMENES
DE DATOS EN ORGANIZACIONES
Luis Joyanes Aguilar
Alfaomega


Sistemas
de Información
en la Empresa
El impacto de la nube, la movilidad y los medios sociales
LUIS JOYANES AGUILAR
LibroWeb
Web
Alfaomega



JOYANES, Luis (Coordinador). *Ciberseguridad. La colaboración público-privada.* Madrid: IEEE.es, 2017

MUCHAS GRACIAS

ljoyanes@fidesol.org

joyanes@gmail.com

www.facebook.com/joyanesluis