# 3RD LATAM IoT & TECH FORUM

**PERSPECTIVAS PARA UN MUNDO FUTURO CON IoT: REGULACIÓN Y PREOCUPACIONES DE IoT EN AMÉRICA LATINA**

**GERMAN DARIO ARIAS PIMIENTA**

**Santiago de Chile, Agosto 14 de 2019**

*"EL INTERNET DE LAS COSAS (IoT) ES SIN DUDA UNO DE LOS MAYORES FACILITADORES PARA LA TRANSFORMACION DIGITAL RESPONSABLE. SE ESTIMA QUE SOLO EL IoT INDUSTRIAL PUEDE AGREGAR* ***US$ 14 TRILLONES*** *DE VALOR ECONOMICO A LA ECONOMIA GLOBAL PARA 2030"*

**INTERNET OF THINGS GUIDELINES FOR SUSTAINABILITY,** WEF 2018

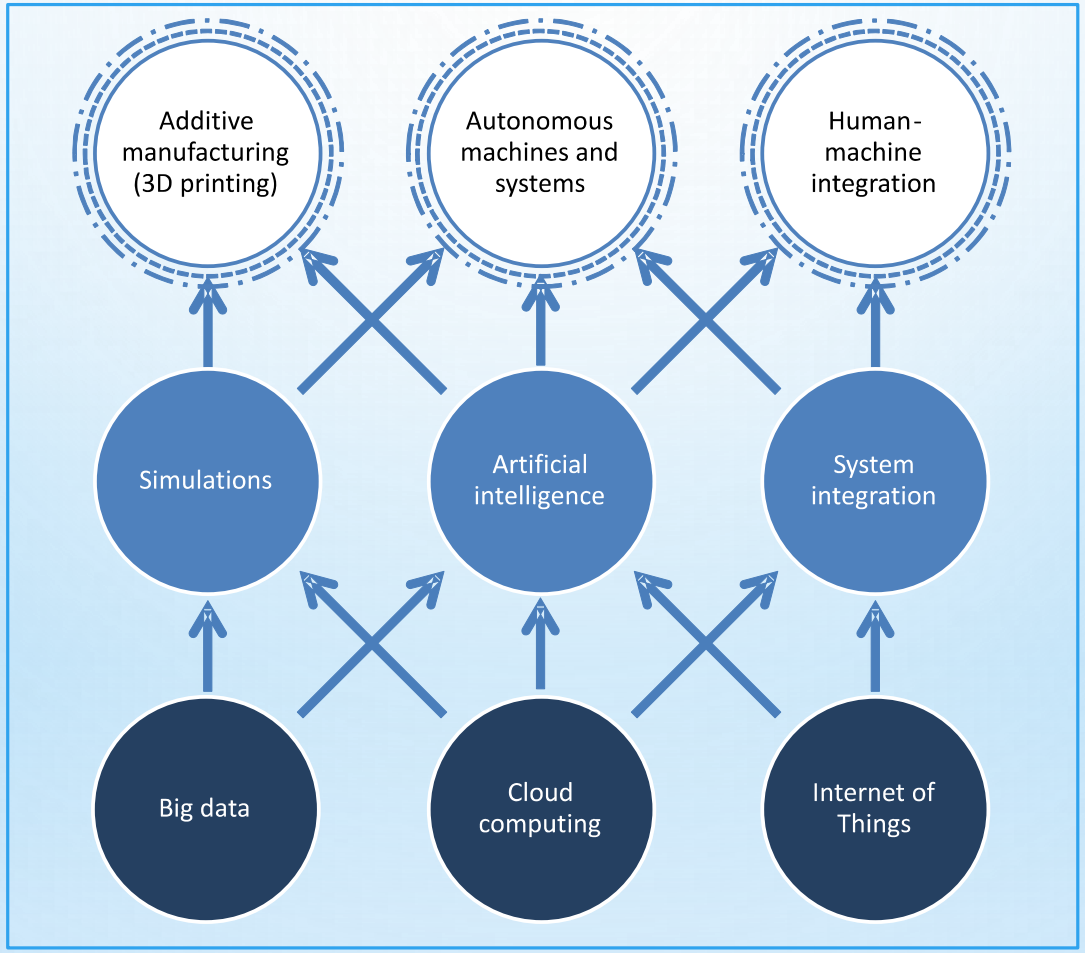
*"….SEGUN GSMA INTELLIGENCE, EL POTENCIAL DE INGRESOS TOTALES PARA LATINOAMERICA HACIA EL AÑO 2023 ES DE* ***USD 33 MIL MILLONES****. SIN EMBARGO, EL IMPACTO GENERAL EN EL PIB SERA PROBABLEMENTE MUCHO MAS SIGNIFICATIVO. TAN SOLO PARA BRASIL, MCKINSEY PRONOSTICA QUE EL IMPACTO DE IoT HACIA 2020 SERA DE AL MENOS* ***USD 50 MIL MILLONES*** *EN EL PBI DEL PAIS…"*

**CIUDADES INTELIGENTES E INTERNET DE LAS COSAS: COMO FOMENTAR SU DESARROLLO EN AMÉRICA LATINA, GSMA 2019.**

# CONTENIDO

- Definición IoT
- Elementos clave
- Política Pública y Regulación IoT
- Desarrollos y avances
- Conclusiones

# LA CONFLUENCIA DE TECNOLOGIAS CLAVE PERMITEN LA TRANSFORMACION DIGITAL INDUSTRIAL.




- FUENTE: OECD: THE NEXT PRODUCTION REVOLUTION, A REPORT FOR THE G20, 2017

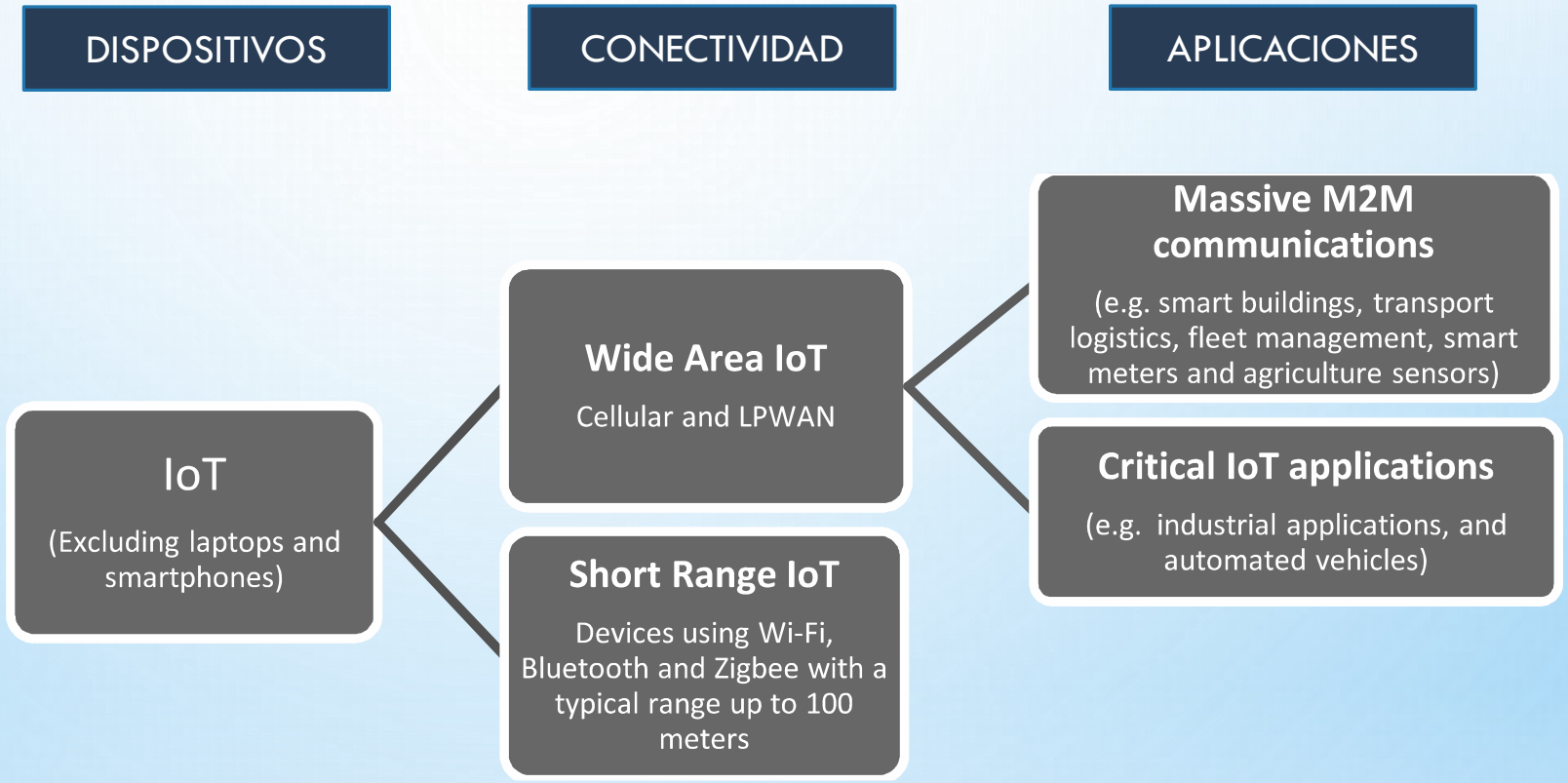
# QUE ES IoT?

- “Internet de los objetos (IoT): Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (Físicos y virtuales) gracias a la interoperatividad de tecnologías de la información y la comunicación presentes y futuras” (Recomendación UIT-T Y.2060).
- “Internet de las cosas se refiere al creciente número de dispositivos conectados e interconectados” (DIGIT Act, U.S Congress).
- “IoT se refiere a la interconexión holística de servicios, aplicaciones, procesos comerciales, personas y dispositivos con una red o Internet para recopilar y analizar datos y realizar ciertas tareas sin intervención humana.” (GlobIalData).
- “Un IoT es una red que **conecta** "Cosas" **identificables** de forma única a Internet. Las "Cosas" tienen capacidades de **detección** / **actuación** y potencial **programabilidad**. A través de la explotación de la identificación y la detección únicas, se puede **recopilar información** sobre la "Cosa" y el estado de la "Cosa" se puede cambiar desde **cualquier lugar**, en **cualquier momento** y por cualquier mecanismo” (IEE, Towards a definition of the Internet of Things (IoT), 2015).

# ELEMENTOS CLAVES EN LA DEFINICIÓN

CARACTERISTICAS CLAVES

- Identificación única
- Siempre conectado
- Autoadaptación
- Autoconfiguración
- Interoperabilidad
- Inteligencia
- Programabilidad




- FUENTE: BASADO EN OECD, ROADMAP MEASURING INTERNET OF THINGS

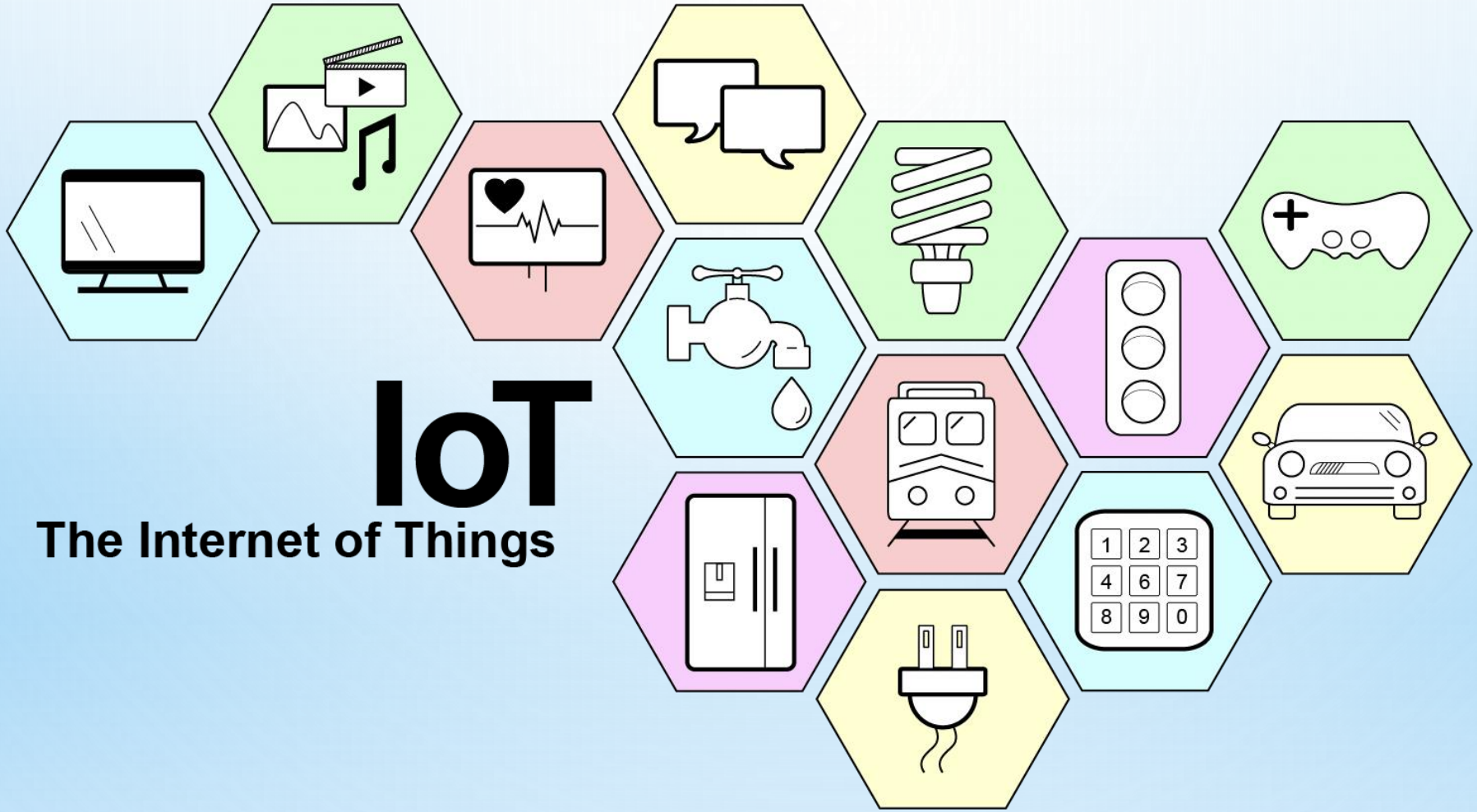
# ELEMENTOS A TENER EN CUENTA PARA LA REGULACIÓN Y LA POLITICA PUBLICA

- Colaboración intersectorial
- Competencia
- Inversión
- Licenciamiento
- Espectro radioeléctrico
- Redes Heterogeneas (HetNet)
- Banda Ancha
- Roaming
- Cloud
- Interoperabilidad
- Telecomunicaciones de Emergencia
- Neutralidad de red

- Numeración y Direcciones
- Big Data y Open Data
- Seguridad
- Protección de datos
- Protección de usuarios
- Privacidad
- Calidad y experiencia (Servicio)
- Derechos de Via
- Green ICTs
- Compartición de Infraestructura
- Data Centres
- E-waste
- Portabilidad

- FUENTE: ITU, POLICIES AND REGULATIONS PERTAINING TO IoT, 2018

# PERO EL IMPACTO DE IOT ES MULTISECTORIAL




FUENTE: NIST (2019), CONSIDERATIONS FOR MANAGING INTERNET OF THINGS (IoT) CYBERSECURITY AND PRIVACY RISKS, HTTPS://NVLPUBS.NIST.GOV/NISTPUBS/IR/2019/NIST.IR.8228.PDF

# CIBERSEGURIDAD Y PRIVACIDAD

## NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, USA

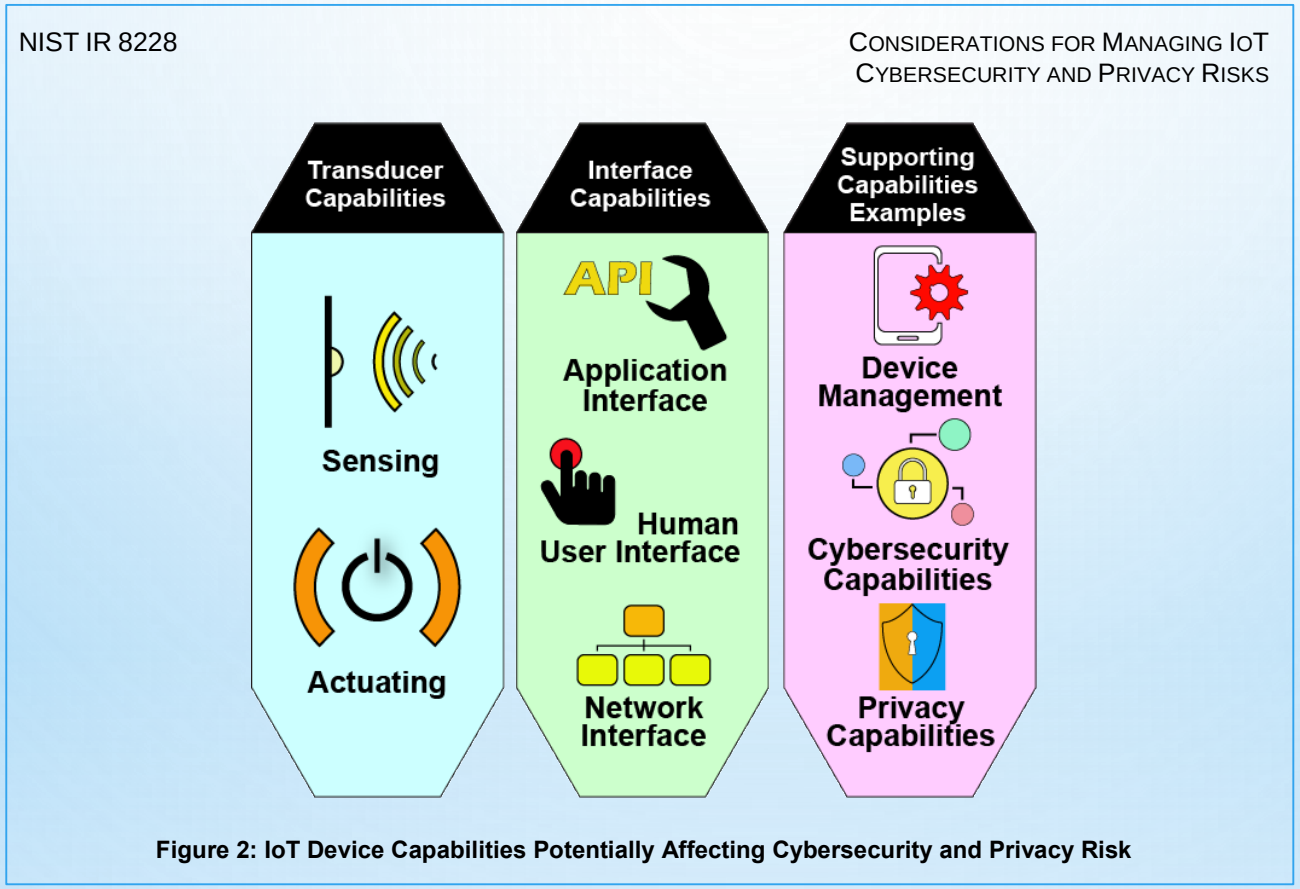



**Figure 2: IoT Device Capabilities Potentially Affecting Cybersecurity and Privacy Risk**

Fuente: NIST (2019), Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

# CIBERSEGURIDAD Y PRIVACIDAD
## NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, USA

LA GESTIÓN DE RIESGOS PARA UNA GRAN PARTE DE DISPOSITOS IoT ES DISTINTA A LA DE DISPOSITIVOS CONVENCIONALES.

- Muchos dispositivos IoT interactúan con el mundo físico de una manera distinta a las interacciones de los dispositivos de TI convencionales. Los requisitos operativos de rendimiento, confiabilidad, resistencia y seguridad pueden estar en desacuerdo con las prácticas comunes de ciberseguridad y privacidad para dispositivos de TI convencionales.
- No se puede acceder, administrar o monitorear muchos dispositivos IoT de la misma manera que los dispositivos de TI convencionales. Esto puede requerir realizar tareas manuales lo que implica que se deben abordar los riesgos con los fabricantes y otros terceros que tienen acceso o control remoto sobre esros dispositivos.
- La disponibilidad, eficiencia y efectividad de las capacidades de ciberseguridad y privacidad a menudo son diferentes para los dispositivos IoT que para los dispositivos de TI convencionales. Esto significa que las organizaciones pueden tener que seleccionar, implementar y administrar controles adicionales, así como determinar cómo responder al riesgo cuando no hay suficientes controles para mitigarlo.

Fuente: NIST (2019), Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

# CIBERSEGURIDAD Y PRIVACIDAD
## NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, USA

**TRES NIVELES PARA LA MITIGACIÓN DEL RIESGO**

- **Proteger la seguridad del dispositivo.** En otras palabras, evitar que un dispositivo se use para realizar ataques, incluida la participación en ataques de denegación de servicio distribuido (DDoS) contra otras organizaciones y espiar el tráfico de red o comprometer otros dispositivos en el mismo segmento de red. Este objetivo se aplica a todos los dispositivos IoT.
- **Proteger la seguridad de los datos.** Proteger la confidencialidad, integridad y / o disponibilidad de los datos (incluida la información de identificación personal) recopilados, almacenados, procesados o transmitidos hacia o desde el dispositivo IoT. Este objetivo se aplica a cada dispositivo IoT, excepto aquellos sin datos que necesiten protección.
- **Proteger la privacidad de las personas.** Proteger la privacidad de las personas afectadas por el procesamiento más allá de los riesgos administrados a través de la protección de seguridad de datos y dispositivos. Este objetivo se aplica a todos los dispositivos IoT que procesan o que impactan directa o indirectamente a las personas.

Fuente: NIST (2019), Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

# DESARROLLOS Y AVANCES A ESCALA GLOBAL

- **USA**
  - **S.2020 - Cyber Shield Act of 2017**: Establece un programa voluntario para identificar y promover productos conectados a Internet que cumplan con las normas, directrices, mejores prácticas, metodologías, procedimientos y procesos de ciberseguridad y seguridad de datos líderes en la industria.
  - **H.R.6032 - SMART IoT Act of 2018**: El Departamento de Comercio, adelantará un estudio (un año como máximo) sobre la industria de dispositivos conectados a Internet de EE. UU., donde se incluiran estándares voluntarios y obligatorios que se estén desarrollando para el sector de IoT.
  - **S.1611: Developing Innovation and Growing the Internet of Things (DIGIT) Act**: Crea un grupo de trabajo para definir recomendaciones al Congreso para el fomento de IoT relacionadas con la protección del consumidor, la privacidad y la seguridad, uso de IoT por parte de las agencias federales.
  - **S. 734: IoT Cybersecurity Improvement Act of 2019**: Para Aprovechar el poder de adquisición del gobierno federal para fomentar una mayor seguridad cibernética para dispositivos de Internet de las cosas y para otros fines.

# DESARROLLOS Y AVANCES A ESCALA GLOBAL

- **UE**
  - **Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo**: Objetivos, tareas y aspectos organizativos de ENISA**, objetivos de la política europea para la ciberseguridad, certificación para productos, servicios y procesos TIC, lineamientos para las autoridades nacionales de certificación de ciberseguridad.
  - **Reglamento General de Protección de Datos GDPR (UE) 2016/679**: Permite el control de sus datos a las personas, mejorar el entorno regulatorio y unifica las reglas al interior de la Unión Europea.
  - **Directrices éticas para la inteligencia artificial**: Derechos humanos, Robustez, Seguridad, Privacidad y Gobernanza, Transparencia, Diversidad (No discriminación y equidad), Bienestar Social y Ambiental, Responsabilidad. (Para comentarios 2019).
  - **Iniciativa de digitalización de la industria europea**, cuyos pilares son: Plataforma Europea de Iniciativas, Innovaciones Digitales para todos, Fortalecimiento del liderazgo a través de asociaciones y plataformas industriales, Un marco regulatorio adecuado para la era digital, Preparando a los europeos para el futuro digital.

**ENISA: The European Union Agency for Cybersecurity

# DESARROLLOS Y AVANCES A ESCALA GLOBAL

- UE
  - INVERSION ESTRATEGICA EN INTERNET DE LAS COSAS:
    - RETOS PRINCIPALES
      - Aceleración de la adopción de IoT en Europa.
      - Superar preocupaciones de seguridad y privacidad.
      - Miedo al bloqueo de clientes por plataformas propietarias.
      - Superar la fragmentación de los mercados, las barreras a la interoperabilidad y el intercambio de datos.
      - Incertidumbre sobre las oportunidades de negocio.
    - ACCIONES DEL PROGRAMA
      - Financiación consorcios de innovación.
      - Satisfacer las necesidades de la demanda demostrando múltiples aplicaciones de IoT.
      - Creación de interoperabilidad, arquitecturas de referencia comunes y estándares.
      - Desarrollar ecosistemas abiertos y abrir oportunidades comerciales.

Fuente: https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf

# DESARROLLOS Y AVANCES A ESCALA GLOBAL

**OCDE (2019): RECOMENDACIONES SOBRE INTELIGENCIA ARTIFICIAL PARA EL DISEÑO DE POLITICAS PUBLICAS**

- La IA debería beneficiar a las personas y al planeta impulsando el crecimiento inclusivo, el desarrollo sostenible y el bienestar.
- Los sistemas de IA deben diseñarse de una manera que respete el Estado de derecho, los derechos humanos, los valores democráticos y la diversidad, y deben incluir salvaguardas apropiadas, por ejemplo, permitir la intervención humana cuando sea necesario, para garantizar una sociedad justa y equitativa.
- Debe haber transparencia y divulgación responsable entorno a los sistemas de IA, para garantizar que las personas entiendan los resultados basados en la IA y puedan desafiarlos.
- Los sistemas de IA deben funcionar de manera robusta y segura a lo largo de sus ciclos de vida y los riesgos potenciales deben evaluarse y gestionarse continuamente.
- Las organizaciones e individuos que desarrollan, despliegan u operan sistemas de IA deben ser responsables de su correcto funcionamiento en línea con los principios anteriores.

Fuente: https://www.mintic.gov.co/portal/604/w3-article-101922.html

# QUE ESTA PASANDO EN NUESTROS PAISES

- COLOMBIA

  - **Ley 1273 de 2009**: Se crea un nuevo bien júridico llamado “de la protección de la información y los datos”.
  - **Ley 1266 de 2008 y Ley 1581 de 2012:** Habeas Data
  - **Consulta Pública IOT (2015):** ?Son servicios de Información?, ¿Las OTT son servicios transfronterizos?, ¿Se debe cobrar el acceso a las redes de telecomunicaciones a los proveedores de soluciones para IoT?, ¿El desarrollo de las IoT afecta la neutralidad de red?, ¿Numeración para M2M?, Roaming internacional para IoT.
  - **CONPES 3854 de 2016**: Ciberseguridad, creación del CSIRT**
  - **Hoja de Ruta para la economía digital** (CRC 2017)
  - **Plan Nacional de Desarrollo** (2019).
  - **Cartilla guia de transición de IPv4 a IPv6 y Resolución 2710 de 2017**: Las entidades públicas del orden nacional deberán culminar la transición el 31 de diciembre de 2019.
  - **Plan TIC 2018 – 2022**: Se destaca la creación de centros de excelencia para IoT y Big Data. Primer Centro de la 4RI de habla hispana en el mundo (WEF)

**Computer Security Incident Response Team

# QUE ESTA PASANDO EN NUESTROS PAISES

- BRASIL
  - **Estrategia para la transformación digital** (2018): Herradicación de la pobreza, hambre cero, salud y bienestar, Educación de calidad, Industria, innovación e infraestructura, cambio climático.
  - **Plan Nacional de Internet de las cosas** (2019): Los sensores y dispositivos IOT no se tratarán como equipos de comunicaciones, sino como valor agregado, se crea una cámara que le hará seguimiento. Se crearán plataformas de innovación de Iot, Centros de Competencia para Tecnologías Habilitadoras en IoT, y un Observatorio Nacional de Monitoreo de la Transformación Digital.
  - **Consulta pública sobre la reevaluación de la regulación para reducir las barreras regulatorias a la expansión de las aplicaciones de IoT y las comunicaciones de máquina a máquina** (Agosto 2019). Su objetivo es verificar si todos los modelos de negocio están representados en la regulación, ya sea que se traten de servicios de telecomunicaciones o de valor agregado, y en que tipo específico de servicio se deben clasificar para efectos de aplicar regulación.

# QUE ESTA PASANDO EN NUESTROS PAISES

- ARGENTINA
  - **Estrategia de Ciberseguridad**: Principios Generales y objetivos, se crea el Comité de Ciberseguridad.
  - **Resolución N° 8-E/2016** de la Secretaría de Tecnologías de la Información y las Comunicaciones: Se crea el Grupo de Trabajo de Servicios de Internet con la finalidad de - entre otros objetivos - promover el desarrollo de Internet de las Cosas
  - **Consulta Pública Comunicaciones M2M-** EX-2018-49680074-APN-DCYNT#JGM (2018)
- CHILE
  - **Decreto 533 de 2015**: Se crea el Comité Interministerial sobre ciberseguridad
  - **Política Nacional sobre ciberseguridad 2017 – 2022**: Seguridad de las personas y del país, colaboración y coordinación entre instituciones, gestion de riesgos en el ciberespacio.
  - **Chile, Ecosistema Digital 2017/2030,** Subtel
  - **Proyecto de Ley de Protección de datos**

# CONCLUSIONES

- El desarrollo del internet de las cosas tiene un impacto considerable en todas las economías.
- El desarrollo de IoT implica retos para los gobiernos en muchos frentes, en especial relacionados con la privacidad y la seguridad.
- Es necesario lograr estandares de la industria y no regulaciones nacionales.
- Las estrategias de IoT debe priorizar y focalizar sus esfuerzos por sectores.
- Las reglas actuales para el mundo de las telecomunicaciones desarrolladas por cada administración de manera independiente, no parecen reflejar las necesidades de los nuevos modelos de negocio, ejemplo de ello es la prestación de servicios en modo transfronterizo, el roaming internacional de datos, compartición de infraestructura, y el derecho de la competencia, entre otros.
- Es necesario que los gobiernos de latioamerica dediquen mayores recursos a su desarrollo y fomento. Los avances logrados especialmente por Europa en términos de política pública da cuenta de ello.
- Es fundamental repensar el papel del estado en la regulación, de tal manera que esta no sea una barrera para la innovación y el desarrollo. Incluso se debe pensar en modelos de co-regulación, sandbox y autoregulación.

GERMAN DARIO ARIAS PIMIENTA

germandarioarias@gmail.com

@GERMANARIAS