ANEXO Plan de Acción Nacional para el Desarrollo de Internet de las Cosas en Uruguay

Entre los avances tecnológicos de los últimos años con mayor expansión mundial se encuentra el Internet de las Cosas (IoT por sus siglas en inglés). Su desarrollo como bienes de consumo y proveedores de servicios, su incorporación en los procesos tecnológicos y productivos y su aplicación como fuentes de monitoreo de información en diversas esferas sociales, biológicas, ambientales, por mencionar algunos ejemplos de uso, evidencian la escala en que han permeado en nuestras sociedades.

Según la recomendación de la UIT-T Y.2060 el IoT puede considerarse un concepto ambicioso con repercusiones tecnológicas y sociales. Desde la perspectiva de la normalización técnica, IoT puede concebirse como una infraestructura global de la sociedad de la información, que permite ofrecer servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación (TIC) presentes y futuras. Aprovechando las capacidades de identificación, adquisición de datos, procesamiento y comunicación, IoT utiliza plenamente los "objetos" para ofrecer servicios a todos los tipos de aplicaciones, debiendo garantizar a su vez el cumplimiento de los requisitos de seguridad y privacidad.

Esta “interconexión digital de objetos” representa grandes oportunidades como puede ser la mejora en la eficiencia y precisión de procesos, su automatización, adecuación de bienes a preferencias y costumbres de uso de los consumidores, etc.

No obstante, también plantea desafíos, inquietudes e interrogantes para su desarrollo y adopción en pos de maximizar su beneficio social, en función de los cambios dinámicos y la diversidad de atributos que caracterizan al IoT, muchos de los cuales aún no están resueltos.

En el contexto internacional, consultas a múltiples actores interesados e involucrados se han desarrollado para conocer los puntos de vista y preocupaciones en torno a este avance tecnológico, en vista de la complejidad de dimensiones que los caracterizan: interconectividad con la infraestructura global TIC, licencias y espectro para su uso, direcciones y numeración asignada, interoperabilidad entre dispositivos heterogéneos, seguridad y protección, privacidad, tratamiento de datos, la adopción de un marco normativo que cuente con capacidad de adaptarse ante las innovaciones, entre otros.

Tanto desde la Comisión Europea como desde la Federal Trade Commission (FTC) en Estados Unidos, las acciones en esta línea coinciden en destacar entre sus conclusiones la preocupación especialmente en torno a temáticas de Privacidad, seguridad y protección, legislación acorde y promoción de la competencia e innovación de servicios[1]. En Marzo de 2015, la Comisión Europea lanza la Alianza para la Innovación de IoT (AIOTI, por sus siglas en inglés), como una plataforma abierta de stakeholders que abarca todos los actores claves involucrados en la cadena de valor de IoT[2].

En América Latina los trabajos realizados por Argentina y Brasil han ido en esta línea también. Argentina convocó en 2016 la jornada “Diálogo Público-Privado: IoT. Una Oportunidad para Argentina” con el apoyo y la participación de diversos sectores, y generó posteriormente una consulta pública en el que se obtuvieron aportes y conclusiones que formarían parte de los planes de acción que se promoverán.[3]

Si bien todavía no se ha concretado dicho Plan, se avanzó en recomendaciones en articulación con la UIT, concluyendo que “Construir los caminos más eficaces para el avance y el progreso tecnológico

---

[1] Ministerio de Modernización (s/d): Internet de las Cosas. Argentina: Secretaría de Tecnologías de la Información y las Comunicaciones.

[2] OECD (2016) The internet of things seizing the benefits and addressing the challenges. 2016 Ministerial meeting on the digital economy. Background report. OECD DIGITAL ECONOMY PAPERS No. 252.

[3] Ministerio de Modernización (2017): Informe IOT Consulta Pública SeTIC 2017 sobre Internet de las Cosas. Argentina: Presidencia de la Nación.

argentino requiere la participación informada, el diálogo y la colaboración de todas las partes interesadas, el análisis de las tendencias en las TIC y sus implicancias."[4]

Por su parte, algunas evaluaciones realizadas sobre el estado de situación de IOT para América Latina y el Caribe a cargo del BID, destacan enfoques innovadores y acciones de diversos stakeholders para alcanzar todo su potencial.[5]

En Uruguay, en el marco del 4° Plan de Acción Nacional de Gobierno Abierto, se define como uno de sus compromisos el punto 11.2: "Estrategia de ciberseguridad para IoT", que establece el desarrollo de un proceso participativo que involucre diferentes actores para crear una propuesta con recomendaciones y lineamientos para la elaboración de una estrategia país sobre políticas y buenas prácticas de ciberseguridad para IoT. Para su ejecución Agesic junto a Internet Society (ISOC), impulsaron la creación de un grupo de trabajo que fue integrado por representantes del gobierno, la academia, la comunidad técnica, el sector privado y la sociedad civil.

Su trabajo se desarrolló en torno a dos áreas prioritarias:
- Protección del consumidor: Capacitar a la ciudadanía para que tome decisiones informadas sobre los proveedores de servicios, comprenda mejor los riesgos de la adopción de IoT y sea más activa en la protección de sus datos personales.
- Resiliencia de la red: Generar las condiciones para fortalecer la resiliencia de redes, software y servidores nacionales que transmiten y almacenan datos.

En función de este proceso, en septiembre de 2019 se genera el documento denominado: Seguridad en IOT. Proceso de Uruguay con un conjunto de recomendaciones sobre posibles líneas de acción a seguir en estos ejes.[6] Este informe destaca entre sus conclusiones que "se considera que sería deseable trabajar sobre un marco de seguridad, así como desarrollar herramientas y procesos que permitan la integración y el soporte teniendo como centro a las personas." (p. 17) y que "Es necesario considerar a todos los sujetos comprendidos para poder desarrollar mecanismos de seguridad en todas las etapas." (p. 3)

Posteriormente, en ocasión de la definición de la Agenda Uruguay Digital 2025 recientemente publicada, la contemplación explícita a aspectos vinculados a IoT detallados en los compromisos 19 y 20, se han orientado fundamentalmente a impulsar la aplicación de estas tecnologías en sectores estratégicos del sector productivo y servicios públicos. La AUD 2025 no recoge las recomendaciones sobre políticas y buenas prácticas de ciberseguridad para IoT vinculados a protección de los consumidores y resiliencia de las redes. Sin embargo, los objetivos vinculados a Ciudadanía Digital (Objetivo I), Ciberseguridad (Objetivo X) y Seguridad jurídica para la transformación digital (Objetivo XII) habilitan la posibilidad de desarrollar acciones en este sentido.

La generación del 5to Plan Nacional de Gobierno Abierto se plantea por lo tanto como un espacio propicio para profundizar el trabajo iniciado en ocasión del anterior Plan Nacional, para trabajar en un proceso de co-creación de acciones y líneas de trabajo que permitan implementar las recomendaciones ya hechas. Se entiende fundamental promover la participación ciudadana en este proceso, contemplando al Estado, sociedad civil, sector privado y la academia, de manera que los stakeholders involucrados en las diversas etapas de la implementación y uso de IoT tengan un rol activo que jugar en su desarrollo.

---

[4] UIT (2019): Bases para el Plan Nacional de Internet de las Cosas. Argentina: Universidad Tecnológica Nacional

[5] Pérez Colón, R.; Navajas, S. & Terry E. (2019): IoT IN LAC 2019: Taking the Pulse of the Internet of Things in Latin America and the Caribbean. BID.

[6] https://miradordegobiernoabierto.agesic.gub.uy/SigesVisualizador/ga/o/GA/p/1997

Objetivo: Construir de manera participativa un Plan de Acción de Ciberseguridad de IoT al 2025 como conjunto de lineamientos estratégicos y acciones a desarrollar para promover una implementación segura de IoT desde el punto de vista técnico y de su adopción por parte de la sociedad.[7]

Metas:

- Convocar espacios de trabajo colaborativo entre integrantes de Estado, sociedad civil, sector privado y la academia para ratificar la validez de las recomendaciones sugeridas en 2019, priorizar las líneas estratégicas a las que se puedan comprometer participantes de todas las partes involucradas y sumar aportes para la definición preliminar de acciones asociadas a estas líneas.
- Continuar el trabajo iniciado en el 4to Plan de Acción, con base en las recomendaciones obtenidas, desarrollando una hoja de ruta para llevar a cabo ideas tales como un sistema de Etiquetado que señale las características tanto de seguridad como de manejo de información del dispositivo.
- Elaborar documento final del Plan de Acción de Ciberseguridad de IoT al 2025 coordinando los compromisos y aportes de los actores involucrados, estableciendo proyectos, equipos, cronogramas y presupuestos asignados según ejes.
- Conformar un grupo de trabajo con referentes de las instituciones partícipes para articular y dar seguimiento a las acciones asumidas, teniendo como centro a las personas.
- Establecer los mecanismos de transparencia y rendición de cuentas de las acciones ejecutadas por los actores involucrados hacia la ciudadanía.

Duración: set 2021 a dic 2022.

Posibles responsables: AGESIC, ISOC, CUTI y UdelaR.

Comentarios adicionales:

Existen las líneas de acción específicas factibles de desarrollar ya especificadas en el Informe Seguridad de IoT - Proceso para Uruguay, las cuales también evidencian la necesidad coordinar su ejecución con diferentes actores de la sociedad, no únicamente desde el Estado. Algunos ejemplos de ello son:

Implementar una Guía de buenas prácticas basada en OTA[8] – que facilite información clara y sencilla sobre aspectos a atender por parte de los consumidores a fin de protegerlos adecuadamente. (p. 9)

Unir esfuerzos y centralizar la información a través de servicios a la ciudadanía. De esta forma, se podría facilitar un listado de sistemas y/o dispositivos de IoT y disponer de un sitio donde reportar incidentes, coordinando la colaboración de los Equipos de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés) o Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés). De esta manera, se puede llegar rápidamente a centros especializados y tomar medidas adecuadas a tiempo. Asimismo, sería deseable generar CSIRT colaborativos, específicos para seguridad en IoT, donde participen actores de diversos sectores de actividad. (p. 12)

Realizar campañas de sensibilización dirigidas a los usuarios sobre los posibles riesgos. Se proponen tres abordajes:
• Aumentar los mecanismos de control de infraestructura que colaboren en la mitigación de posibles ataques que pongan en riesgo la disponibilidad, integridad y/o confidencialidad de los sistemas y/o dispositivos.

---

[7] Ejemplos en esta línea a nivel nacional en otras áreas son: La creación de los propios Planes de Acción Nacionales de Gobierno Abierto, el Plan Nacional de Aguas, el Plan Nacional de Género en las Políticas Agropecuarias, Plan Nacional Ambiental para el Desarrollo Sostenible.

[8] Online Trust Alliance (OTA)

• Mejorar el diseño y la gestión del ciclo de vida de los sistemas y/o dispositivos de IoT, fomentando estándares, conocimiento, medidas de concientización y guías de buenas prácticas.
• Adoptar medidas relacionadas con la gestión de las redes, como por ejemplo, ayudar a proteger a los sistemas y/o dispositivos para evitar que sean atacados. (p. 14)