Ciudades inteligentes, ciberseguridad y privacidad

Edgar Vega Briceño (*)
edgar.vega.briceno@una.cr

En los últimos años, el concepto de "ciudades inteligentes" se ha consolidado, desde el enfoque tecnológico, como el uso de soluciones basadas en Tecnologías de Información y Comunicación (TIC) para mejorar la calidad de vida de los ciudadanos, mejorar la interacción con el gobierno y promover el desarrollo sostenible. Se puede afirmar que una ciudad implementa características inteligentes cuando los factores de desarrollo social, medioambiental y económico están equilibrados y vinculados mediante procesos descentralizados que hacen más eficiente la dinámica urbana y la administración de los recursos por parte de gobiernos locales.

Las ciudades inteligentes deben estar diseñadas o planteadas en torno a una infraestructura basada en sensores para diferentes casos de uso, lo que comúnmente conocemos como el Internet de las Cosas (IoT, por sus siglas en inglés) para respaldar la interconectividad social y urbana a través de una mayor interacción ciudadana y eficiencia gubernamental; pero además se hace necesario contar con las bondades de nuevas tecnologías de telecomunicaciones que permitan soportar la monumental cantidad de datos generados por las nuevas formas de interacción, por ejemplo, la infraestructura avanzada de 4G y la prometedora tecnología 5G. En una ciudad inteligente se utilizan tecnologías modernas como computación en la nube, tecnología móvil, objetos electrónicos, redes avanzadas diseñadas por software, sensores y tecnologías de aprendizaje automático para permitir que los diferentes componentes cooperen e interactúen con la arquitectura de la red.

Ahora bien, la complejidad inherente y los nuevos métodos de interacción ciudadana requeridos conllevan importantes desafíos políticos, regulatorios y técnicos para los gobiernos y las autoridades municipales. Uno de los desafíos clave en el desarrollo de las ciudades inteligentes es el procesamiento y la gestión de datos de forma segura y confiable. Esto se relaciona no solamente con aquellos que ya están presentes en las bases de datos de—por ejemplo—la administración municipal, sino también con la vinculación de los datos con los nuevos sistemas y sensores presentes o propuestos dentro de una ciudad inteligente, cuyos riesgos a la seguridad y la privacidad no pueden pasar por alto. Las amenazas a la seguridad de la información y a la privacidad en conjunto con aspectos de ciberseguridad, resaltan la importancia de abordar estos desafíos no solo desde una etapa de planificación y diseño pero también del despliegue de las ciudades inteligentes; lo contrario a esto sería causante de consecuencias no deseadas y una pérdida de confianza por parte de la población.

El concepto de confianza es fundamental en el contexto de una ciudad inteligente, ya que el diseño integrado y la arquitectura técnica subyacente dependen en gran medida de la comunicación eficiente y segura de grandes cantidades de datos. La utilización de datos de rastreo basados en GPS, integrados con información personal detallada sobre hábitos de compra, ubicación, intereses personales, comunicados a través de la infraestructura basada en IoT, plantea importantes preocupaciones de seguridad y privacidad.

Cualquier iniciativa y plan gubernamental o municipal serio debe contemplar integralmente aspectos de ciberseguridad y privacidad desde sus primeras etapas para así brindar a la población no solamente un alto nivel de confianza y preservación de la privacidad sino también elementos tecnológicos que disminuyan los riesgos de ataques cibernéticos que comprometan la disponibilidad de los servicios desplegados para uso de la ciudadanía.

(*) Sede Regional Chorotega