Los retos de la ciberseguridad en ciudades inteligentes

DOI: 10.29236/sistemas.n148a6

Resumen

Según Naciones Unidas –ONU–, en el año 2050, casi el 70% de la población vivirá en áreas urbanas, debido a su desplazamiento gradual hacia estos lugares. Estos procesos migratorios fuerzan el cambio del modelo de gestión de las ciudades con el fin de mantener su sostenibilidad y mejorar la eficiencia de sus servicios.

Este nuevo modelo de gestión que se ha establecido en las ciudades contempla como catalizadores las tecnologías referentes a Internet de las cosas (IoT), Big Data o Cloud y aprovecha los comportamientos del ser humano frente a estas nuevas alternativas. Estar "siempre conectado" permite obtener información de localización, acceder a redes sociales, realizar actividades económicas y consultar datos de las personas, lo que podría implicar un riesgo para su privacidad, por la información identificable (PII) usada en los procesos de provisión de servicios.

Este riesgo requiere enfocar esfuerzos por parte de las ciudades, organizaciones y centros académicos para evaluar y proponer soluciones frente al estado de la seguridad cibernética en entornos de las ciudades inteligentes, enfocados principalmente en la privacidad del usuario.

Palabras claves

Ciudad inteligente, ciberseguridad, IoT, Big Data, información personal.

Introducción

Los gobiernos locales han utilizado las tecnologías de la información (TIC), principalmente como un motor para la mejora de los servicios públicos y la transparencia de su gestión, mediante el uso de datos abiertos, análisis de datos para la toma de decisiones y la reestructuración de procesos, así como su automatización. La revolución tecnológica y digital, en los últimos años, ha permitido la inclusión de las TIC en los entornos ambientales, económicos, sociales y culturales de la ciudad, lo que ha llevado a la definición de conceptos en todo el mundo, como ciudades inteligentes.

Sobre este tema, la Unión Internacional de Telecomunicaciones (UIT), establece la siguiente definición: "Una ciudad inteligente sostenible es una ciudad innovadora que utiliza las tecnologías de información y comunicación (TIC) y otros medios para mejorar la calidad de vida, la eficiencia de la operación y los servicios urbanos, y la competitividad, asegurando que satisface las necesidades de las generaciones presentes y futuras con respecto de los aspectos económicos, sociales, ambientales y culturales".

Por otra parte, de acuerdo con la publicación de Frost y Sullivan, se espera que el mercado mundial de las ciudades inteligentes alcance los $1,565 billones de dólares en 2020, considerando el empoderamiento de los ciudadanos en el uso de servicios electrónicos en tiempo real, tales como e-government, e-Banking, pago electrónico, etc.

Esto será posible porque las ciudades inteligentes buscan aprovechar las múltiples inteligencias del ámbito urbano respecto a la calidad de vida, la competitividad económica y la sostenibilidad. A continuación, se indican las aplicaciones que se pueden implementar en las ciudades inteligentes:

- Infraestructura inteligente: redes de sensores para gestión de energía, agua y residuos.
- Energía inteligente: redes inteligentes, medidores inteligentes.
- Movilidad inteligente: gestión del tráfico, gestión del estacionamiento.
- Conectividad inteligente: redes WiFi 4G gratuitas.
- Salud inteligente: sistemas de salud electrónica y m-Health.
- Seguridad cognitiva: seguridad inteligente para sistemas de información.
- Seguridad inteligente: seguridad inteligente para la infraestructura física.
- Educación inteligente: tablero electrónico, proyector interactivo, e-learning.
- Campus inteligente: todos los conceptos definidos para la ciudad inteligente aplicados a las universidades, que pueden considerarse para este concepto como una ciudad pequeña.

Infraestructura de la ciudad inteligente

La implementación de la ciudad inteligente requiere cuatro infraestructuras para su funcionamiento.

1. Infraestructura institucional, se refiere a los recursos humanos o de las TIC que permiten desarrollar las actividades de gestión y planificación de una ciudad. El fortalecimiento actual de soluciones tecnológicas como Big Data, Inteligencia Artificial e Internet de las Cosas han aumentado la participación de las TIC en los modelos de gestión de las ciudades bajo el concepto de ciudad inteligente.
2. Infraestructura física, se refiere a la infraestructura física que respalda las actividades de la ciudad.
3. Infraestructura social, se refiere al desarrollo humano y social.
4. Infraestructura económica, se refiere a las inversiones económicas y la generación de empleo en la ciudad.

Riesgos de ciberseguridad en la ciudad inteligente

Sin embargo, esta interconexión del "todo" a Internet (Iod) y el uso de "toda" la información posible implica nuevos riesgos de ciberseguridad para la ciudad y sus ciudadanos, lo que ha creado un interés particular de los gobiernos, los fabricantes y los investigadores. A continuación, se indican algunos de estos riesgos:

- Un dispositivo vulnerable puede generar un punto de entrada a todo el entorno de la ciudad inteligente.
- Un dispositivo vulnerable puede infectar a otro dispositivo.
- Se puede acceder a los sistemas de información no sólo desde dentro de la organización que brinda los servicios, sino también desde el exterior. Internamente se puede acceder utilizando cualquier tipo de dispositivo para el enfoque BYOD.
- Puede haber saturación de los servidores de la computadora y su ancho de banda, porque varios dispositivos se conectan para compartir información.
- Pueden existir vulnerabilidades en los dispositivos Cloud, Big Data e IoT.

El análisis de estas premisas plantea algunas preguntas tales como:

- ¿Cómo se maneja la seguridad en la ciudad inteligente?
- ¿La privacidad de la persona está protegida en la ciudad inteligente?
- ¿Pueden los gobiernos locales o cualquier persona conocer toda la información de los ciudadanos?
- ¿Tiene dispositivos IoT con suficiente seguridad?
- ¿Están protegidas las infraestructuras críticas de la ciudad?
- ¿Existen leyes que regulan la seguridad de la información personal y las infraestructuras críticas?
- ¿Los servicios públicos utilizados de manera tradicional son más seguros que el uso de servicios electrónicos?

Al respecto, una contribución interesante es la de Lilian Edwards, en su obra "Privacidad, seguridad y protección de datos en ciudades inteligentes: una perspectiva crítica de la legislación de la Unión Europea (EU)", en la que menciona varios aspectos en el ámbito tecnológico, urbano, ambiental y social, sobre la amenaza potencial a la privacidad de los ciudadanos, al tener una gran cantidad de información

personal en la arquitectura de la ciudad inteligente.

En su trabajo también analiza los riesgos de seguridad que pueden afectar la privacidad de los ciudadanos, como:

- Las vulnerabilidades existentes en IoT, Big Data y Cloud exponen a las ciudades inteligentes.
- Las debilidades en las regulaciones de la privacidad.
- La ambigüedad entre el enfoque público de la ciudad inteligente y el mantenimiento de la privacidad de los ciudadanos.

Respecto a las vulnerabilidades IoT, Big Data y Cloud, se menciona lo siguiente:

Los dispositivos IoT fueron diseñados explícitamente para ser discretos y sin interrupciones para la experiencia del usuario, por lo que carece de procesos de autorización para el uso de información personal.

Big Data, indirectamente usa información personal para el procesamiento del análisis de datos y realiza técnicas de reidentificación de datos anonimizados o pseudoanónimos. La recopilación exhaustiva de "todos los datos" no está de acuerdo con los principios de minimización de la recopilación de datos promovidos en las leyes de protección de datos.

En la nube, los datos suelen ser almacenados y procesados en un lugar desconocido y variable, lo que complica la implementación de la protección de la información personal.

Por otra parte, de acuerdo con la publicación de la empresa Ernst & Young (EY) que fue presentada en la India Security Conference en 2016, existen algunas actividades que forman parte del ecosistema de la ciudad inteligente y pueden considerarse inaceptables, si se habla de la protección de la privacidad, pero son necesarias para los procesos de gestión dentro de la ciudad inteligente, tales como:

- Vigilancia: observar, rastrear o registrar las actividades de una persona.
- Agregación: combinación de varios aspectos de los datos de una persona para identificar un patrón de actividades.
- Fugas de datos: las políticas débiles pueden provocar fugas o acceso incorrecto a información sensible.
- Uso prolongado: uso de datos recopilados por un período más prolongado que el propuesto o que pueden utilizarse para otros fines.

Es evidente el grado de amenaza que representan estos riesgos de ciberseguridad para las ciudades inteligentes, de ahí su importancia de gestionarlos, sobre todo en términos de privacidad.

Gestión de la seguridad cibernética desde la perspectiva de privacidad

En términos de gestión de seguridad cibernética, hay tres niveles que se deben considerar:

- Planificación de seguridad estratégica.
- Planificación de seguridad táctica.

- Planificación operacional de seguridad.

Planificación estratégica. En esta fase se establecen objetivos y estrategias para la gestión de riesgos y el cumplimiento de leyes, normas, etc. Además, se define la gobernanza de la seguridad de la información a través de la definición de las políticas de privacidad y los modelos de madurez de seguridad.

En las organizaciones de América del Norte se debe cumplir con las normas de privacidad, tales como:

- Ley de privacidad y derechos educativos de la familia (FERPA).
- Estándares de seguridad de datos de la industria de tarjetas de pago (PCI DSS).
- Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA).
- Ley de Oportunidad de Educación Superior (HEOA).
- Gramm-Leach-Bliley Act (GLB).
- Reglas de Bandera Roja (Comisión Federal de Comercio).

Las organizaciones europeas deben cumplir con leyes y regulaciones tales como:

- Protección ACT.
- El Reglamento General de Protección de Datos de la UE (GDPR).
- Comunicaciones electrónicas.
- Datos de empleo.
- Datos médicos.
- Procesamiento de datos con fines estadísticos.

En América Latina aún no se dispone de reglamentación específica, sin embargo, existe un primer acercamiento realizado por Colombia, que en abril de 2018 aprobó la primera política pública de explotación de datos de la región.

Planificación táctica. En este nivel se definen los procesos, procedimientos y tareas que respaldan el cumplimiento de la planificación estratégica. Los controles técnicos a nivel de red, aplicaciones, seguridad física y lógica deben implementarse en la ciudad inteligente.

Algunos controles de seguridad podrían implementarse en las organizaciones, según SANS, ISO 27001, COBIT y OWASP.

Por otra parte, la información puede contener datos confidenciales, como el nombre completo y el número de identidad; en este aspecto es importante mejorar la seguridad de la información de identificación personal (PII). A continuación, se exponen algunas debilidades que deben gestionarse:

- Falta de técnicas de anonimización para PII.
- Pobres técnicas de encriptación aplicadas en puntos finales y servidores para proteger PII.
- PII que se distribuye en redes usando texto claro, no se usan técnicas de encriptación.
- Falta de controles para descargar PII a dispositivos móviles como computadoras portátiles, tabletas o teléfonos inteligentes, que conlleva un alto riesgo en caso de robo.
- Pobres sistemas de control de acceso digital.
- Falta de Equipo de Respuesta a Emergencias de Computadoras (CERT).

- Falta de tecnologías de mejora de la privacidad (PET).
- Falta de privacidad por diseño o seguridad por diseño en el desarrollo de aplicaciones o sistemas informáticos.
- Falta de educación a los ciudadanos sobre el riesgo de privacidad.
- Falta de técnicas o tecnología como códigos QR para obtener las políticas de privacidad de los dispositivos IoT.

Planificación operacional. Establece las tareas orientadas a mantener las operaciones diarias de la ciudad inteligente, así como la implementación de controles de seguridad, el análisis de vulnerabilidades y el monitoreo del cumplimiento de políticas, leyes o estándares.

Algunas técnicas o implementaciones para la operación de ciudades inteligentes son:
- Identificación única de usuarios para servicios tecnológicos; esto facilita la flexibilidad de usar su propio dispositivo y conectarse desde cualquier lugar, pero mantiene la trazabilidad de las conexiones.
- Integración de sistemas de información para tener una administración centralizada.
- Integración de redes para la movilidad.

En este nivel, es importante establecer un control adecuado e identificar a los atacantes, las técnicas de ataque, el período de los ataques.

Adicional, es importante considerar los siguientes desafíos:
- Aún existe la debilidad en las técnicas de monitoreo.
- A pesar de disponer de herramientas de seguridad, no es posible identificar todas las fuentes de ataques y el tipo de ataque.
- La detección del incidente es reactiva y se requieren procedimientos para poder actuar de manera más proactiva y rápida.

Conclusión

La ciberseguridad es un aspecto complejo que debe gestionarse en las ciudades inteligentes; no podemos hablar de transformación de servicios públicos o privados en beneficio del usuario, si al hacerlo se puede producir un riesgo mayor y, en este caso puntual, vulnerar uno de sus derechos adquiridos en cualquier constitución, el derecho a la privacidad. Por tal razón, gobiernos, empresas e instituciones académicas y de investigación deben trabajar de manera coordinada para investigar la problemática, los desafíos y retos de la ciberseguridad en las ciudades inteligentes.

Ahora, este nuevo paradigma de las ciudades inteligentes, basado en TIC, plantea adaptar los conceptos y metodologías utilizados en gestión de seguridad cibernética en organizaciones, al entorno de la ciudad, donde se debe priorizar la privacidad de la información personal de los ciudadanos.

Este enfoque también debe empezar a generar nuevas habilidades en los ciudadanos digitales miembros de las ciudades inteligentes para conocer los riesgos, entender los modelos de interacción de los dispositivos de IoT y los beneficios

de la *open data* dentro de la gestión pública de las ciudades.

Las ciudades inteligentes son una realidad que crece, sin embargo, sólo podrán funcionar si se dispone de las condiciones para confiar en ellas.

Los usuarios necesitamos estar seguros de que la información que se almacena y circula en el ecosistema de la ciudad inteligente está protegida.

Los datos confiables y precisos hacen que las ciudades inteligentes funcionen correctamente, mientras que cualquier alteración puede afectar en gran medida las actividades habituales de los ciudadanos y resultar muy costosa su reparación, por lo que la gestión de la seguridad que involucra los aspectos de disponibilidad, integridad y confidencialidad de la información, debe ser una prioridad; se requiere analizar el uso de tecnologías como *Big Data*, Inteligencia Artificial y *Blockchain*, para la generación de soluciones, de manera de garantizar la seguridad de los datos, en las ciudades inteligentes.

Por otra parte, las ciudades inteligentes dependen de dispositivos interconectados que proveen datos en tiempo real, a través de los cuales pueden optimizar y mejorar los servicios; sin embargo, este auge en la conectividad digital también abre la puerta a numerosas vulnerabilidades; por lo tanto, la seguridad en IoT plantea un reto a toda la comunidad involucrada en la fabricación, uso y gestión de los dispositivos conectados, de tal forma que los fabricantes deben incorporar la seguridad en los dispositivos que desarrollan, las entidades de control deben velar porque se definan y cumplan normas de seguridad de información en estos dispositivos y los usuarios deben tomar conciencia sobre las implicaciones del uso de estas tecnologías y las medidas que pueden adoptar para asegurar sus dispositivos.

La ciberseguridad es un aspecto complejo que debe gestionarse en las ciudades inteligentes, no podemos hablar de transformación de servicios públicos o privados en beneficio del usuario, si al hacerlo se puede producir un riesgo mayor y, en este caso puntual, vulnerar uno de sus derechos adquiridos en cualquier constitución, el derecho a la privacidad. Por tal razón, gobiernos, empresas e instituciones académicas y de investigación deben trabajar de manera coordinada para investigar la problemática, los desafíos, y retos de la ciberseguridad en las ciudades inteligentes, así como también, integrar soluciones innovadoras de ciberseguridad, definir una normativa que regule la seguridad de la información personal, establecer mecanismos de protección de infraestructuras críticas de la ciudad y disponer de planes de recuperación eficiente frente a desastres.

Referencias

E. a. Y. F. M. N. Enerlis, Libro Blanco Smart Cities, Madrid: Imprintia, 2012.
F. a. Sullivan, "Frost&Sullivan," Frost and Sullivan, 26 Noviembre 2014. [Online]. Available: https://ww2.frost.com/news/press-releases/frost-sullivan-global-smart-cities-market-reach-us156-trillion-2020.

ITU, "ITU Committed to connecting the world," ITU, Octubre 2015. [Online]. Available: http://www.itu.int/en/ITU-T/ssc/united/Pages/default.aspx.

E. L, "Privacy, security and data protection in smart cities: a critical EU law perspective," 2015.

H. J. S. M. D. M. K. A. B. D. Bartoli A, "Se-curity and Privacy in your Smart City," 2011.

L. M. Elmagraby A, "Cyber security challenges in Smart Cities: Safety, security and privacy," *Journal of Advanced Research,* vol. V, no. 4, pp. 491-497, 2014.

EY, "Cyber Security A necessary pillar of smart cities," 2016.

R. Kitchin, "Getting smarter about smart cities: Improving data privacy and data security," Department of the Taoiseach, Dublin, 2016.

Roberto Omar Andrade Paredes. *Director de Gestión de Información y Procesos de la Escuela Politécnica Nacional (EPN) del Ecuador; miembro del Centro de Respuesta de Incidentes Informáticos (CSIRT) de la EPN; estudiante del Doctorado de Informática de la EPN; Certificado en Gestión de Incidentes de Seguridad Informática y Hackeo Ético de EC Council y miembro de la IEEE.*

Tania Guadalupe Gualli Culqui. *Profesional de la Dirección de Gestión de Información y Procesos de la Escuela Politécnica Nacional (EPN) del Ecuador, en el área de Analítica de Datos; Mba.; mención Gestión de Proyectos; miembro de R-Ladies Quito (Comunidad de Programación de R en Quito para las mujeres) y miembro de It-Women, Registro de Direcciones de Internet de América Latina y Caribe (LACNIC).*