El valor de construir ciudades inteligentes con ciberseguridad

POR **EVA MARTÍN IBÁÑEZ**

El artículo se acerca a los problemas de seguridad a los que se exponen las *smart cities* debido a su dependencias de las TIC. Se propugna que es imprescindible construir ciudades inteligentes alrededor de la ciberseguridad y no al revés. Es esencial introducir los requisitos de seguridad desde su concepción, en el momento del diseño.

Desde hace años, las ciudades han ido incorporando las nuevas tecnologías a su gestión, pero últimamente la adopción tecnológica se ha acelerado y ciudades de todo el mundo están haciéndose más 'inteligentes'. Eso permite optimizar recursos, ahorrar dinero y proporcionar mejores servicios a los ciudadanos. Unas ciudades son más inteligentes que otras, pero casi todas han implantado alguna clase de tecnología. Las *smart cities* son un fenómeno global, creciente e imparable (Cerrudo, 2015, p. 3).

El auge de las *smart cities*

Más de la mitad de la población mundial vive en zonas urbanas, pero esa proporción aumenta a dos tercios en la Unión Europea. Hay *smart cities* en todos los Estados de la UE, pero están desigualmente distribuidas, con países como Reino Unido, España e Italia a la cabeza en cifras absolutas. Sin embargo, los mayores porcentajes de concentración se producen en Italia, Austria, Dinamarca, Noruega, Suecia, Estonia y Eslovenia (European Parliament, 2014, p. 9). Se estima que en el año 2030 casi un 60 por ciento de la población mundial residirá en zonas urbanas. En España ya lo hace más del 80 por ciento de la población (Gobierno de España, 2015, p. 2).

Actualmente «es difícil encontrar una ciudad española que no esté abordando iniciativas *smart*. Municipios como Santander, Barcelona, Málaga, Rivas Vaciamadrid, Valencia o Madrid han

Fundación Telefónica
Telefónica

desarrollado experiencias pioneras de transformación urbana que pueden considerarse exitosas y que son reconocidas como referentes a nivel global» (PwC & IE Business School, 2015, p. 8). A menudo, la ciudad se considera una vía de transformación para crear «un ecosistema digital innovador y emprendedor, ampliando y convirtiendo en inteligente la información de ciudadanos y organizaciones» (Telefónica, 2015).

Para el Parlamento Europeo, *smart city* es una ciudad que busca abordar las cuestiones públicas a través de soluciones basadas en las Tecnologías de la Información y la Comunicación (TIC) sobre la base de una colaboración municipal con múltiples partes interesadas (European Parliament, 2014, p. 9).

En nuestro país, el *Plan Nacional de Ciudades Inteligentes* de 2015 recoge la definición de AENOR (Asociación Española de Normalización y Certificación) en este sentido: «Ciudad inteligente (*smart city*) es la visión holística de una ciudad que aplica las TIC para la mejora de la calidad de vida y la accesibilidad de sus habitantes y asegura un desarrollo sostenible económico, social y ambiental en mejora permanente. Una ciudad inteligente permite a los ciudadanos interactuar con ella de forma multidisciplinar y se adapta en tiempo real a sus necesidades, de forma eficiente en calidad y costes, ofreciendo datos abiertos, soluciones y servicios orientados a los ciudadanos como personas, para resolver los efectos del crecimiento de las ciudades, en ámbitos públicos y privados, a través de la integración innovadora de infraestructuras con sistemas de gestión inteligente» (Gobierno de España, 2015, p. 3).

Concepciones de la ciberseguridad

Desde el punto de vista de la ciberseguridad, conviene conocer las visiones subyacentes a este término tan amplio, entre las que destacan tres concepciones:
– Instrumentalizar digitalmente las *smart cities* para cambiar el modo en que las infraestructuras urbanas y los servicios municipales están configurados y gestionados.
– Mejorar las políticas urbanas, el desarrollo y la gobernanza usando los avances en las TIC para reconfigurar el capital humano, la creatividad, la innovación, la educación, la participación, la sostenibilidad y la gestión.
– Utilizar las tecnologías digitales y las TIC para promover un modelo de desarrollo urbano orientado al ciudadano que fomente la innovación y la justicia sociales, la participación de la sociedad civil y una gobernanza responsable y transparente (Kitchin, 2016, pp. 11-12).

Estas tres concepciones no son mutuamente excluyentes, sino una mezcla de elementos en distintas proporciones. Además, las visiones varían según los países. En Europa y EEUU, el desarrollo de las *smart cities* está relacionado con la mejora de la eficiencia de los servicios de la ciudad, la creación de resiliencia y sostenibilidad, el refuerzo de la seguridad y el control y el fomento del desarrollo económico. En China, India y África, las iniciativas de *smart cities* pretenden facilitar la modernización y el desarrollo nacionales, responder al crecimiento de la población y a las migraciones y gestionar las transiciones económicas y urbanas (Kitchin, 2016, p. 12).

El punto de partida es distinto en cada caso, según las situaciones sociales y económicas, las localizaciones naturales y geográficas, las estructuras económicas, la experiencia con

Fundación Telefónica

soluciones tecnológicas y el grado de madurez de las infraestructuras (CAICT & PDSF, 2014, p. XIII).

Dentro de un mismo continente existen grandes variaciones, dependiendo de las prioridades de las Administraciones y de la influencia de la cultura local, la historia, la política y la economía. Aparte, aunque muchas iniciativas tratan de remodelar ciudades preexistentes, otras se gestan como *smart cities* desde el principio, como Songdo en Corea del Sur o Masdar en Emiratos Árabes Unidos (Kitchin, 2016, pp. 11-12).

Un posible motivo de la falta de consenso es que el término se aplica en dos dominios: duro y blando. En el dominios ‘duros’, como edificios, redes de suministro de energía, recursos naturales, gestión del agua, gestión de basuras, movilidad y logística, las TIC desempeñan un papel decisivo en el funcionamiento de los sistemas. Por otro lado, el término también se aplica a dominios ‘blandos’ como educación, cultura, innovaciones políticas, inclusión social y gobierno, donde las TIC no suelen ser decisivas (Albino, Berardi y Dangelico, 2015, p. 10).

Una manera de acotar es establecer unas condiciones básicas para distinguir una ciudad inteligente. Para la UE, las iniciativas de *smart cities* deben incluir como mínimo una de estas seis características: gobernanza inteligente, gente inteligente, modo de vida inteligente, movilidad inteligente, economía inteligente y medioambiente inteligente. La mera presencia de características específicas no garantiza el éxito de los resultados de un proyecto de *smart city* (European Parliament, 2014, pp. 17, 28-30).

El ciberespacio y la ciudad

Conocer los planos del ciberespacio en la ciudad puede ayudar a comprender cómo está organizada la infraestructura de TIC del municipio. Es posible distinguir cinco planos: geográfico, físico, lógico, de las ciberpersonas y supervisor.

En la base está el plano geográfico, donde reside el físico con los sistemas y los dispositivos de tecnologías de la información. A continuación está la capa del plano lógico, formado por el modelo de interconexión de sistemas, las aplicaciones, los protocolos de red y los controladores de los dispositivos. Encima se encuentra el plano de las ciberpersonas, que son cuentas asociadas a individuos o grupos. Por último está el plano supervisor, que incluye las personas, las organizaciones y los sistemas encargados del mando y control (Conti, Cross y Raymond, 2015, pp. 3-4). La tabla 1 muestra esos cinco planos.

Fundación Telefónica
Telefónica

Tabla 1. Planos del ciberespacio en las ciudades

Plano supervisor	Puede ser muy complejo, debido a potenciales desavenencias políticas. Además suele ser proclive a la compartimentación, lo que lastra todavía más la cooperación en asuntos de seguridad.
Plano de las ciberpersonas	Engloba a las identidades de los líderes y empleados municipales. Estas pueden estar abiertas a la interacción con los votantes para conseguir ganancias electorales, pero también facilitar ataques de *spear-phishing* y otros fraudes.
Plano lógico	Las incompatibilidades entre el *software* de los sistemas son frecuentes. Muchos sistemas pueden estar funcionando en *hardware* y *software* heredados, debido a requerimientos normativos o a elevados costes de actualización.
Plano físico	Puede ser muy importante en supuestos de desastres naturales o causados por el hombre. Su rendimiento puede verse mermado por conexiones de bajo ancho de banda y por la falta de redundancia en la capa física de la conectividad.
Plano geográfico	Es de gran relevancia, porque la infraestructura de TIC de una ciudad generalmente está ligada al área geográfica del municipio. Cualquier desastre puede acabar causando pérdidas de energía o de conectividad en red.

Fuente: Elaboración propia a partir de Conti, Cross y Raymond (2015).

Arquitectura de las *smart cities*

Un modelo simplificado de la arquitectura de una *smart city* se puede estructurar en cuatro capas: sensores y dispositivos conectados; infraestructura de red y comunicaciones urbanas inteligentes; plataformas para la gestión de M2M (*Machine-to-Machine*) y computación en la nube, y aplicaciones verticales (Bergenti, Chiappone y Gotta, 2015, pp. 227-228).

La primera capa está integrada por los sensores y los actuadores distribuidos por toda la ciudad. Los dispositivos inteligentes siempre están conectados. Entre ellos figuran sensores meteorológicos, acústicos, de inundaciones, de niveles de contaminación, de tráfico, de alumbrado público o cámaras de vigilancia. Incluso los propios ciudadanos se convierten en sensores y actuadores con un alto grado de autonomía. Cada vez son más frecuentes las aplicaciones de tráfico, meteorología, contaminación y turismo que están basadas en la información que proporcionan los usuarios.

La segunda incluye la infraestructura de red y la conectividad. No está limitada a la conectividad de Banda Ancha, ya sea cableada o inalámbrica, sino que se completa con otra de corto alcance que podría denominarse de redes capilares, de gran importancia para los objetos de Internet de las Cosas (IoT). Dichas redes están compuestas por puertas de enlace y concentradores que recopilan datos de los sensores a través de enlaces inalámbricos de baja potencia. Es una infraestructura compartida por una gran cantidad de servicios y que transporta gran cantidad de datos.

En la tercera residen las plataformas M2M (*Machine-to-Machine*) y de computación en la nube (*Cloud Computing*). Abarca las capacidades de computación y de almacenamiento y los procesos de gestión. Esos procesos posibilitan las conexiones de control, analizan y redirigen los datos, garantizan la seguridad de las transacciones y aseguran que los proveedores de servicios puedan interactuar con sus aplicaciones y crear nuevos servicios y aplicaciones.

En la última capa están las aplicaciones verticales, responsables de gestionar los servicios y

Fundación Telefónica
Telefónica

los objetos desplegados en la ciudad. Esas aplicaciones se encargan, por ejemplo, del alumbrado público, la movilidad, los contadores inteligentes, el suministro de agua, la gestión de basuras, la educación o la sanidad. Aquí se encuentra el centro de mando y control, desde donde los decisores pueden supervisar los servicios que la ciudad está proporcionando. La información recogida en las capas anteriores se presenta de forma sintética en tableros de control (Bergenti, Chiappone y Gotta, 2015, pp. 227-228).

Las ciudades son frágiles incluso cuando no hay nadie intentado subvertir las infraestructuras críticas u otros sistemas importantes. Abundan los ejemplos de fallos en cascada causados por mal funcionamiento, desastres naturales o accidentes industriales, cuyo resultado es la disrupción de toda la ciudad y, a veces incluso, el caos (Conti, Cross y Raymond, 2015, p. 1). Las redes de las ciudades son complicadas, porque emplean tecnologías dispares. Según van creciendo, mezclan tecnologías y aplicaciones que datan de varias décadas con otras recién estrenadas (Hayslip, 2016, p. 2). Nuevas tecnologías están siendo integradas con otras viejas que pueden ser vulnerables. Además, muchas ciudades están implantando nuevas soluciones sin probar previamente su ciberseguridad (Cerrudo, 2015, pp. 7 y 10).

Infraestructuras ciberfísicas

En las ciudades inteligentes confluyen distintos tipos de infraestructuras. Parte de ellas son puramente digitales y otras son físicas. Los avances tecnológicos han propiciado la aparición de infraestructuras híbridas, que integran aspectos físicos y cibernéticos. Estas nuevas infraestructuras ciberfísicas propician la innovación y el desarrollo económico, pero no están exentas de riesgos. Antes las ciber-vulnerabilidades estaban contenidas dentro del ámbito de las infraestructuras digitales. Ahora se han extendido al mundo físico, gracias al aumento de la integración de componentes digitales en las infraestructuras físicas. Y esos riesgos de ciberseguridad no son meramente teóricos. En concreto, esa integración ha facilitado el desarrollo de sistemas de control industrial, como los de tipo SCADA (Supervisión, Control y Adquisición de Datos), utilizados para gestionar y vigilar a distancia complejos procesos industriales como la generación de energía eléctrica y el tratamiento de aguas residuales. Desgraciadamente, las vulnerabilidades de dichos sistemas abren la puerta de las infraestructuras físicas a posibles ciberataques que pueden interrumpir servicios esenciales para millones de personas (Atkinson, Castro, Ezell y McQuinn, 2016, p. 21).

Las tecnologías ciberfísicas son aquellas que conectan los cibersistemas con sistemas físicos y, por tanto, suprimen la barrera entre el mundo físico y el ciberespacio. Las *smart cities* están incorporando cada vez más tecnologías ciberfísicas en las infraestructuras preexistentes y en las de nueva construcción.

Eliminar las fronteras ciberfísicas en el entorno urbano presenta grandes oportunidades para aumentar la eficiencia y la comodidad, pero ese incremento de conectividad también amplía la superficie de ataque para los actores maliciosos. Aparte de incidentes físicos con consecuencias físicas, también pueden explotar cibervulnerabilidades con consecuencias igualmente físicas. Con el surgimiento de las *smart cities* y las innovaciones ciberfísicas, los factores mitigadores y las consecuencias potenciales de esas tecnologías todavía son desconocidas (National Protection and Programs Directorate, 2015, p. 2). La tabla 2 resume las

BY NC ND

principales tecnologías ciberfísicas relacionadas con las infraestructuras de la ciudad inteligente.

Tabla 2. Tecnologías ciberfísicas relacionadas con las infraestructuras de la ciudad inteligente

Transporte en ciudades inteligentes	Vehículos autónomos	Permiten que los automóviles entiendan el entorno en el que operan y ejecuten comandos seguros y eficientes basados en ese conocimiento. Los vehículos autónomos pueden tomar decisiones y realizar operaciones, de manera que los conductores se convierten en pasajeros.
	Control ferroviario positivo	Sistemas de sensores remotos y dispositivos de control automatizados diseñados para parar, acelerar y desacelerar un tren automáticamente y evitar situaciones peligrosas (colisiones, descarrilamientos y movimientos no autorizados). Emplean conexiones cableadas e inalámbricas para automatizar los controles.
	Sistemas de transporte inteligentes	Recogen datos en tiempo real para tomar decisiones informadas de forma automatizada sobre las infraestructuras y el *hardware* de tráfico. Suelen estar formados por sensores que recopilan información sobre la situación del tráfico; controladores que realizan cambios en los dispositivos de control de tráfico (como los semáforos) y un servidor central que analiza los datos, sugiere ajustes y comunica el sistema con sus componentes.
	Vehículo a Vehículo (V2V) y Vehículo a Infraestructura (V2I)	V2V usa comunicaciones dedicadas de corto alcance para que los vehículos se comunicen entre sí y con las infraestructuras estacionarias, como edificios y semáforos. V2I posibilita que la infraestructura física (señales de tráfico o vías de acceso) informe a los vehículos de su presencia y facilita que los vehículos envíen información a la infraestructura.
Electricidad en ciudades inteligentes	Plantas de generación de energía inteligentes	Despliegan una red de sensores y contadores para recopilar datos en tiempo real, tanto desde dentro de la planta generadora de electricidad como fuera, incluyendo los sistemas de distribución. Esos datos se transmiten a través de redes de comunicaciones a un punto de control central para su análisis. Después, dispositivos electrónicos inteligentes (como los controladores lógicos programables) y sistemas SCADA (Supervisión, Control y Adquisición de Datos) responden automáticamente con instrucciones de generación automáticas.
	Distribución de electricidad inteligente	Están diseñados para aumentar la inteligencia general de la *smart grid* (red de suministro de electricidad), su eficiencia y flexibilidad, y reducen los errores de distribución y transmisión. Utilizan sistemas SCADA y otros dispositivos de automatización para reducir los tiempos de respuesta, localizar cortes de energía locales y recopilar datos sobre el desempeño de la red de suministro rápidamente.
	Contadores inteligentes	Los contadores inteligentes miden, almacenan y transmiten datos sobre el uso de energía y voltaje en residencias y negocios. Usan comunicaciones bidireccionales, generalmente inalámbricas. Los centros de distribución y gestión pueden controlar físicamente los contadores para conectar y desconectar la energía a distancia.
Agua en ciudades inteligentes	Tratamiento de agua inteligente	Los sistemas de agua potable y los de aguas residuales inteligentes tienen en común el uso de una red de sensores y contadores para recoger datos, conectividad bidireccional y redes de comunicación para transportar datos entre los dispositivos y los sistemas de control central. Esto se completa con controladores lógicos programables conectados en red y con dispositivos SCADA que automatizan los ajustes del sistema.
	Distribución de agua inteligente	Reemplazan o mejoran las infraestructuras de gestión con tecnologías en red automatizadas. Válvulas y bombas inteligentes son capaces de adaptarse al entorno, modificando automáticamente velocidades y niveles de presión, además de redirigir el agua donde es necesario. Esos dispositivos se comunican de forma inalámbrica entre ellos y con el centro de control. Una red de sensores y monitores recoge datos sobre la calidad del agua, alerta de anomalías, y anticipa posibles fallos.
	Almacenamiento de agua inteligente	Engloban tecnologías de red automatizadas que se integran en reservorios, depósitos y otras instalaciones de almacenamiento, aparte de enlazar esas instalaciones con otros sistemas de agua. Para satisfacer una demanda cambiante, sistemas SCADA y de control industrial gestionan el flujo del agua. También vigilan las entradas en los reservorios para evitar desbordamientos y bloquean el paso de agua contaminada. Una red de sensores informa sobre la calidad del agua y la presencia de sustancias extrañas o peligrosas.

Fuente: Elaboración propia a partir de National Protection and Programs Directorate (2015).

Fundación Telefónica
Telefónica

Comprender las interdependencias entre infraestructuras críticas es el primer paso para evaluar la vulnerabilidad real. A raíz de desastres naturales como el paso del Huracán Katrina por Nueva Orleans en 2005, los investigadores empezaron a estudiar los potenciales efectos en cascada para las infraestructuras críticas. Existen interdependencias entre los sistemas de energía, agua, transporte, información y telecomunicaciones y los servicios de emergencia (Pederson, Dudenhoeffer, Hartley y Permann, 2006, p. 13). El objetivo es conocer el impacto que un fallo en una infraestructura puede producir sobre otras. Por ejemplo, un corte de electricidad puede afectar al suministro de gas y también puede reducir la cogeneración de energía. Asimismo, la falta electricidad puede influir en la distribución del agua, con pérdidas en la agricultura y en el sistema financiero.

La situación se agrava porque la mayoría de las infraestructuras críticas son propiedad del sector privado o están gestionadas por otras Administraciones. Esa mezcla de titularidades y competencias presenta retos de coordinación. En primer lugar, por el gran número de partes interesadas implicadas. En segundo, porque las infraestructuras críticas suelen estar dispersas y requieren cooperación interna. Por último, existen resistencias a compartir información sensible o de naturaleza competitiva (Office of the Auditor General of Canada, 2012, p. 18).

En España, la Ley 8/2011, de Protección de las Infraestructuras Críticas, en su artículo 2.e) establece que infraestructuras críticas son «las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permiten soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales». Dentro del catálogo figuran doce sectores: Administración, agua, alimentación, energía, espacio, industria química, industria nuclear, instalaciones de investigación, salud, sistema financiero y tributario, TIC y transporte.

Amenazas y vulnerabilidades

Las ciudades, como cualquier entorno TIC, pueden experimentar distintos tipos de ciberataques. Conforme los sistemas se hacen más complejos, están más interconectados y gestionan más información, aumenta su exposición a vulnerabilidades, ya sean debidas a actividades maliciosas o a errores humanos. El gobierno de la ciudad necesita identificar las áreas más críticas que proteger y los tipos de amenazas, incluyendo las categorías de atacantes y sus posibles motivaciones (económicas, criminales o financieras). Es importante que los diseñadores de una *smart city* elaboren planes que incorporen estrategias de ciberseguridad y mitigación para los supuestos de ataques o pérdidas de datos (Symantec, 2013, pp. 9-10).

Las ciudades inteligentes presentan escenarios atractivos para diversos actores, como naciones enemigas, ciberterroristas, cibercriminales y ‘hacktivistas’. Las operaciones de ciberguerra pueden tener como objetivo los servicios y las infraestructuras de las ciudades. El ciberterrorismo está a la vuelta de la esquina. Grupos extremistas tienen en sus filas personas con educación universitaria y habilidades para usar nuevas tecnologías en ataques terroristas. Por otro lado, países extranjeros emplean el ciberespionaje para conseguir información de empresas y gobiernos de todo el mundo y planear ciberataques. El cibercrimen busca nuevas oportunidades de negocio, que puede encontrar secuestrando el control de sistemas críticos y

Fundación Telefónica
Telefónica

servicios municipales para pedir un rescate. Y los 'hackitivistas', conocidos por lanzar ciberataques a empresas, organizaciones, colectivos y gobiernos, también pueden actuar contra las tecnologías de la ciudad como parte de una campaña contra un país o un área determinada (Cerrudo, 2015, p. 17).

Áreas de la ciberseguridad

La ciberseguridad comprende tres grandes áreas: confidencialidad y privacidad; integridad, y disponibilidad de la información y de los servicios (Elmaghraby y Losavio, 2014, p. 493).

La seguridad es muy importante en las infraestructuras de las *smart cities*, porque las redes son propensas a una amplia variedad de ataques maliciosos. Las metas de una ciudad inteligente no se lograrán si la información no está correctamente asegurada. Asimismo, debería tenerse en cuenta la privacidad de los sistemas que recopilan datos y que activan respuestas de emergencia (Ijaz, Shah, Khan y Ahmed, 2016, p. 613).

En las *smart cities* muchos dispositivos son inalámbricos, lo que facilita el despliegue; pero también son más susceptibles de ser 'hackeados' si el canal de comunicación no está adecuadamente cifrado. Incluso algunos sistemas cableados están basados en tecnologías PowerLine Communication (PLC) y también quedan expuestos. Muchos proveedores incluyen protocolos de comunicación inalámbricos o cableados con poca o ninguna seguridad. Y el cifrado utilizado, cuando existe, suele estar mal implementado. Los problemas de cifrado más comunes están relacionados con una pobre generación de claves y con el uso de algoritmos de cifrado desfasados o débiles.

Otras veces el fallo reside en una gestión endeble de las claves de cifrado, aunque el estándar de cifrado sea robusto. En ocasiones, las funciones de cifrado están disponibles pero las ciudades no las activan, ya sea por falta de conocimientos de seguridad o por la complejidad de su implantación (Cerrudo, 2015, pp. 8-9). Cuando la seguridad de las comunicaciones es escasa, cualquier atacante puede interceptarlas fácilmente y tomar el control de dispositivos y redes.

Toda nueva tecnología acarrea nuevos problemas. Cualquier ciudad, sea o no considerada inteligente, puede sufrir incidentes de ciberseguridad, cuyo impacto afecta al gobierno de la ciudad, a los residentes, a las empresas y a otras organizaciones dentro del municipio (Cerrudo, 2015, p. 7). La *smart city* presenta una baja tolerancia a los daños causados por ciberataques, mucho menor que otros ámbitos. Es comparable a los entornos de infraestructuras críticas, pero es mucho más exigente (Hasbini et al., 2016, p. 3).

En las *smart cities* la superficie de ataque es enorme y a menudo desconocida. Con tanta complejidad e interdependencia, resulta difícil saber qué es lo que está expuesto y en qué medida. Así, un pequeño incidente puede causar un gran impacto debido a reacciones en cadena; por eso es tan importante realizar un modelado de amenazas (Cerrudo, 2015, p. 9).

Cuanto más inteligente sea una ciudad, más sistemas incorporará, lo que aumenta el riesgo y el impacto de un ataque. Esto requiere un mayor control y una mejor visibilidad. Otro factor que

Fundación Telefónica
Telefónica

aumenta la complejidad es la integración de soluciones de distintos proveedores, especialmente durante las fases de rápida transformación tecnológica (Hasbini et al., 2016, p. 5).

La mayor parte de los suministradores tiene poca o nula experiencia en cuestiones de seguridad, especialmente en las áreas de sistemas industriales y de IoT. Cada vez es más común que las ciudades utilicen dispositivos y sistemas vulnerables, porque los proveedores o bien son muy lentos a la hora de distribuir parches o sencillamente los parches no están disponibles. Incluso cuando los parches existen y además funcionan, los dispositivos siguen siendo vulnerables si el parcheo no se aplica en todo el mundo (Cerrudo, 2015, pp. 8-10).

Análisis

Muchas iniciativas de *smart cities* a menudo ignoran o conceden escasa importancia a la seguridad frente a la funcionalidad y la interoperabilidad (Conti, Coss y Raymond, 2015, p. 5).

El *Plan Nacional de Ciudades Inteligentes* de 2015 no menciona la palabra ciberseguridad en todo el texto. El término seguridad solamente aparece asociado a accesibilidad, a la normativa técnica de automatización y a la seguridad de edificios y viviendas. El Plan está elaborado desde el punto de vista del fortalecimiento del sector industrial. Forma parte de la *Agenda Digital para España*, dedicada a promover «el incremento de la productividad de las empresas industriales incorporando las TIC a su proceso productivo y mejorar la disponibilidad de las infraestructuras de alta velocidad [y su objetivo es] contribuir al desarrollo económico» (Gobierno de España, 2015, pp. 1-2 y 10).

No es el único caso. El Plan estratégico de implantación de *smart cities*, auspiciado por la Comisión Europea, tampoco recoge las palabras seguridad ni ciberseguridad (European Innovation Partnership on Smart Cities and Communities, 2013). Las iniciativas de *smart cities* se han realizado con poca coordinación respecto a los daños a la privacidad y la seguridad y se han encajado en la gestión de la ciudad de manera improvisada y con una mínima visión estratégica (Kitchin, 2016, p. 54).

La ciberseguridad no solo está ausente de los planes estratégicos. En general, los métodos de evaluación tampoco la consideran. Suelen centrarse en sostenibilidad y resiliencia; rendimiento y competitividad de la ciudad; y gobernanza urbana. Solo dos modelos intentan valorar las soluciones TIC para *smart cities* directamente (Anthopoulos, Janssen y Weerakkody, 2015, p. 527).

Los sistemas TIC que supervisan y controlan una ciudad inteligente necesitan estar diseñados desde su concepción considerando la ciberseguridad, la robustez, la privacidad, la integridad de la información y, sobre todo, la resiliencia (Symantec, 2013, p. 1).

Conseguir la seguridad de las ciudades es un gran paso hacia la seguridad nacional frente a ciberataques. Entender los puntos de presión de una ciudad y las interdependencias entre infraestructuras críticas y no críticas puede contribuir a probar los límites de las defensas de la ciudad y a encontrar maneras de mitigar las vulnerabilidades derivadas de añadir nuevas

Fundación Telefónica
Telefónica

tecnologías originariamente diseñadas para mejorar la eficiencia energética y facilitar la habitabilidad.

Cualquier ciudad puede convertirse en una ciudad segura si incorpora análisis de inteligencia sobre amenazas y centros de operación en red y además realiza ejercicios y simulaciones de forma regular e inicia un régimen robusto de tests de penetración (Conti, Cross y Raymond, 2015, p. 11).

Un enfoque pragmático opta por una vía intermedia: consiste en identificar soluciones que permitan el despliegue de tecnologías de *smart city*, pero de manera que no sean perjudiciales para los ciudadanos. Por una parte, que minimicen activamente las brechas de datos y afronten las cuestiones de ciberseguridad. Por otra, que funcionen durante todo el ciclo de vida de las soluciones (desde el aprovisionamiento a la retirada) y se extiendan por todo el ecosistema (todos los componentes y todas las partes interesadas) (Kitchin, 2016, p. 48). Para conseguirlo, expertos en ciberseguridad recomiendan que las soluciones de *smart city* cumplan unos requerimientos básicos de seguridad, como muestra la tabla 3.

Tabla 3. Requerimientos básicos de seguridad para las soluciones de *smart cities*

Criptografía robusta	Para salvaguardar los datos almacenados y en tránsito todas las comunicaciones cableadas e inalámbricas deben estar correctamente protegidas con cifrado robusto.
Autenticación	Todos los sistemas deben requerir un nombre usuario y una contraseña para acceder a sus funciones, como mínimo. Para mejorar la autenticación, la solución debe ser compatible con métodos de autenticación robustos, como contraseñas de un solo uso, certificados o biometría, por ejemplo.
Autorización	Todas las funciones deben requerir el uso de permisos antes de realizar cualquier acción.
Actualizaciones seguras de todo el *software*	Las actualizaciones del *software* y del *firmware* deben estar disponibles y deben estar distribuidas de forma automática y segura.
Auditoría, alerta y registro de actividades	Todos los sistemas deben proporcionar mecanismos para auditar y llevar un registro de actividades de los usuarios. Además, esos registros deben guardarse de modo seguro y protegidos contra manipulaciones.
Capacidades anti-manipulación	Los dispositivos deben contar con mecanismos para evitar la manipulación por personas no autorizadas.
Cuentas sin puertas traseras, no documentadas o incrustadas en el código	Algunos proveedores comercializan sistemas con cuentas con puertas traseras, no documentadas o incrustadas en el *hardware* o el *software*. A menudo esas cuentas no se pueden eliminar, ni desactivar, y sus contraseñas no se pueden cambiar. Son una vía para comprometer el sistema.
Funciones no básicas desactivadas por defecto	Solo las funciones básicas deben estar activadas por defecto; el resto deben estar disponibles según las necesidades de la organización.
Cierre seguro anti-fallos	En casos de mal funcionamiento o de caída del sistema, este debe permanecer seguro y con las protecciones de seguridad activadas.
Seguridad por defecto	Todas las soluciones deben venir con una configuración segura por defecto.

Un método para garantizar que los proveedores se comprometen a cumplir los requisitos de seguridad en sus soluciones para *smart cities* es introducir cláusulas en los acuerdos de nivel de servicio (SLA), como las siguientes:
1) Un acuerdo sobre las características específicas de seguridad del producto. Debe quedar claro que la ausencia o el mal funcionamiento de esas prestaciones podrían tener consecuencias legales y/o financieras para el proveedor.
2) Un acuerdo por el que el proveedor proporcionará soporte fiable y probado las veinticuatro horas del día durante todo el año (24/7/365) para los incidentes de seguridad relacionados con sus productos. También se debe definir un marco temporal para proporcionar parches u otras soluciones cuando se descubran fallos de seguridad. El incumplimiento de esas condiciones podría conllevar consecuencias legales y/o financieras para el proveedor.
3) Un acuerdo mediante el cual el proveedor demuestre que cumple los requerimientos de seguridad a través de certificaciones y auditorías realizadas por terceros u otros medios.

Fuente: Elaboración propia a partir de Cerrudo, Hasbini y Russell (2016).

Fundación Telefónica
Telefónica

Conclusiones

La superficie de ataque de las ciudades es extensa y está completamente expuesta. Es un peligro real e inmediato. Cuanta más tecnología use una ciudad, más vulnerable será. Así, las *smart cities* tienen los riesgos más elevados. Es el momento de actuar para hacer ciudades más seguras y protegerlas frente a ciberataques. Resulta esencial auditar adecuadamente la seguridad de todas las tecnologías utilizadas en las ciudades antes de implantarlas. No hacerlo es temerario. La ingente cantidad de datos que alimentan los sistemas de una *smart city*, confiados ciegamente a la ciudad, puede ser fácilmente manipulada y los sistemas son fáciles de 'hackear'; así es como las ciudades inteligentes se convierten en ciudades tontas (Cerrudo, 2015, pp. 18-19).

La gestión de riesgos está relacionada con las zonas grises. El entorno tecnológico está en cambio constante. Es necesario emplear marcos adaptables para evaluar continuamente los puntos de referencia relacionados con los riesgos; eso permite identificar las lagunas de seguridad a lo largo del tiempo y enfrentarse a ellas adecuadamente (Hayslip, 2015, p. 4).

La ciberseguridad está prácticamente ausente de planes estratégicos y de métodos de evaluación sobre ciudades inteligentes. Eso es así incluso a pesar de que los sistemas de las *smart cities* están directamente relacionados con infraestructuras críticas, como las de transporte, energía, agua, administración, TIC o salud. Por interdependencias y reacciones en cadena, los fallos pueden afectar a otras infraestructuras, críticas y no críticas. Un simple error puede producir un gran impacto, por ejemplo, colapsos de tráfico, apagones generalizados o pasajeros atrapados en transportes públicos. Esto convierte la ciberseguridad de las *smart cities* en un asunto de seguridad nacional.

Se trata de construir ciudades inteligentes alrededor de la ciberseguridad y no al revés. Para lograrlo es fundamental introducir los requisitos de seguridad desde su concepción (*security by desig*n), en el momento del diseño. También es esencial tenerlos en cuenta a la hora de contratar soluciones para *smart cities* y durante toda su vida útil. Todo ello sin olvidar que la ciberseguridad está compuesta por estos elementos: confidencialidad y privacidad, integridad y disponibilidad.

Oferta y disponibilidad de libros digitales

El último aspecto está relacionado con la oferta y disponibilidad de libros digitales. En 2015, entre el 18 y el 25 por ciento de los títulos registrados en la región fueron digitales, una cifra que no ha variado demasiado en los últimos tres años.

Son muy pocas las editoriales que ponen a disposición su oferta de contenidos en formato digital y esto se convierte claramente en otra barrera para la evolución del negocio. Dentro de lo que se registra, se continúa publicando aún mucho en formato PDF y en menor proporción en ePub, y son excepcionales los casos donde se trabaja un formato enriquecido o interactivo o se piensa el libro digital bajo otro formato. Dentro de los rubros editoriales, los que más han decidido apostar por la digitalización son las editoriales de ficción, las que producen libros universitarios y las editoriales de textos escolares.

Fundación Telefónica
Telefónica

En el impulso de este y otros aspectos, es vital para América Latina la participación del Estado, ya sea como promotor de políticas específicas de fomento a la industria o bien generando las condiciones necesarias por cuenta propia. Esto último se ve con claridad a través de los planes de compra y distribución de netbooks, como el *Plan Conectar Igualdad* en Argentina[7] o el Plan Ceibal en Uruguay[8], donde millones de alumnos recibieron gratuitamente su computadora mientras transitan la escuela pública.

El Estado es también el principal comprador de contenidos para las bibliotecas y para el sistema educativo, pero hasta el momento lo ha realizado prioritariamente en formato papel. Se sabe ya que en varios países de la región comenzará a darse en los próximos años una mayor compra de contenidos digitales y eso podría impulsar a cambiar drásticamente el escenario. En los países de América Latina, las políticas estatales en esta dirección suelen ser el principal argumento para traccionar una dirección en las industrias.

Futuro incierto

Frente a estas condiciones, si el futuro del libro digital en el mundo es algo incierto y se encuentra en debate permanente, en esta fase donde toda la industria se encuentra explorando y buscando el modelo de negocio más adecuado, el escenario en América Latina es aún más incierto. Termina resultando nada sencillo para un lector animarse a leer un libro en formato digital. Por las dificultades que supone, es difícil que encuentre la versión digital de la obra que está buscando leer y, a falta de tiendas y proveedores con fuerte presencia, deberá explorar este camino prácticamente solo, sin ningún tipo de asistencia.

En un contexto tecnológico que claramente no acompaña, complejiza aún más el asunto una industria editorial que no ha sabido más que resistirse y negarse al cambio, a la espera hasta último instante para tomar la decisión. Esta resistencia está basada en varios pilares: el desconocimiento profundo en materia de nuevas tecnologías; el temor a la no posibilidad de negociación con los grandes grupos tecnológicos (Amazon, Apple y Google); la pérdida del monopolio de la producción y la distribución, tras la emergencia con fuerza de la autopublicación (y de plataformas que la incentivan); la idea aún muy presente de que lo digital atenta contra el actual negocio en papel (en ferias regionales, es todavía frecuente escuchar frases del tipo «No público en digital, porque si lo hago dejaré de vender en papel»); la negación absoluta a aplicar estrategias de *marketing*, asociándolas a la idea de una pérdida del valor del rol del editor en su labor de selección de contenidos, etc. En fin, una serie de motivos que actúan paralizando a la industria a la espera de que algo emerja, de que alguien les diga a los editores: «Señores, ya es negocio, ya pueden distribuir sus libros en formato digital».

Y lo cierto es que, si alguna vez eso ocurre, tal vez ya sea demasiado tarde.

Una revolución con enormes posibilidades

Estamos frente a la mayor revolución de la industria editorial. Una revolución que supone pensar en una forma mucho más amplia y superadora al clásico debate ‘lectura en papel’ versus ‘lectura en pantalla’. Una era en la que, del autor al lector, todo el flujo de producción editorial se desdibuja por completo y los roles ya no son tan claros y definidos.

Fundación Telefónica

Es lógico que un cambio de semejante magnitud genere miedos y temores. Pero es momento de pensar en lo digital como la respuesta para muchos de los problemas que hoy tenemos en la región.

Pensar en digital significa pensar en la posibilidad de democratizar los centros de producción de contenidos. Comenzar a equilibrar la balanza en este sentido implica que se puedan producir contenidos editoriales en cualquier parte del mundo para cualquier parte del mundo, y no únicamente desde los grandes centros urbanos, como ha ocurrido desde siempre.

Pensar en digital significa pensar que cualquier región de América Latina, incluso las más pobres y pequeñas, hoy tengan acceso y disponibilidad a la misma oferta de contenidos que cualquier ciudad de las principales urbes en Europa.

Pensar en digital significa unir y conectar a autores y lectores de una forma nunca antes imaginada y potenciar los lazos de América Latina. Y ahí está el más profundo sentido de la revolución digital que se le propone a la industria del libro (y al libro mismo), viendo la tecnología no como una amenaza, sino como una herramienta que la ayude a evolucionar más allá de sus límites físicos. Porque, en definitiva, lo que está en discusión es la forma misma que tenemos hoy de almacenar, compartir y consumir conocimientos, ideas, historias y sentimientos.

Pero para que todo esto sea posible en la región, se requiere de una evolución tecnológica muy fuerte, acompañada de un soporte de los Estados nacionales y de una nueva impronta del sector editorial, o bien de nuevos actores que puedan emerger, atravesados por nuevos saberes. Así dicho, y viendo el panorama preliminar, suena a un desafío casi imposible.

Lo cierto es que no debemos esperar que nada mágico ocurra. No debemos quedarnos de brazos cruzados y esperar a que una plataforma como Amazon u otra similar llegue a la región para que se comience a debatir el asunto. América Latina tiene una muy rica historia editorial y puede crear su propio camino digital también. Confío en que, más tarde o más temprano, así ocurrirá.

Bibliografía

Albino, V., Berardi, U. y Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology*, 22(1), 3-21.

Anthopoulos, L., Janssen, M. y Weerakkody, V. (2015). Comparing Smart Cities with Different Modeling Approaches. *Proceedings of the 24th International Conference on World Wide Web (WWW '15 Companion)*, 525-528. Nueva York: ACM.

Atkinson, R., Castro, D., Ezell, S. y McQuinn, A. (2016). *A Policymaker's Guide to Digital Infrastructure* [en línea]. Disponible en: *https://itif.org/publications/2016/05/16/policymakerE28099s-guide-digital-infrastructure* [Consulta: 2016, 1 de junio].

Fundación Telefónica
Telefónica

Bergenti, F., Chiappone, M. y Gotta, D. (2015). Smart Maintenance to Support Digital Life. En Murino, Vittorio, Puppo, Enrico, Sona, Diego, Cristani, Marco & Sansone, Carlo (Eds.), *New Trends in Image Analysis and Processing – ICIAP 2015 Workshops*, 226-233. Suiza: Springer.

CAICT & PDSF (2014). *Comparative Study of Smart Cities in Europe and China 2014*. Berlín: Springer.

Cerrudo, C. (2015). *An Emerging US (and World) Threat: Cities Wide open to Cyber Attacks* [en línea]. Disponible en: *http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf* [Consulta: 2016, 25 de mayo].

-, Hasbini, A. y Russell, B. (2016). *Cyber Security Guidelines for Smart City Technology Adoption* [en línea]. Disponible en: *http://securingsmartcities.org/wp-content/uploads/2016/03/Guidlines_for_Safe_Smart_Cities-1.pdf* [Consulta: 2016, 25 de mayo].

Conti, G., Cross, T. y Raymond, D. (2015, agosto). *Pen Testing a City. Black Hat USA, Las Vegas (Estados Unidos)*. Disponible en: *https://www.blackhat.com/docs/us-15/materials/us-15-Conti-Pen-Testing-A-City-wp.pdf* [Consulta: 2016, 17 de mayo].

Elmaghraby, A. S. y Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research 5*, 491-497.

European Innovation Partnership on Smart Cities and Communities (2013, 14 de octubre). *Strategic Implementation Plan* [en línea]. Disponible en: *http://ec.europa.eu/eip/smartcities/files/sip_final_en.pdf* [Consulta: 2016, 17 de mayo].

European Parliament (2014). *Mapping Smart Cities in the EU* [en línea]. Disponible en: *http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET282014 29507480_EN.pdf* [Consulta: 2016, 25 de mayo].

Gobierno de España (2015, marzo). *Plan Nacional de Ciudades Inteligentes* [en línea]. Disponible en: *http://www.minetur.gob.es/turismo/es-ES/Novedades/Documents/Plan_Nacional_de_Ciudades_Inteligentes.pdf* [Consulta: 2016, 25 de mayo].

Hasbini, M. A., Cerrudo, C., Jordan, D., El-Haddadeh, R., Seow, A. y Pawaskar, S. (2016). *The Smart City Department Cyber Security role and implications* [en línea]. Disponible en: *http://securingsmartcities.org/wp-content/uploads/2016/03/SCD-guidlines.pdf* [Consulta: 2016, 25 de mayo].

Hayslip, G. (2016). *What I have learned as CISO for a Smart City* [en línea]. Disponible en: *https://www.linkedin.com/pulse/what-i-have-learned-ciso-smart-city-cissp-cisa-crisc-ccsk*

Fundación Telefónica
Telefónica

[Consulta: 2016, 17 de mayo].

Ijaz, S., Shah, M. A., Khan, A. y Ahmed, M. (2016). Smart Cities: A Survey on Security Concerns. *International Journal of Advanced Computer Science and Applications*, 7 (2), 612-625.

Kitchin, R. (2016, 28 de enero). *Getting smarter about smart cities: Improving data privacy and data security* [en línea]. Dublín: Data Protection Unit, Department of the Taoiseach. Disponible en: *http://www.taoiseach.gov.ie/eng/Publications/Publications_2016/Smart_Cities_Report_January_2016.pdf* [Consulta: 2016, 25 de mayo].

National Protection and Programs Directorate. Office of Cyber and Infrastructure Analysis. U.S. Department of Homeland Security (2015, agosto). *The Future of Smart Cities: Cyber-Physical Infrastructure Risk* [en línea]. Disponible en: *https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA20-20The20Future20of20Smart20Cities20-20Cyber-Physical20Infrastructure20Risk.pdf* [Consulta: 2016, 17 de mayo].

Office of the Auditor General of Canada (2012). *Report of the Auditor General of Canada to the House of Commons. Chapter 3 Protecting Canadian Critical Infrastructure Against Cyber Threats* [en línea]. Disponible en: *http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf* [Consulta: 2016, 18 de mayo].

Pederson, P., Dudenhoeffer, D., Hartley, S. y Permann, M. (2006, agosto). *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research* [en línea]. Disponible en: *https://inldigitallibrary.inl.gov/sti/3489532.pd*f [Consulta: 2016, 25 de mayo].

PwC & IE Business School (2015). *Smart Cities: La ciudad como plataforma de transformación digital* [en línea]. Disponible en: *https://iot.telefonica.com/libroblanco-smart-cities/media/libro-blanco-smart-cities-esp-2015.pdf* [Consulta: 2016, 25 de mayo].

Symantec (2013). *Transformational 'smart cities': cyber security and resilience* [en línea]. Disponible en: *https://eu-smartcities.eu/sites/all/files/blog/files/Transformational20Smart20Cities20-20Symantec20Executive20Report.pdf* [Consulta: 2016, 25 de mayo].

Telefónica (2015). *Una Ciudad. Cientos de posibilidades. Smart Cities: La Ciudad como plataforma de Transformación Digital* [en línea]. Disponible en: *https://www.telefonica.com/documents/341171/3261893/POLICY+PAPER_Smart+Cities_ES+La+Ciudad+como+plataforma+de+TransformaciC3B3n+Digital++Abril+2016.pdf/2c8ed5af-8690-44c2-aab0-4cbe3d1d89c2* [Consulta: 2016, 25 de mayo].

Fundación Telefónica

Fundación Telefónica
Telefónica