Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Análisis de seguridad en las Smart Cities

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Andrés Gutiérrez Hernández

DIRECTORES: Javier Vales Alonso

Francisco Javier Rodríguez Martínez

CURSO ACADÉMICO: 2021-2022

Universidade Vigo

Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Análisis de seguridad en las Smart Cities

Máster Universitario en Dirección TIC para la Defensa

Especialidad de Sistemas y Tecnologías de la Información

Universidade Vigo

RESUMEN

Las ciudades son una de las características más identificables de la especie humana, las hay en todas las culturas y representan un poderoso indicador de crecimiento económico y social. Hoy en día la mayor parte de la población se desplaza a áreas urbanas para la mejora de su calidad de vida.

El propósito de este trabajo es el de ofrecer mediante un ejercicio teórico de análisis de riesgos una visión de la seguridad en la ciudad inteligente.

Una ciudad inteligente es aquella que se encuentra en un proceso de mejora continua, especialmente TIC, para mejorar su sostenibilidad, calidad de vida, eficiencia de servicios y competitividad.

En ese sentido llama la atención la incorporación de nuevas tecnologías como Big Data, Data Mining, el uso de la nube y aquellas relacionadas con el Internet de las Cosas.

Durante el análisis se identifican los servicios que describen con más exactitud a la mayor parte de las ciudades inteligentes de hoy en día en España, como la gestión de residuos o control avanzado de tráfico. Se identifican los activos más importantes de estos servicios. Posteriormente se analizan las ciberamenazas más comunes. Finalmente se correlaciona amenaza y activos para obtener un mapa de calor de riesgos.

Como resultado se observa que aumentan algo nuevos entornos de riesgos como contadores inteligentes y dispositivos IoT. Sin embargo, lo más llamativo es cómo aumenta la dependencia con la infraestructura TIC tradicional, el aumento de puntos de acceso a internet y las relaciones con terceros, especialmente por la nube.

PALABRAS CLAVE

CIUDAD, INTELIGENTE, SEGURIDAD, RIESGOS, ANÁLISIS

AGRADECIMIENTOS

Agradezco este proyecto a todas las personas que me han prestado apoyo, mi tutor Javier Vales Alonso y a mi familia que ha aguantado estoicamente este último año.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

Las ciudades son una de las características más identificables de la especie humana, las hay en todas las culturas y representan un poderoso indicador de crecimiento económico y social. Hoy en día la mayor parte de la población se desplaza a áreas urbanas para la mejora de su calidad de vida.

No obstante, el funcionamiento de las ciudades dista de ser perfecto, las agrupaciones de población exigen una demanda muy alta de recursos, energía, agua y de servicios como educación, seguridad o sanidad entre otros. Las ciudades son un agente importante en el calentamiento global por sus emisiones y consumo. Además, el crecimiento se prevé que seguirá incrementándose en el tiempo y para 2050 se estima que el 70% de la población vivirá en grandes ciudades.

A este contexto se le une la evolución de las Tecnologías de Información de las Comunicaciones (TIC) cuyo uso y utilidad ha crecido exponencialmente durante las últimas décadas y especialmente por la llegada de las redes de datos e Internet. Estas tecnologías se han demostrado muy eficientes en la mejora y adaptación de procesos, creando nuevas maneras de hacer las cosas que aportan más valor. También se pueden aplicar a las administraciones mejorando muchos aspectos de funcionamiento de estas como economía, toma de decisiones, gobernanza, etc.

La unión de estas dos situaciones ha creado el concepto conocido como Ciudades Inteligentes. Este comprende la necesidad de propiciar un desarrollo sostenible y eficiente de las ciudades junto a la necesidad de transformar digitalmente el funcionamiento de estas. A este respecto merece la pena el nombre utilizado en el idioma anglosajón, Smart and Sustainable Cities (SSC). Lo que nos indica que el concepto de Ciudad Inteligente va más allá de digitalizar una ciudad, sino que involucra también una reestructuración del funcionamiento de la misma, incluido una orientación sostenible y de conciencia con el medio ambiente.

La Ciudad Inteligente es un objetivo complejo, que implica líneas estratégicas, tácticas y operativas sostenidas en el tiempo. La correcta gestión de nuevos proyectos e inversiones. Y, sobre todo, una entrega total a las TIC, que se implicarán en todos los procesos y mejoras en la ciudad. Esto conlleva muchas ventajas, pero también inconvenientes, con la llegada de las TIC aparecen vulnerabilidades que no existían previamente y por tanto se requiere aplicar conceptos de seguridad TIC en todos los procesos en los que las nuevas tecnologías se involucren.

En ese sentido la seguridad TIC se considera un concepto holístico, aplica a todos los niveles de gestión, abarca todos los ámbitos de tecnología y especialmente se debe contemplar en todas las fases, incluyendo por supuesto el diseño. Y a ese respecto es por lo que se ha realizado este trabajo fin de máster.

1.2 Objeto del trabajo

El propósito de este trabajo es el de ofrecer mediante un ejercicio teórico de análisis de riesgos una visión de la seguridad en la Ciudad Inteligente. Al realizarlo de esta forma se ofrece una forma práctica y con perspectiva de lo que un responsable de seguridad debe tener en cuenta cuando se trate con dichas ciudades. De forma genérica también sirve para ver como los análisis de riesgos deben adaptarse cuando se ejecuten, deben contemplar mientras se realizan las propiedades de las organizaciones y situaciones.

Más concretamente durante el trabajo se abordarán los siguientes puntos:

- Definir el estado del arte de la ciudad y ciudad inteligente.
- Investigar aquellas tecnologías más utilizadas en la implantación de la ciudad inteligente.
- Identificar los servicios de la ciudad inteligente y ponderar su relevancia con respecto a la ciudad y la seguridad de la información.
- Analizar los diferentes servicios y comprender a alto nivel su estructura y funcionamiento y su encaje en la arquitectura de una ciudad inteligente.
- Realizar una investigación del estado actual en cuanto al panorama de ciberamenazas.
- Específicamente revisar las amenazas propias de aquellas tecnologías empleadas por los sistemas que componen la ciudad inteligente.
- Ponderar las amenazas encontradas en función a su posible daño a la ciudad inteligente y la posibilidad de que se materialicen.
- Extraer el los riesgos de forma ordenada en función de su criticidad.
- Desarrollar posibles medidas y controles de seguridad contra los riesgos encontrados.

Desde el punto de vista del máster DIRETIC se pretenden poner en práctica muchos conceptos de los aplicados durante éste. Especialmente relevantes serán los conceptos de las materias de seguridad TIC y análisis de riesgos.

2 ESTADO DEL ARTE

2.1 Descripción de ciudad.

Según la real academia española el término ciudad, proviene del término *civĭtas, -ātis, y* tiene como significado:

1. f. Conjunto de edificios y calles, regidos por un ayuntamiento, cuya población densa y numerosa se dedica por lo común a actividades no agrícolas.
2. f. Lo urbano, en oposición a lo rural.
3. f. Ayuntamiento o cabildo de cualquier ciudad.
4. f. Título de algunas poblaciones que gozaban de mayores preeminencias que las villas.
5. f. Conjunto de diputados o procuradores en Cortes que representaban una ciudad.

Tabla 2-1 Definición de ciudad. [1]

Estrictamente, en España se considera ciudad a aquellos municipios de más de 10.000 habitantes. Como se indica en el diccionario la ciudad suele tener una morfología determinada que se compone de edificios y calles. Finalmente, la ciudad lleva aparejado un conjunto de actividades variadas en las que destacan especialmente los servicios públicos que se prestan en ellas.

No obstante, el concepto de ciudad es muy antiguo y complejo, varía de país en país y es una entidad que se ha desarrollado históricamente dentro de diferentes sociedades humanas y está muy ligado a la cultura de una determinada población. Se conocen restos de ciudades que datan desde el 3.000 a.c, las hay en todos los continentes y de todas las culturas. En Europa muchas de las más antiguas se distribuyen por la costa del mar Mediterráneo y oriente próximo, algunas de las mas antiguas pueden ser Tiro, Sidón, Cartago o concretamente en España, Cádiz.

Figura A1-1 Puerta de acceso a la ciudad de Persépolis, Irán [2]

Una ciudad no es solamente el asentamiento de una determinada población. Hay festivales como el Tomorrowland que puede llegar a tener como asistentes 360.000 personas durante los días de duración y disponen de edificios y diferentes servicios durante ese tiempo; también hay campamentos y bases militares durante el desarrollo de una operación militar con características similares y no son consideradas ciudades. Las ciudades tienen atribuciones y funciones políticas, administrativas, económicas y religiosas.

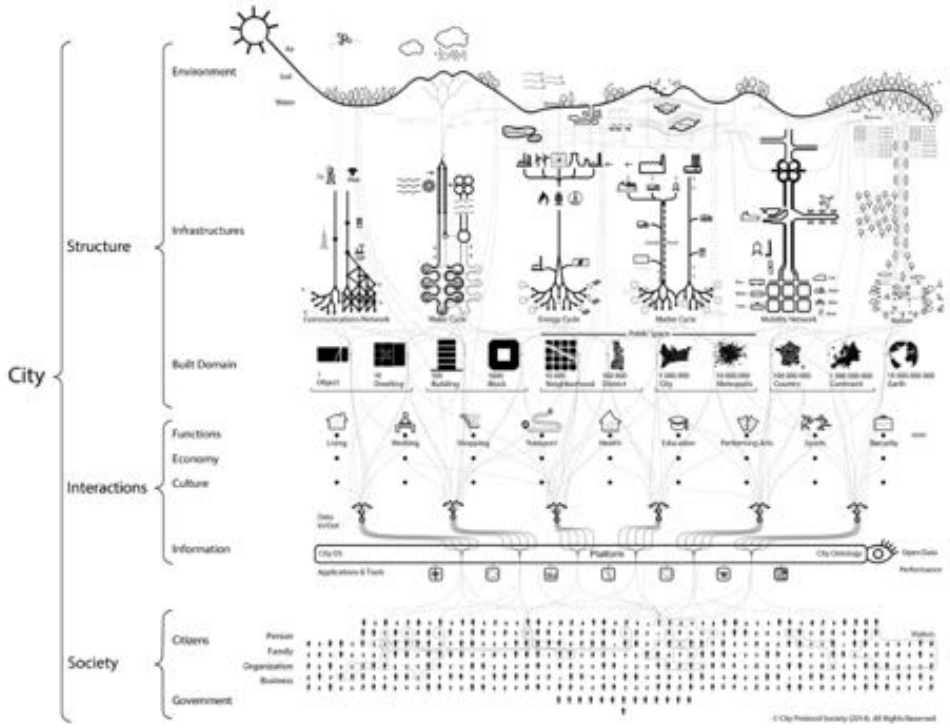


Figura A1-2 Esquema ontológico de una ciudad [3]

Desde el punto de vista político y legislativo la ciudad tiene cierto grado de autonomía y responsabilidad de acuerdo a las normas nacionales y tratados internacionales, normalmente es el eslabón más bajo de la cadena y por tanto órgano de gobierno más próximo a los ciudadanos.

En el aspecto cultural y religioso las ciudades tienen la responsabilidad de satisfacer las necesidades que tienen los propios ciudadanos a dicho respecto. En ese sentido están muy influidas por las corrientes sociales y culturales de su población y la historia de la propia ciudad, que definirán muchas de las actividades, legislación y características de estas.

Por ejemplo: la ciudad de Sevilla tiene la responsabilidad de desarrollar y facilitar actividades como la feria de Sevilla o la Semana Santa, de carácter religioso. También la arquitectura es diferente: Ciudad Rodrigo es una ciudad medieval amurallada debido a su evolución histórica.

Otras atribuciones que tienen las ciudades es la gestión e impulso de medidas de tipo económico. Este tipo de medidas incluyen la asignación de espacios urbanos para uso industrial y de oficinas, la creación de ordenanzas para los locales comerciales, actividades de impulso a la innovación. También medidas de bienestar como ayudas para ciudadanos en situación de pobreza.

Respecto a ese último punto, la principal atribución legal que suele tener el gobierno de una ciudad es el de prestar servicios públicos al ciudadano, enmarcado en el estado del bienestar. Los más importantes para una ciudad media son la infraestructura eléctrica, agua corriente y de tráfico. Pero hay muchos más

como la gestión de la gestión de residuos, garantizar la seguridad ciudadana, control de la urbanización y gestión de los recursos naturales, colaboración en la prestación de servicios de salud y de asistencia al ciudadano, facilitar trámites administrativos, garantizar niveles óptimos de contaminación del medio ambiente o la gestión de medios de transporte de diferente tipo.

En resumen, es una entidad que responde a muchas condiciones de contorno. Estas condiciones de contorno afectan mucho a su composición, servicios y actividades y se deben de tener en cuenta a la hora de llevar a cabo un análisis de seguridad TIC.

2.1.1 Aspectos legales de una ciudad. Caso particular en España.

En el ámbito de la legislación española, las ciudades o municipios son una de las entidades que conforman la parte del sector público correspondiente a la administración local. Otras entidades serían las provincias, las islas, o mancomunidades etc.

El municipio es el intermediario directo entre la ciudadanía y asuntos públicos, gestiona con autonomía los intereses de los vecinos que lo componen y a través del ayuntamiento como órgano de gobierno pueden promover actividades y prestar servicios públicos.

Las fuentes de derecho que afectan a las entidades locales son muchas en general se pueden resumir en las siguientes aplicadas en orden:

- La Constitución española de 1978.
- Los tratados internacionales.
- La ley y las disposiciones normativas con fuerza de ley.
- El reglamento.
- La costumbre.
- Los principios generales del derecho.

Destacar en ese respecto el reconocimiento de la autonomía local en la CE en su Título VIII. Los artículos 137, 140 y 141 recogen declaraciones expresas. También destacar la Ley Reguladora de Bases del Régimen Local, LBRL (LO Ley Orgánica 7/1985) donde se desarrolla la actual legislación en materia de administración local.

En cuanto a la legislación, el Estado tiene las competencias para desarrollar la legislación básica de acuerdo a lo indicado en la Constitución española, sin perjuicio de que esta sea desarrollada por las comunidades autónomas de las que formen parte. Las entidades locales también tienen potestad reglamentaria para elaborar ordenanzas y reglamentos locales.

Entre las competencias que la legislación atribuye a las entidades locales se encuentra la prestación de servicios mínimos, estos vienen delimitados en función del númerode habitantes que disponga la ciudad [4]:

Todos los municipios

- Alumbrado público
- Cementerio
- Recogida de residuos

- Limpieza viaria
- Alcantarillado
- Abastecimiento domiciliario de agua potable
- Acceso a los núcleos de población
- Pavimentación de las vías públicas
- Control de alimentos y bebidas

Municipios de más de 5.000 habitantes

- Parque público
- Biblioteca pública
- Mercado
- Tratamiento de residuos

Municipios de más de 20.000 habitantes

- Protección civil
- Prevención y extinción de incendios
- Prestación de servicios sociales
- Instalaciones deportivas de uso público

Municipios de más de 50.000 habitantes

- Transporte colectivo urbano de viajeros
- Protección del medio ambiente

Los municipios serán apoyados en esta labor por las diputaciones provinciales, especialmente aquellos de pocos habitantes.

Normativa	Denominación
Ley Orgánica 7/1985	Ley reguladora de las Bases de Régimen Local.
Ley Orgánica 15/1999	Ley Orgánica de Protección de Datos de Carácter Personal
Real Decreto Legislativo 781/1986	Texto Refundido de las disposiciones legales vigentes en materia de Régimen Local.
Real Decreto Legislativo 2/2004	Texto Refundido de la Ley Reguladora de las Haciendas Locales
Real Decreto Legislativo 3/2011	Texto Refundido de la Ley de Contratos del Sector Público
Decreto	Reglamento de Servicios de las Corporaciones Locales.
Real Decreto 1372/1986	Reglamento de Bienes de la Entidades Locales.
Real Decreto 2568/1986	Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.
Ley 9/2001	Suelo de la Comunidad de Madrid

Ley 33/2003	Patrimonio de las Administraciones Públicas.
Ley 19/2013	Transparencia, acceso a la información pública y buen gobierno
Ley 39/2015	Procedimiento Administrativo Común de las Administraciones Públicas
Ley 40/2015	Régimen Jurídico del Sector Público

Tabla 2-2 Legislación básica del Estado en el ámbito de la administración local. [5]

2.2 Descripción de ciudad inteligente

2.2.1 Definición

Según la norma UNE 178201:2016. " Ciudades Inteligentes Definición, atributos y requisitos"

"Una ciudad inteligente es una ciudad justa y equitativa centrada en el ciudadano que mejora continuamente su sostenibilidad y resiliencia aprovechando el conocimiento y los recursos disponibles, especialmente las TIC, para mejorar la calidad de vida, la eficiencia de los servicios urbanos, la innovación y la competitividad sin comprometer las necesidades futuras en aspectos económicos, de gobernanza y medioambientales. " sic [6]

2.2.2 Atributos principales

Las ciudades inteligentes, al igual que el concepto de ciudad, son entidades complejas. Para poder comprenderlas mejor se suelen dividir en partes según el enfoque que se utilice para su análisis. En el caso de la ITU y su norma UNE correspondiente, que es el más utilizado, se pueden diferenciar seis ámbitos clave:

Ámbito		
• Economía inteligente		Persigue añadir valor a la economía mediante eficiencia y nuevos modelos de negocio que fomenten la innovación. Implica interconexión y compartición de conocimientos. Todo ello respetando y con un enfoque de sostenibilidad económica y medioambiental.

• Gobernanza inteligente		En este ámbito se incluye una gestión global, donde se integran todos los elementos de dirección, gobierno y organizaciones públicas y privadas. Se deben aplicar las TIC para conseguir un gobierno justo, eficiente, coordinado (Buen gobierno), transparente, con una gestión mejorada e integrada en las TC (electrónico) y que contemple la proyección de la información como un derecho de la ciudadanía.
• Entorno inteligente		Este pretende la gestión eficiente de los recursos que se sirven a la ciudadanía o que permiten la gestión de estos dentro de la ciudad. Se podría dividir en tres, cuidado al entorno natural, infraestructuras y urbanismo. Siempre atendiendo a parámetros de eficiencia y sostenibilidad medioambiental.
• Movilidad inteligente		En este se engloban los sistemas logísticos y de transporte para facilitar la movilidad de las personas y el acceso a todos los servicios. En este ámbito se prioriza el transporte accesible y ecológico, reduciendo tiempos de desplazamiento, costes y contaminantes. Para ellos se enfoca en infraestructuras de tráfico o transportes, gestión de las vías y rutas de una forma más eficiente, y se prioriza el uso de las TIC para el tratamiento y solución de problemas.
• Sociedad inteligente		Se entiende como la parte que se enfoca en la interacción con las personas, entre sí y con los actores de la ciudad con el objetivo de potenciar el capital humano y social. En este punto influye la educación, potenciar la creatividad, respeto a la pluralidad, inclusión social y participación activa.
• Bienestar inteligente		Este ámbito se enfoca hacia la calidad de vida. Es un concepto amplio y probablemente dependa del tipo de ciudad, pero en resumen se relaciona con el atractivo para vivir y trabajar. Por tanto, podremos encontrar medidas como calidad del equipamiento urbano, la vivienda, seguridad, sanidad, patrimonio histórico, ocio y otros.

Tabla 2-3 Principales atributos de una ciudad inteligente. [6]

Mientras que los atributos definen los dominios o ámbitos clave, los requisitos son las condiciones que tiene que cumplir una ciudad en cada uno de esos dominios que la acercan a considerarse una ciudad inteligente.
Los anteriores dominios son más estables, los indicadores de ciudad lo son menos. AENOR define seis que abarcan la mayor parte de indicadores utilizados. Estos conjuntos pueden componerse a su vez de diferentes tipos de métricas y subcategorías. Nos referiremos a las más generales.

• Tecnologías de la información y las comunicaciones	Indicadores de madurez relacionados con las TIC. Todo lo que engloba tratamiento de la información, redes, telefonía, etc. Incluidos la privacidad y seguridad TIC. Los relacionados con la infraestructura de comunicaciones física se agrupa en el de infraestructura.
• Sostenibilidad Medioambiental	Eficiencia de aprovechamiento de la energía y utilización de recursos naturales. Se incluye la sostenibilidad medioambiental.
• Productividad	Desempeño de variables económicas: empleo, capital , inflación, comercio ahorro, exportación / importación, ingresos, consumo, innovación e intangibles como conocimiento.
• Calidad de Vida	Relacionados con bienestar: educación, salud, seguridad, y espacio publico.
• Igualdad e Inclusión Social	Igualdad de derechos, justicia e inclusión social. También se incluyen aspectos democráticos como transparencia, participación y gobernanza.
• Infraestructura física	Divide las infraestructuras respecto a servicios comunitarios y vivienda. El primero relacionado con los servicios (agua, alcantarillado, electricidad, TIC), gestión de residuos, infraestructura de conocimientos (bibliotecas o museos), infraestructura de salud, transporte y vial. En cuanto a la vivienda se refiere al tipo de espacio y características.

Tabla 2-4 Requisitos de una ciudad inteligente. [6]

Como se puede observar, el concepto de ciudad inteligente abarca más allá de las tecnologías de la información. En este proyecto, no obstante, no nos centraremos en otros parámetros salvo que estos afecten de alguna forma a la seguridad de la información.

2.2.1 Legislación aplicada las TIC en la administración local en España

Al igual que la entidad de ciudad se desarrolla como enmarcada en la administración local dentro del ámbito legislativo, la ciudad inteligente también tiene un reflejo en la normativa española. Desde hace unos años el estado ha tomado conciencia de la importancia de las nuevas tecnologías en la gestión de las actividades y en consecuencia desarrollando leyes que amplían los derechos y procesos administrativos para incluir el uso de las nuevas tecnologías.

Los primeros conceptos TIC que se legislan son los clásicos en cuanto a las telecomunicaciones, especialmente debido al uso de la radio y televisión y la necesidad de configurar el espacio radioeléctrico de una manera racional. También supuso la liberación de las telecomunicaciones.

Respecto a la sociedad de la información y el mudo TIC de procesamiento de información como lo conocemos se comienza a legislar a través de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. En ella se recogen conceptos de la sociedad de la información y comienza a definir figuras para adaptar a la administración española a los nuevos conceptos.

En ella por ejemplo se contempla una figura para regular el espacio de nombres ".es" (Red.es aprobado por el estatuto RD 164/2002, de 8 de febrero) .También se define una gestión de incidentes de seguridad autoridad a nivel estatal, responsable coordinar entidades administración en el uso de cifra, garantizar la seguridad de la información de las TIC y formar al personal de la administración en este campo. Esta labor la asume el CCN a través de las atribuciones del CNI y del propio estatuto del CCN. Cualquier administración debe informar al CCN en caso de tener un incidente de seguridad. (Ley 11/2002 reguladora del CNI y art. 1 del Real Decreto 421/2004, por el que se regula el CCN)

Posteriormente y con apoyo del CCN se elabora el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad. Este real decreto es una adaptación de las medidas de sistemas de gestión de la seguridad de la información a la legislación española con lo que ahora por ley las administraciones locales deberán adscribirse a medidas similares a las de una empresa con certificación ISO 27001 de seguridad de la información.

Otras leyes que merece la pena destacar son la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos, o la Ley 25/2013, de impulso de la factura electrónica y creación del registro contable de facturas en el sector público. Estas fueron las primeras leyes que reconocían el derecho de los ciudadanos a relacionarse por medios digitales con la administración.

La ley 11/2007 se sustituye con la nueva Ley de Procedimiento Administrativo Común de las Administraciones Públicas (Ley 39/2015) en el que ya se contempla el uso de dichos medios en los procedimientos administrativos. El Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público que desarrolla la ley también es interesante dado que en él se declara el uso obligatorio y preferente de los servicios

Los medios y servicios TIC de la AGE y sus OOPP serán declarados de uso compartido cuando, en razón de su naturaleza o del interés común, respondan a necesidades transversales de un número significativo de unidades administrativas. (art. 10.1 del Real Decreto 806/2014, de 19 de septiembre).
La utilización de los medios y servicios compartidos será de carácter obligatorio y sustitutivo respecto a los medios y servicios particulares empleados por las distintas unidades. (art. 10.3).

Por último, pero no menos importante está el reglamento de protección de datos y derechos digitales europeo y su trasposición a la legislación española mediante la Ley Orgánica 3/2018. En ella se regulan las medidas que se deben tomar cuando se desea tratar datos de carácter personal, es complementaria en este caso a las medidas del ENS.

Normativa	Denominación
Ley 34/2002	Servicios de la sociedad de la información y de comercio electrónico
Ley 11/2007	Ley de acceso electrónico de los ciudadanos a los servicios públicos
Ley 25/2007	Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones
Ley 56/2007	Medidas de Impulso de la Sociedad de la Información: modifica en parte la legislación del sector
ENS 3/2010	Esquema nacional de seguridad
ENI 4/2010	Esquema nacional de interoperabilidad
Ley 19/2013	Transparencia, acceso a la información pública y buen gobierno
Ley 25/2013	Impulso de la factura electrónica y creación del registro contable de facturas en el sector público.
Ley 9/2014	Ley General de Telecomunicaciones
Ley 39/2015	Procedimiento Administrativo Común de las Administraciones Públicas
Ley 40/2015	Régimen Jurídico del Sector Público
LO 3/2018	Reglamento de protección de datos y garantía de derechos digitales.
RD 203/2021	Reglamento de actuación y funcionamiento del sector público

Tabla 2-5 Legislación relacionada con las TIC y la sociedad de la información.

2.2.2 Tecnologías principales

Durante el análisis de riesgos es preciso conocer los activos que en conjunto construyen los sistemas que dan servicio a la ciudad inteligente.

Las diferentes tecnologías empleadas en la ciudad inteligente pueden cubrir prácticamente todo el espectro disponible en las TIC. En ese sentido, para el trabajo se ha intentado reducirlo a aquellas tecnologías novedosas o que afectarían más a lo que viene siendo una aplicación de la transformación digital a los municipios de la actualidad.

En ese sentido se incluyen aquellas tecnologías relacionadas con el Internet de las Cosas y procesos de Big Data y Data Mining. También se describen algunos conceptos que incluyen muchas veces la literatura de ciudad inteligente y son importantes para comprender las implicaciones.

Algunos conceptos generales son:

- **Redes eléctricas inteligentes o Smart Grid** [7] .

  Los Smart Grid aparecen prácticamente siempre que se habla del IoT o más en concreto de la ciudad inteligente. Consisten en dotar de procesos de análisis y sincronización avanzada a la infraestructura de los proveedores de energía eléctrica.

  Normalmente cuando se habla de ellos se refiere al último tramo, el que dota a los hogares de energía, ya a baja potencia, y con contadores que hacen lecturas del consumo de la vivienda. Sin embargo, el concepto es más amplio y hace referencia a toda la cadena de producción, estaciones generadoras, centros de transformación, líneas de alta tensión, etc.

  Para la ciudad inteligente se aplica en la lectura y control del sistema de alumbrado eléctrico y medidas de bienestar en edificios para controlar el consumo o comprobar que determinadas zonas tienen un acceso correcto.

  Estas redes se suelen dividir en tres partes:

  - Contadores inteligentes. Los diferencian en dos tipos: AMR (Automatic Meter Reading) y AMI (Advanced Metering Infrastructure). Ambos realizan la función de telemedida. La diferencia entre uno y otro estriba en que mientras el primero es un elemento pasivo de comunicación unidireccional el otro permite realizar tareas de telegestión. Los utilizan las distribuidoras para realizar tareas de facturación o seguimiento.

    Esta tecnología no deja de ser la aplicación de dispositivos sensores / actuadores de IoT a la red eléctrica.

    - Comunicaciones MCI (Meter Communication Infrastructure). Con esto se refieren a las comunicaciones empleadas por los contadores para enviar la información que obtienen. Utilizan las mismas tecnologías que se pueden emplear en IoT (GPRS, GSM, LTE, ZigBee u otros) pero la más utilizada es PLC (Power Line Communications) en las que se utiliza la propia red y por tanto reduce la dependencia con un proveedor.

    - Por último se tiene la capa de datos, Meter Data Management MDM. Esta capa suele constituirse por un sistema Big Data capaz de analizar toda la información que proviene de contadores, estaciones, facturación, etc.

- **Sistemas M2M** [8]**.**

Hacen referencia al intercambio de datos entre dos máquinas conectadas (machine to machine) a través de un enlace directo o de la propia red. Se pueden hablar de sistemas capilares cuando se hace uso de un conmutador para la transmisión de información hacia la red y de sistemas móviles cuando se hace uso con una tecnología tipo LTE-M que permite conectar los dispositivos directamente a las redes de proveedores.

- Redes inalámbricas de sensores (WSN) [9]

  Son redes inalámbricas que consisten en un gran númerode dispositivos equipados con sensores y repartidos en un área grande de trabajo. Estos dispositivos se enlazan entre ellos de una manera autónoma sin la intervención de un administrador.
  Son una clase de red de tipo ad-hoc. En este tipo de redes los nodos se comunican entre sí a través de un canal inalámbrico común, no se necesita infraestructura adicional. Todos los nodos tienen transceptores que también implementan lógica de enrutado para pasar paquetes a otros nodos. La virtud de este tipo de red es la capacidad de autorregularse una vez desplegados los dispositivos.

  Una red WSN es una red ad-hoc especializada en la monitorización y empleo de dispositivos IoT mientras que las redes ad-hoc normales se suelen utilizar más para comunicaciones.

- **Cloud computing o la Nube.**

Cuando se habla de la nube en general no se hace una idea precisa del significado. Hay varias interpretaciones, pero en general se suele hablar de un ecosistema de recursos de computación que permite facilitar la aplicación de servicios y desarrollos de nuevas aplicaciones. Al hablar de ecosistema nos indica que debe proporcionar un mínimo sistema de abstracción de los servicios TIC tradicionales, ya sea en forma privada o público. Por ejemplo, un CPD propio o un servicio de hosting no se considerará como nube tal cual.

Las nubes se pueden clasificar en distintos tipos según el propietario de ese ecosistema. De esta forma tenemos nubes privadas cuando es la propia organización la que ha creado o mantiene ese ecosistema. Las nubes públicas son aquellas que utilizan los servicios de terceros para los sistemas TIC, las más conocidas son AWS (Amazon), Azure (Microsoft) y GCP (Google). Con diferencia Amazon es la más utilizada.

En cuanto al tipo de servicio, las nubes se pueden clasificar según el nivel de abstracción que se consiga en el ecosistema. Aquí podemos diferenciar IaaS en las que se gestionan los recursos de computación, almacenamiento, software básico y redes. El segundo tipo sería PaaS en la que se ofrecen ayudas para el despliegue de aplicaciones y el desarrollo de entornos DevOps. Y finalmente SaaS en donde el nivel de abstracción llega al punto que solo se dispone del servicio final. Los sistemas comerciales como AWS ofrecen servicios en todos estos niveles. En cuanto sistemas open source tendríamos algunos como Open-Stack o Eucalyptus (IaaS), Foundry y WSO2 (PaaS) y SaaS muchísimos como por ejemplo NextCloud para compartición de ficheros, pero también de análisis de datos, salvaguarda, etc.

En cuanto a las tecnologías a más bajo nivel, las más importantes son las relacionadas con el IoT, el análisis de datos y el uso de teléfonos inteligentes:

- **Relacionadas con IoT:**

  El IoT se define de muchas formas, algunos lo definen como un entorno en el que todo tiene capacidad de computación y comunicación con otros sistemas de información. Otros autores lo señalan como la interacción del mundo físico con el digital mediante sensores y actuadores. El trabajo se centra en esta última dado que refleja lo que se utiliza en una ciudad inteligente. Dentro de esta categoría podemos destacar:

  - Sensores [8]. Se encargan de recoger la información del mundo físico y transformarla en algún tipo de señal interpretable y transmitida a la red de información para su procesamiento. Se pueden clasificar en:
    - Físicos: Transforman una magnitud física (sensores de temperatura, presión, luz, giróscopos, …)
    - Químicos y bioquímicos: Miden concentraciones de elementos o moléculas. Entre estos sensores se pueden incluir algunos para uso en sistemas antiincendios.

  - Actuadores [8]. Son dispositivos que permiten a la red interactuar con el mundo físico. En esta categoría podemos ver:
    - Motores: Reaccionan a pulsos de ancho variable que hacen que el motor funcione durante un tiempo o potencia proporcional al giro.
    - Servomotores: Funcionan de forma similar, por pulsos, pero en este caso se utilizan para mantener fija una posición en función de la intensidad de señal que reciban.
    - Steppers o motores de paso: Similares a los servomotores con la diferencia que estos no quedan liberados al perder la señal con lo que aplicar un pulso supone avanzar en una posición determinada poco a poco.
    - Electroválvulas: Son dispositivos de bloqueo para canalizaciones, en este caso las señales sirven para abrir o impedir el paso de gases o líquidos.

  - Smartphone:

    Los teléfonos móviles son una tecnología importante a la hora de modernizar los servicios TIC de cualquier organización. Son dispositivos portátiles que tienen una capacidad de computación alta. La mayor parte de ellos utilizan procesadores ARM y los principales sistemas operativos son Android e IOS. Permiten a los usuarios una conexión permanente con internet a través de las tecnologías móviles como LTE, GPRS o GSM. Son los interfaces de usuarios más utilizados y lo harán mediante aplicaciones propias o a través de servicios web mediante el uso del navegador.

    Respecto al IoT es importante destacar en que pueden actuar como un dispositivo con múltiples sensores (acelerómetros, giróscopos, sensor de temperatura, acústicos, barómetros, localización GPS, etc.) y actuadores (notificaciones, vibraciones, uso de periféricos conectados).

  - Protocolos M2M [8]:

En este apartado se incluyen los protocolos que se suelen utilizar en IoT para la comunicación entre dispositivos. La mayor parte de las aplicaciones y las APIs que utilizan IoT se hacen sobre la web. En ese sentido los protocolos son similares a los encontrados en internet como HTTP, pero especializados en el traspaso de objetos de información e instrucciones a través de servicios de tipo REST (Representational State Transfer). En este tipo de aplicaciones se utilizan comandos de tipo CRUD e identificadores tipo URIs para ejecutar diferentes tipos de tratamiento a la información como guardar un determinado objeto de información, eliminarlo, solicitarlo, etc.

Hay varios protocolos que se emplean: HTTP, CoAP, MQTT, XMPP, AMQP y DDS.

- CoAP.

  CoAP surge de la necesidad de reducir el tamaño de los paquetes para integrarlo en sistemas IoT como 6LoWPAN. Para poder integrar IPv6 se reduce el tamaño de los paquetes del nivel de enlace. CoAP se diseña para una sobrecarga baja, que elimina la necesidad de fragmentar en niveles inferiores de comunicación.

  Está ideado para entornos cuyas condiciones de contorno sean restringidas, especialmente en cuanto a necesidades energéticas. CoAP modifica algunas funcionalidades de HTTP para crear un sistema REST de trabajo que utiliza UDP como protocolo de transporte.

  Para complementar UDP se introduce mecanismo de recuperación de errores y sistemas de confirmación de mensajes.

- MQTT

  Message Queue Telemetry Transport es un protocolo de mensajes estandarizado por OASIS. Este protocolo permite la comunicación entre dispositivos empotrados. Se utiliza un mecanismo de enrutado para dispositivos o clientes y permite la publicación y suscripción de nuevos dispositivos de forma sencilla, lo que lo convierte un protocolo útil para M2M. Se construye sobre TCP y permite la gestión de calidad del servicio. En este caso no es RESTful.

Protocolos de aplicación	RESTFul	Transporte	Publicación/ suscripción	Petición/respuesta	QoS	Tamaño cabecera
HTTP	Si	TCP	No	Si	No	
CoAP	Si	UDP	Si	Si	Si	4 bytes
MQTT	No	TCP	Si	No	Si	2 bytes
XMPP	No	TCP	Si	Si	No	
AMQP	No	TCP	Si	No	Si	8 bytes
DDS	No	TCP/UDP	Si	No	Si	

Figura A1-3 Comparativa de diferentes protocolos en IoT [8]

- Redes HLAN:

  - PLC [10]

    Power Line Communications es un sistema de transmisión que utiliza como medio la línea eléctrica. Se emplea en la última parte de la transmisión de energía cuando se encuentra en baja tensión.

    Para enviar la señal se emplea una portadora que transmite la señal en zonas donde no se ven interferidas por ruido o la propia electricidad de la línea.

    Tiene la ventaja de no necesitar cableado adicional, es especialmente útil para las distribuidoras de red eléctrica dado que se ahorran los costes de implementar un medio de comunicación para el último nivel de distribución. Además, es una tecnología fiable, probada y madura.

- Redes LPWAN [8] [11]:

  LPWAN es el acrónimo de redes de área de baja potencia. Este define redes que se caracterizan por conexiones de dispositivo de bajo consumo como aquellos con baterías, de requerimiento de ancho de banda leves y que pretendan operar en grandes distancias.

  Dentro de estas comunicaciones podemos distinguir dos tipos de redes.

  - Con espectro no-licenciado.

    Entre este tipo de tecnologías destacan LoRaWAN y Sigfox. Este tipo de tecnologías tienen la ventaja del menor coste de despliegue, el alcance incluso en interiores y la optimización del coste energético.

    El funcionamiento es similar y ofrecen un esquema de comunicaciones completo con una división con un nivel entre los dispositivos gestionados y conmutadores y otro de tipo backbone hasta los núcleos de servicio.

    Mientras que LoRaWAn es más bien una tecnología, Sigfox pretende convertirse en una especie de proveedor orientado a dispositivos IoT.

  - Con espectro licenciado

    Son tecnologías de tipo móvil pero adaptadas a requisitos de IoT. Entre estas destacan NB-IoT y LTE-M. Las características del trabajo móvil están pensadas para el uso de usuarios humanos, mucho más intensivo que el de los dispositivos IoT. Por ello 3GPP intenta establecer estándares específicos para ellos, simplifica los protocolos y disminuye la tasa binaria lo que mejora el alcance y reduce costes de energía.

Como ventajas tienen el despliegue, que aprovecha la infraestructura móvil, cobertura (nivel global), evita interferencias, aprovecha la seguridad establecida en sistemas móviles.

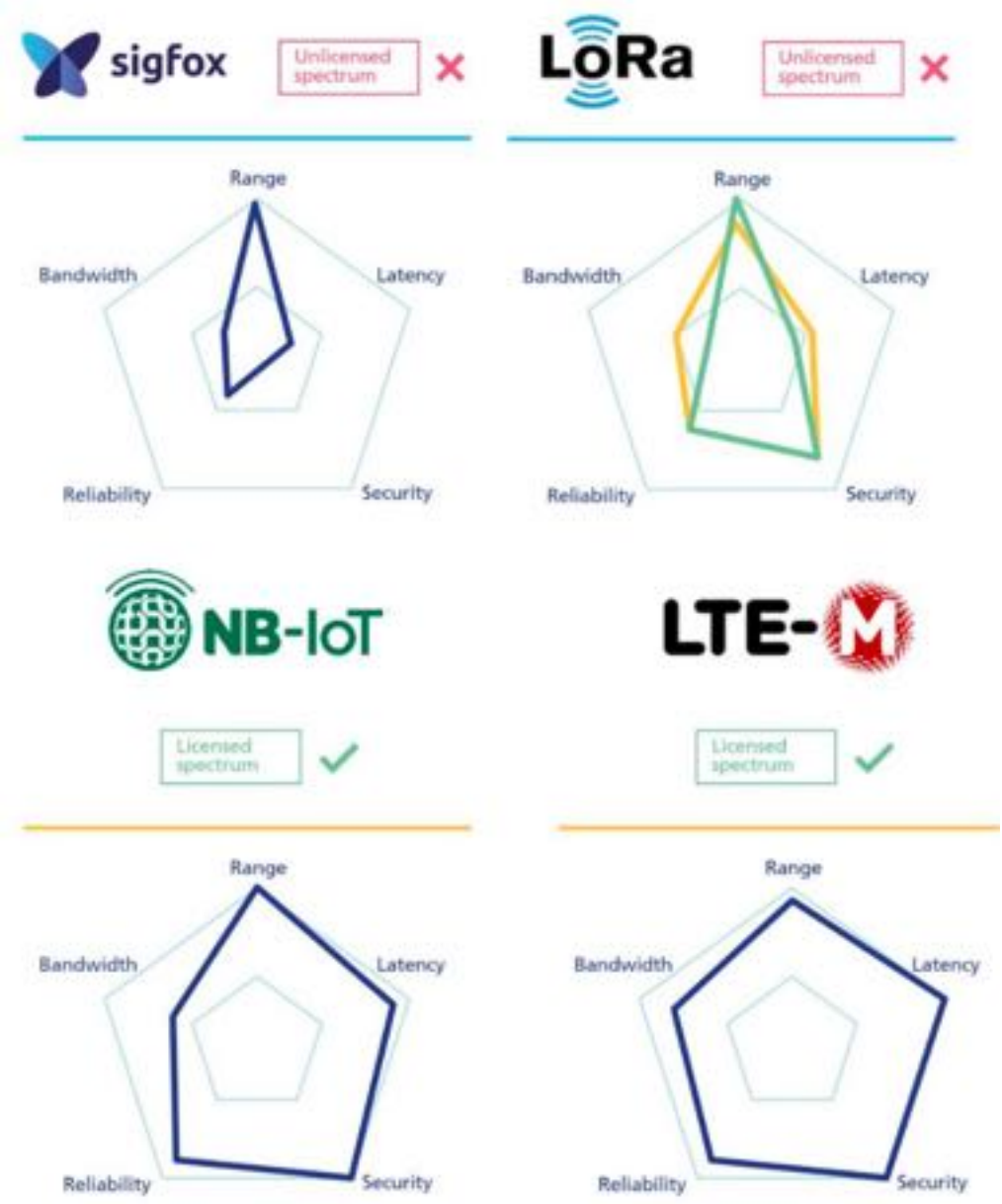


Figura A1-4 Comparación de tecnologías LPWAN [12]

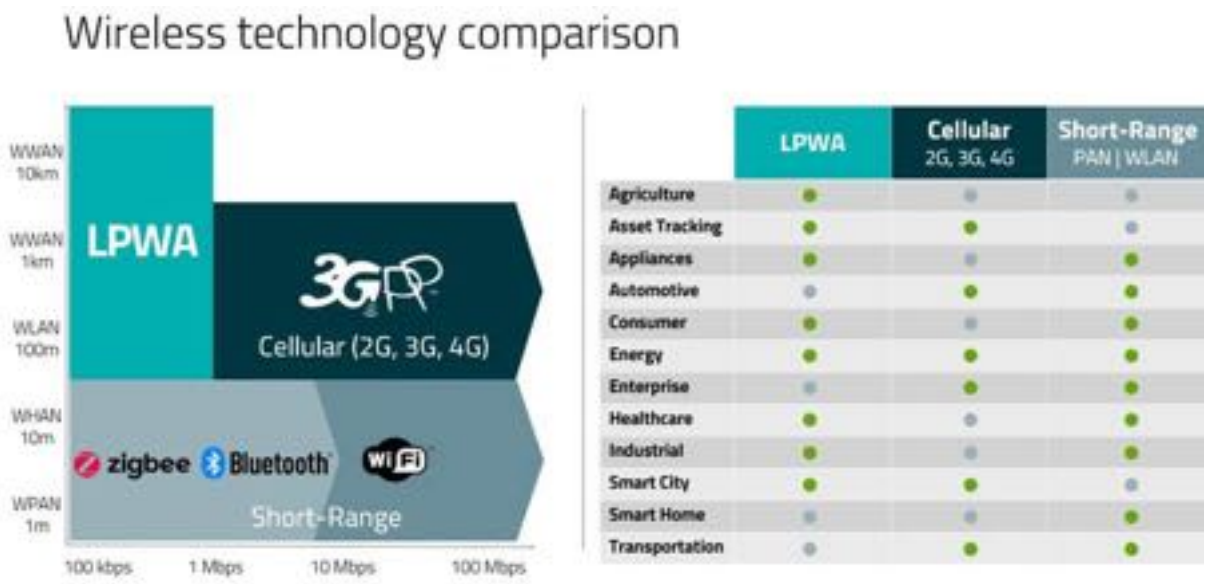


Figura A1-5 Comparación de tecnologías inalámbricas en IoT [13]

- Redes inalámbricas de área local (WLAN):

  - WiFi [8] .

    Estándar del IEEE 802.11. Es uno de los más populares y conocidos para las comunicaciones de red de área local. Utilizan las bandas de 2,4GHz y 5GHz. Su tasa de transferencia puede ser de cientos de Mbps. Comparativamente su consumo es elevado comparado con tecnologías WPAN como bluetooth para un alcance relativamente moderado. Es por esto que no se suele usar en soluciones IoT.

    En 2016 se anuncia la salida de WiFi HaLow que opera a frecuencias inferiores a 1GHz y permite una gama de conectividad de menor potencia ideado para su uso en IoT.

- Redes inalámbricas de área personal (WPAN):

  - Bluetooth [8].

    Especificación de la industria para conectividad de corto alcance de dispositivos y personas portátiles. Inicialmente tiene unas transferencias medias de hasta 1Mbps en la frecuencia 2,4 GHz. Se define en la norma IEEE802.15.1.

    A partir de 2011 aparece la versión Low Energy. Con esta versión las baterías pueden durar años, cosa vital para su uso en parques, calles e instalaciones que no se pueden permitir cambiar de forma continua. Se utilizan en aplicaciones que envían datos de forma periódica, no transmite continuamente información.

  - Zigbee [8]:

Otra especificación dentro del IEEE 802.15.4. Esta tecnología implementa capas de protocolo hasta nivel de enrutamiento de paquetes, aplicación y gestión de dispositivos (ZDO – ZigBee Device Objects).

Se diseña para mejorar el uso de dispositivos sensores con redes de baja potencia. Entre dispositivos adyacentes se puede llegar hasta los 10 metros de distancia. Opera en la misma banda que WiFi, 2,4 GHz y en las 868MHZ y 915MHz.

Las redes ZigBee están compuestas por miles de nodos que transmiten la información en un procedimiento de relevos, de forma descentralizada. Esto le permite generar redes WSN en forma de mallas y con acceso a puntos a los que un nodo central no llegaría.

- 6LoWPAN [8]:

  Acrónimo de IPv6 sobre Low Power Personal Area Network. Básicamente se puede ver como la adaptación del protocolo IPv6 a redes de consumo bajo el estándar IEEE802.15.4.

  Tienen un tamaño de paquete pequeño, limitado a 127 bytes, diferentes longitudes y anchos de banda . Para la adaptación de IPv6 se necesitó una capa intermedia. Tiene compresión en el encabezado para reducir la sobrecarga y cumplir con la MTU requerida por IPv6.

- RFID [8]:
  Son los sistemas de identificación por radiofrecuencia. Se utilizan para la identificación de objetos a distancia corta sin necesidad de contacto. Para ello es necesario una etiqueta o tag RFID, consiste en un microchip unido a una pequeña antena de radio en forma de circuito 2D. El dispositivo lector genera un campo electromagnético que permite la lectura de la información del chip.

  Trabaja en torno a los 125 o 134 KHz para baja frecuencia y 13,56 MHz para alta. Las bandas pueden ser utilizadas por otros dispositivos y eso genera ruidos en el funcionamiento.

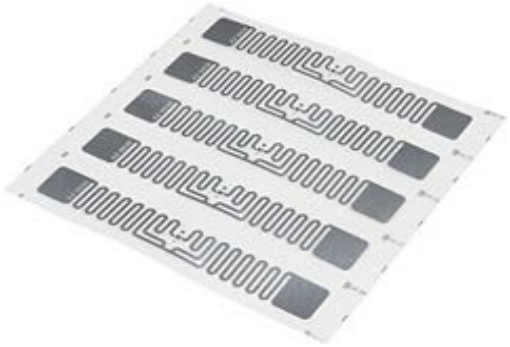


Figura A1-6 Imagen de etiquetas RFID [14]

- NFC. Es una tecnología de comunicación inalámbrica de muy corto alcance que permite a los dispositivos móviles comunicarse entre sí. NFC se basa en RFID, utiliza la variación del campo magnético para la transmisión y opera en la banda de las 13,56 MHz, En NFC la comunicación es en ambos sentidos, se puede intercambiar el modo de funcionamiento dependiendo de qué dispositivo genere el campo magnético.

	ZigBee	Z-Wave	6LowPAN	WirelessHART	Bluetooth	WiFi	NFC	RFID
Frecuencia de operación	2.4 GHz, 915 MHz, 868 MHz	900 MHz	2.4 GHz	2.4 GHz	2.4GHz	2.4 GHz, 5 GHz	13.56 MHz	LF:125-134KHZ HF:13.56MHz UHF:856-960MHz
Alcance	500 m	100 m	200 m	250 m	50 m	100 m	10cm	10cm,30cm,100m
Tasa de datos	250 Kbps	40 Kbps	200 Kbps	250 Kbps	1 Mbps	600 Mbps	424Kbps	424 kbps
Número de nodos	65.536	232	100	30.000	8	N/A	2	N/A
Consumo medio	Tx:25-30mA Rx:20-30mA	Tx:30-40mA Rx:20-30mA	Tx:20-35mA Rx:12-25mA	Tx:18-25mA Rx:6-10mA	Tx:15-20mA Rx:15-20mA	Tx: >220mA Rx:>215mA	Bajo con baterías	Depende del modelo de etiqueta
Interoperabilidad	Alta	Alta	Baja	Alta	Media	alta	alta	alta

Figura A1-7 Comparativa de diferentes estándares de comunicaciones IoT [8]

- **Relacionadas con análisis de datos** [15]**:**

Una de las cosas que caracteriza hoy en día a la sociedad de la información es que la cantidad de datos que acumula el mundo digital no para de crecer exponencialmente. Para dar solución al tratamiento de todos estos datos se adoptan en gran parte las siguientes tecnologías.

- **Big Data:**

Esta tecnología hace uso de bases de datos no relacionales para almacenar ingentes cantidades de datos no estructurados, como por ejemplo documentos. Se les caracteriza por la gran cantidad de datos, la variedad de fuentes de información que agrupan, la comprobación de la veracidad de los datos y la velocidad con la que se procesan los mismos.

Dentro del abanico de soluciones de big data que hay se pueden adoptar un tipo de soluciones u otras. Algunos ejemplos de Big Data podrían ser el uso de BigTable como herramienta de almacenamiento de información, MapReduce como ejemplo de procesamiento de datos estáticos o Storm como ejemplo de procesamiento de datos dinámicos. En este contexto hay muchas herramientas como Apache Hadoop y Spark (de las más populares), Cassandra o MongoDB.

- **Data Mining:**

De forma complementaria al Big Data se presenta la minería de datos o data mining. Aunque es un proceso independiente y se puede efectuar con pocos datos, las posibilidades que ofrece su empleo con grandes cantidades aportan mucho más valor

añadido. En este caso lo que pretende la tecnología es obtener información oculta y valiosa entre los datos que posea la organización.

Se compone por un ciclo completo de tratamiento de la información en la que se obtienen, preprocesan y analizan los datos con el propósito de recuperar información útil.

Para ello se vale de dos tipos de técnicas de análisis.:

- Predictivas o supervisadas: Se pretende predecir valores en función de otros ya conocidos. En este apartado podemos encontrar técnicas como regresión, clasificación o predicción en series temporales

- Descriptivas o no supervisadas. Aquí se encuentran técnicas como agrupamiento, extracción de asociaciones, detección de anomalías entre otros.

Dentro de esta categoría merece la pena destacar el uso de la inteligencia artificial para llevar a cabo este tipo de análisis y especialmente el uso de redes neuronales mediante Deep Learning.

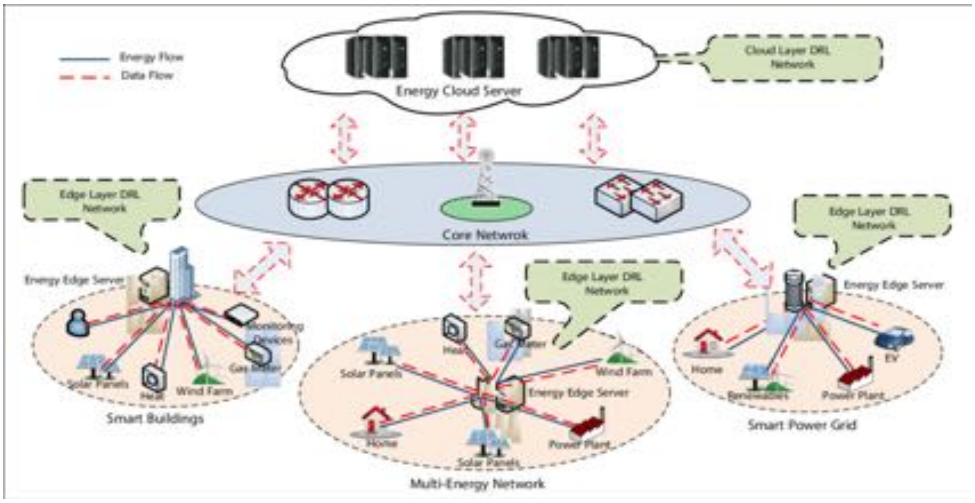


Figura A1-8 Esquema de solución Smart Grid [16]

2.3 Análisis de riesgos de seguridad y seguridad de la información

2.3.1 Introducción

La información y los datos son uno de los principales activos de las organizaciones. La protección de su seguridad y privacidad es una tarea fundamental para asegurar el correcto desarrollo del negocio.

Esta realidad es aplicable a todo tipo de organización, las Ciudades Inteligentes no son una excepción. Es más, debido a la alta integración con las TIC es más que necesario establecer alguna forma de protección de este tipo de información.

A la hora de trabajar con posibles perjuicios debido a la pérdida, deterioro, manipulación u otros efectos negativos con respecto a la información o los activos que la tratan en general se trabajan con riesgos, debido a que esto se tiene que tratar antes de que se produzcan y es imposible establecer un mecanismo de seguridad que garantice al cien por cien cualquier tipo de daño. En resumen, es un proceso probabilístico en el que siempre hay probabilidades de impactos.

Los estándares internacionales dan respuesta a este problema mediante los llamados sistemas de gestión de seguridad de la información (SGSI). Estos sistemas son procesos continuos en los que se evalúan los activos en relación a la información, los riesgos y se establecen medidas de forma continuada en el tiempo. Son sistemas vivos que cambian en función de las condiciones de contorno de la organización.

Un SGSI eficaz debe garantizar que se aseguren las siguientes dimensiones de seguridad [17].

- su **confidencialidad**, asegurando que sólo quienes estén autorizados puedan acceder a la información.
- su **integridad**, asegurando que la información y sus métodos de proceso son exactos y completos.
- su **disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

A esto añadimos otras dos dimensiones más que se trataría de:

- su **autenticidad**, asegurando que los actores implicados en el tratamiento o acceso a la información son quienes dicen ser.
- su **trazabilidad o auditoría**, asegurando que las acciones que se realizan sobre la información quedan registradas correctamente para un posible análisis o detección posterior.

La herramienta básica que utilizan los SGSI para conseguir esto es mediante el análisis de riesgos. En un análisis de riesgos se identifican dentro de la organización la localización de los activos que disponen de información crítica. Se analizan las posibles amenazas que se pueden materializar y finalmente se establecen los riesgos baremados por importancia en función de las amenazas, vulnerabilidades y activos del momento del análisis. En definitiva, un análisis de riesgos es una fotografía de un mapa de calor de los problemas TIC que pueden surgir en una organización.

Debido a su carácter particular (sobre una organización) y temporal, los análisis hacen difícil la extrapolación de datos para su comparación en el tiempo o entre organizaciones. Esto es un problema porque las medidas que se necesitan adoptar necesitan tener un contorno estable para saber cuando son efectivas. Es por ello que se recomienda el uso de procesos formales siempre (para por lo menos poder evaluar la evolución en el tiempo) y estandarizado (para poder comparar con otras organizaciones). Es en este último caso por lo que la utilización de estándares como MAGERIT sean importantes.

2.3.2 Normativa y estándares de seguridad aplicables a las ciudades inteligentes en España.

2.3.2.1 27001 [18]

La ISO 27001:2013 es la norma internacional que proporciona un marco de trabajo para los SGSI con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal. La certificación ISO 27001 es esencial para proteger sus activos más

importantes, la información de sus clientes y empleados, la imagen corporativa y otra información privada. La norma ISO incluye un enfoque basado en procesos para lanzar, implantar, operar y mantener un SGSI.

2.3.2.2 Magerit [19]

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

2.3.2.3 ENS [20]

El ENS se define en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

3 ANÁLISIS DE SEGURIDAD

3.1 Objetivo

El objetivo del análisis de seguridad es ofrecer una perspectiva del estado actual de amenazas, riesgos y posibles medidas de seguridad que actualmente tiene la ciudad inteligente. También permite demostrar cómo es necesario aplicar conceptos de seguridad ya existentes como el SGSI, políticas de seguridad o controles, pero desde la perspectiva de los sistemas TIC de una ciudad inteligente.

3.2 Metodología

Para la elaboración del análisis de riesgos se ha utilizado una versión simplificada de MAGERIT v3. A continuación se describen brevemente los pasos:

3.2.1.1 Identificación y valoración de activos

El primer paso es la identificación de aquellos activos que contienen la información crítica de la ciudad. (Aquella información cuyo tratamiento equivocado puede afectar negativamente a la ciudad). Para ello primero se ha definido el alcance en función de los servicios TIC ofertados que hacen que la ciudad entre dentro de la definición de ciudad inteligente.

Estos servicios serán analizados en función de las dimensiones de seguridad y la criticidad para cada dimensión de seguridad analizada.

	AUTENTICIDAD Garantía de la identidad de los datos.	CONFIDENCIALIDAD Grado de restricción en cuanto al acceso y la divulgación.	INTEGRIDAD Grado de veracidad, consistencia y fiabilidad de la información.	DISPONIBILIDAD Necesidad de tener la información siempre lista para su uso .	AUDITABILIDAD Registro de las acciones u operaciones que hace el usuario.
5	CRÍTICA: Información que requiera certificación por una tercera parte, del origen, del destino, así como del contenido de la información enviada. Ej.: Documentos firmados digitalmente por centros autorizados con validez legal, Notificación por conducto notarial.	SECRETA. Solo miembros del Comité de Dirección de la Organización	CRUCIAL: Información de suma importancia desde el punto de vista de la veracidad, coherencia y exactitud para la Organización. Ej.: Información económica y financiera de la organización.	Menos de dos horas	TRAZA TOTAL: Se debe registrar a nivel de usuarios TODAS las acciones de Alta, Baja, Modificación, lecturas, e intentos de lectura. Ej.: Datos de salud.
4	CERTIFICADA: Información que requiera certificación por una tercera parte del origen y del destino. Ej.: E-mail con firma digital, notario.	CONFIDENCIAL: . Solo personal con cierto grado de responsabilidad dentro de la organización o de forma puntual para un uso temporal	SENSIBLE: Información que debe tener alto nivel de exactitud. Ej.: Ofertas entregadas a clientes.	2 a 8 horas	RESTRINGIDA: Se debe registrar a nivel de usuarios las acciones críticas de Alta, Baja, Modificación y Lecturas. Ej.: Contabilidad.
3	CONFIRMADA: Información que precise confirmar el origen y el destino, así como la necesidad de verificar la recepción. Ej.: Notificación con acuse de recibo.	USO RESTRINGIDO. Solo para el área de tratamiento uso	GARANTIZADA: Información que exige disponer de medidas que garanticen su veracidad. Ej.: Inventarios de clientes, Documentos técnicos.	> 8 y <=3 días	PARTICULAR: Se debe registrar a nivel de usuarios las acciones críticas de Alta, Baja y Modificación. Ej.: Configuración de servidores.

2	REMITIDA: Información que requiera conocer los datos del emisor y el origen de la misma. Ej.: Circulares firmadas, uso de usuario y contraseña.	USO INTERNO: Validación periódica de la integridad del dato. (trazabilidad: registro de quien/como se realiza la validación)	FIABLE: Información restringida en su actualización a cualquier persona de la organización con acceso permitido. Ej.: Modelos de plantillas de documentación definidos.	> 3 día <= 1 semana	GENÉRICA: Solo se registran datos de forma genérica. Ej.: Accesos a la Intranet.
1	ANÓNIMA: Información que no requiere conocer el origen / autor, ni el responsable de la misma. Ej.: propaganda, folletos informativos.	PUBLICA: el grado de fiabilidad de la información no es relevante (trazabilidad nula)	BAJA: Información cuya modificación no implica ningún riesgo y puede realizarla cualquier persona. Ej.: Tablón de anuncios.	>= 1 semana <2 semanas	LIBRE: No hay necesidad de registrar ninguna acción o evento. Ej.: Documentos propios administrativos.

Tabla 3-1 Guía de valoración de activos según dimensiones de seguridad

Una vez definidos los servicios y evaluados, estos se dividen en los activos que los componen. A continuación, se trasladarán los valores y se obtendrán las puntuaciones de cada activo.

En este caso para cada activo se sumarán las puntuaciones y en función de ello obtendremos un valor para cada activo. Como guía se presentan las tablas Tabla 3-1 Guía de valoración de activos según dimensiones de seguridad y la Tabla 3-2 Ayuda para valoración de activos.

Valor del activo		
Valor acumulado (A+C+I+D+A)	Clasificación del activo	Valor numérico
Entre 5 y 13	Bajo	1
Entre 14 y 20	Medio	2
Entre 21 y 25	Alto	3

Tabla 3-2 Ayuda para valoración de activo

3.2.1.2 Identificación y valoración de amenazas

Una vez se disponen de los activos, se procede a la evaluación de las amenazas. En función de las vulnerabilidades y condiciones de contorno temporales y particulares de la organización se identifican las posibles amenazas y valora la probabilidad de que estas se produzcan.

Además, se evalúan las consecuencias que, en caso de materializarse, podrían provocar esas amenazas en los activos. Para ayudar a estandarizar esa evaluación se utilizan las siguientes tablas como guía:

Impacto de amenaza
(en caso de materialización)

Impacto	Valor	Descripción
Alto	3	Afecta a toda la organización Degradación del activo >= 60%

		Mucha visibilidad por parte del cliente
		Afecta la producción de más del 50% de empleados
		Compromete el cumplimiento de SLA
Medio	2	Afecta a algunos servicios de la organización
		Degradación del activo 30% - 60%
		Baja visibilidad por parte del cliente
		Afecta a la producción de menos del 50% de empleados
		Puede que comprometa el cumplimiento de SLA
Bajo	1	Afecta a funciones aisladas
		Degradación del activo < 30%
		Baja visibilidad por parte del cliente
		Afecta a menos del 5% de la producción de los empleados
		No compromete la entrega de SLA

Tabla 3-3 Tabla de valoración del impacto de una amenaza.

Probabilidad

Probabilidad	Valor	Descripción
Alta	3	Dependerá de la relación entre active y amenaza y el entorno del activo
Media	2	
Baja	1	

Tabla 3-4 Tabla guía para valoración de probabilidad de una amenaza.

3.2.1.3 Obtención de riesgo

Una vez se disponen de los servicios y amenazas más relevantes valorados, se realizará una correlación en la que se mide riesgo que provoca la unión de ambos factores.

El riesgo será por tanto la probabilidad por el impacto aplicado al valor de cada activo o servicio. Para la realización de esta parte se ha utilizado la siguiente tabla como base por cada servicio.

Probabilidad Amenaza	3	3	6	9	6	12	18	9	18	27
	2	2	4	6	4	8	12	6	12	18
	1	1	2	3	2	4	6	3	6	9
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 3-5 Tabla de análisis de riesgos.

Se observa que el valor de cada riesgo resultante será en función de los factores citados anteriormente. El riesgo resultante tendrá una puntuación que permitirá compararlo. En un caso real se estimará límites que permiten tomar decisiones para transferir el riesgo, mitigarlo o aceptarlo.

3.3 Construcción de ciudad modelo

El primer paso del análisis de riesgos será definir las características y servicios de una ciudad inteligente. En el estado del arte se ha podido establecer dominios o ámbitos que definen una ciudad inteligente. A continuación, se definirán las características generales de la ciudad y posteriormente se analizarán los servicios TIC de SSC.

3.3.1 Características de la ciudad:

Como se menciona en el apartado anterior, en el análisis de riesgos influyen las condiciones de contorno que definen el negocio y que afectan a los servicios TIC.

En el trabajo se ha intentado recrear una ciudad que se aproxima a la actualidad española en este aspecto. A título informativo se han definido algunos datos generales de la ciudad que podrían ser útiles en la valoración del riesgo.

Datos de ciudad modelo:

- País: España
- Número de habitantes: 300.000
- Localización y medio ambiente: Se encuentra situada en la costa, en el delta de un río de poco caudal. El cambio de estaciones suele ser suave pero los últimos años se ha incrementado las temperaturas en verano y el frío en invierno. Los últimos años ha habido nevadas.

- Religión: La mayor parte de la población es cristiana. El segundo grupo más poblado es ateo/agnóstico y el tercero la comunidad islámica.

- Celebraciones: Las principales celebraciones se producen de acuerdo al progreso de las estaciones, la única de carácter religioso es la navidad

- Cultura, historia y aspectos relevantes: Ciudad de origen medieval. Se dispone de mucho patrimonio histórico en forma de fortalezas y templos religiosos.

- Economía: La ciudad dispone acceso marítimo a través de un puerto, estación de tren, conecta con una de las principales autovías del país. No dispone de aeropuerto.

- Seguridad: La principal fuente de inseguridad suele deberse al contrabando producido por los accesos a través del puerto. Hay algunos barrios de nivel económico bajo que tienen algo de delincuencia marginal.

- Otros: La ciudad tiene un centro de protección de datos en el edificio del ayuntamiento. Hay otro pequeño centro de datos en la comisaría de policía local. Se tienen medidas estándar de gestión y de seguridad TIC en ambos sitios.

3.3.2 Sistemas y servicios de ciudad inteligente:

La ciudad seleccionada para el caso de uso debe ser representativa de una ciudad inteligente contemporánea para poder extraer conclusiones válidas en cuanto a la seguridad de estas. El primer paso será averiguar qué servicios serán en los que se centrará el alcance del análisis de riesgos.

Como recordamos la ciudad inteligente se divide en seis dominios diferentes. Para cada uno de ellos se identifican los siguientes servicios.

Entorno inteligente	**Servicios a la ciudad**	**Servicios de Atención y relación con el ciudadano**	**Servicios de soporte a la Ciudad Inteligente**
Medio ambiente urbano	Mantenimiento de parques, jardines y playas		
	Gestión del riesgo		
	Medición medioambiental: Calidad del aire		
	Medición medioambiental: Ruido		
Gestión de Residuos	Limpieza varia		
	Recogida de residuos		
	Gestión de la red de puntos limpios		
Energía	Gestión de la red y consumo de gas en edificios municipales		
	Gestión de la red eléctrica y consumo del alumbrado público		
	Gestión de la red eléctrica y consumo en edificios municipales		

	Monitorización del consumo energético en edificios privados y hogares
Agua	Consumo y calidad del agua
	Gestión de la red de saneamiento y depuradoras

Tabla 3-6 Servicios detectados del sector entorno inteligente [21].

Movilidad inteligente	**Servicios a la ciudad**	**Servicios de Atención y relación con el ciudadano**	**Servicios de soporte a la Ciudad Inteligente**
Transporte y tráfico	Control del tráfico		
	Control de tráfico en zonas peatonales o de acceso restringido		
	Gestión de flotas municipales		
	Gestión de los medios de transporte de viajeros		
	Gestión de peajes		
	Gestión de puntos de recarga de vehículos eléctricos		
	Gestión de red de bicicletas públicas		
Estacionamiento	Gestión de estacionamiento limitado		
	Gestión de aparcamientos		
Infraestructura varia	Gestión de semáforos y señalética		
	Gestión de paneles de información		
Accesibilidad	Accesibilidad viaria		
	Accesibilidad en establecimientos públicos		
	Accesibilidad en establecimientos privados		
	Accesibilidad en medios de transporte urbano		
Movilidad inteligente	**Servicios a la ciudad**	**Servicios de Atención y relación con el ciudadano**	**Servicios de soporte a la Ciudad Inteligente**
Conectividad TIC	Cobertura móvil		
	Zonas wifi público		

Tabla 3-7 Servicios detectados del sector de movilidad inteligente [21].

Gobernanza inteligente	**Servicios a la ciudad**	**Servicios de Atención y relación con el ciudadano**	**Servicios de soporte a la Ciudad Inteligente**
Transparencia	Portal de transparencia		
	Redes sociales		
Participación	Espacios digitales de participación		
Administración Digital	Sede electrónica		
	Trámites on-line		

	Páginas web corporativa		
	Páginas web sectoriales		
	Aplicaciones móviles de información y atención al ciudadano		
Gobernanza inteligente	**Servicios a la ciudad**	**Servicios de Atención y relación con el ciudadano**	**Servicios de soporte a la Ciudad Inteligente**
Planificación estratégica	Plan Estratégico Municipal y Plan de Ciudad Inteligente		
Información geográfica de la ciudad	"Inventario electrónico de activos municipales"		
	Cartografía electrónica		

Tabla 3-8 Servicios detectados del sector gobernanza inteligente [21].

Economía inteligente	**Servicios a la ciudad**	**Servicios de Atención y relación con el ciudadano**	**Servicios de soporte a la Ciudad Inteligente**
Turismo	Aplicaciones móviles para el turista		
	Otros servicios electrónicos para el turista		
Comercio y Negocios	Aplicaciones móviles para el comercio		
	Otros servicios electrónicos para el comercio		
Empleo y emprendimiento	Servicios electrónicos de orientación de empleo y emprendimiento		
Consumo	Servicios electrónicos de información al consumidor		
Economía inteligente	**Servicios a la ciudad**	**Servicios de Atención y relación con el ciudadano**	**Servicios de soporte a la Ciudad Inteligente**
Empresa Digital	Servicios a las empresas para la incorporación de las TIC		
Ecosistema de innovación	Servicios, recursos e infraestructuras para la innovación		

Tabla 3-9 Servicios detectados del sector economía inteligente [21].

Sociedad inteligente	**Servicios a la ciudad**	**Servicios de Atención y relación con el ciudadano**	**Servicios de soporte a la Ciudad Inteligente**
Colaboración ciudadana	Plataforma local de colaboración colectiva para restos de la ciudad (Crowdsourcing)		
	Plataforma local de micro financiación colectiva (Crowdfunding)		
Sociedad inteligente	**Servicios a la ciudad**	**Servicios de Atención y relación con el ciudadano**	**Servicios de soporte a la Ciudad Inteligente**
Empresa Digital	Asesoramiento y capacitación en nuevas tecnologías		

Tabla 3-10 Servicios detectados del sector sociedad inteligente [21].

Bienestar inteligente	Servicios a la ciudad	Servicios de Atención y relación con el ciudadano	Servicios de soporte a la Ciudad Inteligente
Seguridad y emergencias	Video vigilancia		
	Seguimiento y actividad de efectivos y brigadas		
	Centros de control de seguridad y emergencias		
Urbanismo y Vivienda	Planeamiento Urbanístico		
	Servicios electrónicos para la vigilancia de cumplimiento de la normativa urbanística		
Infraestructuras públicas y equipamiento urbano	Gestión, mantenimiento de las infraestructuras y equipamiento urbano		
	Conservación y rehabilitación del patrimonio histórico		
	Detección de incidencias en la infraestructura urbana		
Bienestar inteligente	**Servicios a la ciudad**	**Servicios de Atención y relación con el ciudadano**	**Servicios de soporte a la Ciudad Inteligente**
Salud	Servicios de teleconsulta		
	Servicios de telediagnóstico		
Asuntos sociales	Servicios de teleasistencia		
	Otros servicios para colectivos específicos		
Educación	Servicios electrónicos sobre oferta educativa local		
Seguridad y emergencias	Servicios electrónicos de información sobre emergencias		
Urbanismo y Vivienda	Servicios electrónicos para demandantes de vivienda libre y protegida		
Cultura y Ocio	Servicios electrónicos para el uso de los recursos y escuelas deportivas		
	Servicios electrónicos para el uso de los recursos culturales		

Tabla 3-11 Servicios detectados del sector de bienestar inteligente [21].

En el espacio de la ciudad inteligente puede que haya muchos más servicios, pero nos hemos centrado en aquellos encontrados entre los municipios españoles en 2015. [21]

De entre estos se extrae la conclusión de que las ciudades en 2015 prestaban unos 10 u 11 de servicios de ciudades inteligentes de media.

Los servicios que se encontraron en la mayor parte de las ciudades fueron:

Servicios	Dominio

1	Página web corporativa	Gobernanza
2	Portal de transparencia	Gobernanza
3	Sede electrónica	Gobernanza
4	Trámites on-line	Gobernanza
5	Espacios digitales de participación	Gobernanza
6	Redes sociales	Gobernanza
7	Cartografía electrónica	Gobernanza
8	Aplicaciones móviles de información y atención al ciudadano	Gobernanza
9	Consumo y Calidad del Agua	Entorno
10	Inventario electrónico de activos municipales	Gobernanza

Tabla 3-12 Diez servicios TIC más implantados en 2015 para municipios de España [21].

Observamos que principalmente se refieren al entorno de gobernanza inteligente. Esto es así porque la inversión y evolución en ciudad inteligente es costosa y los servicios de gobernanza suelen ser los que proporcionan más valor añadido en relación con el coste de implementarlos. Conforme la ciudad es mayor o se dispone de más recursos se suelen abarcar otros.

Para que el análisis conste de una mayor profundidad nuestra ciudad también dispondrá de otros servicios considerados importantes a largo plazo. Para ello nos hemos basado por tanto en la agenda digital de las ciudades inteligentes prevista para 2030. [22]

En este documento se puede ver que áreas de la ciudad inteligente necesitan de más desarrollo y cuales son las más relevantes a la ciudad. Nos hemos centrado en aquellas que tienen relevancia alta para la ciudad a corto/ medio plazo (cinco años). La selección de estas se puede encontrar en la Tabla 0-1 Tabla resumen de líneas de investigación de importancia alta con implantación en cinco años .

De entre las líneas de acción planteadas podemos observar como las acciones que se consideran importantes en las ciudades serían aquellas relacionadas con la gestión eléctrica, la automatización de la gestión de tráfico y facilidades a los vehículos de energías sostenibles, mejoras en el diseño de las ciudades empleando materiales sostenibles, comprobación de la contaminación y gestión del transporte público. Por eso propondremos añadir a nuestra ciudad los siguientes servicios.

	Servicios	Dominio
1	Monitorización del consumo energético en edificios privados y hogares	Entorno
2	Recogida de residuos	Entorno
3	Control de tráfico	Movilidad
4	Gestión de puntos de recarga de vehículos eléctricos	Movilidad
5	Medición medioambiental: Calidad del aire	Entorno
6	Seguimiento y actividad de efectivos y brigadas	Bienestar

Tabla 3-13 Servicios extraídos de procesos de innovación.

Si se unen los servicios de ciudad inteligente más comunes de las ciudades españolas en la actualidad y los extraidos de procesos de innovación que se esperan se implanten en un corto plazo, podemos tener un caso de uso realista para realizar el análisis de riesgos. Hemos añadido por interés académico el seguimiento de brigadas, para que haya servicios de todos los ámbitos.

La ciudad a analizar tendrá por tanto estos servicios, que serán los considerados para hacer el análisis de riesgo. Puede que la ciudad disponga de otros servicios, pero en la metodología del análisis se escoge aquellos que se consideran apropiados. Por ejemplo, puede que hubiera un servicio de bicicletas inteligente pero no se considera relevante por su madurez y alcance dentro de la ciudad.

	Servicios	Domino
1	Página web corporativa	Gobernanza
2	Portal de transparencia	Gobernanza
3	Sede electrónica	Gobernanza
4	Redes sociales	Gobernanza
5	Aplicaciones móviles de información y atención al ciudadano	Gobernanza
6	Consumo y Calidad del Agua	Entorno
7	Monitorización del consumo energético en edificios privados y hogares	Entorno
8	Recogida de residuos	Entorno
9	Control de tráfico	Movilidad
10	Gestión de puntos de recarga de vehículos eléctricos	Movilidad
11	Medición medioambiental: Calidad del aire	Entorno
12	Seguimiento y actividad de efectivos y brigadas	Bienestar

Tabla 3-14 Servicios a analizar

3.4 Análisis de riesgos de la ciudad inteligente

3.4.1 Identificación de activos

Ahora que disponemos de los servicios de la ciudad inteligente el siguiente paso del análisis sería ver qué activos están involucrados en este alcance de la ciudad.

Para la clasificación de los activos utilizaremos MAGERIT y los desglosamos en los activos definidos entre los elementos:

- [D] Datos / Información
- [K] Claves criptográficas
- [S] Servicio
- [SW] Software - Aplicaciones informática
- [HW] Equipamiento informático (hardware)
- [COM] Redes de comunicaciones
- [Media] Soportes de información

- [AUX] Equipamiento auxiliar
- [L] Instalaciones
- [P] Persona

Por ejemplo: los servicios página web y portal de transparencia son un servicio [S] se proporcionan desde un servidor web [SW] [HW] alojado en un CPD de la administración local [L].

3.4.1.1 Marco de referencia

Al tratarse de una ciudad ficticia se intenta desglosar en una arquitectura coherente. Para ello distribuiremos los elementos teniendo en cuenta que se suelen enmarcar en una arquitectura por ejemplo como la definida por el ITU:

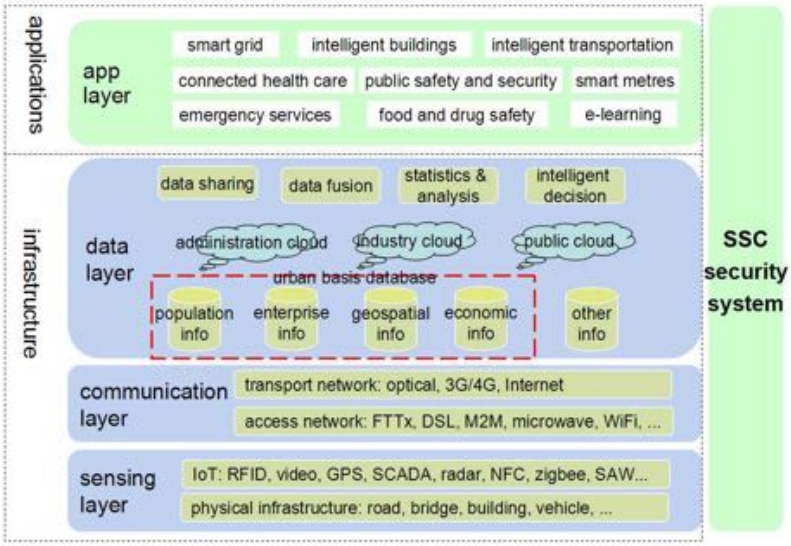


Figura A1-1 Arquitectura de referencia de una SSC según el grupo para ciudades inteligentes de la ITU [23]

O también podemos usar la elegida por el ministerio de interior japonés para la definición de medidas de seguridad en la ciudad inteligente [24]:

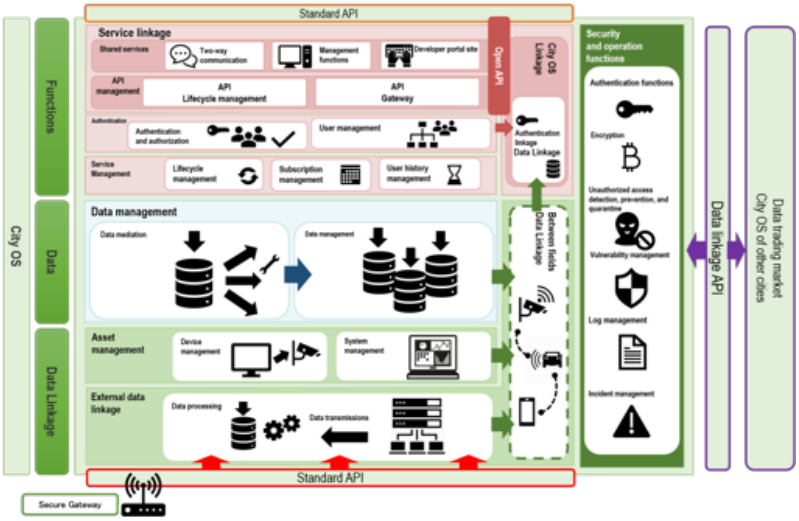


Figura A1-2 Desglose de un entorno de ciudad inteligente según el Ministerio de asuntos internos japonés [24] (En este caso tratan la arquitectura de Smart City como un sistema global, el City OS)

En concreto a la hora de relacionar los activos se tendrán en cuenta sus relaciones para prestar el servicio. En general se tendrán en cuenta los más relevantes.

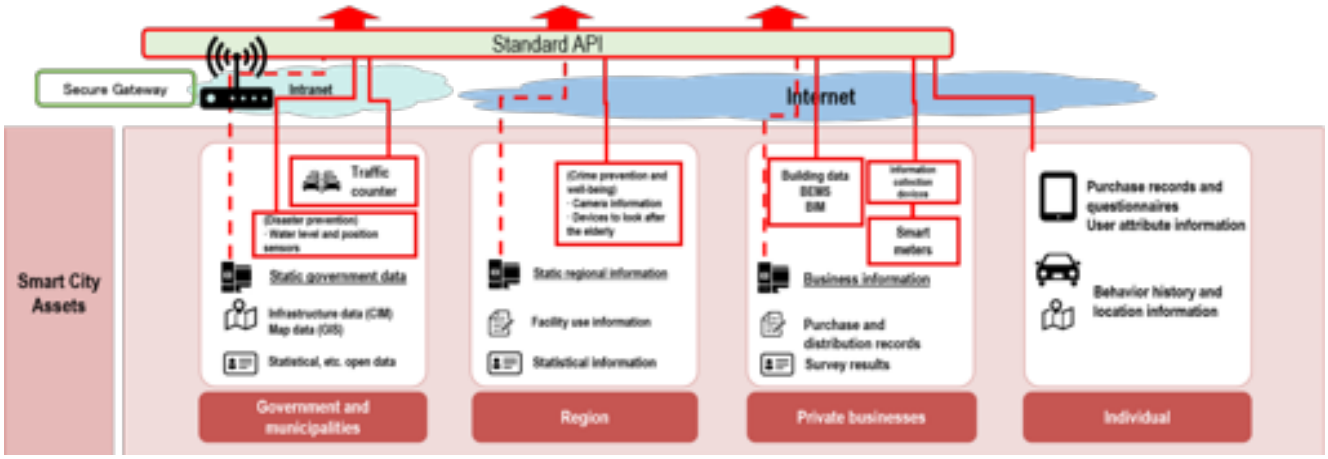


Figura A1-3 Relación de activos de una ciudad inteligente según las guías del Ministerio de Interior Japonés [24]

3.4.1.2 Desglose de los activos

Por cada servicio prestado deberemos asignar una puntuación en función de las dimensiones de seguridad de la información. Posteriormente y en función de la relación de los activos se transmitirá e irá asignado valor según las dependencias entre estos.

A continuación, se analizan todos los servicios:

1. PÁGINA WEB CORPORATIVA
Información:
General: Con este servicio la administración de la ciudad pretende mostrar toda la información posible de una manera sencilla y accesible a todos sus ciudadanos y turistas. La web ofrece información cultural e informativa. Además, también incluye información de todos los trámites en relación al ciudadano y enlaces para aquellos que se pueden realizar vía telemática. Para los trámites se utilizará la sede electrónica principalmente. Tecnología: Se utilizará principalmente un servidor web, situado en las instalaciones del ayuntamiento en el CPD principal del consistorio. Serán los servicios informáticos del ayuntamiento los que lo gestionarán y el departamento de comunicaciones será el que lo opere en el día a día cambiando contenido. Para su desarrollo se ha utilizado el servicio disponible en la CTT, el Portal de Entidades Locales Como ejemplo:

Figura A1-4 Portal para Entidades Locales . [25]

Dimensiones de seguridad	A	C	I	D	A
Valores	2	1	4	4	3
Activos dependientes del servicio:					
[D] Datos / Información					
[K] Claves criptográficas	[x506-1] Certificado portal Ayto.				
[S] Servicio dependiente	[pki] Servicio PKI Ayto.				
[SW] Software - Aplicaciones informática	[dbms1] Base de datos portal [www1] Servidor de presentación portal [hypervisor1] Hypervisor CPD Ayto.				
[HW] Equipamiento informático (hardware)	[host1] Servidores CPD Ayto. [network1] Electrónica CPD Ayto. [pc1] Equipos cliente Ayto.				
[COM] Redes de comunicaciones	[lan1] Red Ayto. [internet1] Servicio ISP Ayto.				
[Media] Soportes de información					
[AUX] Equipamiento auxiliar					
[L] Instalaciones	[site1] CPD del ayuntamiento				
[P] Persona	[adm1]Administradores Ayto. [op2] Operadores Ayto. [ue1] Usuarios externos				

Tabla 3-15 Análisis del servicio de Página web corporativa.

2. SEDE ELECTRÓNICA
Información:

General:

Las sedes son una plataforma digital para la tramitación de expedientes administrativos. Como servicio es interesante dado que el ciudadano puede realizar las gestiones desde cualquier parte y reduce los costes de atención en los edificios gubernamentales. Además, al digitalizar su tramitación íntegramente se facilita la recopilación y tratamiento de los datos de estos.

Tecnología:

En este caso se realizará mediante un servidor de aplicaciones. El sistema es similar al del portal web excepto que este permite al ciudadano interactuar con procesos administrativos a través de este. Para la implementación se vuelve a utilizar servicios comunes ofrecidos por la Secretaría de Administración Digital como se recomienda en la legislación. En este caso se basará en la plataforma ACCEDA.

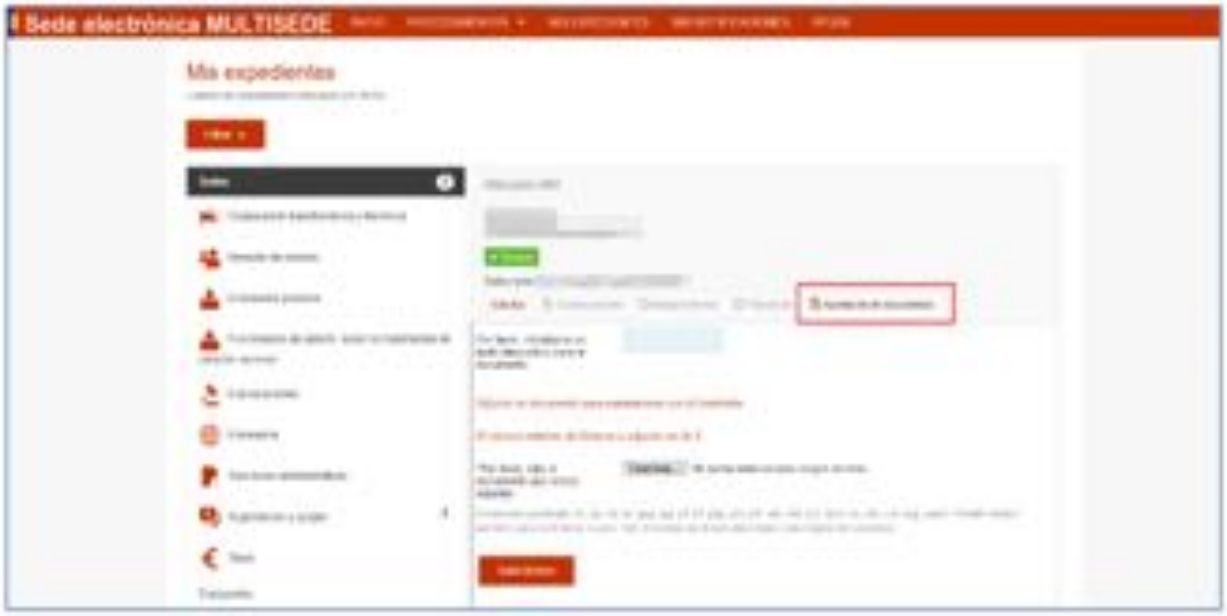


Figura A1-5 Plataforma ACCEDA . [26]

Dimensiones de seguridad	A	C	I	D	A
Valores	4	3	4	4	4
Activos dependientes del servicio:					
[D] Datos / Información					
[K] Claves criptográficas	[x506-2] Certificado sede-e				
[S] Servicio dependiente	[pki] Servicio PKI Ayto.				
[SW] Software - Aplicaciones informática	[dbms2] Base de datos sede-e [www2] Servidor de presentación sede-e [app1] Servidor de aplicaciones sede-e [hypervisor1] Hypervisor CPD Ayto.				
[HW] Equipamiento informático (hardware)	[host1] Servidores CPD Ayto. [network1] Electrónica CPD Ayto. [pc1] Equipos cliente Ayto.				

[COM] Redes de comunicaciones	[lan1] Red Ayto. [internet1] Servicio ISP Ayto.
[Media] Soportes de información	
[AUX] Equipamiento auxiliar	
[L] Instalaciones	[site1] CPD del ayuntamiento
[P] Persona	[adm1]Administradores Ayto. [op2] Operadores del ayuntamiento [ue1] Usuarios externos

Tabla 3-16 Análisis del servicio de sede electrónica.

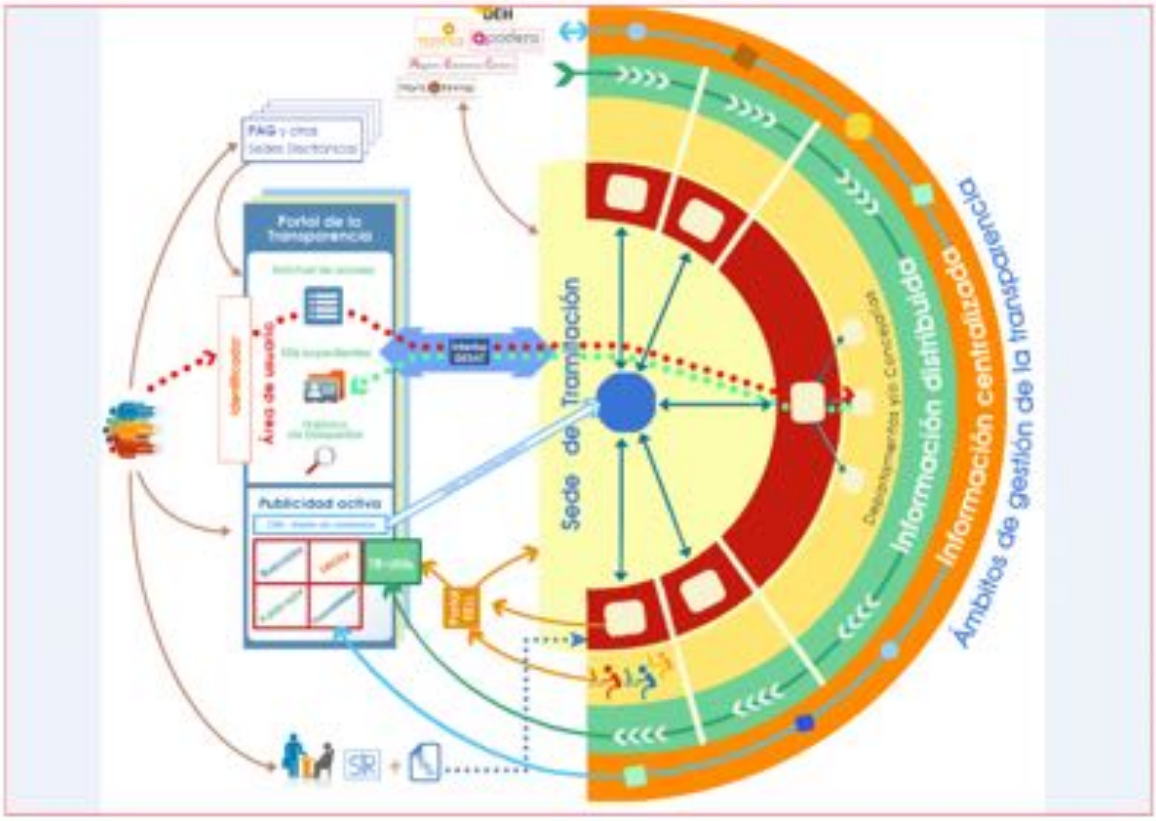
3. PORTAL DE TRANSPARENCIA
Información:
General: Con este servicio se pretende ofrecer al ciudadano información pública para su comprobación o reutilización. El objetivo es mejorar la claridad y calidad del gobierno de la ciudad. Tecnología: Para la creación del portal de transparencia la ciudad utilizará la funcionalidad de portal en la nube para administraciones locales. Este es un servicio previsto por el Ministerio de Asuntos Económicos y la Transformación Digital y la Federación Española de Municipios y Provincias.   

Figura A1-6 Portal de transparencia en la nube. [27] (Se puede observar como su principal fuente de alimentación es a través de su API GESAT pero también se integra con portal y otras aplicaciones)

Como se puede observar el portal se relacionarán a través de otras herramientas de la AGE, de la administración local y principalmente por la interfaz proporcionada. Esta interfaz se puede integrar con otros servicios o manualmente a través de los departamentos de la ciudad.

Dado que hemos eliminado este servicio del ámbito local no tendrá activos en las instalaciones.

Dimensiones de seguridad	A	C	I	D	A
Valores	2	1	3	2	2
Activos dependientes del servicio:					
[D] Datos / Información					
[K] Claves criptográficas					
[S] Servicio dependiente	[nube1] portal de transparencia				
[SW] Software - Aplicaciones informática					
[HW] Equipamiento informático (hardware)	[network1] Electrónica CPD Ayto. [pc1] Equipos cliente Ayto.				
[COM] Redes de comunicaciones	[lan1] Red Ayto. [internet1] Servicio ISP Ayto.				
[Media] Soportes de información					
[AUX] Equipamiento auxiliar					
[L] Instalaciones	[site1] CPD del ayuntamiento				
[P] Persona	[adm1]Administradores Ayto. [op2] Operadores Ayto. [ue1] Usuarios externos				

Tabla 3-17 Análisis del servicio de portal de transparencia.

4. INTEGRACIÓN EN REDES SOCIALES

Información:

General:

En este caso el servicio que se pretende utilizar es una gestión multicanal de todas las redes sociales empleadas por la ciudad. Además, el servicio unifica el control de cuentas a los servicios de emergencia, educación y salud de la ciudad.

Tecnología:

Se instalará un sistema de CRM con módulos de gestión de cuentas en redes sociales. El mantenimiento y administración se realizará a través de internet. La plataforma que se montará será una de tipo código abierto basado en por ejemplo una arquitectura LAMP como por ejemplo Suite CRM. [28]

Figura A1-7 Ejemplo de CRM (Salesforce). [29]

Este tipo de portales permiten tener mayor control sobre todas las publicaciones e información disponible en las redes sociales. También ayudan a establecer un control de comunicaciones e interacciones con el ciudadano o cualquier usuario que desee hacer uso o consulta a los servicios del gobierno de la ciudad.

Dimensiones de seguridad	A	C	I	D	A
Valores	3	1	2	4	4
Activos dependientes del servicio:					
[D] Datos / Información	[passwd1] Credenciales de redes sociales				
[K] Claves criptográficas					
[S] Servicio dependiente	[nube2] redes sociales				
[SW] Software - Aplicaciones informática	[dbms3] Base de datos CRM [www3] Servidor de presentación CRM [app2] Servidor de aplicaciones CRM [hypervisor1] Hypervisor CPD Ayto.				
[HW] Equipamiento informático (hardware)	[host1] Servidores CPD Ayto. [network1] Electrónica CPD Ayto. [pc1] Equipos cliente Ayto.				
[COM] Redes de comunicaciones	[lan1] Red Ayto. [internet1] Servicio ISP Ayto.				
[Media] Soportes de información					
[AUX] Equipamiento auxiliar					
[L] Instalaciones	[site1] CPD del ayuntamiento				
[P] Persona	[adm1]Administradores Ayto.				

	[op1] Operador community manager. [ue1] Usuarios externos.

Tabla 3-18 Análisis del servicio de integración en redes sociales.

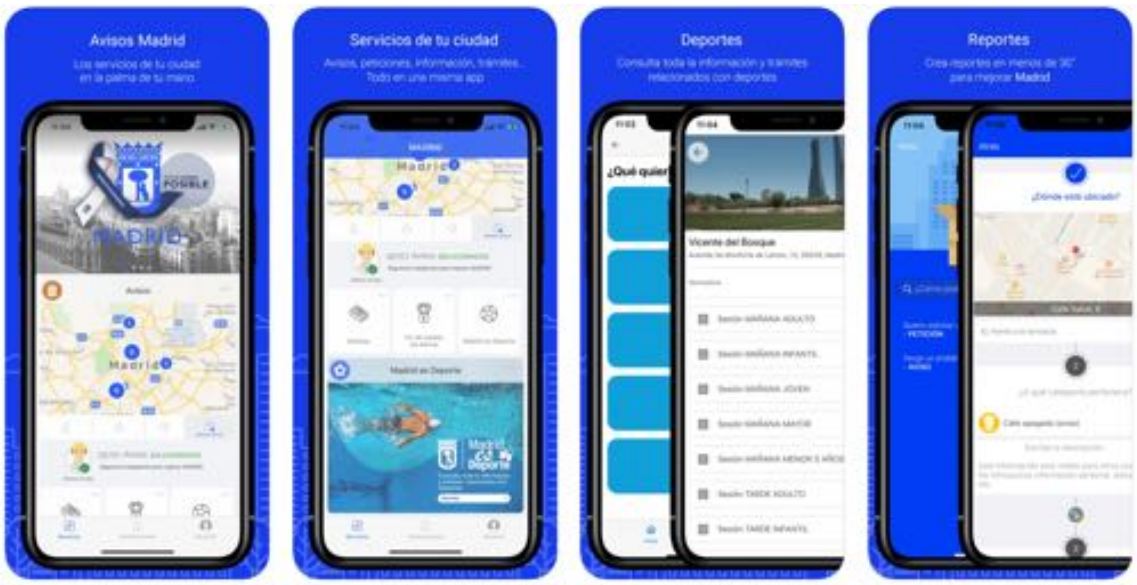
5. APLICACIONES MÓVILES DE INFORMACIÓN Y ATENCIÓN AL CIUDADANO
Información:
General: Con este servicio se pretende ofrecer al ciudadano información similar a la encontrada en el portal, pero en este caso a través de una aplicación móvil. Tecnología: En este caso lo que se utiliza es un entorno de trabajo que publica un servicio RESTful desde los sistemas del ayuntamiento que alimentan a una aplicación móvil desarrollada tanto para sistemas Android como para sistemas IOS.   

Figura A1-8 Aplicación del ayuntamiento de Madrid.

Dimensiones de seguridad	A	C	I	D	A
Valores	2	1	3	2	2
Activos dependientes del servicio:					
[D] Datos / Información	[source1] Código fuente de app Android [source2] Código fuente de app IOS				
[K] Claves criptográficas	[x506-3] Certificado API apps				
[S] Servicio dependiente	[pki] Servicio PKI Ayto. [nube3] Tiendas de Android e IOS				
[SW] Software - Aplicaciones informática	[dbms4] Base de datos API apps [app3] Servidor de aplicaciones API apps [hypervisor1] Hypervisor CPD Ayto.				

[HW] Equipamiento informático (hardware)	[host1] Servidores CPD Ayto. [network1] Electrónica CPD Ayto. [pc1] Equipos cliente Ayto.
[COM] Redes de comunicaciones	[lan1] Red Ayto. [internet1] Servicio ISP Ayto.
[Media] Soportes de información	
[AUX] Equipamiento auxiliar	
[L] Instalaciones	[site1] CPD del ayuntamiento
[P] Persona	[adm1] Administradores Ayto. [op1] Op. Community manager. [ue1] Usuarios externos

Tabla 3-19 Análisis del servicio de aplicación móvil del ciudadano.

6. CONSUMO Y CALIDAD DEL AGUA
Información:

General:

El objetivo de este servicio es monitorizar y gestionar la infraestructura de distribución de agua corriente y de alcantarillado.

Tecnología:

En este caso se pueden diferenciar dos partes. Hay una aplicación que recopila todos los datos y gestiona los diferentes tipos de sensores distribuidos en las infraestructuras. Luego hay una segunda aplicación que extrae todos esos datos y los representa en un cuadro de mandos. La primera utiliza una base de datos de tipo noSQL basado en columnas para almacenamiento Big Data.

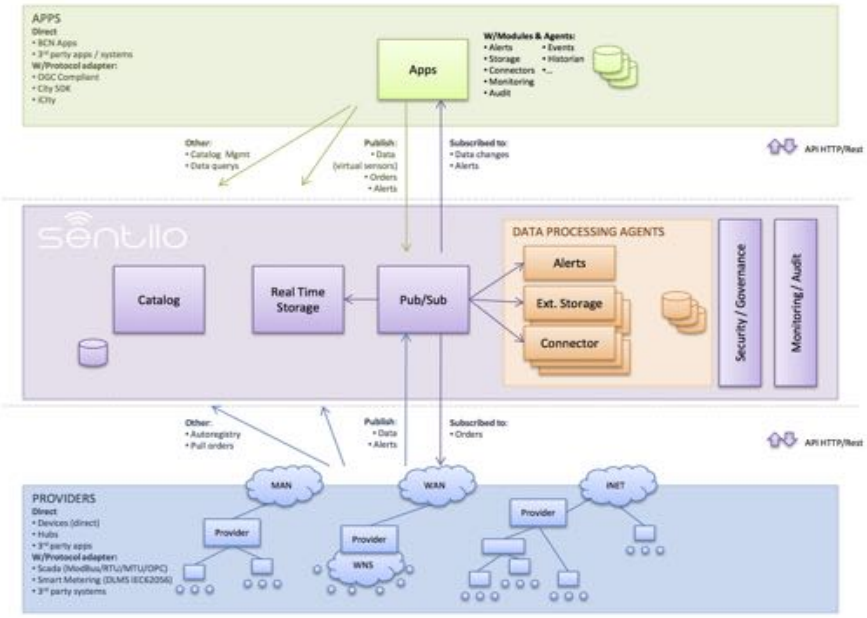


Figura A1-9 Aplicación SENTILO. [27] (Aplicación disponible al servicio publico para la integración de IoT. Se pueden observar el front-end -arriba–, el back-end – centro- y la sección de IoT – abajo)

Dimensiones de seguridad	A	C	I	D	A
Valores	3	3	2	5	3
Activos dependientes del servicio:					
[D] Datos / Información					
[K] Claves criptográficas	[x506-4] Certificado API sensores				
[S] Servicio dependiente	[pki] Servicio PKI Ayto.				
[SW] Software - Aplicaciones informática	[dbms5] Base de datos monitor agua [dbms6] Base de datos noSQL agua [www4] Servidor de presentación monitor agua [app4] Servidor de aplicaciones agua [app5] Servidor de aplicaciones monitor agua [hypervisor1] Hypervisor CPD Ayto.				
[HW] Equipamiento informático (hardware)	[host1] Servidores CPD Ayto. [network1] Electrónica CPD Ayto. [hub] Dispositivo frontera concentradores [sensor IoT] sensores de infra agua [actuador IoT] actuadores de infra agua [pc1] Equipos cliente Ayto.				
[COM] Redes de comunicaciones	[lan1] Red Ayto. [internet1] Servicio ISP Ayto. [Lan2] Red de área local de agregación disp. IoT [internet2] Servicio ISP concentradores				
[Media] Soportes de información					
[AUX] Equipamiento auxiliar					
[L] Instalaciones	[site1] CPD del ayuntamiento [infra1] Infraestructura agua				
[P] Persona	[adm1] Administradores Ayto. [op2] Operador Ayto. [ui1] Usuarios internos – jefatura Ayto.				

Tabla 3-20 Análisis del servicio de consumo y calidad del agua.

7. MONITORIZACIÓN DEL CONSUMO ENERGÉTICO EN EDIFICIOS PRIVADOS Y HOGARES
Información:
General: Este servicio, aunque puede ser más propio de una empresa privada, se incluye como necesario en la ciudad analizada por su utilización de las Smart Grid. Las proveedoras de electricidad suelen monitorizar de esta forma dado que tienen el requerimiento legal de utilizar contadores inteligentes. En este caso suponemos que es como estudio para monitorizar el consumo.

Tecnología:

En este caso se utilizarán contadores inteligentes que a través de PLC transmitirán la información hasta concentradores, estos a su vez enviarán la información a un servidor principal que analizará los datos.

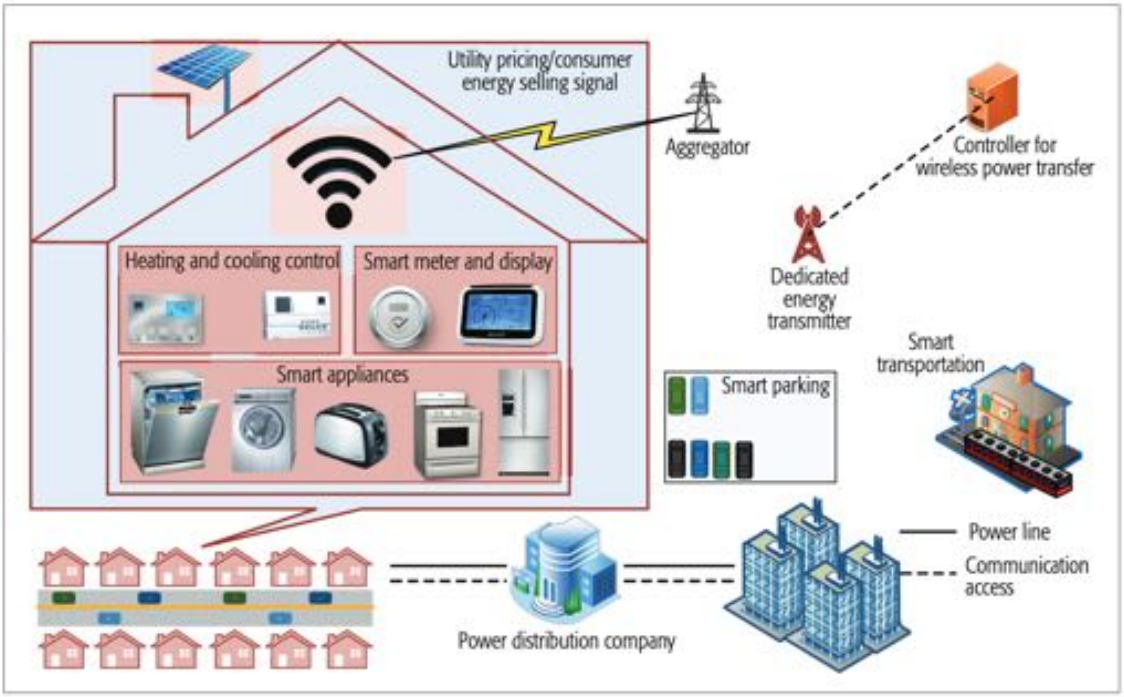


Figura A1-10 Esquema de Ciudad Inteligente enfocado a gestión de energía en hogares. [30]

Dimensiones de seguridad	A	C	I	D	A
Valores	3	3	2	2	2
Activos dependientes del servicio:					
[D] Datos / Información					
[K] Claves criptográficas	[x506-5] Certificado API sensores electricidad				
[S] Servicio dependiente	[pki] Servicio PKI Ayto.				
[SW] Software - Aplicaciones informática	[dbms7] Base de datos noSQL electricidad. [www5] Servidor de presentación electricidad. [app6] Servidor de aplicaciones electricidad. [hypervisor1] Hypervisor CPD Ayto.				
[HW] Equipamiento informático (hardware)	[host1] Servidores CPD Ayto. [network1] Electrónica CPD Ayto. [hub2] Dispositivo frontera concentradores de electricidad. [contador] contadores inteligentes [pc1] Equipos cliente Ayto.				
[COM] Redes de comunicaciones	[lan1] Red Ayto.				

	[internet1] Servicio ISP Ayto. [PLC] Red PLC hasta concentradores [internet3] Servicio ISP concentradores electricidad
[Media] Soportes de información	
[AUX] Equipamiento auxiliar	
[L] Instalaciones	[site1] CPD del ayuntamiento [infra2] Infraestructura eléctrica
[P] Persona	[adm1] Administradores Ayto. [ui1] Usuarios internos – jefatura Ayto.

Tabla 3-21 Análisis del servicio de monitorización del consumo eléctrico.

8. RECOGIDA DE RESIDUOS

Información:

General:

La ciudad tiene contratado a una empresa que realiza la gestión de residuos. Ofrece un sistema por el que se puede monitorizar y controlar toda la flota de recogida y además informa en tiempo real del estado de contenedores etc.

Tecnología:

La aplicación en este caso está basada en la nube. El ayuntamiento en este caso lo que realiza son comprobaciones para asegurar que se cumplen una serie de SLAs.

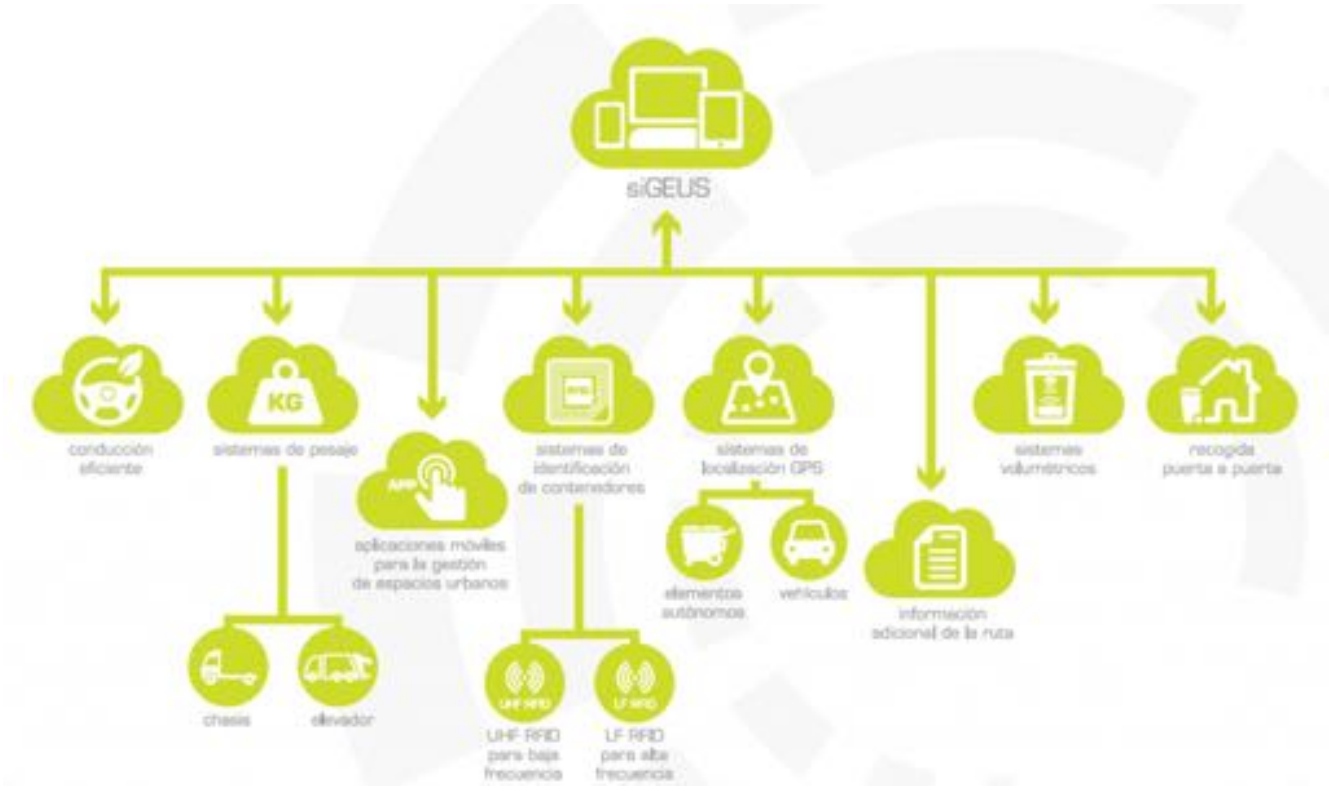


Figura A1-11 integración de la plataforma siGEUS para la gestión de residuos. [31] (Se trata de una aplicación para el control integral de residuos)

Dimensiones de seguridad	A	C	I	D	A
Valores	3	3	2	3	3
Activos dependientes del servicio:					
[D] Datos / Información					
[K] Claves criptográficas					
[S] Servicio dependiente	[nube4] cuadro de mandos de residuos				
[SW] Software - Aplicaciones informática					
[HW] Equipamiento informático (hardware)	[network1] Electrónica CPD Ayto. [pc1] Equipos cliente Ayto.				
[COM] Redes de comunicaciones	[lan1] Red Ayto. [internet1] Servicio ISP Ayto.				
[Media] Soportes de información					
[AUX] Equipamiento auxiliar					
[L] Instalaciones	[site1] CPD del ayuntamiento				
[P] Persona	[adm1]Administradores Ayto. [ui1] Usuarios internos – jefatura Ayto.				

Tabla 3-22 Análisis del servicio de gestión de residuos.

9. CONTROL DE TRÁFICO
Información:
General: La ciudad tiene como sus principales prioridades garantizar el buen estado de las vías y facilitar la circulación. Para ello se presenta un servicio de control con CCTVs y gestión de la señalética. Tecnología: El sistema es similar al de la gestión del agua. En este caso en vez de dos aplicaciones es solo una. Ahora bien, el control se hace desde la policía local y en un site secundario se ha instalado una tecnología similar.

Figura A1-12 Ejemplo de conexión de sensores a un sistema de tráfico. [32]

Figura A1-13 Mapa de control sistema ADIMOT. [33]

Dimensiones de seguridad	A	C	I	D	A
Valores	3	3	2	3	3
Activos dependientes del servicio:					
[D] Datos / Información					

[K] Claves criptográficas	[x506-6] Certificado API sensores tráfico
[S] Servicio dependiente	[pki] Servicio PKI Ayto.
[SW] Software - Aplicaciones informática	[dbms8] Base de datos noSQL tráfico [www6] Servidor de presentación tráfico [app7] Servidor de aplicaciones tráfico
[HW] Equipamiento informático (hardware)	[host2] Servidores CPD comisaría [network2] Electrónica CPD comisaría [hub3] Dispositivo frontera concentradores tráfico [sensor IoT2] sensores de infra tráfico [actuador IoT2] actuadores de infra tráfico [pc2] Equipos cliente comisaría
[COM] Redes de comunicaciones	[lan3] Red comisaría [internet4] Servicio ISP comisaría [Lan4] Red de área local de agregación disp. IoT tráfico [internet5] Servicio ISP concentradores tráfico
[Media] Soportes de información	
[AUX] Equipamiento auxiliar	
[L] Instalaciones	[site2] CPD de la comisaría [infra3] Infraestructura tráfico
[P] Persona	[adm2] Administradores comisaría [op3] Operador comisaría [ui2] Usuarios internos – jefatura comisaría. [ui1] Usuarios internos – jefatura Ayto.

Tabla 3-23 Análisis del servicio de control de tráfico.

10. GESTIÓN DE PUNTOS DE RECARGA DE VEHÍCULOS ELÉCTRICOS
Información:
General: Con este servicio se ofrece en una aplicación el estado de todos los puntos de recarga de vehículos eléctricos. Desde el punto de vista del ciudadano, éste puede ver la localización y el estado del punto de recarga. Desde el punto de vista de la administración, puede revisar historiales, detalles y predicciones de puntos de recarga futuros. Tecnología: Se utilizará un módulo de la aplicación móvil para proporcionar esta información. Los puntos de vehículos estarán conectados con dicha aplicación, es este caso no habrá hubs que concentren la señal. Además, se añadirán tarjetas RFID en los puntos para que alguien que pase cerca pueda identificar el punto de recarga.

Figura A1-14 Puntos de recarga de vehículos en el centro de la ciudad de Madrid.

Dimensiones de seguridad	A	C	I	D	A
Valores	2	1	2	1	2
Activos dependientes del servicio:					
[D] Datos / Información					
[K] Claves criptográficas	[x506-7] Certificado API sensores carga				
[S] Servicio dependiente	[pki] Servicio PKI Ayto.				
[SW] Software - Aplicaciones informática	[dbms9] Base de datos puntos de carga. [app8] Servidor de aplicaciones puntos de carga. [hypervisor1] Hypervisor CPD Ayto.				
[HW] Equipamiento informático (hardware)	[host1] Servidores CPD Ayto. [network1] Electrónica CPD Ayto. [sensores IoT3] Sensores puntos carga				
[COM] Redes de comunicaciones	[lan1] Red Ayto. [internet1] Servicio ISP Ayto. [internet6] Servicio ISP puntos de carga				
[Media] Soportes de información					
[AUX] Equipamiento auxiliar					
[L] Instalaciones	[site1] CPD del ayuntamiento [infra4] Infraestructura carga				
[P] Persona	[adm1] Administradores Ayto. [ue1] Usuarios externos				

Tabla 3-24 Análisis del servicio de control de puntos de recarga.

11. MEDICIÓN MEDIOAMBIENTAL: CALIDAD DEL AIRE
Información:

General:

Con este servicio se monitoriza la calidad del aire, especialmente el estado de concentración de aquellas partículas contaminantes peligrosas para la salud. En caso de superar un determinado umbral se presenta un aviso para poner en funcionamiento protocolos anticontaminación.

Tecnología:

Este caso es similar a los servicios presentados anteriormente. Se compone de una red de estaciones que mediante conexión LTE-M informan periódicamente de la calidad del aire a un servicio back-end situado y mantenido en el consistorio. Este servidor alimenta bases de datos NoSQL con la información obtenida. Además, otra aplicación que aprovecha nuevas tecnologías de big data aprovecha esta información e información abierta de AEMET para establecer predicciones en cuanto a la calidad del aire.

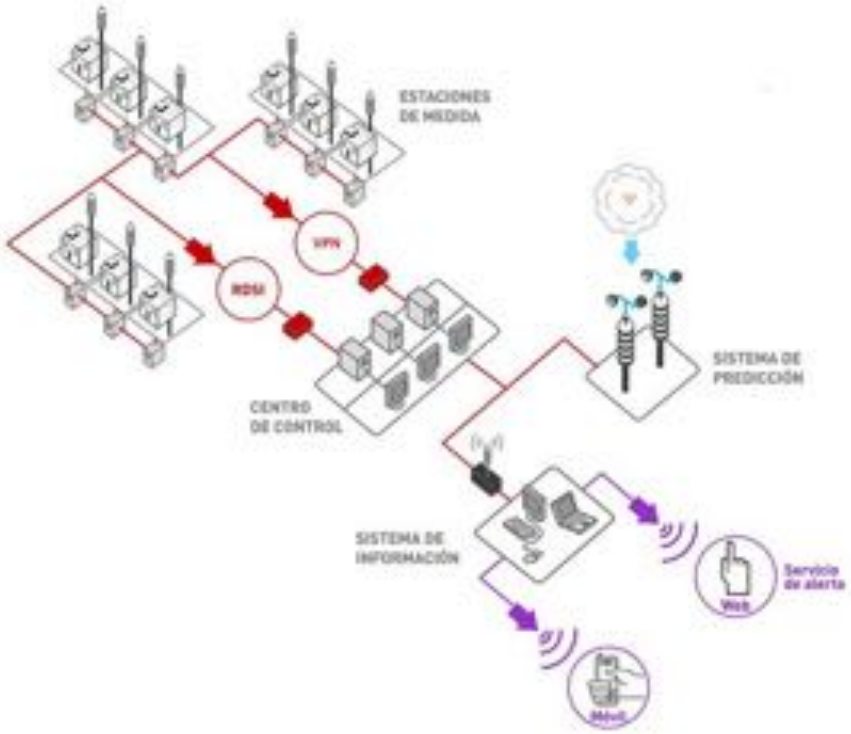


Figura A1-15 Esquema sistema de calidad del aire de la comunidad de Madrid. [34]

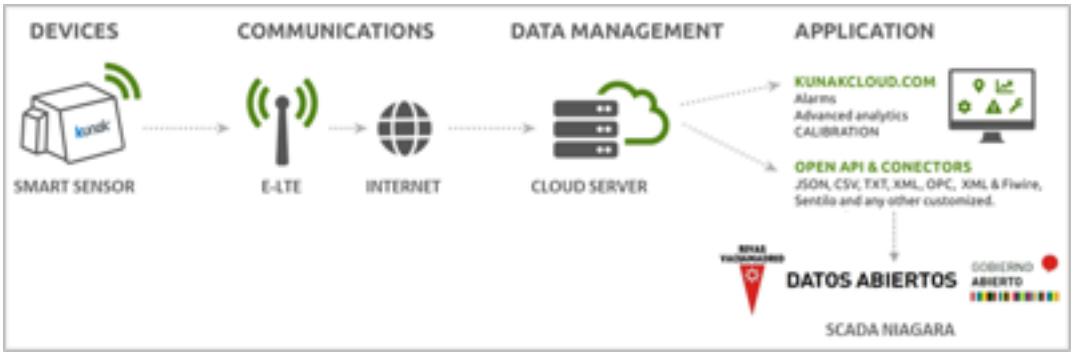


Figura A1-16 Esquema de comunicaciones de la red de sensores e integración en la vertical de calidad de aire (Caso de uso de Rivas Vaciamadrid) [35]

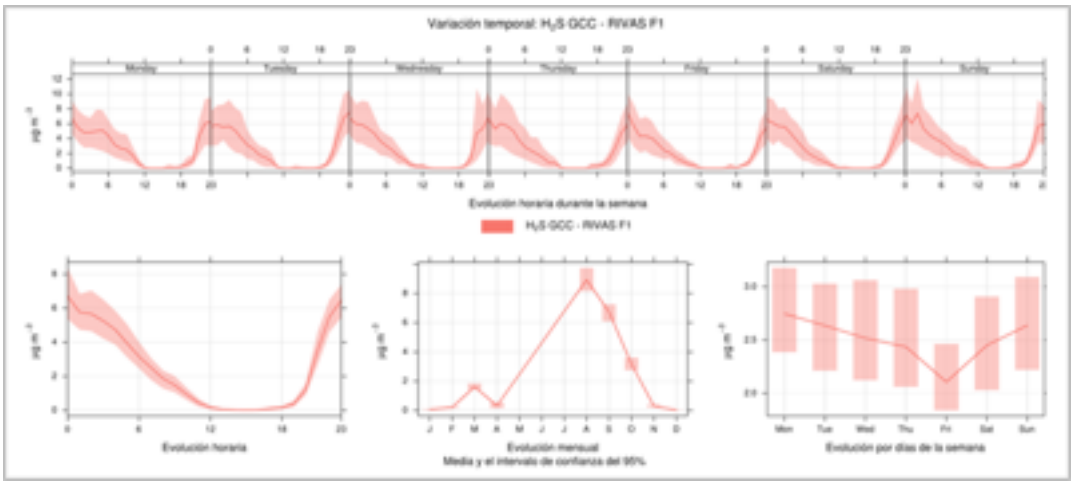


Figura A1-17 Variación temporal de la monitorización (Caso de uso de Rivas Vaciamadrid) [35]

Dimensiones de seguridad	A	C	I	D	A
Valores	2	1	2	1	2
Activos dependientes del servicio:					
[D] Datos / Información					
[K] Claves criptográficas	[x506-1] Certificado portal Ayto.				
[S] Servicio dependiente	[pki] Servicio PKI Ayto.				
[SW] Software - Aplicaciones informática	[dbms10] Base de datos noSQL contaminación [www1] Servidor del portal web [app9] Servidor de aplicaciones contaminación. [hypervisor1] Hypervisor CPD Ayto.				
[HW] Equipamiento informático (hardware)	[host1] Servidores CPD Ayto. [network1] Electrónica CPD Ayto. [sensores IoT4] Sensores estaciones atmosféricas				
[COM] Redes de comunicaciones	[lan1] Red Ayto. [internet1] Servicio ISP Ayto. [internet7] Servicio ISP estaciones				

[Media] Soportes de información	
[AUX] Equipamiento auxiliar	
[L] Instalaciones	[site1] CPD del ayuntamiento [infra5] Infraestructura estaciones
[P] Persona	[adm1] Administradores Ayto. [ue1] Usuarios externos

Tabla 3-25 Análisis del servicio de control de calidad del aire.

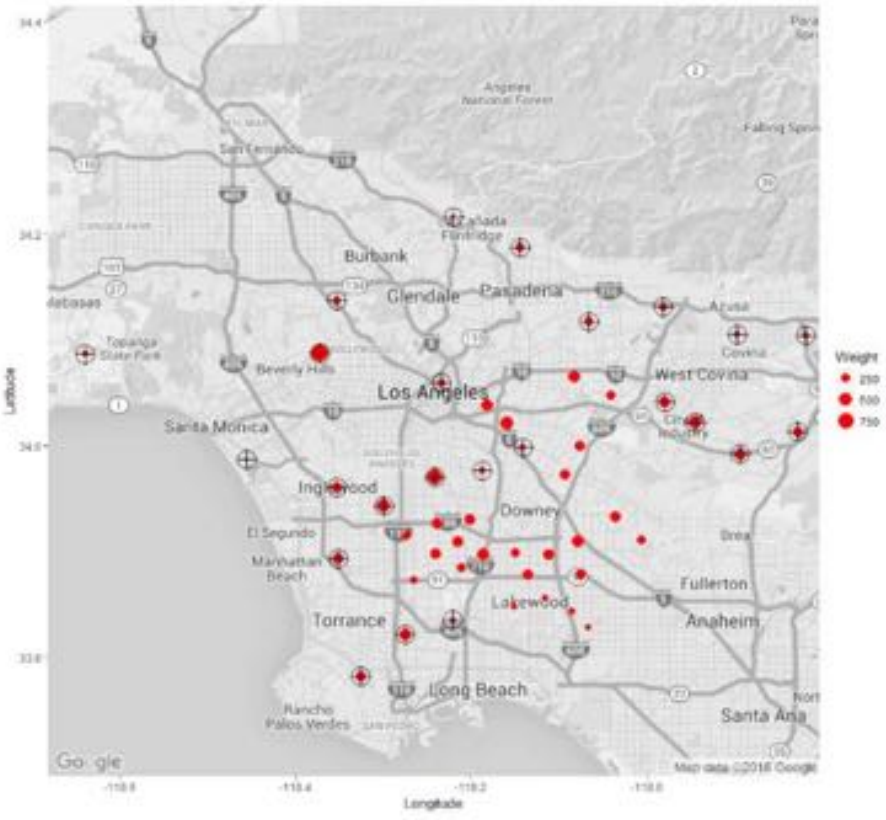
12. SEGUIMIENTO Y ACTIVIDAD DE EFECTIVOS Y BRIGADAS
Información:
General: Este servicio es de uso interno. Se utiliza para predecir los puntos conflictivos en la ciudad en cada momento y así regular las patrullas y brigadas en cada periodo de tiempo. Tecnología: Para esto se utilizará una aplicación de desarrollo propio que la comisaría de policía ha encargado. La aplicación utilizará una arquitectura basada en LAMP y servicios de computación. Para ello dispondrán de un clúster de virtualización en un pequeño CPD de la comisaría. La aplicación utilizará información cartográfica de la ciudad, servicios de datos abiertos y la información de los crímenes cometidos en la ciudad.   

Figura A1-18 Predicción estadística sobre crímenes cometidos en la ciudad de Los Ángeles. **[36]** (Los puntos rojos indican los lugares con más probabilidad de producirse incidentes)					
Dimensiones de seguridad	A	C	I	D	A
Valores	4	5	3	2	4
Activos dependientes del servicio:					
[D] Datos / Información					
[K] Claves criptográficas					
[S] Servicio dependiente					
[SW] Software - Aplicaciones informática	[dbms11] Base de datos noSQL policía [www7] Servidor de presentación policía [app10] Servidor de aplicaciones policía				
[HW] Equipamiento informático (hardware)	[host2] Servidores CPD comisaría [network2] Electrónica CPD comisaría [pc2] Equipos cliente comisaría				
[COM] Redes de comunicaciones	[lan3] Red comisaría				
[Media] Soportes de información					
[AUX] Equipamiento auxiliar					
[L] Instalaciones	[site2] CPD de la comisaría				
[P] Persona	[adm2] Administradores comisaría [op3] Operador comisaría [ui2] Usuarios internos – jefatura comisaría.				

Tabla 3-26 Análisis del servicio de organización de brigadas

3.4.1.3 Valoración de los activos

A continuación, se muestra una lista con todos los activos de todos los servicios que hemos cubierto en el alcance. Se ha intentado ser realista, pero para mayor capacidad de análisis se deben emplear herramientas automáticas como PILAR. Esta herramienta está provista por el CCN para facilitar la construcción de análisis con cientos de activos y amenazas.

Como se puede observar hay activos que se repiten entre los diferentes servicios. Estos activos heredarán las valoraciones más restrictivas de los servicios.

Por ejemplo: Un servicio necesita una disponibilidad alta, en la que como mucho el sistema puede estar caído dos horas, y hace uso de un balanceador. Otro servicio puede que no necesite tanta rapidez para recuperarse, pero el balanceador debe hacerlos en menos de dos horas dado que vulneraría los niveles de servicio del que necesita disponibilidad alta.

Se han tratado los servicios de contrato de internet como un activo entre servicio y comunicación. Se puede observar como con la llegada de IoT aumenta la dependencia con este tipo de proveedores

Finalmente, se han marcado de color diferentes aquellos que por su relevancia serán seleccionados para hacer el análisis de riesgos. Los activos que no se consideran tan críticos en verde, los medios en amarillo y los muy críticos en rojo.

Nº	Activo	Tipo	Valoración (ACIDA)					Resultado
1	[source1] Código fuente de app Android	[D]	2	1	3	2	2	10
2	[source2] Código fuente de app IOS	[D]	2	1	3	2	2	10
3	[passwd1] Credenciales de redes sociales	[D]	3	1	2	4	4	14
4	[x506-1] Certificado portal Ayto.	[K]	2	1	4	4	3	14
5	[x506-2] Certificado sede-e	[K]	4	3	4	4	4	19
6	[x506-3] Certificado API apps	[K]	2	1	3	2	2	10
7	[x506-4] Certificado API sensores	[K]	3	3	2	5	3	16
8	[x506-5] Certificado API sensores electricidad	[K]	3	3	2	2	2	12
9	[x506-6] Certificado API sensores tráfico	[K]	3	3	2	3	3	14
10	[x506-7] Certificado API sensores carga	[K]	2	1	2	1	2	8
11	[pki] Servicio PKI Ayto.	[S]	4	3	4	5	4	20
12	[nube1] portal de transparencia	[S]	2	1	3	2	2	10
13	[nube2] redes sociales	[S]	3	1	2	4	4	14
14	[nube3] Tiendas de Android e IOS	[S]	2	1	3	2	2	10
15	[nube4] cuadro de mandos de residuos	[S]	3	3	2	3	3	14
16	[internet1] Servicio ISP Ayto.	[S]	2	1	4	4	3	14
17	[internet2] Servicio ISP concentradores	[S]	3	3	2	5	3	16
18	[internet3] Servicio ISP concentradores electricidad	[S]	3	3	2	2	2	12
19	[internet4] Servicio ISP comisaría	[S]	4	5	3	2	4	18
20	[internet5] Servicio ISP concentradores tráfico	[S]	3	3	2	3	3	14
21	[internet6] Servicio ISP puntos de carga	[S]	2	1	2	1	2	8
22	[internet7] Servicio ISP estaciones	[S]	2	1	2	1	2	8

Nº	Activo	Tipo	Valoración (ACIDA)					Resultado
23	[hypervisor1] Hypervisor CPD Ayto.	[SW]	4	3	4	5	4	20
24	[dbms1] Base de datos portal	[SW]	2	1	4	4	3	14
25	[dbms2] Base de datos sede-e	[SW]	4	3	4	4	4	19
26	[dbms3] Base de datos CRM	[SW]	3	1	2	4	4	14
27	[dbms4] Base de datos API apps	[SW]	2	1	3	2	2	10
28	[dbms5] Base de datos monitor agua	[SW]	3	3	2	5	3	16
29	[dbms6] Base de datos noSQL agua	[SW]	3	3	2	5	3	16
30	[dbms7] Base de datos noSQL electricidad.	[SW]	3	3	2	2	2	12
31	[dbms8] Base de datos noSQL tráfico	[SW]	3	3	2	3	3	14
32	[dbms9] Base de datos puntos de carga.	[SW]	2	1	2	1	2	8
33	[dbms10] Base de datos noSQL contaminación	[SW]	2	1	2	1	2	8
34	[dbms11] Base de datos noSQL policía	[SW]	4	5	3	2	4	18
35	[www1] Servidor de presentación portal	[SW]	2	1	4	4	3	14
36	[www2] Servidor de presentación sede-e	[SW]	4	3	4	4	4	19
37	[www3] Servidor de presentación CRM	[SW]	3	1	2	4	4	14
38	[www4] Servidor de presentación monitor agua	[SW]	3	3	2	5	3	16
39	[www5] Servidor de presentación electricidad.	[SW]	3	3	2	2	2	12
40	[www6] Servidor de presentación tráfico	[SW]	3	3	2	3	3	14
41	[www7] Servidor de presentación policía	[SW]	4	5	3	2	4	18
42	[app1] Servidor de aplicaciones sede-e	[SW]	4	3	4	4	4	19
43	[app2] Servidor de aplicaciones CRM	[SW]	3	1	2	4	4	14
44	[app3] Servidor de aplicaciones API apps	[SW]	2	1	3	2	2	10
45	[app4] Servidor de aplicaciones agua	[SW]	3	3	2	5	3	16
46	[app5] Servidor de aplicaciones monitor agua	[SW]	3	3	2	5	3	16

Nº	Activo	Tipo	Valoración (ACIDA)					Resultado
47	[app6] Servidor de aplicaciones electricidad.	[SW]	3	3	2	2	2	12
48	[app7] Servidor de aplicaciones tráfico	[SW]	3	3	2	3	3	14
49	[app8] Servidor de aplicaciones puntos de carga.	[SW]	2	1	2	1	2	8
50	[app9] Servidor de aplicaciones contaminación.	[SW]	2	1	2	1	2	8
51	[app10] Servidor de aplicaciones policía	[SW]	4	5	3	2	4	18
52	[host1] Servidores CPD Ayto.	[HW]	4	3	4	5	4	20
53	[host2] Servidores CPD comisaría	[HW]	4	5	3	3	4	19
54	[network1] Electrónica CPD Ayto.	[HW]	4	3	4	5	4	20
55	[network2] Electrónica CPD comisaría	[HW]	4	5	3	3	4	19
56	[pc1] Equipos cliente Ayto.	[HW]	4	3	4	5	4	20
57	[pc2] Equipos cliente comisaría	[HW]	4	5	3	3	4	19
58	[hub] Dispositivo frontera concentradores	[HW]	3	3	2	5	3	16
59	[hub2] Dispositivo frontera concentradores electricidad.	[HW]	3	3	2	2	2	12
60	[hub3] Dispositivo frontera concentradores tráfico	[HW]	3	3	2	3	3	14
61	[contador] contadores inteligentes	[HW]	3	3	2	2	2	12
62	[sensor IoT] sensores de infra agua	[HW]	3	3	2	5	3	16
63	[sensor IoT2] sensores de infra tráfico	[HW]	3	3	2	3	3	14
64	[sensores IoT3] Sensores puntos carga	[HW]	2	1	2	1	2	8
65	[sensores IoT4] Sensores estaciones atmosféricas	[HW]	2	1	2	1	2	8
66	[actuador IoT] actuadores de infra agua	[HW]	3	3	2	5	3	16
67	[actuador IoT2] actuadores de infra tráfico	[HW]	3	3	2	2	2	12
68	[lan1] Red Ayto.	[COM]	4	3	4	5	4	20
69	[Lan2] Red de área local de agregación disp. IoT agua	[COM]	3	3	2	5	3	16
70	[lan3] Red comisaría	[COM]	4	5	3	3	4	19

Nº	Activo	Tipo	Valoración (ACIDA)					Resultado
71	[Lan4] Red de área local de agregación disp. IoT tráfico	[COM]	3	3	2	3	3	14
72	[PLC] Red PLC hasta concentradores	[COM]	3	3	2	2	2	12
73	[site1] CPD del ayuntamiento	[L]	4	3	4	5	4	20
74	[site2] CPD de la comisaría	[L]	4	5	3	3	4	19
75	[infra1] Infraestructura agua	[L]	3	3	2	5	3	16
76	[infra2] Infraestructura eléctrica	[L]	3	3	2	2	2	12
77	[infra3] Infraestructura tráfico	[L]	3	3	2	3	3	14
78	[infra4] Infraestructura carga	[L]	3	3	2	2	2	12
79	[adm1]Administradores Ayto.	[P]	4	3	4	5	4	20
80	[adm2]Administradores comisaría	[P]	4	5	3	3	4	19
81	[op1] Op. Community manager.	[P]	3	1	4	4	4	16
82	[op2] Operadores Ayto.	[P]	4	3	4	5	4	20
83	[op3] Operador comisaría	[P]	3	3	2	3	3	14
84	[ue1] Usuarios externos	[P]	4	3	4	5	4	20
85	[ui1] Usuarios internos – jefatura Ayto.	[P]	3	3	2	5	3	16
86	[ui2] Usuarios internos – jefatura comisaría.	[P]	4	5	3	2	4	18

Tabla 3-27 Propagación de las valoraciones sobre todos los activos.

3.4.2 Identificación de amenazas

Una vez se dispone de un inventario de los activos ponderados y valorados según sus dimensiones de seguridad, se puede pasar a ver qué amenazas son las que afectan a dichos activos.

Al igual que con los activos vamos a clasificarlas siguiendo el método MAGERIT con lo que tendremos de diferentes tipos:

[N] Desastres naturales	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[I] De origen industrial	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
[E] Errores y fallos no intencionados	Fallos no intencionales causados por las personas.
[A] Ataques intencionados	Fallos deliberados causados por las personas. La numeración que emplea MAGERIT no es consecutiva para coordinar con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto

Tabla 3-28 Tipos de amenazas definidas por Magerit.

Para el descubrimiento de las amenazas nos hemos basado en diferentes factores. Normalmente en una organización, en este caso la ciudad, se deberá dedicar recursos para hacer ciberinteligencia y estudiar todas las amenazas que puedan acaecer sobre esta. Ese tipo de acciones en una administración local se suele llevar a cabo por la policía y equipos de seguridad de los ayuntamientos.

En los análisis de ciberinteligencia se hace uso de informes de entidades especializadas: en el caso de desastres naturales entidades de predicción meteorológica como AEMET, o en el de ciberamenazas otras como el INCIBE o el CCN. Estas entidades sacan informes periódicos informando sobre las amenazas más comunes y atienden a las administraciones cuando hay riesgos o incidentes. Hay muchas otras entidades, en el trabajo hemos acudido a ENISA, que actúa a nivel europeo.

También se debe hacer uso de histórico de incidencias o el uso de bases de datos de vulnerabilidades. Una técnica muy utilizada es el uso de *honeypots* que simulan sistemas TIC. Los responsables de seguridad simulan con ellos organizaciones con características similares a la nuestra para estudiar qué ataques son los más utilizados.

Un analista hará uso de toda esta información y del conocimiento adquirido de la dirección y personas clave de la organización, por ejemplo, para conocer amenazas internas, para hacer un baremo de las posibles amenazas.

Estas amenazas serán propias de cada organización y variarán en función de sus características y condiciones de contorno. Por ejemplo: una ciudad en la sociedad occidental tiene una probabilidad leve de una amenaza intencional como es la ocupación enemiga. En otros países esta amenaza puede ser relevante.

Este trabajo se ha basado principalmente en estudios de vulnerabilidades técnicas y también de informes de amenazas de los últimos años tanto del CCN como del ENISA.

La tecnología empleada por la ciudad inteligente es susceptible a diferentes tipos de ataque. Como se observa en el estado del arte la mayor parte de la tecnología proviene del IoT y los ataques suelen aplicarse contra las tecnologías que se utilizan. Algunos ejemplos pueden ser el jamming, el uso de

interferencias o métodos de denegación de servicio contra las tecnologías de las redes de agregación de datos. También se encuentran muchos problemas con los dispositivos IoT debido a diseños que no tienen en cuenta la posible manipulación o que están al alcance de las personas. Finalmente se encuentran amenazas que afectan directamente a los servicios de la ciudad y que atacan de forma transversal a otras organizaciones como bancos, comercios, servicios de salud entre otros. Estas se corresponden con las encontradas normalmente en los sistemas TIC. [37] [38] [39] [40].

En el caso de las tecnologías big data [41] la mayor parte de estas son debido a incumplimientos de la legislación vigente, fallos de procesos de negocio, planeamiento inadecuado, interfaces inseguras que provocan fugas de información, o denegación de servicio.

En cuanto a la situación actual de amenazas en el ciberespacio, en el informe ENISA [42] del mapa de amenazas en el año 2021 se identifican las siguientes clases de amenazas:

1. Ransomware. Tipo de ataque malicioso donde se cifran los datos de la organización a cambio de una cuantía de dinero. ENISA lo considera la amenaza más importante del 2021. Algunos ejemplos pueden ser REvil o Wanna Cry.

2. Malware. Se trata de un software o firmware que intenta realizar procesos no autorizados que pueden tener un impacto en las dimensiones de seguridad de un sistema. Es una de las amenazas que se han mantenido estables a lo largo del tiempo, aunque estos últimos años se ha notado un retroceso. El uso de nuevas tecnologías y operaciones de las fuerzas del orden han reducido su importancia. Se ha visto incrementado su uso en móviles y contenedores de software como los empleados por Docker.

3. Cryptojacking. Es un tipo de cibercrimen en el que secretamente se utilizan dispositivos de una víctima para realizar operaciones de minería de criptomonedas. Un ejemplo de este tipo de ataques puede ser XMRig.

4. Ataques relacionados con emails. Estos ataques buscan explotar la psicología humana, el factor más débil de la cadena de seguridad. Aunque se han realizado muchas campañas de seguridad la amenaza persiste y de manera notable. En particular se suele dar en entornos corporativos y parecen estar en alza. Este tipo de amenaza podemos encontrar el Spearfishing o el Whaling. Se han dado casos en los que se aprovecha la situación con el Covid 19.

5. Ataques contra la información. Estos ataques comprenden las brechas o exfiltración de información. Un ejemplo sería la publicación de un documento confidencial. Suelen ser el resultado de un ataque avanzado, un atacante interno o un error humano. Algunos ejemplos son la extorsión, difamación, chantaje, robo de ordenadores, etc.

6. Ataques contra la disponibilidad e integridad. Tras esta categoría hay muchos tipos de amenazas y ataques. En estos ataques se encuentran principalmente los de tipo denegación de servicio, especialmente contra servicios web. La evolución de estos ataques es el ataque de denegación de servicio de tipo distribuido que aprovechan botnets para realizar ataques desde varios puntos.

7. Desinformación. Se ha observado el aumento de campañas de desinformación, sobre todo debido a actores con motivaciones geopolíticas. También parece que la conectividad de la gente propiciada por el Covid-19 ha afectado negativamente la situación. Ejemplos de estas amenazas pueden ser las noticias falsas.

8. Finalmente, se incluyen las amenazas no maliciosas. En esta categoría encontraríamos errores de configuración, errores humanos y también desastres naturales o debido a la evolución temporal.

En cambio, el último informe de amenazas del CCN [43], del año 2020 indica que vulnerabilidades de software, la inyección SQL y el uso de troyanos fueron los incidentes más detectados. No obstante, también hace mención a las noticias falsas, el ransomware, al uso de botnets, al creciente número de ataques procedentes de la parte interna de forma involuntaria debido a ataques de tipo Spearfishing.

Especialmente importante es la mención sobre IoT y el crecimiento de las amenazas en dichos informes se expone el crecimiento exponencial de dispositivos IoT. Entre las vulnerabilidades que se mencionan se encuentra la implementación insegura de dispositivos, la falta de actualizaciones de seguridad, falta de enfoque de seguridad en los dispositivos o contraseñas y aspectos no seguros que quedan por defecto.

Para finalizar, parece que aumentan las amenazas que suponen un ataque a la cadena de suministro. Estos ataques afectan a las organizaciones a través de los propios proveedores. Ejemplos de estos ataques pueden ser firmware infectado desde el fabricante, teléfonos móviles con aplicaciones maliciosas por defecto o ataques dirigidos a software empleado por organizaciones como parte de su infraestructura TIC.

TIPOLOGÍA DE INCIDENTES DETECTADOS POR CCN-CERT	Q1 2020	Q2 2020	Q3 2020	Q4 2020
Explotación de vulnerabilidad SW	8100	7619	7780	7544
Inyección SQL	3101	2964	2649	2448
Troyano	2756	2434	1298	1561
Otros	1673	1581	1085	938
Intrusiones	1449	901	862	922
Malware	1392	1799	1294	1122
RFI	749	672	525	556
Identificación de vulnerabilidades	82	71	117	322
Acceso no autorizado a red	121	238	265	290
Spyware	933	630	493	373
DoS/DDoS	1656	234	126	160
Ataque de fuerza bruta	383	278	202	150
RAT	5645	391	147	137
Recopilación de información	1	0	70	125
Acceso a servicios no autorizados	3	14	57	48
Sistema no actualizado	1	0	0	13
Phishing	593	9	8	68
Ransomware	86	46	11	32
Política de seguridad	12	2	3	4
Exfiltración de información	5	7	7	5
Gusano	11	1	2	3
Fraude	1	0	0	0
Rootkit	1	0	0	0

Figura A1-19 Tipologías de incidentes encontrados en 2020 por el CCN [43] (Se observa que la mayor parte de incidentes han sido debido a exploits, ataques web y malware)

3.4.2.1 Valoración de amenazas

Tras el anterior análisis se han seleccionado diez vulnerabilidades. El criterio para su selección ha sido su variedad respecto a tipos de MAGERIT, la probabilidad de acuerdo a los informes de ciberamenazas y su relación con las tecnologías de la ciudad inteligente. También se ha seleccionado la amenaza de nevadas, dado que como se dice en las condiciones de contorno son habituales los últimos años.

Se les ha asignado una probabilidad en este caso en función de la accesibilidad que pueda tener un actor en el ataque, en cuanto al impacto se considera el daño que puede tener un activo medio en el caso de materializarse dicha amenaza.

Nº	Amenaza	Aproximación Magerit	Probabilidad	Impacto
1	Ransomware;	[A.29] Extorsión	MEDIA	ALTO
2	Cryptojacking;	[A.7] Uso no previsto	MEDIA	MEDIO
3	Spearfishing	[A.30] Ingeniería social	MEDIA	MEDIO
4	Robo de información	[A.19] Divulgación de la información	BAJO	MEDIO
5	DDoS	[A.24] Denegación de servicio	MEDIA	ALTA
6	Nevadas	[I.7] Condiciones inadecuadas de temperatura y húmedas	BAJA	MEDIO
7	Campaña de noticias falsas	[E.15] Alteración accidental de la información	BAJA	BAJA
8	Error de configuración	[E.4] Errores de configuración	ALTA	BAJO
9	Covid-19	[E.28] Indisponibilidad del personal	BAJA	MEDIO
10	Inundación	[N.2] Daños por agua	BAJA	ALTO

Tabla 3-29 Amenazas seleccionadas para análisis de riesgos.

3.4.3 Obtención de riesgo

Para terminar el análisis se procede a calcular los riesgos. Para ello se han elaborado las tablas de riesgos siguiendo la metodología. Se pueden encontrar en el Anexo I las utilizadas para el análisis realizado a nivel de servicio.

Un analista de riesgos puede decidir a qué nivel de abstracción es más conveniente llevar a cabo el cálculo de riesgos. Es importante que se realice aplicando la misma metodología en análisis posteriores. De esta forma se puede comparar los resultados entre análisis y ver la progresión en el tiempo. Además, esto no impide bajar el nivel de abstracción en determinados puntos posteriormente.

En el caso práctico se puede observar como los servicios críticos son la sede electrónica y la aplicación de planificación de patrullas. Esto es así debido a su carácter confidencial y en el caso de la sede por ser una aplicación central para todos los trámites y por tanto muy sensible a ataques.

Los ataques más importantes son el ransomware y la denegación de servicio. Probablemente por el efecto que tienen sobre los activos una vez se ejecutan dado que cortan completamente los servicios y por tanto el impacto es alto. Ambos suelen provenir de actores que utilizan internet como medio de acceso.

	Fake news	Robo de información	Nevadas	Covid-19	Error de configuración	Inundación	Cryptojacking	Spearfishing	Ransomware	DDoS
Aplicaciones móviles de información y atención al ciudadano	1	2	2	2	3	3	4	4	6	6
Consumo y Calidad del Agua	2	4	4	4	6	6	8	8	12	12
Control de tráfico	2	4	4	4	6	6	8	8	12	12
Gestión de puntos de recarga de vehículos eléctricos	1	2	2	2	3	3	4	4	6	6
Medición medioambiental: Calidad del aire	1	2	2	2	3	3	4	4	6	6
Monitorización del consumo energético en edificios privados y hogares	1	2	2	2	3	3	4	4	6	6
Página web corporativa	2	4	4	4	6	6	8	8	12	12
Portal de transparencia	1	2	2	2	3	3	4	4	6	6
Recogida de residuos	2	4	4	4	6	6	8	8	12	12
Redes sociales	2	4	4	4	6	6	8	8	12	12
Sede electrónica	3	6	6	6	6	9	12	12	18	18
Seguimiento y actividad de efectivos y brigadas	3	6	6	6	6	9	12	12	18	18

Tabla 3-30 Resultado del análisis de riesgos para estos servicios y amenazas. El mapa de calor oscila entre verde y rojo según la criticidad del riesgo.

Para finalizar el análisis se ha realizado una tabla por cada activo relevante y se han aplicado las amenazas según su probabilidad e impacto. Se utiliza en este caso un mapa de calor entre riesgo cero en verde y máximo en rojo para los diferentes activos.

Además, dado que no todos los activos se ven afectados por las amenazas se ha eliminado el riesgo que puede aparecer entre algunos de ellos. Por ejemplo, la indisponibilidad del personal solo afecta a personal, aunque indirectamente puede provocar vulnerabilidades en otros activos que harán más sencilla la aparición de amenazas.

		Ransomware	**Cryptojacking**	**Spearfishing**	**Robo de información**	**DDoS**	**Nevadas**	**Fake news**	**Error de configuración**	**Covid-19**	**Inundación**
Activos	Tipo	[A.29] Extorsión [A.18] Destrucción de información	[A.7] Uso no previsto	[A.30] Ingeniería social	[A.19] Divulgación de la información	[A.24] Denegación de servicio	[I.7] Condiciones inadecuadas de temperatura y húmedas	[E.15] Alteración accidental de la información	[E.4] Errores de configuración	[E.28] Indisponibilidad del personal	[N.2] Daños por agua
[source1] Código fuente de app Android	[D]										
[source2] Código fuente de app IOS	[D]										
[passwd1] Credenciales de redes sociales	[D]										
[x506-1] Certificado portal Ayto.	[K]										
[x506-2] Certificado sede-e	[K]										
[x506-3] Certificado API apps	[K]										
[x506-4] Certificado API sensores	[K]										
[x506-5] Certificado API sensores electricidad	[K]										
[x506-6] Certificado API sensores tráfico	[K]										
[x506-7] Certificado API sensores carga	[K]										
[pki] Servicio PKI Ayto.	[S]										
[nube1] portal de transparencia	[S]										
[nube2] redes sociales	[S]										
[nube3] Tiendas de Android e IOS	[S]										
[nube4] cuadro de mandos de residuos	[S]										
[internet1] Servicio ISP Ayto.	[S]										
[internet2] Servicio ISP concentradores	[S]										
[internet3] Servicio ISP concentradores electricidad	[S]										
[internet4] Servicio ISP comisaría	[S]										
[internet5] Servicio ISP concentradores tráfico	[S]										

		Ransomware	Cryptojacking	Spearfishing	Robo de información	DDoS	Nevadas	Fake news	Error de configuración	Covid-19	Inundación
[internet6] Servicio ISP puntos de carga	[S]										
[internet7] Servicio ISP estaciones	[S]										
[hypervisor1] Hypervisor CPD Ayto.	[SW]										
[dbms1] Base de datos portal	[SW]										
[dbms2] Base de datos sede-e	[SW]										
[dbms3] Base de datos CRM	[SW]										
[dbms4] Base de datos API apps	[SW]										
[dbms5] Base de datos monitor agua	[SW]										
[dbms6] Base de datos noSQL agua	[SW]										
[dbms7] Base de datos noSQL elect.	[SW]										
[dbms8] Base de datos noSQL tráfico	[SW]										
[dbms9] Base de datos puntos de carga.	[SW]										
[dbms10] Base de datos noSQL contaminación	[SW]										
[dbms11] Base de datos noSQL policía	[SW]										
[www1] Servidor de presentación portal	[SW]										
[www2] Servidor de presentación sede-e	[SW]										
[www3] Servidor de presentación CRM	[SW]										
[www4] Servidor de presentación mon agua	[SW]										
[www5] Servidor de presentación elect.	[SW]										
[www6] Servidor de presentación tráfico	[SW]										
[www7] Servidor de presentación policía	[SW]										
[app1] Servidor de aplicaciones sede-e	[SW]										
[app2] Servidor de aplicaciones CRM	[SW]										
[app3] Servidor de aplicaciones API apps	[SW]										

		Ransomware	Cryptojacking	Spearfishing	Robo de información	DDoS	Nevadas	Fake news	Error de configuración	Covid-19	Inundación
[app4] Servidor de aplicaciones agua	[SW]										
[app5] Servidor de aplicaciones mon agua	[SW]										
[app6] Servidor de aplicaciones elect.	[SW]										
[app7] Servidor de aplicaciones tráfico	[SW]										
[app8] Servidor de aplicaciones puntos de carga.	[SW]										
[app9] Servidor de aplicaciones contaminación.	[SW]										
[app10] Servidor de aplicaciones policía	[SW]										
[host1] Servidores CPD Ayto.	[HW]										
[host2] Servidores CPD comisaría	[HW]										
[network1] Electrónica CPD Ayto.	[HW]										
[network2] Electrónica CPD comisaría	[HW]										
[pc1] Equipos cliente Ayto.	[HW]										
[pc2] Equipos cliente comisaría	[HW]										
[hub] Dispositivo frontera concentradores	[HW]										
[hub2] Dispositivo frontera concentradores elect.	[HW]										
[hub3] Dispositivo frontera concentradores tráfico	[HW]										
[contador] contadores inteligentes	[HW]										
[sensor IoT] sensores de infra agua	[HW]										
[sensor IoT2] sensores de infra tráfico	[HW]										
[sensores IoT3] Sensores puntos carga	[HW]										
[sensores IoT4] Sensores estaciones atmosféricas	[HW]										
[actuador IoT] actuadores de infra agua	[HW]										
[actuador IoT2] actuadores de infra tráfico	[HW]										

		Ransomware	Cryptojacking	Spearfishing	Robo de información	DDoS	Nevadas	Fake news	Error de configuración	Covid-19	Inundación
[lan1] Red Ayto.	[COM]										
[Lan2] Red de área local de agregación disp. IoT agua	[COM]										
[lan3] Red comisaría	[COM]										
[Lan4] Red de área local de agregación disp. IoT tráfico	[COM]										
[PLC] Red PLC hasta concentradores	[COM]										
[site1] CPD del ayuntamiento	[L]										
[site2] CPD de la comisaría	[L]										
[infra1] Infraestructura agua	[L]										
[infra2] Infraestructura eléctrica	[L]										
[infra3] Infraestructura tráfico	[L]										
[infra4] Infraestructura carga	[L]										
[adm1]Administradores Ayto.	[P]										
[adm2]Administradores comisaría	[P]										
[op1] Op. Community manager.	[P]										
[op2] Operadores Ayto.	[P]										
[op3] Operador comisaría	[P]										
[ue1] Usuarios externos	[P]										
[ui1] Usuarios internos – jefatura Ayto.	[P]										
[ui2] Usuarios internos – jefatura comisaría.	[P]										

Tabla 3-31 Mapa de calor de riesgos para activos de la ciudad modelo. (Se puede observar en verde aquellos riesgos bajos y en rojo los altos, se observa que por ejemplo los activos de tipo persona no se ven afectados por muchos tipos de amenazas, en cambio los CPD – e incluimos sistemas comunes de estos – incrementan los suyos).

3.4.4 Resultados

Para el caso particular de la ciudad analizada se puede extraer las siguientes conclusiones.

De la propagación del valor y criticidad de los activos que componen los servicios:

- Los activos más importantes transmiten su criticidad a los sistemas sobre los que se soportan. Esto se ve reflejado en como el valor de riesgo de los dos sitios, el CPD del ayuntamiento y de la comisaría, junto a elementos transversales como la electrónica de red aumentan considerablemente.

- La ciudad inteligente fomenta la participación de diferentes organizaciones y es importante gestionarlas correctamente:

  Eso se puede observar en cómo pueden crecer servicios en otras instituciones del municipio tal y como se refleja en la aplicación de big data a patrullas policiales.

  También en ese sentido se observa un aumento exponencial de conexiones a proveedores de internet para satisfacer las comunicaciones de todos los sensores IoT. En el caso solo suponemos que se contratan servicios de conexión (LTE, LPWAN, etc.).

  Finalmente, en los servicios que se llevan a la nube, aunque se había planificado la dependencia de alguno, como el portal de transparencia, sorprende que para el empleo de otros sistemas aparezcan servicios SaaS como por ejemplo las tiendas de aplicaciones móviles.

- Las aplicaciones suelen dividirse en tres partes, un back-end en el que se procesa la información, un front-end desde el que accede el usuario y una parte novedosa es que ahora se tiene una zona de captación de la información. De entre esas tres, no obstante, la criticidad se sigue acumulando en la zona del back-end.

- Las aplicaciones de big data en ese sentido no cambian mucho a nivel de composición con respecto a sus contrapartidas tradicionales. Aunque sean bases de datos noSQL siguen siendo una fuente de información (crítica o no según su aplicación) y se el proceso de tratamiento no reporta muchas diferencias en términos de seguridad.

De la los riesgos encontrados:

- Pese a la aparición de las redes de dispositivos IoT para la captación de la información, el mayor riesgo se sigue acumulando en aplicaciones de negocio críticas. Un ejemplo de este tipo de riesgo es el que se encuentra en la sede electrónica que puede tener repercusiones legales y que pueden comprometer, en este caso, a la ciudadanía en general.

- Después de estas aplicaciones críticas, y de una manera coherente con los informes y la legislación, se observa que las infraestructuras que afectan a tráfico, canalización de agua y aprovisionamiento de energía tienen una importancia alta para una ciudad y por tanto es recomendable plantear medidas de seguridad.

- Otras aplicaciones, aunque aportan valor añadido no comportan tanto riesgo. En esta categoría podríamos incluir sobre todo las de tipo informativo para el ciudadano: portales de transparencia, información meteorología o de otro tipo sobre la ciudad.

4 CONCLUSIONES Y LÍNEAS FUTURAS

4.1 Conclusiones

Tras la realización de la investigación del concepto de ciudad inteligente, la evolución normativa, las tecnologías empleadas y analizar la seguridad siguiendo el proceso de un análisis de riesgos basado en estándares internacionales se puede extraer lo siguiente:

- Actualmente todavía no se ha llegado a una implantación suficiente, en España, como para decirse que la mayor parte de las ciudades se consideran inteligentes. Esto parece así con los municipios de mayor tamaño, pero no es una línea general.

  Los servicios que las ciudades ofrecen son evoluciones continuistas de otros previos (Portal Web, Sede Electrónica) y además son parte de sistemas que la Administración General del Estado facilita y obliga a usar, como por ejemplo el portal de transparencia.

- Aunque no se hayan implantado muchos servicios de ciudad inteligente, no es necesariamente contraproducente. Del análisis se puede ver que los riesgos TIC de las organizaciones aumentan al acumularse el número de aplicaciones y servicios que se utilizan. Luego es mejor retrasar la implantación para que se pueda llevar a cabo con la seguridad suficiente.

- Pese a que el concepto de ciudad inteligente está muy extendido y hay varios estándares. En lo referente a seguridad de la información e implantación de una arquitectura todavía hay margen de trabajo. Especialmente para establecer un marco para implantar sistemas en el que diferentes entidades puedan participar, es decir, que entidades privadas y públicas puedan coordinar sus aplicaciones TIC dentro de una arquitectura capaz de balancear la seguridad y la funcionalidad.

- Que la irrupción de nuevos servicios que se construyen con nuevas tecnologías ofrece mayor valor, pero conllevan nuevos riesgos. No obstante, en general estos riesgos son similares a los ofrecidos por servicios TIC tradicionales y el valor añadido que se obtiene es superior.

4.1.1 Medidas que se pueden aplicar a una ciudad inteligente.

Tras la realización del análisis de riesgos se pueden aventurar una serie de medidas que reducirían los riesgos y mejorarían la seguridad.

Desde el punto de vista estratégico:

- Tal y como exige el ENS y recoge el estándar ISO 27001 es necesario la elaboración de una política de seguridad que sea apoyada por la Dirección. Esto ofrece una visión de trabajo que engloba a la seguridad y marca un compromiso de la organización con ella.

- El empleo de un punto de vista de seguridad holístico se hace más necesario. Esto significa incluir el punto de vista de seguridad a todos los niveles del ciclo de vida de los sistemas TIC. Es especialmente importante en el diseño de la arquitectura y en la compra o desarrollo de nuevos sistemas.

Desde punto de vista táctico:

- Dado que la ciudad presenta muchos actores, es importante el desarrollo de la política en procedimientos, especialmente los más críticos como los relacionados con la continuidad del negocio.

- Se deben incluir criterios de calidad y seguridad en la compra y puesta en funcionamiento de dispositivos IoT. Tal y como se recoge en los informes del CCN, los ataques a la cadena de suministro están en aumento. Evitar comprar elementos inseguros reducirá incidentes de seguridad en el futuro.

- Establecer principios de seguridad en las relaciones con terceros. Asegurar que los SLAs y acuerdos contractuales con servicios en la nube o con proveedores de servicios públicos incluyen apartados relacionados con la seguridad de la información que satisfagan los requisitos de seguridad de la ciudad.

- Elaborar campañas de concienciación y servicios de soporte a incidentes. Pese a la formación actual, que ya incluye seguridad de la información, los incidentes debido a ingeniería social y correos siguen en aumento. Es necesario seguir concienciando en las organizaciones de la ciudad inteligente y a los ciudadanos que hagan uso de ellas.

Desde el punto de vista técnico y operativo:

- Establecer sistemas de recuperación de la información que contemplen en diferentes ubicaciones los datos y los sistemas. Además, asegurar que parte de estos se almacenan de forma aislada para evitar que se contaminen en caso de que se encuentren con amenazas del tipo ransomware o malware.

- Debido a que muchas de las tecnologías que se emplean se aprovechan de protocolos web y APIs de servicios es recomendable el uso de WAFs y revisión de medidas de seguridad web, como las que se definen en OWASP para garantizar la seguridad de los puntos de entrada. Esto es también válido muchas veces para servicios en la nube.

- Procurar reducir la superficie de exposición de los sistemas de la ciudad unificando sitios sobre los que se gestionan los sistemas TIC. Por el contrario, dentro de cada sitio se segmentan los sistemas en función de sus necesidades para equilibrar las necesidades de seguridad.

- Usar arquitecturas de IoT que permitan que los dispositivos se conecten con un conmutador puede facilitar su protección, reduciendo la ventana de ataque de sujetos que operan mediante internet. La probabilidad de que los ciudadanos o habitantes comprometan los dispositivos es menor que la de que sean fuerzas ajenas a la ciudad como entidades con objetivos políticos, delincuentes y demás.

- Muchas de las principales amenazas se propagan por las redes y áreas de trabajo de los sistemas TIC. Es importante evitar que se puedan utilizar equipos y sistemas sin documentar o ajenos a la visión de los administradores dado que supondría un punto de acceso para este tipo de amenazas.

- El uso de sistemas IoT que sean capaces de actuar sobre infraestructura critica de la ciudad puede considerarse un riesgo. En caso de fallo estos sistemas deben estar pensados para poder seguir

funcionando, aunque se produzca una degradación del servicio. Un ejemplo es la prioridad de la señalética en caso de corte de luz de un semáforo.

- Se deben disponer de sistemas para la actualización de los dispositivos IoT de forma automática. Aunque individualmente no suponen un riesgo alto para la ciudad, las vulnerabilidades de estos dispositivos pueden suponer un riesgo en su conjunto sobre todo si con el paso del tiempo no son actualizados.

- Las campañas de desinformación pueden afectar a los resultados de los análisis de big data. Empleado de forma adecuada es posible que afecten en procesos de la ciudad o en la percepción ciudadana de ellas. Es conveniente detectarlos a tiempo y corregirlos con una respuesta rápida, además es necesario que haya responsables humanos que velen por el correcto resultado de los procesos de análisis.

- En algunas ocasiones puede ser útil utilizar la tecnología *blockchain* aplicada a los dispositivos sensores / actuadores. Dado que pueden necesitar de bases de datos que ayuden para un pequeño análisis que se pueda realizar en los capilares es posible que usar una base de datos distribuida sea una solución. Esto permitiría seguir operando en conjunto en caso de denegación de conexión y caída de la base de datos central.

- Intentar en la medida de lo posible mantener los dispositivos fuera del alcance de los viandantes o que sean de fácil acceso para personal no autorizado. Se pueden utilizar protecciones, vallas, recintos o colocarlos en altura.

- Una ciudad que dependa mucho de los sistemas TIC debe disponer de un sitio de respaldo. Valorar el uso de un sistema híbrido de nube y propietario puede ser útil

4.1.1 Aplicación particular en ciudades.

En este proyecto se ha centrado en enumerar servicios transversales que pueden encontrarse de forma genérica en otras ciudades, especialmente aquellas españolas. Sin embargo, cada ciudad tiene diferentes particularidades y a la hora de revisar los riesgos un analista debe tener en cuenta esas características. Por ejemplo:

- La ciudad del ejemplo es religiosa. El servicio de aplicaciones móviles podría haberse usado informar a los turistas del movimiento de los tronos durante las celebraciones de Semana Santa. Está claro que aporta un valor añadido a los creyentes que la deseen disfrutar y los turistas, pero también introduce nuevos riesgos. Los datos de carácter religioso están protegidos especialmente en la ley de protección de datos, si dicha aplicación almacenase esos datos al registrar un usuario podría incurrir en un incumplimiento legal.

- La relación cultural y la localización afectan mucho a la ciudad. Las ciudades cambian los materiales y estilos arquitectónicos, las celebraciones y las formas, hasta los sistemas políticos. Por ejemplo, en el norte de Europa tienden a tener sitios de reciclaje para el depósito de basura por cada comunidad y esta se recoge una vez a la semana. En países del sur el calor obliga a acelerar el tiempo de recogida y suele ser diario con puntos mucho más dispersos a lo largo de la ciudad. Estas variaciones afectan a las dimensiones de seguridad y al efecto que tienen posibles amenazas sobre los sistemas.

- El tamaño de las ciudades es otro factor importante. Ciudades como Tokio, Ciudad de México o Nueva York son ciudades enormes que probablemente necesiten muchos más sistemas y más complejos que una ciudad media. Los sistemas TIC en ese sentido aportan más valor porque permiten servicios que de otra forma no se podría, como por ejemplo la logística del transporte público. Pero al igual que con el caso anterior estos servicios pasarían a ser cada vez más críticos y por tanto se deberían extremar las medidas de protección sobre estos.

  En este caso, cuando se tienen tantos servicios y el sistema se complica demasiado es conveniente segmentar a niveles funcionales y probablemente tener instalaciones dedicadas entre sectores relacionados. Por ejemplo: un sitio con sistemas relacionados con el transporte, otro con sistemas de gestión administrativa y legal, etc. Siempre de forma racional y con una visión clara de cómo orquestarlos. Como ventaja unos centros pueden hacer de respaldo a otros y el riesgo acumulativo se reduce.

4.1.1 Cobertura de objetivos

Creo que el propósito general de ofrecer un análisis y obtener resultados a través del marco de gestión de riesgos propuestos se ha conseguido.

Se podrían haber obtenido resultados más detallados sobre riesgos de haber empleado una herramienta como PILAR. No obstante, su uso parece que tiene más sentido al estudiar un caso de uso real, donde un análisis de cientos de amenazas y activos ofrece puntos de riesgos interesantes por su carácter desconocido. En un caso teórico parece que el proceso manual de analizar los activos, entender su relación con las amenazas, las dependencias de unos activos con otros y con los servicios que proporcionan es más útil para extraer conclusiones.

De los puntos concretos propuestos creo que se han cumplido los siguientes tras este proyecto:

- Se entiende el concepto ciudad y de ciudad inteligente.
- Se comprende a alto nivel las tecnologías empleadas en los servicios de una ciudad inteligente.
- Se conocen los ámbitos y servicios principales de una ciudad inteligente, se tienen razones para ponderar estos servicios en función de su importancia.
- Se han analizado varios servicios, desestructurado en activos y sometido a su valoración en función de su criticidad.
- Se ha realizado un estudio del estado de las ciberamenazas en general y aplicadas a las tecnologías de la ciudad inteligente en particular.
- Se han propuesto el estudio de algunas amenazas y ponderado su posible daño a los servicios escogidos, se ha extraído el valor de los riesgos en función de esto.
- Se han podido establecer medidas de seguridad y extraer conclusiones en virtud de dicho análisis.

4.2 Líneas futuras

A raíz de este proyecto se puede continuar en las siguientes líneas:

- Revisión de los estándares arquitectónicos de IoT y de la ciudad inteligente. Desarrollarlos para apoyar la estandarización de sistemas sobre la ciudad inteligente. Mucha documentación argumenta sobre lo que se conoce como CityOS, pero no parece haber una arquitectura clara.

- Se puede realizar un análisis de riesgos a un nivel de detalle mayor. Por ejemplo, utilizando una ciudad como sujeto y analizando a fondo los activos y riesgos de una forma similar a la empleada, o utilizar una herramienta como PILAR para analizar cientos de activos y extraer más información acerca de los riesgos de la ciudad.

- Investigar en profundidad alguno de los servicios correspondientes a la ciudad inteligente mencionados en el trabajo. Verificar sus vulnerabilidades y proponer mejoras respecto a la seguridad de la información o simplemente al funcionamiento de estos.

5 BIBLIOGRAFÍA

[1] «Real Academia Española,» [En línea]. Available: https://dle.rae.es/ciudad. [Último acceso: 15 Enero 2022].

[2] R. B. Casado y S. S. Carretón, «Banco de imagenes y sonidos INTEF,» [En línea]. Available: http://recursostic.educacion.es/bancoimagenes/web/. [Último acceso: 15 Enero 2022].

[3] R. Rallo, «Foundation Ontology for the City Anatomy,» City Protocol Society, 2016.

[4] «elSectorPublico,» [En línea]. Available: https://www.elsectorpublico.es/elsp/capitulo/1687752/1662143/i-las-entidades-locales.html. [Último acceso: 15 1 2022].

[5] Ayto de Pozuelo, «Ayuntamiento de pozuelo de alarcón.,» [En línea]. Available: https://www.pozuelodealarcon.org/tu-ayuntamiento/normativa/normativa-general/legislacion-basica-del-estado-en-el-ambito-de-la-de-la-administracion-local. [Último acceso: 5 1 2022].

[6] AENOR, «UNE 178201 Ciudades inteligentes. Definición atributos y requisitos,» AENOR, Madrid, 2016.

[7] S. L. Fernández, «Uso del big data en empresas eléctricas,,» Universidad de cantabria, 2013.

[8] A. J. G. García, «IoT. Dispositivos, tecnologías de transporte y aplicaciones,» Universidad oberta de Cataluña, 2017.

[9] F. Nack, «An Overview on Wireless Sensor Networks,» Universidad de Berlin.

[10] L. D. C. HERNANDEZ, «Desarrollo en un modelo de trafico de un ared domótica basada en PLC,» Universidad Pontificia Bolivariana, 2018.

[11] D. J. Cancho y C. S. Aparicio, «Redes LPWA para IoT,» Centro Universitario para la Defensa, 2021.

[12] D. J. Cancho y C. S. Aparicio, «Redes LPWA para IoT - Trabajo TEL1,» Universidad de Vigo, 2021.

[13] G. Vos, «What is LPWA for the Internet of Things?,» Sierra Wireless, 1 mayo 2020. [En línea]. Available: https://www.sierrawireless.com/iot-blog/what-is-lpwa-for-iot/.

[14] I. d. e. RFID, «Amazon,» [En línea]. Available: https://www.amazon.es/UHF-RFID-Tag-Set-5/dp/B06XG9HNRR. [Último acceso: 2022].

[15] N. F. Garcia, «Apuntes asignatura almacenamiento y gestión de la información,» 2021.

[16] Y. Liu, C. Yang, L. Jiang y S. Xie, «Intelligent Edge Computing for IoT-Based Energy Management in Smart Cities,» 2019. [En línea]. Available: https://www.researchgate.net/publication/331951759_Intelligent_Edge_Computing_for_IoT-Based_Energy_Management_in_Smart_Cities.

[17] AENOR, «La clave de seguridad y privacidad para sus sistemas de información,» AENOR, [En línea]. Available: https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion. [Último acceso: 3 01 2022].

[18] AENOR, «UNE-ISO/IEC 27001,» AENOR, 2014.

[19] MinHAP, «MAGERIT versión 3,» inisterio de Hacienda y Administraciones Públicas, 2012.

[20] Gobierno de España, «Real Decreto 3/2010 Esquema Nacional de Seguridad,» 2010.

[21] ONTSI, «Estudio y Guía metodológica sobre Ciudades Inteligentes,» Ministerio de Industria Energia y Turismo, 2015.

[22] Grupo de Interplataformas de Ciudades Inteligentes, «Smart Cities Documento de Visión a 2030,» CIRCE, 2015.

[23] ITU T Foucs group, «Cybersecurity, data protection and cyber resilience in smart sustainable cities,» ITU, 2015.

[24] Ministry of Internal Affiars and Communications of Japan, "Smart City Security Guideline," 2020.

[25] MINHAFP, «Centro de transferencia tecnológica - portal para entidades locales,» [En línea]. Available: https://administracionelectronica.gob.es/ctt/portaleell.

[26] Centro de Transferencia tecnologica, «Acceso de los ciudadanos a los expedientes de la administración,» [En línea]. Available: https://administracionelectronica.gob.es/ctt/acceda/descargas.

[27] D. c. p. d. transparencia, «Centro de transferencia tecnoloógica,» [En línea]. Available: https://administracionelectronica.gob.es/ctt/transparencia/descargas.

[28] Suite CRM, «Suite CRM Installation Guide,» 2020. [En línea]. Available: https://docs.suitecrm.com/admin/installation-guide/downloading-installing/.

[29] SAlesForce, «SalesForce CRM,» 2021. [En línea]. Available: https://www.salesforce.com/es/campaign/sem/sales-cloud/?d=7013y000002K2NZAA0&dcmp=ES&ef_id=CjwKCAiA5t-OBhByEiwAhR-hm_Dv7hANgOy3GflODdtTkKvtGnAxRjB44XscqaRf0xloZ45JVNCiGBoCgMQQAvD_BwE:G:s&s_kwcid=AL!7501!3!527646427613!p!!g!!sales%20crm&mkwid=s&pcrid=52764.

[30] W. Ejaz, M. Naeem, A. Shahid, A. Anpalagan y M. Jo, «Efficient Energy Management for the Internet of Things in Smart Cities,» IEEE Communications Magazine, 2017.

[31] Distromel, «Medio Ambiente,» [En línea]. Available: https://www.distromel.com/medio-ambiente/. [Último acceso: 01 2022].

[32] esmartcity.es, «Sistema de sensores para la gestión del tráfico en ciudades,» [En línea]. Available: https://ip21ingenieria.com/blog/sistema-de-sensores-para-la-gestion-del-trafico-en-ciudades/.

[33] Sociedad Ibérica de Construcciones Eléctricas, S.A., «SISTEMA DE CONTROL DEL TRÁFICO URBANO - ADIMOT,» Diciembre 2016. [En línea]. Available: https://www.sice.com/sites/Sice/files/2016-12/TU_ADIMOT.pdf.

[34] Ayuntamiento de Madrid, «Sistema Integral de Calidad de Arie Madrid,» 2022. [En línea]. Available: http://www.mambiente.munimadrid.es/opencms/calaire/SistemaIntegral/concepto.html.

[35] C. V. Quilon, «Estaciones smart de monitorización de la calidad del aire,» 2019. [En línea]. Available: https://www.esmartcity.es/comunicaciones/comunicacion-estaciones-smart-monitorizacion-calidad-aire.

[36] J. Hochstetler, L. Hochstetler y S. Fu, «n Optimal Police Patrol Planning Strategy for Smart City Safety,» IEEE Xplore, 2016.

[37] Z. A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, N. Syed and M. Peacock, "Future challenges for smart cities: Cyber-security and digital forensics," Elsevier, 2017.

[38] S. Ijaz, M. A. Shah, A. Kha and M. Ahmed, "Smart Cities: A Survey on Security Concerns," *International Journal of Advanced Computer Science and Applications,* vol. 7, no. 2, pp. 612 - 625, 2016.

[39] B. Hamid, N. Jhanjhi, M. Humayun, A. Khan and A. Alsayat, "Cyber Security Issues and Challenges for Smart Cities: A survey," IEEE, 2019.

[40] A. AlDairi and L. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies Technologies," Elsevier, 2017.

[41] ENISA, «Big Data Threat Landscape and Good Practice Guide,» 2016.

[42] ENISA, «ENISA THREAT LANDSCAPE 2021,» 2021.

[43] CCN-CERT, «Ciber amenazas y tendencias,» 2021.

[44] Grupo Interplataformas de Ciudades Inteligentes, «Smart Cities documento de visión a 2030,» CIRCE, 2015.

[45] M. Vitunskaite, Y. He, T. Brandstetter and H. Janicke, "Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership," Elsevier, 2019.

[46] H. Habibzadeha, B. H. Nussbaumb, F. Anjomshoac, B. Kantarcid and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical T system deployments in smart citie," Elsevier, 2019.

[47] NIST, «Guidelines for Smart Grid Cybersecurity,» 2014.

[48] S. Rhee, "2019 Global City Teams Challenge: Smart and Secure Cities and Communities Challenge Expo," NIST, 2019.

[49] D. C. LÉVY-BENCHETON y M. E. DARRA, «Cyber security for Smart Cities: An architecture model for public transport,» 2015.

[50] N. Robinson, V. Horvath, J. Cave, A. P. Roosendaal and M. Klaver, "Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts," 2013.

[51] ISO IEC, "Privacy protection — Privacy guidelines for smart cities," ISO, Geneva, 2021.

[52] K. Biswas y V. Muthukkumarasamy, «Securing Smart Cities Using Blockchain Technology,» IEEE, 2016.

ANEXO I: TABLAS DE ANÁLISIS DE RIESGOS

Probabilidad Amenaza	3	3	6 Error de configuración	9	6	12	18	9	18	27
	2	2	4	6	4	8 Cryptojacking Spearfishing	12	6	12 Ransomware DDoS	18
	1	1	2 Fake news	3	2	4 robo de información Nevadas Covid-19	6	3	6 Inundación	9
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-1 Tabla de análisis de riesgos para Página web corporativa.

Probabilidad Amenaza	3	3	6	9 Error de configuración	6	12	18	9	18	27	
	2	2	4	6 Error de configuración	4	8	12 Cryptojacking Spearfishing	6	12	18 Ransomware DDoS	
	1	1	2	3 Fake news	2	4	6 robo de información Nevadas Covid-19	3	6	9 Inundación	
Valor del activo		1	2	3	1	2	3	1	2	3	
Impacto de la amenaza		1			2			3			

Tabla 0-2 Tabla de análisis de riesgos Sede electrónica.

Probabilidad Amenaza	3	3 Error de configuración	6	9	6	12	18	9	18	27
	2	2	4	6	4 Cryptojacking Spearfishing	8	12	6 Ransomware DDoS	12	18
	1	1 Fake news	2	3	2 robo de información Nevadas Covid-19	4	6	3 Inundación	6	
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-3 Tabla de análisis de riesgos Portal de transparencia.

Probabilidad Amenaza	3	3	6 Error de configuración	9	6	12	18	9	18	27
	2	2	4	6	4	8 Cryptojacking Spearfishing	12	6	12 Ransomware DDoS	18
	1	1	2 Fake news	3	2	4 robo de información Nevadas Covid-19	6	3	6 Inundación	9
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-4 Tabla de análisis de riesgos. Redes sociales.

Probabilidad Amenaza	3	3 Error de configuración	6	9	6	12	18	9	18	27
	2	2	4	6	4 Cryptojacking Spearfishing	8	12	6 Ransomware DDoS	12	18
	1	1 Fake news	2	3	2 robo de información Nevadas Covid-19	4	6	3 Inundación	6	
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-5 Tabla de análisis de riesgos. Aplicaciones móviles de información y atención al ciudadano

Probabilidad Amenaza	3	3	6 Error de configuración	9	6	12	18	9	18	27
	2	2	4	6	4	8 Cryptojacking Spearfishing	12	6	12 Ransomware DDoS	18
	1	1	2 Fake news	3	2	4 robo de información Nevadas Covid-19	6	3	6 Inundación	9
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-6 Tabla de análisis de riesgos Consumo y Calidad del Agua.

Probabilidad Amenaza	3	3 Error de configuración	6	9	6	12	18	9	18	27
	2	2	4	6	4 Cryptojacking Spearfishing	8	12	6 Ransomware DDoS	12	18
	1	1 Fake news	2	3	2 robo de información Nevadas Covid-19	4	6	3 Inundación	6	
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-7 Tabla de análisis de riesgos Monitorización del consumo energético en edificios privados y hogares.

Probabilidad Amenaza	3	3	6 Error de configuración	9	6	12	18	9	18	27
	2	2	4	6	4	8 Cryptojacking Spearfishing	12	6	12 Ransomware DDoS	18
	1	1	2 Fake news	3	2	4 robo de información Nevadas Covid-19	6	3	6 Inundación	9
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-8 Tabla de análisis de riesgos Recogida de residuos.

Probabilidad Amenaza	3	3	6 Error de configuración	9	6	12	18	9	18	27
	2	2	4	6	4	8 Cryptojacking Spearfishing	12	6	12 Ransomware DDoS	18
	1	1	2 Fake news	3	2	4 robo de información Nevadas Covid-19	6	3	6 Inundación	9
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-9 Tabla de análisis de riesgos Control de tráfico.

Probabilidad Amenaza	3	3 Error de configuración	6	9	6	12	18	9	18	27
	2	2	4	6	4 Cryptojacking Spearfishing	8	12	6 Ransomware DDoS	12	18
	1	1 Fake news	2	3	2 robo de información Nevadas Covid-19	4	6	3 Inundación	6	
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-10 Tabla de análisis de riesgos Gestión de puntos de recarga de vehículos eléctricos.

Probabilidad Amenaza	3	3 Error de configuración	6	9	6	12	18	9	18	27
	2	2	4	6	4 Cryptojacking Spearfishing	8	12	6 Ransomware DDoS	12	18
	1	1 Fake news	2	3	2 robo de información Nevadas Covid-19	4	6	3 Inundación	6	
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-11 Tabla de análisis de riesgos Medición medioambiental Calidad del aire.

Probabilidad Amenaza	3	3	6	9 Error de configuración	6	12	18	9	18	27
	2	2	4	6 Error de configuración	4	8	12 Cryptojacking Spearfishing	6	12	18 Ransomware DDoS
	1	1	2	3 Fake news	2	4	6 robo de información Nevadas Covid-19	3	6	9 Inundación
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 0-12 Tabla de análisis de riesgos Seguimiento y actividad de efectivos y brigadas.

ANEXO II: LÍNEAS DE INNOVACIÓN EN LA SSC

CODIFICACIÓN	ELEMENTO	AREA	LÍNEA DE APLICACIÓN	FAMILIA	TECNOLOGÍA O FUNCIÓN	IMPORTANCIA PARA LA CIUDAD	PLAZO	OBSERVACIONES
F.1	Automatización de red Eléctrica	Energía y Medio Ambiente	Gestión redes energéticas	Redes Eléctricas	Función	Alta	Corto	El incremento de la automatización de la red en las ciudades permite mejorar la calidad de servicio.
F.8	Tics para Smart Gris	Energía y Medio Ambiente	Gestión redes energéticas	Redes Eléctricas	Tecnología	Alta	Corto	La necesidad de monitorizar y controlar la red de una forma más precisa necesita del despliegue de la red de comunicaciones paralela a la red eléctrica y de la creación de sistemas de gestión de la red próxima al cliente (media y baja tensión). Este mayor control mejora la calidad de servicio.
FE.3	Aprovechamiento de los excedentes de energía ferroviaria	Energía y Medio Ambiente; Movilidad e intermodal dad	Recursos energéticos; Sistemas inteligentes de transporte ITS en el entorno urbano	Recuperación de Energía; ITS para transporte ferroviario	Función	Alta	Corto	El desarrollo de sistemas adecuados que permitan aprovechar excedentes de energía en el sistema ferroviario para el traspase a otros modos permite la utilización de vehículos no contaminantes, que mejoraría la calidad de vida.
BI.1	Climatización de distrito con biomasa	Energía y Medio Ambiente	Gestión redes energéticas	Redes Térmicas	Función	Alta	Corto	La climatización mediante el uso de biomasa sustituyendo a los combustibles tradicionales es una gran apuesta de futuro en las ciudades, ya que permite reducir las emisiones de CO2 y supone un ahorro para el consumidor respecto a otros combustibles, además de ayudar a alcanzar los objetivos de sostenibilidad para 2020 y fermentar el uso de materias primas autóctonas. Por su parte, la climatización de distrito o destrice hosting and colín es un modelo más eficiente con las mismas ventajas ambientales y económicas, que proporcionan la energía al usuario directamente, evitándole la necesidad de manipular y almacenar combustibles. Además, pueden abarcar desde un limitado número de viviendas hasta zonas metropolitanas completas. Las redes urbanas de climatización están ya muy extendidas en el Centro y Norte de Europa y se consideran una gestión eficiente clave en las ciudades.
BI.3	Biocombustibles para transporte	Movilidad e intermodalidad	Vehículos en el entorno urbano	Vehículos Menos Contaminantes	Función	Alta	Corto	El uso de biocombustibles para el transporte urbano permite crear un parque móvil más sostenible, que reduce las emisiones de gases de efecto invernadero a la atmósfera que produce el tráfico rodado en las ciudades y ayuda a alcanzar los objetivos europeos de sostenibilidad de 2020, además de fomentar la utilización de recursos autóctonos. Los biocombustibles son una medida eficaz para disminuir la contaminación ambiental tan acusada que sufren las ciudades hoy en día.
BI.4	Valorización energética de residuos	Energía y Medio Ambiente	Recursos energéticos	Recuperación de Energía	Función	Alta	Corto	La valorización energética de residuos es una medida que aporta soluciones a dos problemas: permite reducir el volumen de los residuos en las ciudades y crear energía a partir de esta fuente de biomasa. Esta solución ya se lleva a cabo en los países del centro de Europa, donde se produce un doble impacto en la ciudad: gestión de residuos y generación de energía térmica limpia para los barrios próximos a las centrales. Por otra parte, se puede producir biogás apto completamente para introducir en la red nacional de gas.
GE.1	District Heating and cooling con geothermic	Energía y Medio Ambiente	Gestión redes energéticas	Redes Térmicas	Función	Alta	Corto	La climatización mediante geotermia no genera impacto visual (sin chimeneas ni unidades externas) ni sonoro, permite reducir las emisiones de CO2 drásticamente y supone un ahorro para el consumidor respecto a otros combustibles tradicionales, entre otros beneficios. Es un modelo eficiente y gestionable (disponible 365 días las 24 h) de climatización que permitiría a las ciudades disminuir su dependencia energética y sus altos niveles de polución. La climatización de distrito o destrice hosting and colín es un modelo con las mismas ventajas, considerado clave para la gestión eficiente de la energía en las ciudades, al aportar energía a varios edificios y viviendas desde un solo foco de generación.

CODIFICACIÓN	ELEMENTO	AREA	LÍNEA DE APLICACIÓN	FAMILIA	TECNOLOGÍA O FUNCIÓN	IMPORTANCIA PARA LA CIUDAD	PLAZO	OBSERVACIONES
GE.2	Climatización de edificios (sector domestico y terciario) con geotermia	Edificios e infraestructuras	Edificación sostenible	Integración de Renovables en Edificios	Función	Alta	Corto	La climatización mediante geotermia no genera impacto visual (sin chimeneas ni unidades externas) ni sonoro, permite reducir las emisiones de CO2 drásticamente y supone un ahorro para el consumidor respecto a otros combustibles tradicionales, entre otros beneficios. Es un modelo eficiente y gestionable (disponible 365 días las 24 h) de climatización que permitiría a las ciudades disminuir su dependencia energética y sus altos niveles de polución.
GE.3	Uso de energía eléctrica renovable en las ciudades	Energía y Medio Ambiente	Recursos energéticos	Integración de Energías Renovables y Generación Distribuida	Función	Alta	Corto	Las ciudades son los grandes sumideros de energía por excelencia. Un aprovechamiento de la electricidad generada a partir de recursos renovables contribuiría de manera notable a la reducción de las emisiones y de la dependencia energética, además de utilizar recursos inagotables y autóctonos que favorecerían la actividad socioeconómica de la región. Existen tecnologías renovables con un modelo de generación completamente gestionable, las cuales jugarán un papel importante en la estabilización de la red de las ciudades.
FO.1	Redes de comunicaciones / fibra óptica	Horizontal	TICs	Redes de Comunicación	Tecnología	Alta	Corto	Fotónica integrada, interconexiones ópticas, redes de comunicación ultrarrápidas e incremento de ancho de banda para facilitar accesibilidad a servicios relacionados con salud (teleasistencia, etc.), seguridad y otros. Disminución de consumo en centros de datos.
FO.3	Sistemas de medición y depuración de aguas	Energía y Medio Ambiente	Medio Ambiente	Tecnologías para el Reciclado y el Tratamiento de Agua	Tecnología	Alta	Corto	Los sistemas fotónicos para medición de parámetros de calidad en aguas pueden permitir un control continuo de su calidad. Además, las técnicas de depuración de aguas emplean habitualmente la irradiación UV empleando lámparas convencionales de descarga de gran consumo energético, que pueden llegar a ser sustituidas por fuentes de mayor eficacia.
FO.4	Sistemas de medida de calidad del aire	Energía y Medio Ambiente	Medio Ambiente	Indicadores y Sensores Medioambientales	Tecnología	Alta	Corto	Sistemas de monitorización calidad del aire en entornos urbanos (medida de contaminación atmosférica, detección sustancias contaminantes, medición de parámetros NRBQ).
FO.9	Alumbrado y señalización luminosa	Edificios e infraestructuras	Gestión de elementos urbanos; Edificación sostenible	Alumbrado Inteligente; Nuevas Tecnologías de Construcción	Tecnología	Alta	Corto	Alumbrado público y privado (nuevas fuentes de luz, sistemas de control y regulación, etc.). Utilización de sistemas híbridos para iluminación (luz natural + artificial).Señalización luminosa vial y señalización vertical (tráfico, publicitaria, etc.).
C.2	Gestión seguridad	Edificios e infraestructuras	Gestión de elementos urbanos	Gestión de la Infraestructura Viaria y Ferroviaria	Tecnología	Alta	Corto	Carreteras monitorizadas que capturen y trasmitan información sobre su estado y aporten información para su mantenimiento preventivo y el aseguramiento físico de su perímetro.
PL.5	Gestión de la sostenibilidad	Gobierno y servicios sociales	Administración	Gestión de la Sostenibilidad	Función	Alta	Corto	Sistemas de auto sostenibilidad de las ciudades monitorizando, evaluando y tomando decisiones sobre los parámetros básicos de la ciudad.

CODIFICACIÓN	ELEMENTO	AREA	LÍNEA DE APLICACIÓN	FAMILIA	TECNOLOGÍA O FUNCIÓN	IMPORTANCIA PARA LA CIUDAD	PLAZO	OBSERVACIONES
PL.6	Tecnologías y Sistemas de Sensorización	Horizontal	Sensores	sistemas de Detección, Medición y Monitorización Basados en Sensores	Tecnología	Alta	Corto	Redes de sensores inalámbricas; Monitorización parámetros físicos y ambientales; Domótica e Inmotica; Smartphones; Eficiencia energética (generación, distribución, consumo): Smart Grid, Smart metering; Medicina (telediagnostico/ambient assisted living, Point of Care diagnostic systems...); Medicina (Caídas, Análisis del andar, ECG, etc.); Urbano: Contaminación lumínica, gestión de residuos, medición de ruidos; Medición de plazas de parking libres; Transporte: Localización de vehículos; Trazabilidad: RFIDs Pasivos y activos (Tags inteligentes).
TH.4	DMS *Destination Management System / Advanced*	Gobierno y servicios sociales	Promoción urbana	Conexión Ciudadano Servicios ; Sistemas de Gestión de Turismo Inteligente	Función	Alta	Corto	Sistemas concebidos para aumentar la eficiencia y eficacia en la gestión diaria de las tareas, productos, recursos y servicios que engloban las ciudades.
TH.6	Sistemas de gestión de residuos	Energía y Medio Ambiente	Medio ambiente	Gestión Sostenible de los Residuos	Función	Alta	Corto	Sistemas orientados al desarrollo e implantación de: Mejora del control y seguimiento de los residuos mediante el empleo de TICs. Control y seguimiento de la contaminación. Aprovechamientos para las sustancias contaminantes presentes en los residuos.
TH.7	Transporte sostenible	Movilidad e intermodalidad	Sistemas inteligentes de trasporte – ITS en el entorno urbano	ITS para transporte Urbano	Tecnología	Alta	Corto	Desarrollo y aplicación de las tecnologías y de los sistemas inteligentes de transporte (ITS) a los vehículos y a la gestión de las flotas, de las infraestructuras y de la demanda (movilidad)
A.2	Almacenamiento de Agua	Energía y Medio Ambiente	Medio Ambiente	Tecnologías para el Reciclado y el Tratamiento de Agua	Tecnología	Alta	Corto	Diferencias en coste de agua y evolución del precio (impacto socioeconómico) riesgos / gastos derivados. almacenamiento local como garante del suministro: – Captación y almacenamiento de agua en depósitos sobre y bajo el edificio. – Reutilización agua de lluvia para limpieza, baldeo, sanitarios...
A.3	Elementos Urbanos	Edificios e infraestructuras	Infraestructuras viarias	Pavimentos más Sostenibles	Función	Alta	Corto	Diseño y selección de pavimentos para reducir impactos: – Aumentar la capacidad de infiltración bajo las ciudades – Reducir el impacto "efecto isla de calor" Conocer el comportamiento de cada pavimento (material) y elegirlo en base a condicionantes: – El comportamiento de permeabilidad y ralentización de escorrentía es un valor de relevancia para el comportamiento de superficies urbanas (inundaciones). – El comportamiento térmico del pavimento afecta al ambiente urbano (isla de calor). – La climatología y el tipo de terreno son factores fundamentales en la fase de diseño y elección de pavimentos.
A.4	Pavimentos	Edificios e infraestructuras	Infraestructuras viarias	Pavimentos más Sostenibles	Función	Alta	Corto	Mayor creación de zonas permeables en la ciudad mayor presencia de sistemas urbanos de drenaje sostenible (SUDS) diseños de elementos urbanos básicos de mayor funcionalidad: alcorques, rotondas, cunetones…

CODIFICACIÓN	ELEMENTO	AREA	LÍNEA DE APLICACIÓN	FAMILIA	TECNOLOGÍA O FUNCIÓN	IMPORTANCIA PARA LA CIUDAD	PLAZO	OBSERVACIONES
PESI.5	Monitorización y gestión de las infraestructuras, redes y equipamientos de la Ciudad	Horizontal	Seguridad	seguridad y Fiabilidad de Infraestructuras Urbanas y Equipamientos	Función; Tecnología	Alta	Corto	Las infraestructuras de la Ciudad están conformadas por una colección de activos físicos en (vías comunicaciones, redes de suministro agua, saneamiento, gas, electricidad, etc.) y los equipamientos y sistemas que los controlan. Estos activos pueden ser de propiedad pública o privada y son los Operadores de los mismos (mayoritariamente privados —propietarios o concesionarios—) los responsables del servicio que prestan. Se precisan sistemas de gestión avanzados de los mismos que aseguren su fiabilidad, disponibilidad, mantenimiento y seguridad (RAMS), incluyendo la seguridad estructural y la gestión del envejecimiento de los mismos. Estos sistemas tendrán un importante componente tecnológico (sensórica, monitorización, simulación, inteligencia artificial, inspección, nuevos materiales, etc.)
PESI.9	Ciberseguridad de Sistemas de control Industrial de Redes y sistemas esenciales	Horizontal	Seguridad	Ciberseguridad	Tecnología	Alta	Corto	Los sistemas de control y automatización industrial de los sistemas y redes de suministro (energía, agua...) y ciertos servicios esenciales de la Ciudad (alumbrado, tráfico,) son especialmente vulnerables a ciber-ataques en la medida que se apoyan en redes públicas de telecomunicaciones (trasmisión de datos y ordenes de actuación). Por ello su protección lógica debe de ser asegurada al máximo a través de estrategias y herramientas de ciberseguridad especificas para estos sistemas.
MT.2	Materiales de Altas Prestaciones	Horizontal	Materiales	Materiales Avanzados	Función	Alta	Corto	Materiales en los que algunas de sus características o propiedades lo hacen adecuado para su uso bajo condiciones o necesidades extraordinarias.

Tabla 0-1 Tabla resumen de líneas de investigación de importancia alta con implantación en cinco años [23].