SOLUCIÓN PARA GARANTIZAR LA PRIVACIDAD EN INTERNET DE LAS COSAS

José-Antonio Sánchez-Alcón, Lourdes López-Santidrián y José-Fernán Martínez

José-Antonio Sánchez-Alcón es doctorando en ingeniería de sistemas y servicios accesibles para la sociedad de la información en la *Universidad Politécnica de Madrid* (*UPM*), licenciado en documentación en la especialidad de gestión de recursos de información por la *Universidad Oberta de Catalunya*, posgrado en dirección general por la misma universidad, e ingeniero técnico de telecomunicación en radiocomunicación por la *UPM*. Ha trabajado como consultor de procesos operativos, proyectos de mejoras *6-Sigma, Lean* y auditorías de calidad para *Telefónica de España*.
http://orcid.org/0000-0002-3673-2735

jose.asanchez-alcon@upm.es

Lourdes López-Santidrián es doctora en informática por la *Universidad Politécnica de Madrid* y licenciada en ciencias matemáticas en la especialidad de computación por la *Universidad Complutense de Madrid*. Es catedrática en la *Escuela Técnica Superior de Ingeniería de Sistemas de Telecomunicación*, secretaria del *Centro de Investigación en Tecnologías de Software y Sistemas Multimedia para la Sostenibilidad* (*Citsem*) e investigadora responsable del *Grupo de Redes y Servicios de Próxima Generación* (*GRyS*).
http://orcid.org/0000-0002-6049-1257

lourdes.lopez@upm.es

José-Fernán Martínez es doctor ingeniero de telecomunicaciones por la *Universidad Politécnica de Madrid*, ingeniero en electrónica y telecomunicaciones por la *Universidad del Cauca* (*Ucauca*, Colombia), y profesor titular en la *Universidad Politécnica de Madrid*. Es investigador responsable de varios proyectos europeos de los programas *Avanza*, *Artemis* y *FP VII* en el *Grupo de Redes y Servicios de Próxima Generación* (*GRyS*) en el centro *Citsem*.
http://orcid.org/0000-0002-2642-3904

jf.martinez@upm.es

Citsem (*Centro de Investigación en Tecnologías de Software y Sistemas Multimedia para la Sostenibilidad*)
Edificio Tecnológico la Arboleda. *Etsi de Telecomunicación*
Campus Sur *UPM*. Ctra. Valencia, Km 7. 28031 Madrid, España

Resumen

Los nuevos productos y servicios de "internet de las cosas" nos harán más eficientes, con mayor capacidad de actuación y comprensión del entorno, habrá nuevas ayudas técnicas que permitirán prolongar nuestra vida activa y más. Sin embargo coexistiremos con una gran cantidad de dispositivos que recopilarán información sobre nuestra actividad, costumbres, preferencias, etc., que podrían amenazar nuestra privacidad. La desconfianza podría ser una barrera para el desarrollo pleno de estos nuevos productos y servicios. Se aporta una posible solución para la garantizar la seguridad y privacidad de los datos personales en internet de las cosas, mediante técnicas que resulten de la colaboración entre las áreas empresarial, legislativa y tecnológica para dar confianza a los actores involucrados.

Palabras clave

Internet de las cosas; Red inalámbrica de sensores; Seguridad; Servicios de seguridad; Privacidad; Protección de datos personales; Monitorización; Matriz de utilidad.

Title: Solution to ensure privacy in the internet of things

Abstract

New products and services offered by the "internet of things" will make us more efficient, more able to understand our environment and take action, and new assistive technologies will allow us to extend our working lives. Nonetheless, we will coexist with a large number of devices collecting information about our activities, habits, preferences, etc. This situation could threaten our privacy. Distrust could be a barrier to the full development of these new products and services. This article offers a possible solution to ensure security and privacy for personal data on the internet of things, using techniques that result from a collaboration between the business, legislative and technological areas and are designed to build trust with all stakeholders.

Artículo recibido el 08-05-2014
Aceptación definitiva: 26-12-2014

Keywords

Internet of things; Wireless sensor network; Security; Security services; Privacy; Personal data protection; Monitoring; Utility matrix.

Sánchez-Alcón, José-Antonio; **López-Santidrián, Lourdes**; **Martínez, José-Fernán** (2015). "Solución para garantizar la privacidad en internet de las cosas". *El profesional de la información*, v. 24, n. 1, enero-febrero, pp. 62-70.

http://dx.doi.org/10.3145/epi.2015.ene.08

1. Introducción

La evolución de internet hacia un intercambio inteligente de información entre objetos (**García-Mexía**, 2013), posibilita la creación una nueva gama de productos y servicios en el mundo real y en el virtual. Se espera que el aumento de las interconexiones entre dispositivos, en su mayoría inalámbricas, genere una gran cantidad de información. Serán necesarias nuevas arquitecturas de red con la suficiente capacidad e inmunes a la ruptura de la seguridad y a la invasión de la privacidad de las personas. Por lo tanto hay que elaborar mecanismos que proporcionen entornos seguros y fiables, que eviten la percepción de los usuarios de que la utilización de estos servicios les hace vulnerables ante personas u organizaciones oportunistas que obtengan beneficio vulnerando la privacidad.

Una gran parte de los servicios de la denominada "internet de las cosas" se proporcionan mediante redes inalámbricas de sensores, en adelante *WSN* (*wireless sensor network*). Los objetos que se interconectan son dispositivos con sensores llamados nodos o motas, que tienen la misión de recopilar información del entorno y transmitirla hacia una estación base donde se almacena y analiza (**Rodríguez-Molina** *et al.*, 2014). Las *WSN* (figura 1) se utilizan en entornos industriales, ambientales, domótica, aplicaciones militares, etc. (**Fernández-Martínez** *et al*., 2009).

Pueden coexistir varias *WSN* especializadas en la prestación de un servicio concreto, supervisando simultáneamente el mismo entorno y proporcionando así una visión más completa de la zona (tráfico de vehículos, parámetros ambientales, e-salud, vigilancia, etc.). Las *WSN* pueden ser de diferentes tecnologías, tipos de conexiones y actores involucrados. Los servicios se pueden prestar de forma aislada o conjunta, como es el caso de las ciudades inteligentes. *http://ec.europa.eu/eip/smartcities*

Toda la información recopilada sobre las personas podría ser tratada y utilizada por terceros para segmentarla en perfiles de conductas, preferencias y hábitos para obtener beneficio.

> La percepción de los usuarios de que su privacidad está en riesgo puede ser una barrera para el despliegue masivo de los productos y servicios de internet de las cosas

Este trabajo se centra en la seguridad y privacidad ante las vulnerabilidades técnicas propias de las *WSN* (**Ukil**, 2010; **Al-Ameen**; **Liu**; **Kwak**, 2012). No tratamos otros aspectos como seguridad de los servidores, antivirus, copias de seguridad, etc. Por "política de seguridad" nos referiremos al conjunto de servicios y mecanismos de seguridad que actúan sobre los elementos que necesitan ser protegidos, según la *Recomendación X.800 de la ITU sobre la seguridad en las redes de comunicación de datos* (*UIT*, 1991).

La *Recomendación* considera que los elementos a proteger son las informaciones y los datos (incluidos los relativos a las medidas de seguridad, como las contraseñas), los servicios de comunicación y procesamiento de datos, los equipos y las instalaciones. Para hacer frente a las vulnerabilidades y a los ataques se debe disponer de un nivel de seguridad y pri-

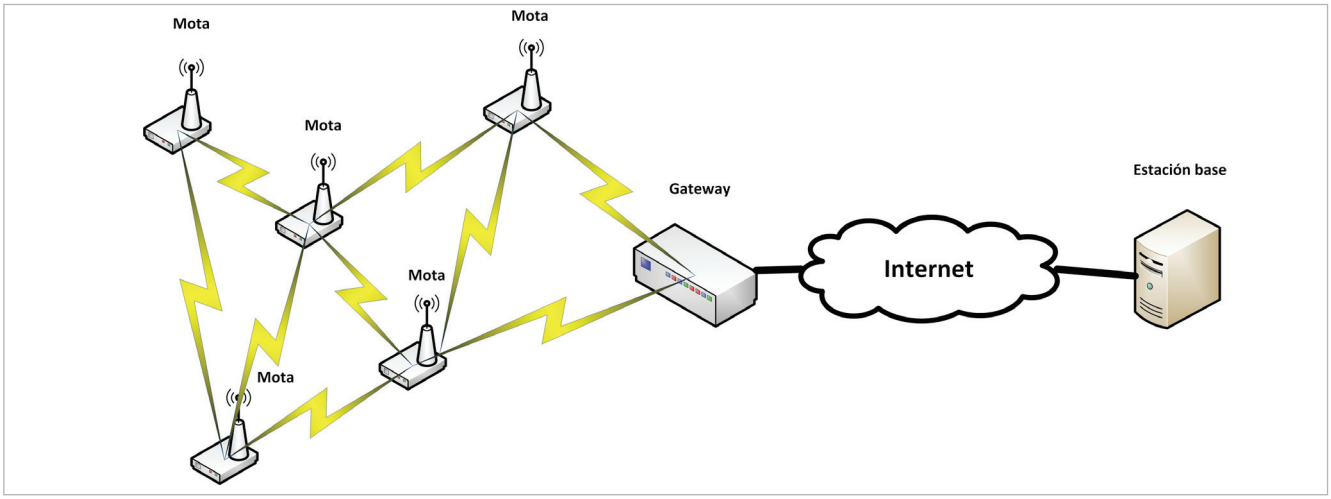

Figura 1. Red inalámbrica de sensores

vacidad acorde al servicio que presta cada red de sensores y de la información involucrada en el servicio final prestado (**Gupta**; **Verma**; **Sangal**, 2013), ya sea por las *WSN* individualmente, o en sentido holístico para todo el servicio final conjunto. Este nivel de seguridad se materializa mediante servicios de seguridad obtenidos mediante un conjunto de mecanismos y contramedidas capaces de contrarrestar los ataques o amenazas sobre los elementos que se deban proteger. La *Recomendación X.800* define los siguientes servicios de seguridad:

- autenticación: para identificar la entidad comunicante y la fuente de datos;
- control de acceso: para prevenir el uso no autorizado de los recursos;
- confidencialidad de los datos: para protegerlos contra la revelación no autorizada;
- integridad de los datos: para garantizar que no han sido alterados o destruidos de una manera no autorizada;
- no repudio: para dar prueba del origen de los datos o de entrega de los mismos;
- disponibilidad: para garantizar la continuidad de la accesibilidad y utilización por las entidades autorizadas.

Estos servicios se proporcionan mediante unos mecanismos de seguridad solos o combinados, como:

- cifrado;
- firma digital;
- mecanismos para el control del acceso;
- mecanismos de integridad de datos;
- intercambio de autenticación;
- relleno de tráfico;
- control de encaminamiento;
- notarización.

Para aprovechar al máximo los recursos de las *WSN* se utilizan protocolos de bajo consumo y procesamiento ligero. En este sentido, también hay que prevenir los ataques cuyo objetivo no es vulnerar la privacidad sino sobrecargar los nodos y provocar consumo extra (**Palafox-Maestre**; **García-Macías**, 2008). Se debe hacer un diseño a medida del caso para obtener la cobertura de seguridad y privacidad necesaria, sin perjudicar a la calidad del servicio final que se ofrece.

2. Estado del arte

Los niveles de seguridad y privacidad sobre los elementos que deben protegerse dependen de los imperativos impuestos por el marco legal al que se encuentre sometido el servicio final.

En el ámbito europeo el *Convenio del Consejo de la Unión Europea n. 108*, Estrasburgo 28/1/1981 (*Council of Europe Treaty Office*, 1981), 5 ratificaciones 1/10/1985, estableció unos criterios comunes de protección de los datos para todos los miembros de la *CE*, coordinado por la *Directiva 95/46/CE* del *Parlamento Europeo* de 24/10/1995 (*Unión Europea*, 1995).

En su informe sobre la *Directiva de protección de datos* de 24/02/2004 (*Parlamento Europeo*, 2004), la *UE* reconoce la heterogeneidad legislativa de sus países miembros y enfatiza la necesidad de que los estados e instituciones europeas adopten un nivel equivalente de protección de los derechos de las personas. Resalta que esta heterogeneidad de las legislaciones nacionales sobre protección de datos dificulta el desarrollo del mercado interior europeo. Como resultado de las líneas de actuación establecidas por el *Parlamento Europeo* en la *Comunicación* del *Comité Económico y Social Europeo* (2009), Europa camina hacia un marco normativo común con la *Propuesta de reglamento general de protección de datos* (*Comisión Europea*, 2012). Una vez aprobado será de aplicación directa en dos años para toda la Unión Europea. Este *Reglamento* afectará a quienes hagan tratamiento de datos de carácter personal y tengan establecimiento en algún estado miembro, aun si el tratamiento de la información se realiza fuera de la Unión Europea. A las empresas no establecidas en Europa les afectará en caso de que traten datos personales para prestar bienes y servicios a residentes en la UE. El *Reglamento* incluye los conceptos de responsabilidad, privacidad por diseño (o desde el diseño), privacidad por omisión, evaluación del impacto sobre privacidad, necesidad de implantar unos criterios de gobierno interno y operativos enfocados a la gestión de riesgos, así como el derecho al olvido.

> “Los niveles de seguridad y privacidad los impone el marco legal que afecta al servicio final que se ofrece”

El grupo de trabajo *Working Party 29* (*WP29*) ha aprobado el primer dictamen conjunto sobre internet de las cosas, el *Dictamen 8/2014 sobre los nuevos desarrollos en la internet de las cosas* de 16/09/2014 (*European Commission*, 2014), cuya elaboración ha sido liderada por la *Agencia Española de Protección de Datos* (*AEPD*) junto con la autoridad francesa *Commission nationale de l’informatique et des libertés* (*CNIL*). Se analizan tres escenarios:

- ”tecnología para llevar puesta” o “informática vestible” (*wearable computing*);
- dispositivos que registran información sobre la actividad de las personas;
- domótica.

Identifica y alerta de los riesgos que estos productos y servicios pueden plantear para la privacidad de las personas, definiendo responsabilidades y ofreciendo recomendaciones. El documento destaca que aunque los objetos recopilen piezas aisladas de información de diferentes fuentes, su análisis conjunto puede revelar patrones de la vida de las personas. El 10 de octubre de 2014 se editó la *Recomendación* (*Comisión Europea*, 2014), relativa al “*Modelo de evaluación del impacto sobre protección de datos para redes inteligentes y sistemas de contador inteligente*”. En su 5º considerando, señala que estos sistemas presagian el futuro internet de las cosas, generalizando así esta idea metodológica.

El *Reglamento general de protección de datos* (*Comisión Europea*, 2012) homogenizará la legislación europea en materia de protección de datos personales, aunque en un mercado de cobertura mundial será necesario convivir aún

con la heterogeneidad legislativa.

En el ámbito tecnológico hay numerosos trabajos como los de **Dener** (2014), **Fatema** y **Brad** (2014), **Maw** *et al.* (2014), **Kumari** y **Shukla** (2013), **Shukla** y **Kumari** (2013), **Malik** (2012), **Kuthadi**, **Rajendra** y **Rajalakshmi** (2010), **Karlof** y **Wagner** (2003) y otros, que han elaborado mecanismos de seguridad eficientes para las *WSN*, y para evitar poner en riesgo la calidad del servicio por excesivo consumo de recursos. Las empresas y suministradores de equipos y redes son muy activos ideando servicios para la sociedad y aumentando su catálogo comercial.

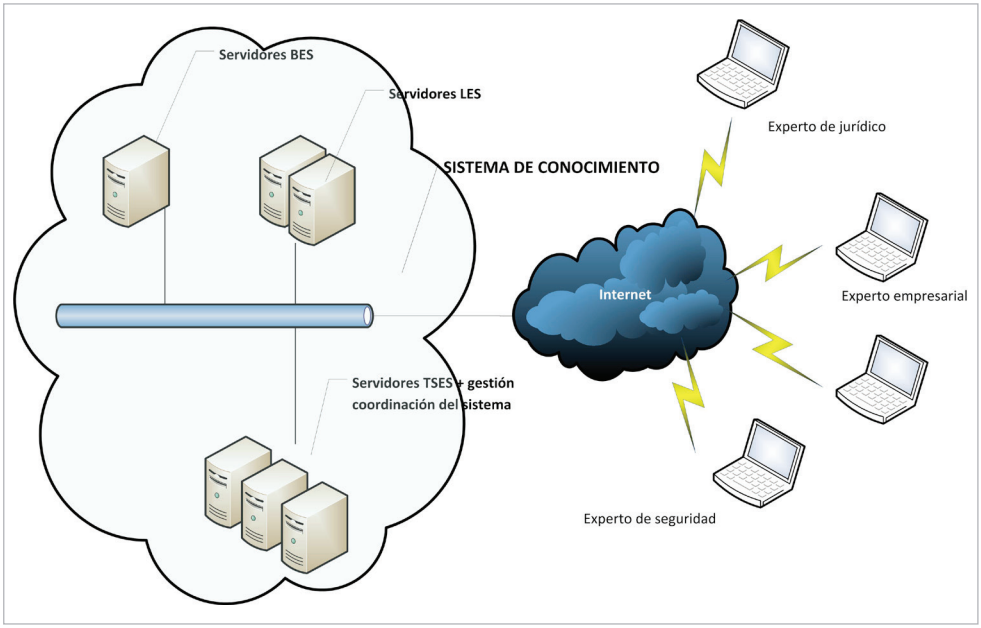

Figura 2. Entorno colaborativo entre los expertos de las tres áreas de conocimiento BES (*business expert system*); LES (*legal expert system*); TSES (*technological solutions expert system*)

Existe aún otra complicación adicional: los dispositivos, productos y servicios de internet de las cosas suelen ser susceptibles de usos diversos y de utilidades alternativas, en entornos y modalidades de utilización que pueden ser muy variadas, y podrían escapar al control de los fabricantes, de los distribuidores, de los proveedores de servicios y quizá también de los reguladores o legisladores. Una seguridad orientada únicamente a los dispositivos, productos o servicios podría ser incompleta e incluso inútil si no se tiene en cuenta su modo de utilización. Si cambia la forma de utilizar el servicio, podría cambiar el marco legislativo que le afecte y por lo tanto el usuario podría quedar desprotegido. Para las empresas las sanciones y los posibles deterioros de la imagen de marca podrían provocar unos costes importantes e incluso hacer ruinoso el desarrollo de estos nuevos productos y servicios. Esta situación requeriría buscar soluciones y habilitar una gestión robusta y garante para todos los agentes involucrados.

3. Propuesta sobre seguridad y protección de datos personales

Nuestra propuesta reúne el conocimiento sobre seguridad y privacidad generado para internet de las cosas por las áreas jurídica, tecnológica y empresarial, en un sistema informático capaz de canalizar la colaboración entre dichas áreas. La finalidad es seleccionar de forma automática las políticas de seguridad y privacidad que deben aplicarse a los nuevos productos y servicios. La colaboración entre esas tres áreas, posibilitaría la emisión de certificaciones de confianza para las partes interesadas y eliminar las posibles barreras de desconfianza.

En este entorno colaborativo (figura 2):

- las empresas dedicadas al diseño de nuevos productos y servicios pueden realizar simulaciones virtuales previas a la toma de decisiones sobre el mercado real;
- en el ámbito legislativo se evalúa el impacto en la sociedad y en el mercado de las posibles modificaciones y nuevas legislaciones en esta materia, pudiendo conocer cómo y en qué medida afectarían a los productos y servicios existentes y sus futuras evoluciones;
- las áreas tecnológicas pueden conocer rápidamente los aspectos críticos que necesiten de nuevas investigaciones e innovaciones.

> La colaboración entre las áreas jurídicas, tecnológicas y empresariales posibilita la emisión de certificaciones de confianza

Para realizar ensayos completos se ha diseñado una maqueta para probar las posibilidades de automatización desde la decisión de la política de seguridad hasta la configuración del funcionamiento de los elementos de la *WSN*. Estos ensayos han sido realizados en el equipo *GRyS* (*Grupo de Redes y Servicios de Próxima Generación*) del *Citsem* (*Centro de Investigación en Tecnologías de Software y Sistemas Multimedia para la Sostenibilidad*) de la *UPM* (*Universidad Politécnica de Madrid*).

4. Maqueta de pruebas del sistema de selección automática de soluciones de seguridad y protección de datos personales

La maqueta de diseño y pruebas (figura 3) se compone de una *WSN*, de una plataforma *middleware* orientada a servicios, *Proyecto Aware* (**Santos-Familiar**; **Martínez-Ortega**; **López**, 2012), y del sistema experto *PDPS-IOT* (*personal data protection system – internet of things*) (**Sánchez-Alcón** *et al.*, 2013).

El sistema experto *PDPS-IOT* decide la política de seguridad y privacidad que se ha de aplicar al servicio (objeto de este artículo), la cual se comunica a la plataforma *Aware*, que conoce bien a las *WSN* a las que se conecta (su tecnología, la

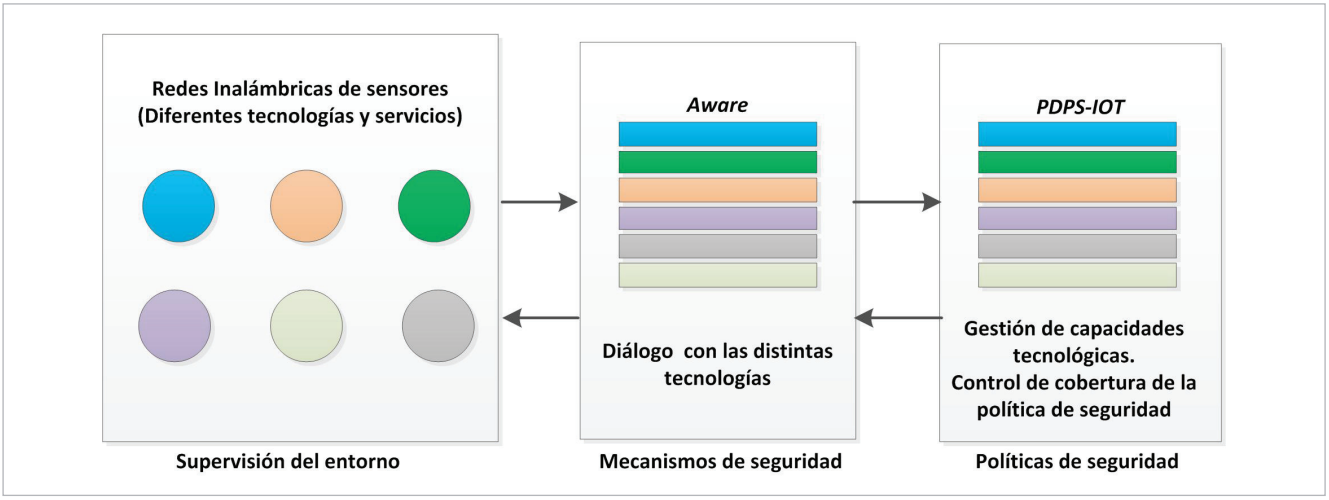

Figura 3. Maqueta de diseño

forma en que debe dialogar con ellas, sus posibilidades, los mecanismos de seguridad que soportan) gestionando sus posibilidades de configuración. Genera los comandos y acciones para configurarlas remotamente haciendo uso de su *middleware*. *PDPS-IOT* conoce el conjunto de mecanismos de seguridad que *Aware* es capaz de gestionar, con lo que se puede establecer un nivel de seguridad homogéneo para todas las redes *WSN*.

El servicio final utilizado para las pruebas monitoriza la salud recopilando datos de pulso y temperatura corporal. Estos datos se procesan y se envían a la estación base para informar a un equipo médico. Este servicio final involucra datos de salud de las personas, protegidos en España por el *Real decreto 1720/2007*, de 21/12/2007, *sobre protección de datos de carácter personal*, y en Europa por *Reglamento general de protección de datos*. Mediante el sistema experto *PDPS-IOT* (figura 4), que tiene como entrada las especificaciones del servicio, se obtiene como salida la política de seguridad y privacidad (nivel de seguridad) que debe tener el servicio.

Esto es posible gracias a que se ha formalizado la información relevante en lo que llamamos matriz de utilidad, a partir de la cual se obtiene el marco legislativo que afecta al servicio. Lo que se busca es obtener los imperativos de seguridad y privacidad que han de actuar sobre los elementos de información que deben ser protegidos. Estos imperativos se transformarán en un conjunto de servicios y mecanismos de seguridad y privacidad. Ante un cambio en el uso o una reutilización de una *WSN* para proporcionar otro servicio, o el mismo servicio en otro ámbito, tras comunicarlo a los gestores y actualizar debidamente la matriz de utilidad se genera el proceso que culmina con la reconfiguración remota de la seguridad en la *WSN*, si fuera necesario.

La tabla 1 muestra el procesamiento básico y las bases de conocimiento afectadas. La idea se ha inspirado en los sistemas

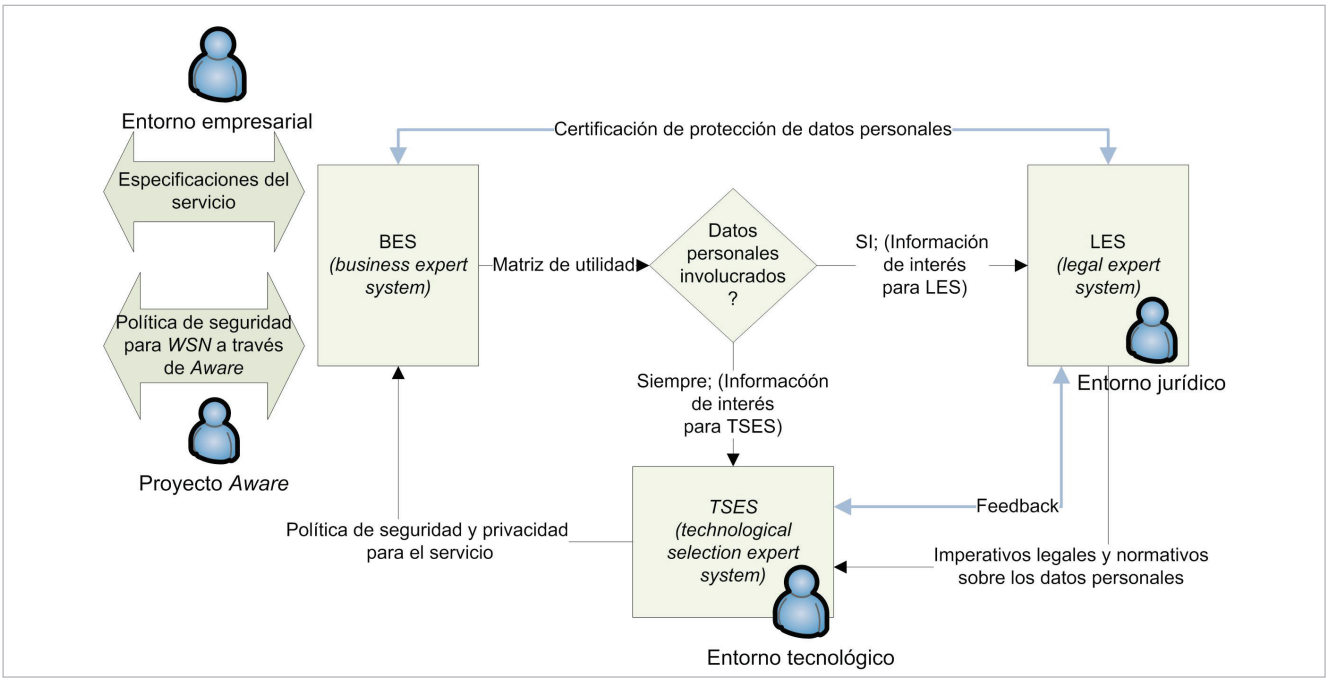

Figura 4. Sistema de protección de datos personales para servicios de internet de las cosas (*PSPS-IOT*). BES (*business expert system*); LES (*legal expert system*); TSES (*technological solutions expert system*)

Tabla 1. Etapas de procesamiento

Etapas de procesamiento e información involucrada		
Entrada	**Base de conocimiento**	**Salida**
1. Requisitos del servicio	Empresarial. Sobre el servicio	2. Matriz de utilidad (MU) y datos involucrados
2. MU y datos involucrados	Jurídico, aspectos legales	3. Imperativos legales; datos a proteger
3. Imperativos legales; datos a proteger	Tecnológico, ataques, servicios y mecanismos de seguridad	4. Servicios y mecanismos de seguridad; datos sensibles
4. Servicios y mecanismos de seguridad; datos sensibles.	Empresarial. Sobre variables críticas de negocio	5. Decisión final
5. Decisión final	Control de validez (ámbito jurídico)	6. Certificación 7. Registro y comunicación

expertos jurídicos (**Cuadrado-Gamarra**, 2004). La cooperación entre los bloques funcionales BES, LES y TSES, se establece mediante la transferencia de información y resultados.

A continuación se describen las partes fundamentales de este procesamiento.

> La información relevante del servicio final se formaliza en la matriz de utilidad, para posibilitar la selección automática de los mecanismos de seguridad y privacidad

4.1. Matriz de utilidad

Se confecciona en BES partiendo de los requisitos del servicio final y de la información que gestiona. El usuario aporta esta información mediante formularios, y de forma guiada. La matriz de utilidad consta de dos partes:

- La primera parte contiene información sobre el tipo de servicio final, el país, el promotor y los usuarios, si monitoriza a personas, animales o cosas, las características de las personas sometidas a monitorización (niños, adultos, mayores, su capacidad legal, sus necesidades especiales, etc.). Con esta información y con los datos involucrados en el servicio (algunos de ellos pueden ser datos personales) se realiza un procesamiento en LES para obtener los imperativos legales que deben actuar sobre la información que debe protegerse.
- La segunda contiene información sobre el tipo de *WSN*, de los recursos de los nodos sensores, de la estación base, así como de los tipos de conexión y comunicación que se utilizan, la topología de la red, el tipo de encaminamiento, señalización, sincronismo, y si se requiere continuidad del servicio o no, así como el nivel de criticidad del servicio (crítico para las personas, para las infraestructuras, etc.), estos datos los necesita TSES para obtener las posibles vulnerabilidades del servicio.

4.2. Base de conocimientos jurídicos

No almacena leyes sino el conocimiento de los expertos del área para obtener los imperativos legales y aplicarlos a los datos personales del servicio final. El marco legal se selecciona con la información que se extrae de la matriz de utilidad (tipo de servicio, país, tipo de entorno, monitorizados, la necesidad de continuidad y la criticidad del servicio). De este marco legal seleccionado se extraen los imperativos legales.

Cada imperativo legal se identifica por el concepto que representa:

- veracidad de los actores;
- autorización del acceso;
- revelación o divulgación de la información;
- veracidad del contenido;
- responsabilidad de los actores;
- disponibilidad y continuidad del servicio.

Los datos que pueden necesitar protección son los que identifican a personas concretas, relacionan a la persona con sus datos recopilados, procesados o históricos, eventos completos que identifiquen el estado o situación de la persona, etc.

4.3. Base de conocimientos tecnológicos

Establece una relación conceptual directa entre los imperativos legales obtenidos de LES y los servicios de seguridad de la *Recomendación X.800* en TSES (tabla 2).

Los ataques dirigidos contra el servicio final se afrontan mediante los servicios de seguridad, que se concretan en contramedidas o mecanismos de seguridad. La base de conocimiento relaciona éstos con los ataques. El resultado buscado es un conjunto de mecanismos y contramedidas para alcanzar el nivel de seguridad que se necesita. En caso de que el sistema no pueda encontrar solución para todos los requisitos de seguridad y privacidad, se lanza un aviso de insuficiencia de conocimiento, indicando el problema encontrado.

Para nuestras pruebas nos ajustamos a los mecanismos de la tabla 3, que forman parte de la propuesta genérica de seguridad para *WSN*, *SensoTrust* (**Castillejo** *et al.*, 2014), propuesta que se aplicó a la plataforma *Aware*.

Tabla 2. Relación entre imperativos, servicios de seguridad y tipos de ataques

Imperativos	Servicios de seguridad	Ataques más habituales
Veracidad de los actores	Autenticidad	Suplantación, usurpación de identidad (o impostura)
Autorización de acceso	Control de acceso	
Revelación / divulgación	Privacidad	Obtención de contenidos, análisis de tráfico
Veracidad del contenido	Integridad	Modificación, repetición
Continuidad de servicio	Disponibilidad	Interrupción, negación de servicio

Tabla 3. Relación entre mecanismos disponibles para las pruebas

Ataque	Ataque contra	Impacto	Mecanismo / Contramedida
Denegación de servicio (DoS)	Disponibilidad	Impide la comunicación: -Por interferencias. -Un nodo malicioso envía paquetes para confundir a la red.	**Alarma DoS** En ambas situaciones, se activa una "alarma DoS" para alertar al personal de seguridad de la situación.
		Desconexión de la red.	Nodo da alarmas audible y lumínica
Ataque *Sybil*[1]	Autenticidad	Invalida la información de los nodos legítimos y modifica el enrutamiento. -Se produce cuando un nodo malicioso presenta numerosas ID (identidades) a la red.	**ID de nodo, revocación de nodo** El nodo reinicia el mecanismo de confianza. Sólo el gestor de seguridad de la *WSN* tiene la lista completa de las ID. Puede revocar o apartar el nodo.
Corrupción de los mensajes	Integridad	El mensaje que llega al receptor es diferente del enviado por la fuente. Interceptado / modificado.	***Hash*** Funcionalidad de cifrado para realizar un *hash* del mensaje (con MD5, SHA1, etc.).
***Eavesdropping*[2] (escucha)**	Privacidad	En la transmisión por radio, otros dispositivos pueden escuchar e interceptar la comunicación entre nodos.	***Keys* (*symmetric* y *PKI*)** Se utilizan capacidades de cifrado simétrico y *PKI*.
Captura de nodos	Privacidad	Algún nodo es capturado y alguien accede a las claves secretas, ID de nodo, etc.	***Few crypto. Data stored*** Minimizar en el nodo la información criptográfica y de seguridad que se almacena. Renovar las claves en la red.
Réplica de un nodo	Autenticidad, Control de acceso (CA)	Un ID es copiado en un nuevo nodo, se introduce en la red y es aceptado con el ID clonado como un nodo autorizado.	**ID de nodo, *security policies*** 1. El ID del nodo, almacenaje externo en el gestor de seguridad, que controla los ID en la red. 2. Si el gestor de seguridad detecta dos nodos operando con el mismo ID, emite un protocolo de revocación del nodo y lo expulsa de la red.
Nodo falso	Autenticidad, Control de acceso, Integridad	Inyecta datos en la red para evitar la comunicación entre nodos legítimos mensajes falsos, petición continua de autorización…	**ID de nodo, *domain keys*** Identificar el nodo falso y, mediante la renovación de la clave de dominio, descartar todos los mensajes enviados por él.

5. Discusión de los resultados

Se han utilizado los casos de uso planteados en **Sánchez-Alcón** *et al.* (2013), donde se usa exactamente el mismo equipamiento técnico para proporcionar el mismo servicio final (un cinturón pectoral con sensores para vigilar, registrar y generar alertas sobre el estado de salud), pero utilizados en diferentes casos de uso, para monitorizar la salud de:

- vacas lecheras en una granja;
- caballos de carreras;
- un equipo de fútbol;
- un grupo de bomberos en sus actuaciones.

Se ha aplicado el *RD 1720/2007*, y el borrador del *Reglamento general de protección de datos* de la Unión Europea.

Los aspectos fundamentales del razonamiento son:

Caso 1. Granja lechera

Servicio propio para controlar la salud del ganado. No involucra datos personales. La información recopilada no es útil para nadie más. No es un servicio crítico (no suple a los controles alimentarios) y no tiene requisitos especiales de continuidad. El acceso al sistema se hace por usuario y contraseña sin mecanismo adicional.

Caso 2. Caballos de carreras

Servicio propio para controlar la salud y rendimiento de los caballos. No involucra datos personales. El impacto de un posible espionaje de resultados podría ocasionar fraude en las apuestas. Protegemos el servicio contra: revelación/divulgación, veracidad de los actores y autorización del acceso. No es un servicio crítico, y no tiene requisitos especiales de continuidad.

Caso 3. Equipo de fútbol

Servicio propio para controlar la salud de los jugadores. Hay datos personales (salud) protegidos por ley ante revelación/divulgación (ocultar todo, o separar la identidad de la persona de sus medidas). Estos datos deben ser gestionados y manejados sólo por personal autorizado: veracidad de los actores y autorización del acceso. Se exige veracidad de los contenidos, según la ley los datos personales deben ser veraces (suponemos que los sensores están calibrados). Es un servicio que no es crítico y sin requisitos especiales de continuidad.

Caso 4. Equipo de bomberos

Servicio que debe ser homologado para controlar la salud de los bomberos y posibles víctimas. Hay datos personales (salud) protegidos por ley ante revelación/divulgación (ocultar todo, o separar la identidad de la persona de sus medidas). Estos datos deben ser gestionados y manejados sólo por personal autorizado: veracidad de los actores y autorización del acceso. Se exige veracidad de los contenidos, según la ley los datos personales deben ser veraces (suponemos que los sensores están calibrados). El servicio es crítico y necesita continuidad del servicio (llevan sensores en su equipamiento para que el equipo médico controle el estado de salud de los bomberos y de los posibles rescatados). En caso de desconexión de la red, los sensores deben poder seguir siendo operativos funcionando en modo autónomo y generando alarmas audibles–visibles ante problemas de salud.

La cobertura de seguridad puede cumplirse para los cuatro casos con los mecanismos disponibles que la *WSN* puede utilizar y la plataforma *Aware* puede configurar.

Tabla 4. Comparativa de los niveles de seguridad para cada caso de uso

	Autenticidad	Control de acceso	Privacidad	Integridad	Disponibilidad
Granja lechera	-	-	-	-	-
Caballos de carreras	X	X	X	-	-
Equipo de fútbol	X	X	X	X	-
Equipo de bomberos	X	X	X	X	X

6. Conclusiones

Mediante la colaboración entre las áreas empresarial, jurídica y tecnológica se puede ofrecer a los usuarios la confianza necesaria sobre la seguridad y la protección de sus datos personales. En internet de las cosas, la limitación de los recursos en las redes inalámbricas de sensores hace necesario el establecimiento de una seguridad a medida que evite poner en riesgo la calidad del servicio por agotamiento de recursos. En general donde coexistan varios servicios y varias tecnologías, la inteligencia y la toma de decisiones sobre las políticas de seguridad pueden integrarse en centros de operaciones de red debidamente certificados y reconocidos. Esto proporciona gran capacidad de gestión y control de cambios para mantener y actualizar remotamente la seguridad a medida para los productos y servicios de internet de las cosas.

> Se establece la cobertura de seguridad y privacidad a medida del caso de uso, para utilizar los mecanismos estrictamente necesarios y optimizar el consumo de recursos

La evolución prevista del sistema pasa por extender la cobertura de seguridad para afrontar la mayoría de los casos, pudiendo incluso aconsejar procedimientos para abordar la seguridad y privacidad en un sentido más amplio que el tratado en este artículo.

Notas

1. Ataque *Sybil*. El atacante introduce uno o varios nodos maliciosos en la red que suplantan identidades para influir en el comportamiento seguro de dicha red y alterar, por ejemplo, el encaminamiento de la información. El nombre se tomó del libro *Sybil*, un estudio de caso de una mujer diagnosticada con trastorno de identidad disociativa.

2. *Eavesdropping*. Escucha secreta de conversaciones o comunicaciones. El nombre proviene de la escucha bajo los aleros (*eaves*) cerca de las casas.

> La inteligencia y la toma de decisiones sobre las políticas de seguridad podrían integrarse en centros de operaciones de red debidamente certificados y reconocidos

Agradecimientos

El proyecto *Aware* ha sido parcialmente financiado por el *Ministerio de Economía y Competitividad* (Ref. TEC2011-28397). Nuestro agradecimiento al *Citsem* (*Centro de Investigación en Tecnologías de Software y Sistemas Multimedia para la Sostenibilidad*) de la *UPM* (*Universidad Politécnica de Madrid*) y en particular al equipo *GRyS* (*Grupo de Redes y Servicios de Próxima Generación*) por poner a nuestra disposición los recursos necesarios.

7. Bibliografía

Al-Ameen, Moshaddique; **Liu, Jingwei**; **Kwak, Kyungsup** (2012). "Security and privacy issues in wireless sensor networks for healthcare applications". *Journal of medical systems*, v. 36, n. 1, pp. 93-101.
http://dx.doi.org/10.1007/s10916-010-9449-4

Castillejo, Pedro; **Martínez-Ortega, José-Fernán**; **López, Lourdes**; **Sánchez-Alcón, José-Antonio** (2014). "SensoTrust: trustworthy domains in wireless sensor networks". *International journal of distributed sensor networks*, article ID 484820, in press.
http://www.hindawi.com/journals/ijdsn/aip/484820

Comisión Europea (2012). *Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)*, n. 2012/0011/COD, 25/01/2012.
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012PC0011&qid=1420389265736

Comisión Europea (2014). "Recomendación de la *Comisión* de 10 de octubre de 2014 relativa al modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente". *Diario oficial*, n. L 300, 18/10/2014, pp. 63-68.
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014H0724&qid=1420390252490

Comité Económico y Social Europeo (2009). "Dictamen sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Internet de los objetos - Un plan de acción para Europa [COM(2009) 278 final]". *Diario oficial*, n. C 255, 22/09/2010, pp. 116-120
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52009AE1951&qid=1420395947268

Council of Europe Treaty Office (1981). *Convention for the protection of individuals with regard to automatic processing of personal data*, n. CETS 108, Strasbourg, 28/1/1981, pp. 1-10.
http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Cuadrado-Gamarra, Nuria (2004). *Aplicación de los sistemas expertos al campo del derecho*. Madrid: Facultad de Derecho, Universidad Complutense de Madrid, ISBN: 84 8481 042 9

Dener, Murat (2014). "Security analysis in wireless sensor networks". *International journal of distributed sensor net-*

works, v. 2014, pp. 1-9.
http://downloads.hindawi.com/journals/ijdsn/2014/303501.pdf
*http://dx.doi.org/*10.1155/2014/303501

European Commission (2014). "Opinion 8/2014 on the on recent developments on the internet of things", n. 14/EN WP 223, adopted on 16 September 2014, pp. 1-24.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Fatema, Nusrat; **Brad, Remus** (2014). "Attacks and counter-rattacks on wireless sensor networks". *International journal of ad hoc, sensor and ubiquitous computing*, v. 4, n. 6, pp. 1-15.
http://arxiv.org/abs/1401.4443
http://dx.doi.org/10.5121/ijasuc.2013.4601

Fernández-Martínez, Roberto; **Ordieres-Meré, Joaquín-Bienvenido**; **Martínez-de-Pisón-Ascacíbar, Francisco-Javier**; **González-Marcos, Ana**; **Alba-Elías, Fernando**; **Lostado-Lorza, Rubén**; **Pernía-Espinoza, Alpha-Verónica** (2009). *Redes inalámbricas de sensores: teoría y práctica.* La Rioja: Servicio de publicaciones de la Universidad de la Rioja. ISBN: 978 84 692 3007 7
http://dialnet.unirioja.es/servlet/libro?codigo=377564

García-Mexía, Pablo (2013). "La internet de las cosas y sus repercusiones jurídicas". *La ley en red. Blogs ABC*, 18 febrero.
http://abcblogs.abc.es/ley-red/public/post/la-internet-de-las-cosas-y-sus-repercusiones-juridicas-15395.asp

Gupta, Sunil; **Verma, Harsh K.**; **Sangal, Amrit L.** (2013). "Security attacks & prerequisite for wireless sensor networks". *Intl journal of engineering and advanced technology (Ijeat*), v. 2, n. 5, pp. 558-566.
http://www.ijeat.org/attachments/File/v2i5/E1809062513.pdf

Karlof, Chris; **Wagner, David** (2003). "Secure routing in wireless sensor networks: Attacks and countermeasures". *Ad hoc networks*, v. 1, n. 2-3, pp. 293-315.
http://nest.cs.berkeley.edu/papers/sensor-route-security.pdf
http://dx.doi.org/10.1016/S1570-8705(03)00008-8

Kumari, Babli; **Shukla, Jyoti** (2013) "Secure routing in wireless sensor networks". *Ijarcsse*, v. 3, n. 8, pp. 746-751.
http://www.ijarcsse.com/docs/papers/Volume_3/8_August2013/V3I6-0109.pdf

Kuthadi, Venu-Madhav; **Rajendra, C**; **Rajalakshmi, Selvaraj** (2010). "A study of security challenges in wireless sensor networks". *Journal of theoretical and applied information technology*, v. 20, n. 1, pp. 39-44.
http://www.jatit.org/volumes/research-papers/Vol20No1/5Vol20No1.pdf

Malik, M. Yasir (2012). "An outline of security in wireless sensor networks: Threats, countermeasures and implementations". En: Zaman, Noor; Ragab, Khaled; Abdullah, Azween. *Wireless sensor networks and energy efficiency: protocols, routing and management.* Hershey, PA: IGI Global, pp. 507-527. ISBN: 978 146 660102 4
http://dx.doi.org/10.4018/978-1-4666-0101-7.ch024

Maw, Htoo-Aung; **Xiao, Hannan**; **Christianson, Bruce**; **Malcolm, James A.** (2014). "A survey of access control models in wireless sensor networks". *Journal of sensors and actuator networks*, v. 3, n. 2, pp. 150-180.
http://dx.doi.org/10.3390/jsan3020150

Palafox-Maestre, Luis E.; **García-Macías, J. Antonio** (2008). "Security in wireless sensor networks". En: Yan Zhang; Miao, Ma. *Handbook of research on wireless security*. Hershey, PA: IGI Global, pp. 547-564. ISBN: 978 1 59 904899 4
http://dx.doi.org/10.4018/978-1-59904-899-4.ch034

Parlamento Europeo (2004). "Resolución del Parlamento Europeo sobre el primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)". *Diario oficial* n. C 102E de 28.4.2004, pp. 147-153.
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52004IP0141&qid=1420387565870

Rodríguez-Molina, Jesús; **Martínez-Ortega, José-Fernán**; **Rubio-Cifuentes, Gregorio**; **Hernández, Vicente** (2014). "A proposal for an internet of things-based monitoring system composed by low capability, open source and open hardware devices". En: *Procs of the 3rd Intl conf on sensor networks*, v. 3, pp. 87-94.
http://dx.doi.org/10.5220/0004697900870094

Sánchez-Alcón, José-Antonio; **López, Lourdes**; **Martínez-Ortega, José-Fernán**; **Castillejo, Pedro** (2013). "Automated determination of security services to ensure personal data protection in the internet of things applications". En: *3rd Intl conf on innovative computing technology (Intech)*, August, pp. 71-76.
http://dx.doi.org/10.1109/INTECH.2013.6653704

Santos-Familiar, Miguel; **Martínez-Ortega, José-Fernán**; **López, Lourdes** (2012). "Pervasive smart spaces and environments: A service-oriented middleware architecture for wireless ad hoc and sensor networks". *Architecture for wireless ad hoc and sensor networks*, v. 2012, pp. 1-11.
http://dx.doi.org/10.1155/2012/725190

Shukla, Jyoti; **Kumari, Babli** (2013). "Security threats and defense approaches in wireless sensor networks: An overview". *Ijaiem*, v. 2 n. 3, pp. 165-175.
http://www.ijaiem.org/Volume2Issue3/IJAIEM-2013-03-15-033.pdf

Ukil, Arijit (2010). "Security and privacy in wireless sensor networks". En: Chinh, Hoang-Duc; Tan, Yen-Kheng. *Smart wireless sensor networks*, pp. 395-418. ISBN: 978 953 307 261 6
http://dx.doi.org/10.5772/14272

Unión Europea (1995). "Directiva 95/46/CE del Parlamento Europeo y del Consejo, 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos". *Diario oficial*, n. L 282 de 23/11/1995, pp. 0031-0050
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L:1995:282:TOC

Unión Internacional de Telecomunicaciones (1991). *Recomendación X.800. Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CITT*.
http://www.itu.int/rec/T-REC-X.800-199103-I/es