DECISIÓN DE EJECUCIÓN (UE) 2017/2288 DE LA COMISIÓN

de 11 de diciembre de 2017

relativa a la identificación de especificaciones técnicas de las TIC a efectos de referenciación en la contratación pública

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo ([1]), y en particular su artículo 13, apartado 1,

Previa consulta a la Plataforma Europea Multilateral de Normalización de las TIC y a expertos sectoriales,

Considerando lo siguiente:

(1) La normalización contribuye de manera significativa a la Estrategia Europa 2020 ([2]). Varias iniciativas emblemáticas de la Estrategia Europa 2020 ponían de relieve la importancia de la normalización voluntaria en los mercados de productos o servicios para garantizar la compatibilidad y la interoperabilidad entre productos y servicios, promover el desarrollo tecnológico y apoyar la innovación.

(2) Las normas son esenciales para la competitividad europea y cruciales para la innovación y el progreso. Las Comunicaciones de la Comisión sobre el mercado único ([3]) y el mercado único digital ([4]) confirman la importancia de las normas comunes para garantizar la interoperabilidad necesaria de las redes y los sistemas en la economía digital europea. El papel de las normas se ha visto reforzado con la adopción de la Comunicación sobre prioridades de normalización en el sector de las TIC ([5]), en la que la Comisión identifica las TIC prioritarias cuya normalización se considera esencial para la realización del mercado único digital.

(3) La Comunicación de la Comisión titulada «Una visión estratégica de las normas europeas: Avanzar para mejorar y acelerar el crecimiento sostenible de la economía europea de aquí a 2020» ([6]) reconoció el carácter específico de la normalización en el campo de las tecnologías de la información y de las comunicaciones (TIC), en el que a menudo las soluciones, las aplicaciones y los servicios son desarrollados por foros y consorcios mundiales de TIC que son hoy organizaciones líderes en el desarrollo de normas en este ámbito.

(4) El Reglamento (UE) n.º 1025/2012, sobre la normalización europea, estableció un sistema por el que la Comisión puede decidir identificar las especificaciones técnicas de las TIC más pertinentes y de más amplia aceptación emitidas por organizaciones que no sean organismos de normalización europeos, internacionales o nacionales que pueden referenciarse, principalmente para permitir la interoperabilidad en la contratación pública. La posibilidad de utilizar toda la gama de especificaciones técnicas de las TIC en la adquisición de *hardware*, *software* y servicios basados en tecnologías de la información permitirá la interoperabilidad entre dispositivos, servicios y aplicaciones, ayudará a las administraciones públicas a evitar los bloqueos que se producen cuando el comprador público no puede cambiar de proveedor tras la expiración del contrato público por estar utilizando soluciones de TIC privativas y fomentará la competencia en el suministro de soluciones de TIC interoperables.

(5) Para que las especificaciones técnicas de las TIC sean admisibles a efectos de referenciación en la contratación pública, deben cumplir los requisitos del anexo II del Reglamento (UE) n.º 1025/2012. El cumplimiento de dichos requisitos garantiza a las autoridades públicas que las especificaciones técnicas de las TIC se han establecido de acuerdo con los principios de apertura, transparencia, imparcialidad y consenso reconocidos por la Organización Mundial del Comercio en el ámbito de la normalización.

([1]) DO L 316 de 14.11.2012, p. 12.
([2]) Comunicación de la Comisión titulada «EUROPA 2020 ¾ Una estrategia para un crecimiento inteligente, sostenible e integrador». COM(2010) 2020 final de 3 de marzo de 2010.
([3]) Comunicación de la Comisión «Mejorar el mercado único: más oportunidades para los ciudadanos y las empresas». COM(2015) 550 final, de 28 de octubre de 2015.
([4]) Comunicación «Una Estrategia para el Mercado Único Digital de Europa». COM(2015) 192 final, de 6 de mayo de 2015.
([5]) COM(2016) 176 final, de 19 de abril de 2016.
([6]) COM(2011) 311 final, de 1 de junio de 2011.

(6) La decisión de identificar las especificaciones de las TIC debe adoptarse previa consulta a la Plataforma Europea Multilateral de Normalización de las TIC creada por la Decisión 2011/C 349/04 de la Comisión ([1]), complementada por otras formas de consulta a expertos sectoriales.

(7) La Plataforma Europea Multilateral de Normalización de las TIC ha evaluado las siguientes especificaciones técnicas y ha emitido un dictamen favorable sobre su identificación a efectos de referenciación en la contratación pública: «SPF-Sender Policy Framework for Authorizing Use of Domains in Email» («SPF»), «STARTTLS-SMTP Service Extension for Secure SMTP over Transport Layer Security» («STARTTLS-SMTP») y «DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security» («DANE-SMTP»), desarrolladas por Internet Engineering Task Force [Grupo de Trabajo de Ingeniería de Internet] (IETF); «Structured Threat Information Expression» («STIX 1.2») y «Trusted Automated Exchange of Indicator Information» («TAXII 1.1»), desarrolladas por Organization for the Advancement of Structured Information Standards [Organización para el Desarrollo de Normas de Información Estructurada] (OASIS). Posteriormente, la evaluación y el dictamen de la Plataforma se han sometido a consulta con expertos del sector, que han confirmado el dictamen favorable sobre su identificación.

(8) La especificación técnica SPF, desarrollada por IETF, es una norma abierta que especifica un procedimiento técnico para detectar la falsificación de la dirección del remitente. SPF ofrece la posibilidad de comprobar si un mensaje ha sido enviado desde un servidor autorizado para ello. Se trata de un sencillo sistema de validación de correos electrónicos diseñado para detectar la suplantación (*spoofing*) de direcciones de correo electrónico, consistente en un mecanismo que permite a los intercambiadores de correo receptores comprobar si el correo entrante de un determinado dominio procede de un servidor autorizado por los administradores de dicho dominio. El objetivo de SPF es evitar el envío de mensajes de correo basura empleando direcciones de remitente falsificadas de un dominio concreto. Los destinatarios pueden referirse a un registro SPF para determinar si un mensaje supuestamente enviado desde ese dominio procede de un servidor de correo autorizado.

(9) La especificación STARTTLS-SMTP, desarrollada por IETF, sirve para convertir una conexión insegura existente en una conexión segura. STARTTLS es una extensión del servicio del protocolo simple de transmisión de correo (SMTP) que permite a un servidor y a un cliente SMTP utilizar el protocolo «seguridad de la capa de transporte» (TLS) para proporcionar una comunicación en línea privada y autentificada. La comunicación por correo electrónico no segura es uno de los vectores de ataque más utilizados para vulnerar la seguridad de las redes de las administraciones públicas. Si un usuario envía un correo electrónico, el servidor de correo del proveedor de servicios de correo de dicho usuario lo enviará al servidor de correo del destinatario. A través de TLS puede garantizarse de antemano la seguridad de la conexión entre dichos servidores de correo. STARTTLS es un método para mejorar una conexión no encriptada (texto simple) y convertirla en una conexión TLS encriptada.

(10) La especificación DANE-SMTP, desarrollada por IETF, es un conjunto de protocolos para mejorar la seguridad de Internet que permite colocar claves en el sistema de nombres de dominio (DNS) y protegerlas mediante el protocolo DNSSEC (seguridad DNS). Al establecer una conexión segura con una parte desconocida, es conveniente realizar una comprobación en línea de la autenticidad del remitente y de su destino. Para ello pueden utilizarse certificados expedidos por las autoridades de certificación del sistema PKI o certificados autofirmados. DANE permite al titular de un dominio («registratario») proporcionar información adicional, además de los certificados en línea, mediante un registro DNS protegido por el protocolo DNSSEC. Por eso resulta especialmente útil para luchar contra atacantes activos.

(11) La especificación STIX 1.2, desarrollada por OASIS, es un lenguaje para describir información sobre ciberamenazas de manera normalizada y estructurada. Abarca cuestiones importantes en materia de datos sobre amenazas cibernéticas, facilitando el análisis de los ataques y los intercambios de información al respecto. Describe un amplio conjunto de datos sobre ciberamenazas, incluidos indicadores de actividad de los adversarios, como direcciones IP y resúmenes criptográficos (*hashes*) de archivos, e información contextual relativa a amenazas, como tácticas, técnicas y procedimientos (TTP) de los adversarios; objetivos de explotación; y campañas y líneas de actuación. En conjunto, esta información caracteriza exhaustivamente las motivaciones, capacidades y actividades del ciberadversario y, de este modo, ayuda a hacer frente a sus ataques.

(12) La especificación técnica TAXII v1.1, también desarrollada por OASIS, normaliza el intercambio automatizado y fiable de información sobre ciberamenazas. TAXII define servicios e intercambios de mensajes para compartir información utilizable sobre amenazas cibernéticas entre organizaciones, productos o servicios con miras a la detección, prevención y mitigación de dichas amenazas. TAXII permite que las organizaciones consigan un mejor conocimiento de la situación en materia de amenazas emergentes y compartan información fácilmente con sus socios, aprovechando relaciones y sistemas existentes.

([1]) Decisión 2011/C 349/04 de la Comisión, de 28 de noviembre de 2011, por la que se crea la Plataforma Europea Multilateral de Normalización de las TIC (DO C 349 de 30.11.2011, p. 4).

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Las especificaciones técnicas enumeradas en el anexo son admisibles a efectos de referenciación en la contratación pública.

Artículo 2

La presente Decisión entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 11 de diciembre de 2017.

Por la Comisión
El Presidente
Jean-Claude JUNCKER

ANEXO

Internet Engineering Task Force (IETF)

N.º	Título de la especificación técnica de las TIC
1	SPF-Sender Policy Framework
2	STARTTLS-SMTP Service Extension for Secure SMTP over Transport Layer Security
3	DANE-SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security (TLS)

Organization for the Advancement of Structured Information Standards (OASIS)

N.º	Título de la especificación técnica de las TIC
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information