INFORME RELATIVO A LA CONSULTA AL MERCADO EN RELACIÓN AL CONTRATO DE SUMINISTRO Y SERVICIOS PARA LA IMPLANTACIÓN DEL NUEVO SISTEMA COMERCIAL YARA EN MODO SAAS Y LOS SERVICIOS ASOCIADOS DE ACOMPAÑAMIENTO Y MANTENIMIENTO PARA CANAL DE ISABEL II, S.A.

(EXP. 20/2020)

Contenido

1. INTRODUCCIÓN

Canal de Isabel II, S.A. (en adelante, "Canal de Isabel II"), empresa pública responsable del ciclo integral del agua en la Comunidad de Madrid, desea llevar a cabo la renovación de su sistema de gestión comercial mediante la implantación de un producto o conjunto de productos de gestión comercial estándares que cubran las necesidades y magnitudes específicas para la empresa. Esta actuación está incluida en su Plan Estratégico 2018-2030.

Teniendo en cuenta que el futuro contrato a licitar por Canal de Isabel II para la renovación de su sistema de gestión comercial plantea una nueva estrategia tanto de alcance de la licitación como de enfoque de implantación de la solución (servicios SaaS o equivalentes), Canal de Isabel II ha considerado necesario realizar una consulta preliminar del mercado sobre los requerimientos de Seguridad (o Ciberseguridad) y Protección de Datos que los servicios SaaS (o equivalentes) cumplen, cuya convocatoria fue publicada el 30 de marzo de 2021 para ser celebrada entre el 6 y el 15 de abril de 2021, y que tuvo lugar entre los días 9 y 15 de abril de 2021, ambos inclusive, con las empresas que expresaron su interés en participar y que se refieren más adelante.

Una vez realizadas las consultas, en el presente informe se hacen constar los extremos previstos en el artículo 41 del Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales.

2. ANTECEDENTES

Canal de Isabel II ha decidido cambiar la plataforma tecnológica que da soporte a sus procesos comerciales pasando a una solución basada en productos estándares de mercado, que contemple todos los requerimientos de negocio necesarios para llevar a cabo su gestión comercial, y donde estén implantadas las mejores prácticas del mercado, que esté alineada con la transformación digital de la compañía y permita acelerar los proyectos de innovación, dando como resultado una mejora en los procesos y relación con los clientes o usuarios a los que presta servicio Canal de Isabel II.

Durante 2017 se llevó a cabo un análisis de lo que el mercado ofrece a este respecto, con el objetivo de elaborar un catálogo de requisitos que pudiera dar cabida a todos los productos existentes en el mercado que cubran los requisitos de negocio demandados por la empresa.

Como resultado de este análisis se decidió llevar a cabo este tipo de proyecto de transformación en dos etapas: una primera en la que se elija y valide el producto o conjunto de productos que conformen la implantación básica de acuerdo a las necesidades de negocio requeridas; y una segunda en la que se seleccione el integrador que llevará a cabo la implantación completa de la solución y su posterior mantenimiento.

En julio de 2018 se llevó a cabo una consulta preliminar al mercado para preparar la licitación, respondiendo 5 fabricantes de software interesados cuyo informe de conclusiones se publicó en noviembre de ese mismo año. A través de esta consulta se detectó que el clausulado estándar del Pliego

de Cláusulas Administrativas Particulares de Canal de Isabel II relativo a la responsabilidad por daños y perjuicios y propiedad intelectual, suponía un obstáculo para que los fabricantes de software presentaran ofertas en el correspondiente procedimiento abierto.

En noviembre de 2018 se preparó el procedimiento abierto 238/2018 modificando parcialmente en el Pliego de Cláusulas Administrativas Particulares las cláusulas de responsabilidad por daños y perjuicios (limitando su importe) y la de propiedad intelectual (limitando el ámbito de los derechos de propiedad intelectual correspondientes a Canal de Isabel II a los nuevos desarrollos realizados específicamente para Canal de Isabel II fuera del producto estándar realizado por el contratista).

Los pliegos del procedimiento 238/2018 se publicaron el 17 de mayo de 2019 en el Portal de la Contratación Pública de la Comunidad de Madrid, mostrando interés, a través de las más de 300 dudas y consultas presentadas para la elaboración de la oferta durante la fase de la convocatoria, 2 de los fabricantes que participaron en la consulta preliminar de mercado realizada: SAP y ORACLE

A pesar de las consultas formuladas por dichos fabricantes y las correspondientes respuestas dadas por Canal de Isabel II, el procedimiento de licitación 238/2018 quedó desierto al no presentarse ninguna oferta.

Tras analizar las dudas y cuestiones planteadas durante la publicación de la licitación, los motivos principales que se identificaron como obstáculos para la presentación de ofertas estaban relacionados con las cláusulas de propiedad intelectual, protección de datos y subcontratación permitida, principalmente, porque las cláusulas afectaban, por un lado, a la posible comercialización del software desarrollado que es el objeto de negocio de los fabricantes de software y, por otro lado, por el modelo de grupo de empresas de los grandes fabricantes de software, donde las prestaciones demandadas no son realizadas en exclusiva por una única empresa del grupo sino por varias de ellas radicadas en diferentes países.

Como resultado de dicho análisis se concluyó que sería viable alcanzar los objetivos y resultados planteados en la licitación 238/2018 permitiendo la subcontratación de las tareas críticas a empresas del grupo, flexibilizando la cláusula de propiedad intelectual -limitando el ámbito de los derechos de propiedad intelectual correspondientes a Canal de Isabel II únicamente a los derechos de reproducción y transformación-, y adaptando la cláusula de protección de datos, para permitir la transferencia internacional de datos.

En consecuencia, Canal de Isabel II licitó de nuevo este contrato a través de otro procedimiento abierto, el procedimiento 215/2019, flexibilizando dichas cláusulas. La convocatoria de este nuevo procedimiento abierto se publicó en octubre de 2019 en el Portal de la Contratación Pública de la Comunidad de Madrid siendo el resultado de esta licitación el mismo que la anterior, al quedar desierto el procedimiento por no presentarse ninguna oferta.

Con fecha 16 de diciembre de 2019 Canal de Isabel II publicó en el Portal de la Contratación Pública de la Comunidad de Madrid una consulta con objeto de conocer en detalle los impedimentos que habían provocado la falta de presentación de ofertas a las licitaciones 238/2018 y 215/2019. A dicha consulta únicamente contestaron SAP y ORACLE, y en ella manifestaron los principales factores limitantes para la presentación de ofertas. Todo ello está recogido en el Informe de resultados de la consulta al mercado, que fue publicado el 11 de mayo de 2020 en el Portal de la Contratación Pública de la Comunidad de

Madrid. En resumen, los impedimentos volvían a hacer referencia a algunas cuestiones anteriormente tratadas (protección de datos, propiedad intelectual y subcontratación), además de otras en torno a la responsabilidad por daños y perjuicios, penalizaciones, política de cumplimiento y auditorías.

Como resultado de los impedimentos para ejecutar la estrategia del proyecto en dos etapas, Canal de Isabel II ha cambiado su estrategia de proyecto y ha decidido ejecutar el proyecto en una única etapa, eligiendo a la vez el producto o conjunto de productos que conformen la solución, y al integrador que llevará a cabo la implantación completa de la solución y su posterior mantenimiento.

Adicionalmente, Canal de Isabel II ha decidido orientar la solución hacia servicios Software-as-a-Service (SaaS), o servicios de nube gestionados por los fabricantes de los productos, como estrategia de implantación. Esta estrategia se alinea tanto con la estrategia de Sistemas de Información de Canal de Isabel II, como con la evolución del mercado, donde los productos se ofrecen y evolucionan hacia soluciones SaaS (o equivalentes).

3. CONSULTA

Teniendo en cuenta que el próximo contrato a licitar por Canal de Isabel II plantea una nueva estrategia tanto de alcance de la licitación como de enfoque de implantación de la solución (servicios SaaS o equivalentes), Canal ha considerado necesario realizar una consulta preliminar del mercado sobre los requerimientos de Seguridad (o Ciberseguridad) y Protección de Datos que los servicios SaaS (o equivalentes) cumplen, conforme a la relación de cuestiones que figuran en el punto 4 de este documento (25 cuestiones relativas a Seguridad y 16 cuestiones relativas a Protección de Datos). Estas cuestiones no constituían una lista cerrada, sino que podían ser ampliadas o matizadas con otras que surgieran como consecuencia de las respuestas facilitadas a Canal de Isabel II por los participantes en la consulta.

Expuesto lo anterior, y teniendo en cuenta que Canal de Isabel II considera imprescindible que los servicios SaaS (o servicios gestionados cloud) sean gestionados por los fabricantes de los productos que constituyan la solución, o que pertenezcan al grupo empresarial del fabricante, se ha convocado a los fabricantes de software que puedan ofrecer servicios SaaS para la solución demandada por Canal de Isabel II, para que pongan de manifiesto a esta empresa pública aquellos requerimientos de Seguridad y Protección de Datos que cumplen sus servicios, así como los requerimientos establecidos en el procedimiento 215/2019.

Publicada la convocatoria de la consulta preliminar de mercado el 30 de marzo de 2021, para que la misma se celebrase entre los días 6 y 15 de abril de 2021, las empresas interesadas podían participar en la consulta remitiendo un correo electrónico a consultas_contratacion@canal.madrid, indicando en el asunto “Consulta al Mercado YARA – Entidad” y añadiendo en el cuerpo una dirección de correo electrónico de contacto para comunicaciones al respecto de la consulta.

Las empresas que mostraron interés en participar en la consulta fueron las siguientes:

- SAP
- ORACLE
- SALESFORCE
- BUNTPLANET

A continuación, se acordaron las fechas y horas para celebrar las reuniones relativas a la consulta con cada una de las empresas interesadas y en función de la disponibilidad de los representantes de cada una de ellas y de Canal de Isabel II, S.A. Las referidas consultas han sido celebradas mediante videoconferencia en las siguientes fechas:

- 8 de abril de 2021 con SAP
- 9 de abril de 2021 con ORACLE
- 14 de abril de 2021 con SALESFORCE

La convocatoria con BuntPlanet había sido convocada para el día 15 de abril, pero finalmente la empresa declinó participar en la convocatoria.

Para mayor objetividad, claridad y definición en la identificación y descripción de las respuestas a las 41 cuestiones planteadas, se solicitó a SAP, ORACLE y SALESFORCE que enviaran un documento con las respuestas que habían facilitado durante la reunión a cada una de las cuestiones planteadas. Se especificó que ese documento se publicaría como anexo al presente informe, por lo que no debía contener información confidencial.

Se facilitan a continuación las cuestiones objeto de la consulta preliminar de mercado acerca de los requerimientos de Seguridad (o Ciberseguridad) y Protección de Datos, así como las respuestas facilitadas a las mismas por las empresas que han participado en la presente consulta.

4. CUESTIONES OBJETO DE CONSULTA

PROTECCIÓN DE DATOS

1. Descripción general de medidas de seguridad adecuadas en el tratamiento de datos personales de cada producto que constituya la solución[1].

2. Clasificación de las actuaciones a realizar por cada grupo de subencargados de tratamiento. Procedimientos documentados para la selección, control, evaluación y auditorias de la cadena de subencargados de tratamientos.

3. Procedimiento de formación en protección de datos del encargado del tratamiento y de la cadena de subencargados y copia del programa de formación.

4. Estructura y posición en la organización e idioma de contacto con el equipo del Delegado de Protección de Datos.

5. Clasificación de los productos que constituyan la solución e identificación de las ubicaciones (países) donde se realizarán tratamientos de datos en ejecución del contrato agrupándolos en función de:

1 Los conceptos datos personales y tratamiento deben ser entendidos conforme la definición recogida en los apartados 1 y 2 del artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE (en adelante RGPD). Recurso disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf

5.1. países pertenecientes al Espacio Económico Europeo (Unión Europa, Liechtenstein, Islandia y Noruega)
5.2. países sobre los cuales la Comisión Europea haya declarado un nivel adecuado de protección de datos (Decisión de Adecuación).
5.3. países distintos de los anteriores que ofrezcan garantías adecuadas de cumplimiento relativa a la normativa europea de protección de datos, bajo alguno de los siguientes mecanismos recogidos en:
5.3.1. el artículo 46, apartado 2, letra a) del RGPD, "Instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos" (excepto Privacy Shield);
5.3.2. el artículo 47 del RGPD "Normas Corporativas Vinculantes";
5.3.3. el artículo 46, apartado 2, letra c) del RGPD "Cláusulas Tipo de Protección de Datos adoptadas por la Comisión con aplicación de garantías adicionales cuando sea necesario";

6. Modelo de documentos utilizados en relación con los instrumentos enumerados en los apartados 5.3.2 y 5.3.3 a través de los cuales se consiga un nivel de protección esencialmente equivalente al de la normativa de la Unión Europea donde quiera que se traten los datos personales y procedimiento para la revisión de los mismos.

7. Decisiones, adaptaciones realizadas, en curso y/o con compromiso de realización en cuanto al tratamiento de datos se refiere, tras la Sentencia del Tribunal de Justicia de la Unión Europea de 16 de julio de 2020 (asunto C-311/18 - Comisario de Protección de Datos vs Facebook Irlanda y Maximillian Schrems)[2].

8. Procedimiento para la identificación de legislación y/o práctica de un tercer país en el que se podrán tratar los datos personales que pueda afectar a la eficacia de las garantías adecuadas de los instrumentos de transferencia en los que se basa enumerados en el apartado 5.3.2 y 5.3.3, en el contexto de su transferencia específica. Mecanismos para implementar la Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia[3].

9. Para los supuestos enumerados en el apartado 5.3.2 y 5.3.3, identificación de las medidas complementarias (técnicas, contractuales y organizativas)[4].

10. Mecanismos previstos para la actualización y comunicación de la ubicación de servidores y servicios asociados a los mismos. conforme al artículo 122 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

11. Procedimiento de brechas de protección de datos.

---

[2] Recurso disponible en https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=9853523

[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_es.pdf

[4] Conforme las Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE. Recurso disponible en https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_es.pdf

12. Política y Sistema de Gestión de Protección de Datos y posición en cuanto a futuras adaptaciones a cambios derivados de jurisprudencia, resoluciones, dictámenes, opiniones, recomendaciones, de las autoridades nacionales y autoridades europeas de protección de datos.

13. Procedimiento documentado de realización de evaluación de impacto, análisis de riesgos, controles y auditorías en protección de datos personales.

14. Procedimiento documentado de colaboración con el responsable del tratamiento.

15. Resumen de medidas adicionales en el cumplimiento de la normativa aplicable de Protección de Datos.

16. Medidas de cifrado de los datos personales en tránsito y en reposo.

SEGURIDAD DE LA INFORMACIÓN

1. Certificaciones de los servicios/productos SaaS (o equivalentes) por cada producto que constituya la solución:
    a. ISO/IEC 27001
    b. ISO/IEC 27017
    c. ISO/IEC 27018
    d. Certificación STAR nivel 2
    e. BSI 25999 o ISO 22301

2. Nivel de certificación de cada producto que constituya la solución del Esquema Nacional de Seguridad (ENS) o informe con el nivel de adecuación de cada producto que constituya la solución a las exigencias de los distintos niveles (BAJO, MEDIO y ALTO).

3. Nivel de adecuación de cada producto que constituya la solución a la Directiva NIS europea para la seguridad de redes y sistemas de información.

4. Auditorías de seguridad anuales, informe de resultados y planes de acción para la subsanación de las deficiencias encontradas.

5. Informe del último análisis de riesgos y plan de acción definido para su eliminación, mitigación, transmisión o aceptación.

6. Medidas de seguridad físicas implementadas en sus instalaciones.

7. Medidas de seguridad multi-tenant implementadas en los productos que constituyen la solución.

8. Procedimientos de monitorización, alerta y reporting.

9. Procedimientos de bastionado y securización de los productos que constituyen la solución.

10. Procedimientos implementados para la aplicación de parches y actualizaciones, tanto de software como de seguridad).

11. Información sobre el nivel de protección y exposición de los entornos o sistemas no productivos (desarrollo, test, calidad, formación, etc.) y de la información que contienen y gestionan.

12. Aseguramiento de la calidad de los desarrollos (por ejemplo, certificaciones ISO/IEC 15504 SPICE, ISO/IEC 33000, modelo de madurez CMMI o equivalentes).

13. Procedimiento de gestión de cambios en los servicios por cada producto que constituya la solución (por ejemplo, certificación ISO/IEC 20000-1 o equivalente).

14. Registro de los eventos producidos por las actividades de todos los usuarios en todos los productos que formen parte de la solución y en todos los registros de información (al menos, creación, modificación, eliminación).

15. Acceso a los servicios mediante protocolos seguros.

16. Protecciones implementadas contra ataques de fuerza bruta de todos los formularios, especialmente los de inicio de sesión.

17. Esquema de BBDD propio. Acceso al esquema exclusivamente por usuarios de aplicación.

18. Cifrado robusto (aquel que se ha comprobado que es altamente resistente a ataques de criptoanálisis) de los datos en la propia BBDD. Cifrado completo o cifrado del dato.

19. Almacenamiento de los datos de autenticación de manera criptográficamente segura.

20. Mecanismos de autenticación y autorización. Soporte al menos para SAML 2.0, OAuth 2.0, Open ID, etc.

21. Procedimientos para la securización de los Web Services a nivel de mensaje (autenticación de los servicios y de los usuarios, garantía de la integridad y la confidencialidad y el no repudio, y definición de la política de seguridad en los Web Services).

22. Segundo factor de autenticación (2FA) para el acceso al servicio.

23. Todas las funciones de la solución relacionadas con la autenticación, la gestión de las sesiones y la autorización (control del acceso) han sido auditadas contra estándares de seguridad internacionalmente reconocidos (por ejemplo, OWASP, WASC, etc.).

24. Procedimientos implementados para la monitorización y reporte de vulnerabilidades que afecten a cada producto que constituya la solución.

25. Información sobre todos los requisitos técnicos a cumplir por la infraestructura tecnológica del cliente, tanto a nivel de sistemas de información, sistemas de comunicación y sistemas de puesto cliente.

5. RESPUESTAS A LAS CUESTIONES OBJETO DE CONSULTA

A continuación, se referencian los documentos de cada participante en esta consulta:

- SAP
  - Referenciar y anexar documento de respuesta a las 41 cuestiones remitido por SAP al buzón de Contratación.
- ORACLE
  - Referenciar y anexar documento de respuesta a las 41 cuestiones remitido por ORACLE al buzón de Contratación.
- SALESFORCE
  - Referenciar y anexar documento de respuesta a las 41 cuestiones remitido por SALESFPRCE al buzón de Contratación.

Canal de Isabel II tendrá en cuenta todas las respuestas aportadas por los distintos interesados a la hora de elaborar los pliegos de la próxima licitación.

Firmado digitalmente Carmen Picazo Veloso / A86488087
Fecha: 31/05/2021

Carmen Picazo
Responsable de Aplicaciones Corporativas

Firmado digitalmente por Sergio Cruceta Gomez / A86488087
Fecha: 2021.05.31 09:31:20 +02'00'

Sergio Cruceta
Coordinador de Proyectos

Firmado electrónicamente por Angel Rodriguez Garcia

Ángel Rodriguez
Subdirector Sistemas Información

Maria Gonzalez Cano / A86488087
Firmado digitalmente por Maria Gonzalez Cano / A86488087
Fecha: 2021.05.28 15:55:35 +02'00'

María González
Subdirectora Desarrollo Negocio

Juan Zubizarreta
Director Comercial

Firmado electrónicamente por JUAN IGNACIO ZUBIZARRETA PARIENTE
el día 02-06-2021 14:03:11