Junta de Andalucía

Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa

Agencia Digital de Andalucía

Consulta preliminar al mercado sobre servicio de auditoría permanente del estado de la seguridad en las smart cities

Agencia Digital de Andalucía
Dirección General de Estrategia Digital
T: 955061501
dged.ada@juntadeandalucia.es

Sumario

1. Objeto de la consulta

Recabar información de los operadores especialistas en el sector, relativa a la puesta en marcha de un servicio de auditoría permanente sobre seguridad en las smart cities, estableciendo precios y plazos de referencia en base a parámetros objetivos y cuantificables, con el fin de que la Agencia Digital de Andalucía pueda incluir, si procede, la información recabada para elaborar los pliegos de futuros expedientes de contratación que, en su caso, se liciten al respecto.

2. Competencias

En la Administración de la Junta de Andalucía, las competencias en materia de ciberseguridad están atribuidas a la Agencia Digital de Andalucía por el Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía (en adelante ADA).

Los fines de la ADA, expresados en el artículo 6.2 de sus Estatutos, incluyen

> "*a) La definición y ejecución de los instrumentos de tecnologías de la información, telecomunicaciones, ciberseguridad y gobierno abierto y su estrategia digital, en el ámbito de la Administración de la Junta de Andalucía, sus agencias administrativas y sus agencias de régimen especial.*
>
> *b) La definición y coordinación de las políticas estratégicas de aplicación y de seguridad de las tecnologías de la información y de las comunicaciones en el ámbito del sector público andaluz no incluido en el párrafo anterior, incluyéndose los consorcios referidos en el artículo 12.3 de la Ley 9/2007, de 22 de octubre, así como la ejecución de los instrumentos comunes que las desarrollen y la definición y contratación de bienes y servicios de carácter general aplicables.*"

En concreto, el artículo 6.3 de los citados Estatutos le atribuye las competencias en

> "*ñ) El desarrollo y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía y del sector público andaluz.*
>
> *o) La gestión de los recursos comunes para la prevención, detección y respuesta a incidentes y amenazas de ciberseguridad en el ámbito de la Administración de la Junta de Andalucía y del sector público andaluz*."

Estas competencias, en virtud del artículo 15.3.c de los Estatutos, serán desarrolladas por la Dirección General de Estrategia Digital.

En este ámbito competencial se encuadra la Participación de la ADA en varias iniciativas del programa RETECH, de Redes Territoriales de Especialización Tecnológica, destinado a articular diversos proyectos regionales orientados a la transformación y especialización digital, asegurando la coordinación, la colaboración y la complementariedad.

Entre estas iniciativas se cuenta la Red Argos, que tiene como objetivo general impulsar y fortalecer el ecosistema regional y nacional de ciberseguridad y aumentar la adopción global de la misma, en base a la generación de capacidades especializadas y al trabajo en red de diferentes agentes, y la generación de capacidades especializadas en ámbitos estratégicos, como son las Smart Cities en el caso de la Comunidad Autónoma de Andalucía. Las actividades derivadas de esta iniciativa se alinean también con la Estrategia de Ciberseguridad de Andalucía 2022 – 2025.

Entre los proyectos que se prevé abordar por la Agencia Digital de Andalucía en el ámbito del proyecto Red Argos, se encuentra la realización de auditorías de ciberseguridad de proyectos Smartcity desplegados en determinadas ciudades andaluzas que impliquen la interconexión de elementos comúnmente denominados iot para la gestión eficaz de los servicios municipales. Como resultado de dichas auditorías se pretende, no sólo determinar posibles problemas de seguridad que puedan identificarse en estos proyectos ya en funcionamiento, así como un plan de securización de los mismos, sino también la elaboración de una metodología general que pueda ser replicable en otras Administraciones locales.

3. Objetivos de la consulta

Se busca, mediante las preguntas reflejadas en el cuestionario anexo a este documento, obtener información sobre las actividades básicas, costes y plazos asociados a la puesta en marcha de un servicio de auditoría permanente que permita conocer el estado de la seguridad global de las smart cities interesadas.

Las auditorías realizadas han de ser, salvo acuerdo entre las partes, integrales, es decir, no circunscribirse únicamente al estado de los dispositivos IoT en sí mismos (actualizaciones o vulnerabilidades), sino a todos los aspectos característicos de este tipo de instalaciones, así como a las peculiaridades de su uso (arquitectura de red, segmentación, protocolos específicos de comunicaciones entre dispositivos, etc.), por lo que deberán incluirse en el alcance de la auditoría los siguientes ámbitos:

1. Dispositivos IoT: sobre todos los dispositivos IoT conectados a la red (salvo BYOD), inventariando, recopilando y documentando sus configuraciones con el fin de mejorar rendimiento, confiabilidad y seguridad, además de asegurar el cumplimiento de estándares, recomendaciones y normativa de aplicación.
2. Redes de comunicaciones: analizando la robustez y fiabilidad de los sistemas desplegados, analizando la tolerancia ante un fallo o bloqueo de un nodo, la escalabilidad, el entorno y topología, las restricciones hardware, la visibilidad requerida, el consumo de energía, etc.
3. Datos: fuentes de datos y los destinos de dichos datos, cómo interactúan con los otros sistemas y redes, cuáles son los requisitos normativos y de obligado cumplimiento, las distintas políticas y procedimientos existentes, qué riesgos y controles clave se tienen en cuenta, etc.
4. Aplicaciones: tanto sobre la plataforma IoT a la cual viertan datos todos los verticales implantados o fuentes de información utilizadas, como aquellos aplicativos, si los hubiera, que se utilicen para gestionar dichos verticales y en general cualquier otro que se utilice para reunir, almacenar, analizar y/u ofrecer inteligencia (especialmente aplicaciones AIoT) a partir de los datos generados

por los dispositivos IoT, su comportamiento y las fuentes externas de información incorporadas (ficheros csv, xml,…).

5. Inter-relación entre dispositivos y sistemas IoT: evaluando que todos los componentes colaboran entre sí de forma satisfactoria y que no se producen pérdidas de paquetes, fallos en las comunicaciones, configuración de equipos erróneas, uso de cableado inadecuado, etc.

Generando como resultado un informe del estado de la seguridad de los distintos ámbitos referidos en el ecosistema smart en el que se encuentran desplegados los dispositivos IoT.

Si bien el cumplimiento del Esquema Nacional de Seguridad (ENS) puede servir como referencia para valorar el estado de la seguridad, las acciones de auditoría no pueden basarse exclusivamente en las medidas para su cumplimiento al no estar el ENS particularizado para dispositivos IoT. Es conveniente indicar que la finalidad última de la auditoría no es el cumplimiento del ENS y, por tanto, las acciones a realizar no deben estar encaminadas exclusivamente a su cumplimiento, sino particularizadas para conocer el estado de seguridad de un ecosistema de dispositivos IoT en una instalación smart.

Dada la amplitud y diversidad de los aspectos a abordar, se admitirán en esta consulta preliminar respuestas parciales que no contemplen el desarrollo de todos los ámbitos, sino aquellos referidos al campo de experiencia de las empresas participantes.

4. Fundamento jurídico de la consulta

Artículo 115 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:

1. Los órganos de contratación podrán realizar estudios de mercado y dirigir consultas a los operadores económicos que estuvieran activos en el mismo con la finalidad de preparar correctamente la licitación e informar a los citados operadores económicos acerca de sus planes y de los requisitos que exigirán para concurrir al procedimiento.

5. Organismo solicitante de la consulta

Agencia Digital de Andalucía.

6. Procedimiento de consulta

La consulta es pública y se dirige a organismos públicos o privados y empresas que deseen colaborar facilitando información del mercado sobre los asuntos reflejados en la misma. Se articula a través del cuestionario publicado en el perfil del contratante de la Agencia Digital de Andalucía junto con este documento. En caso de que se considere oportuno compartir información adicional en otro formato, se puede remitir junto con el cuestionario para su análisis. Es conveniente que el cuestionario se cumplimente en su totalidad, y que las respuestas sean lo más completas posible, para lo que se admitirán los comentarios y aclaraciones que se consideren oportunos en cada caso.

Los cuestionarios rellenos se remitirán a través correo electrónico al Servicio de Ciberseguridad en la dirección sv.ciberseguridad.ada@juntadeandalucia.es incluyendo en el asunto el texto “Consulta Preliminar AUDITORIA IoT SMART”. Para cualquier consulta también se puede contactar con el mismo correo electrónico.

Si se considera necesario, la Agencia podrá contactar con participantes concretos para recabar más información sobre las respuestas incluidas en sus cuestionarios o aclarar dudas.

Se fija para presentar los cuestionarios debidamente cumplimentados un plazo de 15 días naturales desde la publicación de esta consulta.

Finalizado el plazo de presentación de cuestionarios y, en su caso, recabada la información adicional que fuera necesaria, se publicará en el Perfil de Contratante de la Agencia Digital de Andalucía el informe a que se refiere el apartado 3 del mencionado artículo 115 de la Ley de Contratos del Sector Público.

7. Aplicación de los principios de transparencia, igualdad de trato y no discriminación ni falseamiento de la competencia

Sin perjuicio de lo establecido en el artículo 115.3 de la Ley de Contratos del Sector Público en relación con el informe que debe publicarse de las actuaciones realizadas, la información contenida en los cuestionarios recibidos será considerada confidencial y tratada como tal por la Agencia Digital de Andalucía. La Agencia no revelará en ningún caso a los participantes en el mismo la consulta las soluciones propuestas por los otros participantes. El proceso de la consulta y todas las acciones que se deriven de ella se someterán a los principios de transparencia, igualdad de trato y no discriminación.

La participación en esta consulta no otorgará derecho ni preferencia alguna respecto de la adjudicación de los contratos que puedan celebrarse con posterioridad en el ámbito del objeto de esta convocatoria y, como consecuencia de ello, no conlleva ninguna obligación de financiación o aceptación de las propuestas recibidas. No obstante, la participación en la consulta no impide la posterior intervención en el procedimiento de contratación que en su caso se tramite.

EL JEFE DE SERVICIO DE CIBERSEGURIDAD