Presentación de candidatura a los premios "CIBERSEGURIDAD AAPP", en la categoría "Cooperación de las empresas TIC con las AAPP en materia de ciberseguridad"

A continuación, les presento el proyecto de "Servicios de ciberseguridad para el Sistema Portuario", promovido desde Puertos del Estado a través del Área TIC y del Departamento de Ciberseguridad, Comunicaciones y Aplicaciones Corporativas del que soy titular. En el ámbito de la administración pública, y en concreto de Puertos del Estado, es habitual recurrir a la colaboración público/privada a la hora de abordar proyectos de envergadura como este que les presento. La realización de este tipo de proyectos con recursos propios sería inabordable, por lo que desde nuestra perspectiva estamos convencidos de que, únicamente con el apoyo de empresas privadas líderes en tecnología, somos capaces de sacar adelante iniciativas como la que les presento. Espero que la siguiente exposición sea del agrado del Jurado.

José Manuel Cabrera López
Jefe de Departamento de Ciberseguridad,
Comunicaciones y Aplicaciones Corporativas
de Puertos del Estado

Descripción del proyecto y repercusión para el ciudadano y administraciones

España es el país de la Unión Europea que cuenta con mayor longitud de costa: 8.000 kilómetros. Además, su situación geográfica, próxima al eje de una de las rutas marítimas más importantes del mundo, la beneficia de un mayor afianzamiento como área estratégica en el transporte marítimo internacional y como plataforma logística del sur de Europa.

El sistema portuario español de titularidad estatal está integrado por 46 puertos de interés general. Estos enclaves están gestionados por 28 autoridades portuarias, cuya coordinación y control de eficiencia corresponde al organismo público Puertos del Estado, órgano dependiente del Ministerio de Transportes y Movilidad Sostenible y que tiene atribuida la ejecución de la política portuaria del Gobierno.

La importancia de los puertos como eslabones de las cadenas logísticas y de transporte viene avalada por las siguientes cifras: por ellos pasan cerca del 60 por ciento de las exportaciones y el 85 de las importaciones, lo que representa el 53 por ciento del comercio exterior español con la Unión Europea y el 96 con terceros países. Además, la actividad del sistema portuario estatal aporta cerca del 20 por ciento del Producto Interior Bruto (PIB) del sector del transporte, lo que representa el 1,1 del PIB español. Asimismo, genera un empleo directo de unos 100.000 puestos de trabajo y de unos 175.000 de forma indirecta e inducida.

Con estos datos no es difícil inferir la importancia estructural a nivel nacional y europeo del sistema portuario. No en vano, algunos de los puertos de titularidad estatal que forman parte del sistema portuario están catalogados como infraestructuras críticas, por lo que su importancia estratégica en la cadena de transporte y logística es fundamental.

Por otro lado, no hay que obviar el hecho de la profunda y sin precedentes transformación digital de la sociedad en su conjunto. Esta digitalización, impulsada desde la Unión Europea y asumida por el Gobierno, se ha tomado como un asunto ineludible. Incluso se ha creado (entre otras medidas) un ministerio propio dedicado a la digitalización: el Ministerio de Asuntos Económicos y Transformación Digital.

En este contexto resulta indudable que la ciberseguridad constituye un pilar básico para acometer esa labor de transformación digital, por cuanto canaliza, mediante una adecuada protección tecnológica, el impulso del crecimiento y la competitividad en la actividad económica. Todo ello en un entorno seguro que minimiza los riesgos vinculados a esta conversión.

Motivación y estrategia

Desde esta perspectiva, surge la motivación desde el Área TIC de Puertos del Estado de lanzar una iniciativa de provisión de servicios de ciberseguridad, pero llevando ésta un poco más lejos de la mera contratación de servicios para nuestra organización. Se propone ampliar el ámbito del proyecto dotando de estos servicios al conjunto del sistema portuario y tratando de aglutinar en la misma iniciativa a todos los organismos que lo componen.

Esta forma de afrontar la contratación y provisión de servicios de ciberseguridad, que podría resultar obvia y que surge de manera natural, no lo es tanto, ya que el sistema portuario, como ya se ha comentado, está compuesto por 29 entidades (28 autoridades portuarias y Puertos del Estado), pero están todas ellas al mismo nivel orgánico, dependiendo del Ministerio de Transportes y Movilidad Sostenible, y son totalmente independientes en su gestión interna. No hay, por tanto, una relación de dependencia organizativa de las autoridades portuarias con Puertos del Estado.

El fin de este proyecto es dotar de servicios de ciberseguridad a todo el sistema, desde una plataforma común, y que la provisión de dichos servicios de forma conjunta genere sinergias y holísticas que lleven a la implantación de uno de los SOC sectoriales más importantes del país.

Esta estrategia, además, está alineada con la línea marcada por el Centro Criptológico Nacional y su exitosa implantación de la Red Nacional de SOC, que cuenta con más de 140 entidades adheridas. Nuestra iniciativa contribuirá de forma notable en la extensión de la red, integrando uno de los SOC sectoriales más extensos del país, compuesto por la totalidad de organismos que componen el sistema portuario de titularidad estatal.

La contratación conjunta para todas las entidades del sistema está motivada por varios factores. Uno de ellos es la economía de escala, aventurando mejores condiciones de contratación al hacerlo de forma conjunta que si cada organismo lo hiciera de forma independiente. Además, y teniendo en cuenta los procedimientos y normativas a los que una contratación pública ha de atenerse, la gestión de un único expediente de contratación facilitaría, al menos sobre el papel, la contratación de los servicios, que se tramitaría de una forma más ágil.

Desde un punto de vista estratégico, tener unos servicios de ciberseguridad comunes prestados bajo la misma infraestructura proporciona varias ventajas. Haciendo referencia a las de tipo holístico y sinérgico, la prestación de servicios de ciberseguridad de forma común genera un conocimiento compartido para todos los integrantes del sistema, derivado de las actuaciones que hubiera que realizar ante determinados eventos de ciberseguridad y de la propia prestación regular de los servicios, compartiendo experiencias y situaciones que se hayan dado en una autoridad portuaria y utilizando ese conocimiento para poder aplicar medidas y prevenir posibles incidencias en el resto de los integrantes del sistema.

Por otra parte, esta prestación desde una plataforma común simplifica enormemente la coordinación de actuaciones que afecten a todo el sistema portuario. Tener un único interlocutor como prestador de los servicios facilita enormemente la gestión y coordinación de actuaciones que afecten al conjunto de entidades.

Catálogo de servicios de ciberseguridad portuaria

A la hora de contratar los servicios de ciberseguridad, fue primordial diseñar un catálogo que se adaptara a las necesidades de todos los organismos adheridos. Ni que decir tiene que, en nuestro ecosistema portuario, los organismos son muy heterogéneos, y cada uno tiene unas dimensiones, necesidades y capacidades muy distintas.

No queríamos que este catálogo careciera de aquellos servicios que se consideran esenciales a efectos de ciberseguridad. Y teniendo en cuenta la naturaleza pública del sistema portuario, tampoco podíamos dejar de lado aquellos servicios relacionados con el cumplimento normativo que tienen un componente tecnológico importante.

Además, evidentemente, está el componente presupuestario, que no hay que obviarlo por lo que ya se ha comentado: no todos los organismos tienen la misma capacidad y recursos. El catálogo de servicios diseñado está dividido, por un lado, en una colección de servicios principales que se proporcionarán a todas las entidades adheridas; y por otro, en una colección de servicios opcionales para aquellos organismos que los requieran.

Los servicios principales incluidos en el catálogo son:

- Gestión de eventos e incidentes de seguridad, que comprende las tareas de monitorización de servicios y sistemas y detección, notificación y respuesta de incidentes.
- Servicio de alerta temprana.
- Adecuación al Esquema Nacional de Seguridad.
- Detección, análisis y gestión de vulnerabilidades.
- Gestión de crisis y desastres.
- Campañas de sensibilización, concienciación, formación y ejercicios.

El catálogo de **servicios opcionales** está compuesto, por su parte, por:

- Servicio de vigilancia digital.
- Plan director de seguridad y asesoramiento.
- Gobierno de la seguridad.

Afrontar un proyecto de estas dimensiones supone un gran reto institucional. Diseñar un ecosistema de ciberseguridad portuaria con garantías de éxito pasa por que todos sus integrantes se sumen a la iniciativa. En este sentido, la implicación a nivel ejecutivo y de alta dirección es absolutamente imprescindible, y es justo agradecer a la Secretaría General de Puertos del Estado y a su titular, Álvaro Sánchez Manzanares, la implicación y esfuerzo realizado durante todo el proceso previo a la contratación. Ambos han proporcionado las garantías necesarias para cosechar el éxito que finalmente hemos obtenido al conseguir que el cien por cien del sistema portuario se sume a esta iniciativa.

Día 0

Después de un largo proceso administrativo, el proyecto echó a rodar a principios de septiembre de 2023. A día de hoy, ya hay algunos servicios plenamente implementados y funcionando en la mayoría de los organismos portuarios, implantando de forma gradual el resto de los servicios a lo largo de los dos años de duración del contrato.

Evidentemente, los servicios de ciberseguridad han venido para quedarse, y esta primera experiencia de SOC sectorial portuario nos servirá para afinar la contratación en futuras ocasiones. El catálogo de servicios se podrá revisar para incluir aquellos que quedaron fuera del ámbito del contrato, replantear servicios incluidos después de evaluar los datos de prestación y seguimiento o incorporar los que se deriven de la adaptación a nueva normativa que surja en los próximos años.

Esta primera iteración de SOC sectorial para el sistema portuario es un reto personal enorme. Se podría decir que es uno de esos proyectos que marcan la trayectoria

profesional de una persona. Con esa ilusión lo afrontamos todos los que componemos el Área TIC de Puertos del Estado y los compañeros de las autoridades portuarias, sumando nuestro granito de arena a ese marco de ciberseguridad global desde nuestro sector.

Equipo de desarrollo y proveedores

El diseño del proyecto y elaboración del pliego de prescripciones técnicas se llevó a cabo de forma conjunta por personal del Área TIC y del Área de Contratación de Puertos del Estado. La adjudicación del contrato se llevó a cabo a través de licitación pública, cuya oferta ganadora fue la presentada por la empresa GMV Soluciones Globales Internet S.A.U. Por parte de Puertos del Estado, el responsable del contrato es José Manuel Cabrera, Jefe de Departamento de Ciberseguridad, Comunicaciones y Aplicaciones Corporativas.

Valoración económica y plazos de cumplimiento

La firma del contrato para la ejecución del proyecto se realizó en septiembre de 2023 con la empresa GMV, con el siguiente desglose económico y plazos de ejecución:

- Contrato inicial de 2 años por una cuantía de 3.700.000€ (sin IVA)
- Posibilidad de 3 prórrogas anuales por una cuantía de 1.850.000€ (sin IVA) cada una

Por lo tanto, suponiendo la aplicación de las 3 prórrogas previstas, la duración del contrato sería de 5 años por un total de 9.250.000€ (sin IVA).

CABRERA LOPEZ JOSE MANUEL - DNI 28957811Y

Firmado digitalmente por CABRERA LOPEZ JOSE MANUEL - DNI 28957811Y
Fecha: 2024.01.12 12:23:50 +01'00'