



Financiado por
la Unión Europea
NextGenerationEU



ANEXO XXVI: SOBRE 2

Presentación de propuestas

Mixto de suministro y servicios asociados de plataforma de monitorización, y de servicios recurrentes y bajo demanda, para apoyo al Centro de Operaciones de Seguridad de la Junta de Andalucía (AndalucíaCERT) – Lote 2

EXPTE. CONTR. 2023/642838





Junta de Andalucía



**Financiado por
la Unión Europea**
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

0. INSTRUCCIONES.....	3
1. SERVICIOS RECURRENTE.....	4
1.1. <i>Cumplimiento de requisitos</i>	4
1.2. <i>Valoración general de los servicios recurrentes</i>	33
2. SERVICIOS BAJO DEMANDA.....	34
3. PLAN DE EJECUCIÓN DEL PROYECTO.....	35

0. INSTRUCCIONES

Con carácter general, la información presentada deberá estar estructurada de forma clara y concisa. La propuesta será autocontenida y no contendrá referencias a anexos, documentos o enlaces externos.

Cualquier referencia que se haga a características o prestaciones de los suministros y licencias y que esté basada en módulos o licencias adicionales del producto se considerará incluida en la oferta sin coste adicional, a menos que explícitamente se indique lo contrario.

Con respecto a los catálogos específicos de los productos, sólo se analizarán aquellos apartados referenciados de forma explícita en el cuerpo de la memoria técnica.

La proposición técnica de los licitadores deberá contener la documentación necesaria en formato digital para poder valorarla, con una extensión máxima equivalente a 150 páginas (incluida toda la documentación gráfica y catálogos específicos), con fuente no inferior a Arial 12 puntos, e interlineado sencillo. La portada de este documento, el índice e instrucciones no serán contabilizadas en el cómputo total.

Toda la documentación de la oferta deberá ser presentada en los siguientes formatos electrónicos:

- Formato editable ISO/IEC 26300 (formato OpenDocument de OASIS).
- Formato no editable para su preservación a largo plazo ISO 19005-1:2005 (PDF/A-1).

Deberá observarse la máxima diligencia a la hora de elaborar la documentación del sobre 2 para que no incluya ninguna información a valorar mediante criterios objetivos del sobre 3 ya que dicho error podría llegar a ser motivo de exclusión del procedimiento.

Para el apartado “1. SERVICIOS RECURRENTE”, los licitadores indicarán en la tabla que se acompaña en el apartado “1.1. Cumplimiento de requisitos” el mecanismo y forma en que su solución propuesta da cumplimiento a los requisitos enumerados del Sobre 2, es decir, no será suficiente con la mera indicación de que se cumple el requisito, sino que será necesario exponer cómo. El requisito VAL-SVREC-1, para el que hay un subapartado específico con indicaciones, se desarrollará en el apartado “1.2. Valoración general de los servicios recurrentes”, fuera de esta tabla.

Para los apartados “2. SERVICIOS BAJO DEMANDA” y “3. PLAN DE EJECUCIÓN DEL PROYECTO”, los licitadores desarrollarán los apartados 2 y 3 de este documento, respetando las instrucciones dadas en cuanto a tamaño de letras, interlineado y cómputo global de 150 páginas para toda la propuesta de documentación correspondiente al SOBRE 2.

1. SERVICIOS RECURRENTE

1.1. Cumplimiento de requisitos

Requisito	Descripción de requisito según PPT	Descripción de cumplimiento	Sobre 2	Sobre 3
VAL-SVREC-1	<p>Se valorará con carácter general la idoneidad, calidad y flexibilidad de la arquitectura de los servicios recurrentes propuestos y cómo estos dan cumplimiento a los requisitos enumerados.</p> <p><i>Véase el apartado “Valoración general de los servicios recurrentes”.</i></p>		X	
REQ-ATV-1	<p>Será un servicio prestado de manera no intrusiva que se basará en una herramienta puesta por el adjudicatario a disposición de la Junta de Andalucía y que se acompañará en su caso del equipamiento y servicios necesarios para constituir una plataforma de inventariado, contraste y alerta de vulnerabilidades que será denominada en este apartado “la Plataforma”.</p>		X	



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-ATV-2	Dicha herramienta deberá ofrecer soporte para multitenant, permitiendo crear un entorno independiente para cada organismo del Grupo Atendido de AndalucíaCERT. El número inicial de tenants se estima en 85, debiendo garantizarse el correcto funcionamiento de esta Plataforma para al menos 120.		X	
REQ-ATV-3	<p>Deberá ser posible crear como mínimo los dos tipos de cuentas siguientes:</p> <ul style="list-style-type: none"> • Cuentas con acceso a solo uno de los entornos (tenant) definidos y la información contenida en este, para su uso por el correspondiente organismo. Para cada entorno deberá ser posible crear como mínimo 3 cuentas de este tipo. • Cuentas con acceso a todos los entornos definidos, para permitir realizar una gestión global centralizada. Deberá ser posible crear como mínimo cinco cuentas de este tipo. 		X	
REQ-ATV-4	Cada tenant deberá disponer de mecanismos que le permitan la introducción y el almacenamiento de la información detallada de inventario de todos los productos TIC del correspondiente organismo, incluyendo empresa fabricante o desarrolladora, nombre de producto,		X	



	<p>modelos, versiones y otros datos relevantes, incluyendo identificación <i>Common Platform Enumeration</i> (CPE). Estos mecanismos deberán garantizar la posibilidad de introducir la mencionada información de todas las siguientes formas:</p> <ul style="list-style-type: none"> • Masiva, a partir de un fichero en formato normalizado (por ejemplo, CSV). • Interactiva, para realizar altas, bajas y modificaciones. <p>En caso de que las herramientas utilizadas no proporcionaran alguna de estas funcionalidades, esta carencia deberá ser suplida por el adjudicatario, que deberá:</p> <ul style="list-style-type: none"> • Poner un sistema de realización de peticiones de servicio a disposición de AndalucíaCERT y de los organismos de su grupo atendido y mediante el cual se realizarán las peticiones de altas, bajas y modificaciones conforme a un modelo normalizado de petición, cuando esta afecte a un único activo, o a un formato normalizado de archivo, en otro caso. • Atender las peticiones de servicio, llevando a cabo las operaciones solicitadas, conforme a los acuerdos de nivel de servicio y con sujeción a 			
--	---	--	--	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-ATV-5	<p>Por otro lado, la herramienta recogerá de forma continuada información relevante de seguridad de diversas fuentes nacionales e internacionales, tanto gratuitas como de pago, integrándola en una base de datos completa y actualizada de vulnerabilidades.</p>		X	
REQ-ATV-6	<p>La herramienta realizará de forma automática y desatendida la confrontación de la información de inventario de activos con la almacenada en la base de datos de vulnerabilidades, produciendo una relación de posibles vulnerabilidades aplicables al organismo. En esta relación deberá constar:</p> <ul style="list-style-type: none"> • La identificación y descripción de la vulnerabilidad. • La relevancia de la vulnerabilidad según las plataformas, fabricantes y, en su caso, contexto particular de los Organismos de la Junta de Andalucía, con objeto de permitir establecer prioridades en el proceso de remediación. 		X	



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-ATV-7	<p>La plataforma se limitará a identificar de manera pasiva las vulnerabilidades que pudieran mostrar los activos/productos en función de los datos e información que los caracterizan (fabricante, modelo, versión, etc) que consten en el inventario. Debe observarse que estas características, si bien pudieran guardar algún parecido, no son las propias de un escáner de vulnerabilidades, puesto que no se realizarán análisis sustentados en escaneos de las vulnerabilidades sobre los activos TI concretos. Por idénticos motivos, también queda alejada de gestores de vulnerabilidades para activos TI concretos. No se admitirán este tipo de productos si carecen de las capacidades descritas para la identificación automática y pasiva de vulnerabilidades según la información del inventario.</p>		X	
-----------	---	--	---	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-ATV-8	<p>Para cada cuenta, la herramienta deberá permitir definir alertas automáticas que notifiquen de forma automática las posibles vulnerabilidades detectadas en los activos pertenecientes a su tenant a los que se haya suscrito o haya sido asignado. Estas alertas contendrán como mínimo la siguiente información:</p> <ul style="list-style-type: none"> • La identificación y descripción de la vulnerabilidad • La relevancia de la vulnerabilidad y sus indicadores de riesgo asociado. • Si se ha desarrollado una prueba de concepto que explote la vulnerabilidad. En este caso, se deberá ofrecer, de forma directa o indirecta, una referencia al menos a una de estas pruebas de concepto que tenga carácter representativo. • Si se ha detectado que la vulnerabilidad está siendo explotada de forma activa. • Información para eliminar la vulnerabilidad o reducir su impacto. 		X	
-----------	--	--	---	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-ATV-9	<p>La información sobre posibles vulnerabilidades existentes en los activos de cada tenant, así como la de todos los tenant para las cuentas con acceso a todo el conjunto, deberá ofrecerse a través de un servicio de publicación web en el que apliquen las medidas necesarias para garantizar la seguridad del propio servicio y de los datos almacenados.</p> <p>Correrán por cuenta del adjudicatario todos los gastos derivados de los servicios y productos software, así como del hardware y otro equipamiento incluido en la oferta, que sean necesarios para el funcionamiento de la Plataforma.</p> <p>Las ofertas deberán indicar una relación del hardware que AndalucíaCERT y su grupo atendido debe proveer, si es necesario éste, para el funcionamiento de la Plataforma, con indicación pormenorizada de los requisitos que cada elemento debe cumplir. Todo hardware que no sea incluido expresamente en esta relación o que no se atenga a los requisitos indicados deberá ser proporcionado por el adjudicatario sin que pueda imputar coste alguno por él.</p>		X	
-----------	---	--	---	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-ATV-10	Este componente del servicio se integrará con la plataforma del punto anterior, y el adjudicatario planteará un dimensionamiento (FTE) que dedicará al mismo en cada momento.		X	
REQ-ATV-11	El equipo de trabajo asociado a este componente deberá acumular conocimiento sobre AndalucíaCERT y su grupo atendido durante la prestación del servicio y aplicar este conocimiento para adecuar la información proporcionada por la plataforma de inventariado, contraste y análisis de vulnerabilidades a las necesidades de este organismo y su grupo atendido, así como complementarla con conocimiento experto.		X	



REQ-ATV-12	<p>La consultoría y asesoramiento sobre vulnerabilidades incluirá:</p> <ul style="list-style-type: none"> • Análisis del impacto de las vulnerabilidades de acuerdo con las características de los sistemas y del entorno de cada organismo y de la Junta de Andalucía. • En su caso, actualización de la información contenida en la Plataforma de inventariado, contraste y análisis de vulnerabilidades. En particular, se realizará esta actualización de acuerdo con el análisis de impacto a que hace referencia el punto anterior. • Identificación de vulnerabilidades recientes de impacto potencial alto. • Propuesta de prioridades en las actuaciones necesarias para la eliminación o minimización del riesgo asociado a las vulnerabilidades. • Entrega de información, documentos y URLs de referencia relativos a los cambios sobre los activos que sea necesario realizar para eliminar o 		X	
------------	---	--	---	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-ATV-13	<p>Con carácter general, el adjudicatario ofrecerá estos servicios de consultoría y asesoramiento de forma proactiva, prestando especial atención a las circunstancias en que su personal determine que una o varias vulnerabilidades pudieran tener un impacto significativo sobre los activos monitorizados en el ámbito de este contrato. La persona responsable del servicio podrá establecer condiciones concretas en las que se deberá aplicar este punto, sin perjuicio de las situaciones en que el adjudicatario lo considere oportuno a iniciativa propia.</p>		X	
REQ-ATV-14	<p>Cuando el responsable del servicio lo estime necesario, podrá remitir una consulta a la persona de contacto para este servicio con objeto de requerir el tratamiento de vulnerabilidades o circunstancias concretas.</p> <p>Tanto las consultas relacionadas con este servicio como el soporte ofrecido a los organismos se realizarán a través de AndalucíaCERT, que actuará en todo caso de intermediario entre su grupo atendido y el adjudicatario.</p>		X	



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-ATV-15	<p>El adjudicatario remitirá cada mes un informe de potenciales vulnerabilidades detectadas a cada uno de los organismos o tenants, así como un informe global a AndalucíaCERT. Se le proporcionará al adjudicatario la información de contacto necesaria para la remisión a cada tenant u organismo.</p> <p>En caso de que la información de contacto proporcionada no fuera suficiente para hacer llegar el informe a algún organismo o tenant, el adjudicatario lo hará llegar a AndalucíaCERT, indicando las causas que hicieron imposible la entrega a su destinatario.</p>		X	
VAL-ATV-1	<p>Se valorará el incremento de este dimensionamiento base. (SOBRE 3, no incluir en sobre 2).</p>			X



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-ASE-1	<p>El servicio consistirá en la identificación de los servicios pertenecientes a AndalucíaCERT y los organismos que forman su grupo atendido que se encuentren expuestos a Internet, así como en el asesoramiento para la reducción de la superficie de exposición que permita mitigar el riesgo de posibles ataques durante todo el tiempo de vigencia del contrato y sus posibles prórrogas.</p> <p>El servicio deberá ser prestado por el adjudicatario de forma deslocalizada utilizando sus propias infraestructuras o las que tenga contratadas o suscritas, así como las herramientas y los servicios gratuitos de que disponga.</p>		X	
REQ-ASE-2	<p>Como requisito mínimo, el adjudicatario utilizará escáneres con los que realizará sondeos periódicos de los activos publicados en Internet. Durante estos sondeos, basados en el direccionamiento IP, se realizará el descubrimiento, la enumeración, la identificación y la caracterización de servicios publicados.</p>		X	
REQ-ASE-3	<p>Los medios por los que se realice la identificación y caracterización de servicios incluirán como mínimo el análisis de la información proporcionada por las cabeceras (banners) de los diferentes servicios.</p>		X	



REQ-ASE-4	Los accesos a Internet y los servicios y escáneres utilizados deberán estar adecuadamente dimensionados tanto a nivel de hardware como de licenciamiento de uso para cubrir las necesidades derivadas del espacio de direcciones a monitorizar.		X	
REQ-ASE-5	<p>El adjudicatario designará una persona de referencia para este subservicio y proporcionará sus datos de contacto a la persona responsable del servicio conforme a lo indicado en el apartado “Error: no se encontró el origen de la referenciaError: no se encontró el origen de la referencia”. Esta persona y, en su caso, el resto del equipo de trabajo asociado a este servicio deberá acumular conocimiento sobre AndalucíaCERT y su grupo atendido durante la prestación del servicio y aplicar este conocimiento para:</p> <ul style="list-style-type: none"> • Proporcionar una interpretación de los datos obtenidos conforme a las necesidades y características de AndalucíaCERT y de los organismos que forman su grupo atendido. • Complementar y contrastar la información obtenida con la producida por el servicio de Alerta Temprana de Vulnerabilidades. 		X	



	<ul style="list-style-type: none"> • Realizar o proponer actualizaciones de la información obtenida en la Plataforma de Inventariado, Contraste y Análisis de Vulnerabilidades en razón de lo identificado mediante este servicio de Análisis de la Superficie de Exposición. • Proponer la realización de análisis de activos más completos y profundos, en el marco del servicio de Análisis de Vulnerabilidades, según lo identificado a través de este servicio de Análisis de la Superficie de Exposición. • Realizar recomendaciones para la reducción de la superficie de exposición y para la eliminación o mitigación de los riesgos que esta pueda suponer. 			
REQ-ASE-6	<p>Los resultados de los análisis, enriquecidos con la información proporcionada por el personal asignado al servicio, serán presentados mediante informes periódicos, conforme a lo establecido en el apartado "Entregables del Servicio de Análisis de la Superficie de Exposición en Internet".</p>		X	



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-ASE-7	<p>Adicionalmente, se pondrá a disposición de AndalucíaCERT el hospedaje de dos máquinas virtuales en la nube para labores de verificaciones y pruebas de la superficie de exposición. Para evitar suspensiones del servicio, el adjudicatario gestionará con el proveedor de alojamiento de dichas máquinas virtuales las autorizaciones para la realización de pruebas contra el rango de direccionamiento objeto del servicio. Cada una de estas máquinas virtuales en la nube deberá satisfacer los requisitos mínimos indicados en el PPT.</p> <p>El adjudicatario deberá desplegar en estas máquinas virtuales el sistema operativo y el software necesario para su funcionamiento y para realizar las operaciones de análisis.</p>		X	
VAL-ASE-1	<p>Se valorará el incremento de este dimensionamiento base. (SOBRE 3, no incluir en sobre 2).</p>			X
REQ-AVDESAT-1	<p>El adjudicatario pondrá a disposición de AndalucíaCERT y de los organismos integrantes de su grupo atendido una plataforma de análisis de vulnerabilidades web, con objeto de que puedan analizar sus aplicaciones y servicios web de manera autónoma.</p>		X	



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ- AVDESAT-2	<p>La plataforma de análisis desatendido de vulnerabilidades web será implementada sobre la infraestructura de virtualización de la que dispone AndalucíaCERT y estará basada en herramientas de seguridad de tipo proxy, opensource (como, por ejemplo, OWASP Zed Attack Proxy o Burp Suite CE) y/o comerciales (por ejemplo, Burp Suite Enterprise) así como en otros tipos de software.</p> <p>Las ofertas deberán indicar una relación del hardware que AndalucíaCERT y su grupo atendido debe proveer para el funcionamiento de este subservicio, con indicación pormenorizada de los requisitos que cada elemento debe cumplir. Todo hardware que fuera necesario durante la prestación del servicio que no sea incluido expresamente en esta relación o que no se atenga a los requisitos indicados deberá ser proporcionado por el adjudicatario sin que pueda imputar coste alguno por él.</p>		X	
-------------------	---	--	---	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ- AVDESAT-3	Correrá por cuenta del adjudicatario el despliegue, mantenimiento y gestión de dicha plataforma como recurso compartido de los Organismos integrantes del Grupo Atendido, de acuerdo con las directrices e instrucciones recibidas desde AndalucíaCERT, con especial atención al mecanismo de arbitraje/reserva del mismo.		X	
VAL- AVDESAT-1	Se valorará el incremento de este dimensionamiento base. (SOBRE 3, no incluir en sobre 2).			X
REQ- AVULN-1	Este subservicio consistirá en la ejecución de análisis de vulnerabilidades desde plataformas de escaneo y análisis desplegadas por el adjudicatario, en dos posibles modalidades: <ul style="list-style-type: none"> • Periódica - Automatizada (programada) • Puntual - Manual (bajo demanda) Se podrán configurar distintos procesos de análisis de vulnerabilidades, de acuerdo con sus respectivos objetivos y con las características y circunstancias de los activos involucrados. El ámbito de los análisis de vulnerabilidades incluirá, de acuerdo con la configuración que en cada caso se establezca, tanto las		X	



	<p>infraestructuras, redes y sistemas como las aplicaciones y servicios web.</p> <p>De forma independiente a su modalidad, programada o bajo demanda, los análisis de vulnerabilidades pertenecerán a una de las siguientes categorías:</p> <ul style="list-style-type: none">• Análisis de vulnerabilidades sobre un subconjunto de activos de especial interés designados por la Dirección del Proyecto entre los diversos activos revelados por el servicio de Análisis de la Superficie de Exposición a Internet, ejecutado desde la red pública utilizando las infraestructuras propiedad del adjudicatario o las que tenga contratadas o suscritas, así como las herramientas y los servicios gratuitos de que disponga.• Análisis de vulnerabilidades en sistemas y redes ubicadas en la Red Corporativa de la Junta de Andalucía. Para ello, el licitador deberá implementar un entorno de escaneo, que será desplegado sobre la infraestructura existente en AndalucíaCERT y/o puntos y sedes			
--	---	--	--	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

	<p>de interés estratégico en la Red Corporativa de la Junta de Andalucía. La Junta de Andalucía proporcionará el hardware necesario, corriendo en todo caso por cuenta del adjudicatario el despliegue, mantenimiento, operación y explotación de las distintas herramientas.</p> <p>Las ofertas deberán indicar, en su caso, una relación del hardware que AndalucíaCERT y su grupo atendido debe proveer para el funcionamiento de este subservicio, con indicación pormenorizada de los requisitos que cada elemento debe cumplir. Todo hardware que fuera necesario durante la prestación del servicio que no sea incluido expresamente en esta relación o que no se atenga a los requisitos indicados deberá ser proporcionado por el adjudicatario sin que pueda imputar coste alguno por él.</p> <p>El adjudicatario proporcionará los informes obtenidos como resultado de los análisis de vulnerabilidades.</p>			
VAL-AVULN-1	Se valorará que el ofertante podrá incorporar como mejora la puesta a disposición de una plataforma de gestión de		X	



	<p>vulnerabilidades vía web (SOBRE 2). Dicha herramienta sería puesta a disposición de los organismos del grupo atendido por AndalucíaCERT siendo su función la coordinación y seguimiento del ciclo de vida de las vulnerabilidades de activos que estos decidan ahí cargar, y caso de contemplarse en la oferta:</p> <ul style="list-style-type: none"> • Podrá desplegarse sobre la infraestructura hardware propia de la Junta de Andalucía (onprem) o en nube. • Soportará multi-tenant, con un entorno por cada Organismo del Grupo Atendido de AndalucíaCERT y, posibilidad de disponer de varios usuarios con distintos roles por cada uno. Se estima un máximo de 85 entornos/tenants. • Permitirá la importación de ficheros de auditoría de las principales herramientas de auditoría/análisis de vulnerabilidades del mercado. • Se encontrará disponible 24x7. 			
--	---	--	--	--

Caso de ofertarse, el adjudicatario deberá



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

VAL-AVULN-2	Se valorará el incremento de este dimensionamiento base. (SOBRE 3, no incluir en sobre 2).			X
REQ-VDIG-INTEL-1	La vigilancia digital se realizará sobre activos de distintos tipos: nombres de organismo o marcas., dominios, direccionamientos IP, términos específicos (palabras claves), aplicaciones para dispositivos móviles, aplicaciones y servicios web, cuentas de acceso...		X	
REQ-VDIG-INTEL-2	El número mínimo estimado de objetivos a incluir inicialmente en esta lista es de 200.		X	
VAL-VDIG-INTEL-1	Se valorará el incremento de este dimensionamiento base. (SOBRE 3, no incluir en sobre 2).			X



REQ-VDIG- INTEL-3	<ul style="list-style-type: none"> • El personal asignado por adjudicatario a este servicio utilizará un conjunto de fuentes de información que serán monitorizadas en tiempo real con el alcance necesario para la prestación del servicio. Las fuentes cubrirán las siguientes tipologías: • Fuentes abiertas. • Fuentes de acceso restringido. • Fuentes que requieren inteligencia humana, como canales de Telegram, participación en foros, webs en la Dark Web (Tor, Freenet, I2P, ...), etc. • Redes sociales, foros, blogs y comunidades • Sitios de pastes, de defacement y reivindicación de acciones de hacking. • Repositorios públicos de código fuente (Github...). • Feeds de transparencia de certificados, sitios web que monitorizan suplantaciones de typosquatting. • Sitios relativos a fugas de información 		X	
----------------------	--	--	---	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-VDIG-INTEL-4	<p>Las fuentes usadas deberán permitir la detección, identificación y recopilación de información relativa a:</p> <ul style="list-style-type: none"> • Ataques potenciales o en preparación: Hacktivismo, campañas de malware, amenazas directas, etc. • Intrusiones y vulneraciones de la seguridad. • Vulnerabilidades detectadas por terceros. • Filtraciones de datos: Fugas de información, publicación de credenciales robadas, etc. • Posibles fraudes online. • Presencia de aplicaciones maliciosas o fraudulentas. • Suplantaciones de identidad. • Dominios y webs fraudulentas • Noticias falsas con implicaciones tecnológicas referidas a la Junta de Andalucía y sus organismos o al grupo atendido de AndalucíaCERT, que tengan especial repercusión y 		X	
------------------	---	--	---	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

	<p>puedan afectar a la seguridad de los sistemas. No se incluirán en este punto aquellas noticias falsas cuyas repercusiones sean meramente políticas o de imagen corporativa salvo cuando pudieran tener un impacto negativo sobre los activos TIC de la Junta de Andalucía o al grupo atendido de AndalucíaCERT.</p> <ul style="list-style-type: none">• Etc.			
--	---	--	--	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-VDIG-INTEL-5	<p>Ante la detección de una posible amenaza, se deberá enviar de forma inmediata una alerta a AndalucíaCERT, ya sea de forma automática a través de las herramientas usadas por el adjudicatario o de forma manual por parte del equipo de trabajo asignado al servicio. El contenido mínimo de dicha alerta será:</p> <ul style="list-style-type: none"> • Resumen y análisis de la información encontrada. • Justificación de la alerta. • Contexto de la alerta con enlaces, referencias a casos precedentes y cualquier otra información relevante. • Análisis del impacto y posibles consecuencias. 		X	
REQ-VDIG-INTEL-6	<p>El adjudicatario remitirá con periodicidad mensual un informe con el contenido mínimo establecido en el apartado "Entregables".</p>		X	



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-VDIG-INTEL-7	<p>El adjudicatario deberá también proporcionar, durante todo el período de vigencia del contrato y sus posibles prórrogas, al menos una cuenta con acceso completo y, cuando exista la opción, sin publicidad a cada una de las siguientes plataformas, así como a cualesquiera otras que se indique en su oferta para una mejor prestación del servicio:</p> <ul style="list-style-type: none"> • Shodan.io (Small Bussiness) • Censys.io • Pastebin 		X	
VAL-VDIG-INTEL-2	Se valorará que, además de los entregables definidos, se disponga por AndalucíaCERT de acceso a la herramienta subyacente al Subservicio de vigilancia digital.		X	
VAL-VDIG-INTEL-3	Se valorará la disponibilidad de APIs para la explotación e integración del Subservicio de vigilancia digital.		X	
REQ-VDIG-INTEL-8	Este servicio proporcionará información actualizada acerca del contexto y las tendencias en materia de ciberseguridad, contemplando las amenazas, los actores, las campañas de ciberataque y cualquier otro aspecto que contribuya a establecer mecanismos de Prevención, Detección y Respuesta realistas y efectivos.		X	



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-VDIG-INTEL-9	El adjudicatario utilizará una serie de herramientas y servicios de consulta y recopilación de indicadores de compromiso y amenazas de seguridad, consolidando la información procedente de diferentes fuentes para componer una imagen clara y consistente del estado y las tendencias de la ciberseguridad en los ámbitos nacional e internacional, así como en el de las administraciones públicas, las infraestructuras críticas y los servicios públicos a nivel nacional.		X	
REQ-VDIG-INTEL-10	<p>Las fuentes de las que se extraerá la información incluirán:</p> <ul style="list-style-type: none"> • Fuentes internas de que disponga el adjudicatario. • Fuentes formales externas, como: <ul style="list-style-type: none"> ○ Informes y servicios de fabricantes de tecnología TIC y proveedores de servicios. ○ Servicios de alertas tempranas de seguridad. ○ Información procedente de otros CERTS y SOCs. ○ Sistemas y herramientas de 		X	

	<p>reputación de dominios, direcciones IP y URLs.</p> <ul style="list-style-type: none"> ○ Etc. ● Fuentes no formales externas, que en algunos casos podrán requerir actividades de inteligencia humana (HUMINT) <ul style="list-style-type: none"> ○ Uso de técnicas de OSINT. ○ Monitorización de foros y otros entornos y herramientas de intercambio de mensajes. ○ Monitorización de sitios y servicios de intercambio de información (Pastebin y similares). ○ Monitorización de sitios y servicios en la Web, la Deep Web y la Dark Web. ○ Etc. <p>Cabe destacar que ya se tiene acceso a la herramienta REYES del CCN-CERT, por tanto, las propuestas técnicas deberán tener en cuenta las fuentes de inteligencia integradas en esta herramienta para no ofrecerlas de forma redundante.</p>			
--	---	--	--	--



Junta de Andalucía



Financiado por
la Unión Europea
NextGenerationEU

AGENCIA DIGITAL DE ANDALUCÍA
Dirección General de Estrategia Digital

REQ-VDIG- INTEL-11	El personal asignado a este servicio por el adjudicatario analizará la información procedente de las distintas fuentes y generará los informes contemplados en el apartado "Entregables del Servicio de Inteligencias de Amenazas".		X	
REQ-VDIG- INTEL-12	Asimismo, cuando como resultado de este trabajo se detecten o determinen circunstancias que incrementen el nivel de riesgo para AndalucíaCERT o los organismos de su grupo atendido, se realizará de forma inmediata la correspondiente notificación a través de los medios de contacto proporcionados a tal efecto.		X	
VAL-VDIG- INTEL-4	Se valorará que, además de los entregables definidos, se disponga por AndalucíaCERT de acceso a la herramienta subyacente al Subservicio de inteligencia de amenazas.		X	
VAL-VDIG- INTEL-5	Se valorará la disponibilidad de APIs para la explotación e integración del subservicio de inteligencia de amenazas.		X	

1.2. Valoración general de los servicios recurrentes

Las ofertas deberán incluir la siguiente información, que será objeto de consideración y valoración con en el proceso de selección de adjudicatario para el presente Lote:

- En general:
 - Herramientas y servicios que utilizará el adjudicatario para prestar los servicios.
 - Si, además de proporcionar los informes periódicos correspondientes, se facilitará el acceso directo a los servicios y las herramientas de escaneo. En su caso, las condiciones en que se ofrecerá este acceso directo (número de cuentas, limitaciones de uso...).
 - Indicar si será posible acceder a la información contenida en los informes periódicos mediante una consola o escritorio virtual (dashboard) que permita realizar ordenación y filtrado de los datos por distintos criterios (dirección IP, servicio, protocolo, versiones, etc.). En su caso, descripción general de las opciones disponibles en este escritorio virtual, así como las condiciones en que se ofrecerá el acceso y las limitaciones aplicables.
 - Indicar si es posible acceder a la información contenida en los informes periódicos mediante APIs que la proporcionen en formatos estructurados.
 - Capacidades adicionales de integración de las herramientas (APIs de control, de recogida de datos o de suministro de resultados).
 - Capacidades de integración de las plataformas con autenticación LDAP/Active Directory, y restricciones de las mismas.
 - El número de personas que atenderán los servicios, con indicación para cada una de ellas de su titulación, experiencia y certificaciones mínimas, así como de cuál será su contribución a la prestación del servicio y el porcentaje del tiempo de trabajo que dedicará a él.
 - En su caso, los requisitos de equipamiento hardware, con indicación de sus características mínimas, que sea necesario desplegar por parte de AndalucíaCERT o los organismos de su grupo atendido para el funcionamiento de los servicios, detallando en cada caso si el hardware puede ser virtualizado y mediante qué software de virtualización y si será necesaria su disponibilidad de forma continuada durante todo el tiempo de prestación del servicio o si sólo lo será en momentos puntuales. En este último caso se enumerará también los intervalos temporales o las condiciones que deberán darse para que sea necesaria la disponibilidad del hardware.
- Servicio de Alerta temprana y asesoramiento sobre vulnerabilidades:
 - Herramientas de inventario TIC desde las que es posible una incorporación masiva de los datos.
 - Mecanismos de descubrimiento automático de escaneo y descubrimiento de activos que se ofrecen.
 - Si la Plataforma puede emitir notificaciones de alertas con información en formato estructurado que facilite su análisis automático.

- Las APIs que se ofrezcan para establecer la integración con otros sistemas para el procesado automático de las alertas.
- Si la Plataforma ofrece soporte para otras infraestructuras además de la TI estándar: (IoT/OT, electrónica de red, infraestructura de seguridad -- por ejemplo: cortafuegos -- y de servicio – por ejemplo: balanceadores de carga, etc.).
- Servicio de Análisis de la Superficie de Exposición en Internet
 - Las características de las máquinas virtuales en la nube para el servicio de Análisis de la Superficie de Exposición en Internet, indicando para cada una de ellas:
 - Características de las máquinas virtuales:
 - Número y tipo de CPUs, memoria RAM asignada, almacenamiento permanente disponible, ancho de banda de conexión a Internet garantizado, etc.
 - Sistema operativo con el que contará la máquina virtual, con indicación de la versión.
 - Productos software que se instalará en la máquina virtual, con indicación de las versiones y modalidades de uso cuando sean aplicables.
 - Plataforma en la nube en la que se instalará la máquina virtual.
 - Ubicación o zona geográfica de los servidores que alojarán la máquina virtual.
 - Medidas para garantizar que el proveedor de servicios en nube conoce la función de esas máquinas virtuales y no restringirá su uso.
- Servicio de Análisis de vulnerabilidades
 - La herramienta para la gestión de las reservas de la plataforma de análisis desatendido de vulnerabilidades, mantenida y gestionada por el adjudicatario, así como el procedimiento que deberá seguir el grupo atendido para solicitudes, consultas e incidencias.

Se valorará con carácter general la *idoneidad*, calidad y flexibilidad de la arquitectura de los servicios propuestos y cómo estos dan cumplimiento a los requisitos enumerados. (VAL-SVREC-1)

2. SERVICIOS BAJO DEMANDA

De forma común para todos los servicios, se reseñarán y serán objeto de valoración, cuando sea aplicable:

- Herramientas que se usarán para la prestación de los servicios. Arquitectura de despliegue de las mismas.
- Recursos humanos que dedicará a cada uno de los servicios, con indicación de su número y cualificación. Cuando un recurso humano vaya a participar en la prestación de más de un servicio se hará constar expresamente y se indicará el porcentaje de tiempo que dedicará a cada uno.
- Otros recursos que utilizará para prestar cada uno de los servicios.
- Propuesta de procedimientos para la prestación de los servicios. En todo caso, corresponderá a la persona responsable del servicio la aceptación o modificación, total o parcial, de las propuestas realizadas.

- Identificación del SOC o de los SOC's desde el que se realizarán las tareas deslocalizadas previstas en el servicio de operación de la plataforma de monitorización y enumeración de las certificaciones y membresías de dichos SOC's.

Se valorará con carácter general la idoneidad, calidad y flexibilidad de la arquitectura de los servicios propuestos y cómo estos dan cumplimiento a los requisitos enumerados. (VAL-SVDEM-1).

3. PLAN DE EJECUCIÓN DEL PROYECTO

Los licitadores deberán aportar la siguiente información:

- Las fases, subfases, hitos, subhitos y tareas/actividades propuestas.
- El detalle y desglose de las actividades y tareas necesarias que deben realizarse a lo largo del proyecto, incluyendo su duración estimada, secuencia temporal y dependencias.
- El detalle del proceso general, las actividades y las tareas a realizar en la prestación de los servicios incluidos en este lote.
- Propuesta de nuevos entregables a generar (entregables no obligatorios) durante la ejecución del proyecto, especificando para cada entregable la fase o fases del proyecto donde están previstos, o el servicio o servicios asociados.
- La planificación temporal propuesta, teniendo en cuenta la disponibilidad de los recursos y las restricciones temporales existentes.
- Metodologías técnicas, herramientas, etc. que el licitador propone utilizar para la adecuada gestión del proyecto.
- Planes propuestos para reducir los riesgos del proyecto y mecanismos para asegurar el cumplimiento de los plazos del proyecto.
- Actividades y procesos que se desarrollará para aportar mayor valor mediante la agregación y combinación de información y otros resultados proporcionados por los distintos servicios que componen el lote.
- Aseguramiento y control de la calidad, donde se aporte información relacionada con los mecanismos propuestos por la empresa licitadora para controlar y asegurar el nivel de calidad de los trabajos a realizar (medidas de control, frecuencia, criterios, etc.) y para prevenir y para corregir posibles desviaciones.
- La capacitación técnica y experiencia mínimas del personal que empleará el licitador para atender cada uno de los servicios incluidos en el lote.
- El número de recursos humanos con el que se prestará cada uno de los servicios y su modalidad de prestación del servicio (8x5, 12x5, etc.).
- El detalle de los recursos materiales a emplear en cada una de las tareas.

Los licitadores deberán aportar la siguiente información:

- La capacitación técnica y experiencia mínimas del personal que empleará el licitador para atender cada uno de los servicios incluidos en el lote.
- Las titulaciones mínimas exigidas, con indicación de la rama de conocimiento, exigidas al personal que prestará cada uno de los servicios del lote.
- Las certificaciones mínimas exigidas al personal que prestará cada uno de los servicios del

lote.

- El número de recursos humanos con el que se prestará cada uno de los servicios y su modalidad de prestación del servicio (8x5, 12x5, etc.).
- El plan de formación dirigido al personal con el que se prestará cada uno de los servicios.

Cuando para la prestación de un servicio se prevea la participación de personas con distintos perfiles profesionales, esta información se ofrecerá desglosada por servicio y perfil profesional.

Se valorará el nivel de cumplimiento respecto de los requisitos del PPT, la calidad, idoneidad, detalle y explicaciones sobre la propuesta de Plan de ejecución del proyecto. (VAL-PLANL2).

Se valorará positivamente la presentación conjunta y organizada de la información correspondiente a distintos servicios en una única plataforma que permita interrelacionar y poner en contexto los datos proporcionados por estos. (VAL-SVS-1).

Por último, se valorará la propuesta de integraciones y sinergias entre los servicios de este lote y los del lote 1. (VAL-SVS-2).

Las ofertas podrán incluir propuestas de planes de trabajo generales, prediseñados, que tendrán la misma consideración que los presentados durante la ejecución del contrato. (VAL-PLANES-TRAB-GEN).

Nota: En ningún caso la persona licitadora incluirá en la documentación del sobre número 2, referencia alguna ni documentación que deba incluirse en el sobre número 3, siendo causa de exclusión, si así lo hiciera.

