Junta de Andalucía

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

Agencia Digital de Andalucía

Consulta preliminar de mercado para la preparación de expediente de contratación de infraestructura, operación y servicios para AndalucíaCERT – Lote II – Servicios recurrentes de ciberseguridad

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

Sumario

1. Objeto de la consulta

Recabar información de los operadores económicos, especialistas en el sector, relativa a la Infraestructura, operación y servicios para AndalucíaCERT -- LOTE II – SERVICIOS RECURRENTES DE CIBERSEGURIDAD, con el fin de que la Agencia Digital de Andalucía pueda usar, si procede, la información recabada para elaborar los pliegos del próximo expediente de contratación que, en su caso, se licite al respecto.

2. Breve descripción de las necesidades

El objeto de este lote II es la prestación de servicios recurrentes enmarcados en las actividades de AndalucíaCERT. El adjudicatario, prestará, durante el tiempo de ejecución del contrato:

- Servicio de Alerta Temprana de Vulnerabilidades.
- Servicio de Análisis de la Superficie de Exposición en Internet.
- Servicio de Análisis de Vulnerabilidades.
- Servicio de Inteligencia de Amenazas.
- Servicio de Vigilancia Digital.
- Servicio de Red Team.
- Servicio de gestión de programa de Bug Bounty.

3. Servicios

3.1. Servicio de Alerta Temprana de Vulnerabilidades

Persigue la identificación de amenazas y cambios en las mismas para las diferentes plataformas TIC que conforman los sistemas de información e infraestructura TIC de la Junta de Andalucía, así como la prestación de ayuda para minimizar los riesgos asociados a estas.

Se plantean 2 subservicios:

3.1.1. Plataforma de inventariado, contraste y análisis de vulnerabilidades

Será un servicio prestado de manera no intrusiva basándose en una herramienta puesta a disposición de la Junta de Andalucía. Dicha herramienta:

- Podrá desplegarse sobre la infraestructura hardware propia de la Junta de Andalucía (on-permises) o en nube.
- Soportará multitenant, con un entorno por cada Organismo del Grupo Atendido de AndalucíaCERT y, posibilidad de disponer de varios usuarios por cada uno de ellos, separando la información sensible de cada uno de forma que solo sea visible por los usuarios del mismo entorno. Se estima un máximo de 85 entornos/tenants.
- Se encontrará disponible 24x7.

- Deberá recolectar permanentemente la información más relevante de seguridad de diversas fuentes internacionales generando una base de datos completa y actualizada de vulnerabilidades, para filtrarla según su relevancia en función de las plataformas, fabricantes y contexto particular de los Organismos de la Junta de Andalucía.
- Por cada tenant:
  - deberá permitir la introducción y almacenamiento de un inventario con los productos TI de cada Organismo y la base de información necesaria de cada uno de ellos (fabricantes, modelos, versiones, especificaciones, …). Se valorará la facilidad de importación de información de los activos desde otras herramientas de inventario TI, y de integración a través de API.
  - analizará la información del inventario de productos TI, contrastándola con la base de datos de vulnerabilidades, e identificando cuáles pueden verse afectados por alguna de ellas.
  - permitirá de manera configurable la generación de alertas automáticas a los usuarios cuando se identifiquen nuevas vulnerabilidades potenciales que pudiesen afectar a los productos TI dados de alta en su entorno/tenant. Dichas alertas no se limitarán a la emisión del aviso, sino que también contendrán información sobre cómo repararlas (existencia de parches, aplicación de configuraciones específicas, recomendaciones de fabricante, …etc). Se valorará que las alertas estén estructuradas para su análisis automático, y que sean accesibles a través de API.
- Se valorará que la herramienta no se limite a infraestructura TI estándar (servidores de aplicación, de base de datos, sistemas operativos...) sino que incluya elementos adicionales (IoT/OT, electrónica de red, infraestructura de seguridad – cortafuegos, por ejemplo-- y de servicio – balanceadores de carga, por ejemplo--…).

Modelo económico estimado

Cuota mensual de servicio, en función de número de tenants/número de activos distintos/otros conceptos. Ampliable.

3.1.2. Consultoría y asesoramiento en Amenazas

Adicionalmente al servicio desatendido que proporcionará la herramienta descrita en el punto anterior, el adjudicatario deberá complementarlo con servicios de Asesoramiento a nivel consultivo, prestando soporte a través de AndalucíaCERT a los Organismos para implementar los cambios necesarios en sus activos protegidos, colaborando de este modo a minimizar el riesgo de un ataque que aproveche una vulnerabilidad emergente conocida.

Las consultas y solicitudes relacionadas con este servicio serían canalizadas a través de AndalucíaCERT.

Modelo económico estimado

Cuota mensual de servicio fija.

3.2. Servicio de Análisis de la Superficie de Exposición en Internet

El servicio tiene como objetivo la identificación de los servicios expuestos a Internet de la Junta de Andalucía, así como la reducción de la superficie de exposición para mitigar el riesgo de posibles ataques durante todo el tiempo de vigencia del contrato.

Dada la naturaleza externa a la Red Corporativa de la Junta de Andalucía de estos análisis, el servicio deberá prestarse de manera deslocalizada haciendo uso de accesos de datos a Internet y escáneres con capacidad suficiente (ya sea a nivel de hardware y/o licenciamiento).

Estos escáneres deberán ser capaces de ejecutar sondeos periódicos de los activos publicados en Internet desde la Red Corporativa de la Junta de Andalucía en base a su direccionamiento IP, que permitan la enumeración, identificación y caracterización (p.e. basado en información de banners) de los diferentes servicios publicados descubiertos.

A título informativo y a efectos de estimar las necesidades iniciales del servicio, el direccionamiento objetivo estará conformado inicialmente por 8.192 IPs públicas.

Si bien se valorará positivamente que se facilite el acceso a AndalucíaCERT a las herramientas de escaneo, como mínimo el adjudicatario deberá poner a disposición de AndalucíaCERT informes con periodicidad quincenal, donde no solo se recoja el listado/inventario actualizado de los servicios descubiertos accesibles desde Internet en ese momento, sino que se evalúen y caractericen riesgo y vulnerabilidades asociados a los mismos, así como recomendaciones al respecto para su mitigación/corrección en cada caso. Se valorará la accesibilidad de esta información mediante API de forma estructurada.

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, se gestionarán con el proveedor de alojamiento a dichas máquinas virtuales las autorizaciones para la realización de pruebas contra el rango de direccionamiento objeto del servicio.

Modelo económico estimado

Cuota mensual de servicio fija, con ampliación opcional por tramos.

3.3. Servicio de Análisis de vulnerabilidades

Facilitará las capacidades técnicas necesarias para el descubrimiento y análisis de vulnerabilidades de seguridad en las infraestructuras TIC, aplicaciones y servicios de la Junta de Andalucía. Para ello se apoyará en 3 subservicios:

3.3.1. Servicio atendido de Análisis de vulnerabilidades

Ante cada solicitud recibida desde AndalucíaCERT para el análisis de unos activos dados, el servicio proporcionará soporte a la gestión completa del ciclo de vida de las vulnerabilidades, contemplando la planificación y ejecución de las actividades de identificación, el análisis de resultados, la notificación y reporte correspondiente, para su evaluación, priorización y definición de acciones de remediación por

parte de AndalucíaCERT, así como el seguimiento de las acciones correctivas definidas con el Organismo del grupo atendido titular de los activos afectados en caso de así requerirse.

Por consiguiente, dada una petición de servicio sobre una serie de activos objeto de análisis, el servicio deberá cubrir los siguientes requisitos mínimos:

- Elaborar el inventario de los activos en cuestión y catalogar los mismos, permitiendo así un control posterior de las vulnerabilidades que afectan a cada activo y su configuración de seguridad.
- Identificar las principales fuentes de información y clasificación de vulnerabilidades en base a los activos instalados en Junta de Andalucía, siguiendo las referencias de vulnerabilidades publicadas por CVE (Common Vulnerabilities and Exposures).
- Planificar y ejecutar los análisis de vulnerabilidades, tanto de infraestructura como de sitios web, según las franjas horarias y restricciones trasladadas desde AndalucíaCERT.
- Evaluar y validar los resultados obtenidos, en base a los activos y servicios descubiertos y vulnerabilidades detectadas.
- Notificar los resultados para su seguimiento y gestión por parte de AndalucíaCERT.
- Facilitar un soporte técnico experto para la mejor comprensión del impacto de las vulnerabilidades detectadas, su priorización y la definición de plan de acción por parte de AndalucíaCERT.

A efecto meramente indicativo, se estima que el número de peticiones de análisis de vulnerabilidades a demanda para atender será de 10 solicitudes/mes. En todo caso, el adjudicatario deberá dar cobertura a la totalidad de las solicitudes que se tramiten desde AndalucíaCERT.

Para ello el servicio deberá apoyarse en diversas herramientas de escaneo de vulnerabilidades, marcándose como requisito mínimo el software comercial:

- Nessus
- Acunetix
- Otros, a definir por el ofertante para una mejor prestación del servicio

debiendo encontrarse incluidos en el servicio el suministro y gestión de las licencias comerciales que puedan ser necesarias para su utilización en el entorno de interés.

El servicio deberá contemplar la implementación de un entorno central principal de escaneo desplegado sobre la plataforma de virtualización existente en AndalucíaCERT, así como el despliegue de HASTA 5 sondas/escáneres remotos en distintos puntos y sedes de la Red Corporativa de la Junta de Andalucía para el análisis en profundidad de otros segmentos de red/sistemas. La Junta de Andalucía dispondrá el hardware necesario en cada ubicación remota para ello, corriendo por cuenta del adjudicatario el despliegue, mantenimiento, operación y explotación de las distintas herramientas.

Modelo económico estimado

Cuota mensual de servicio fija.

3.3.2. Servicio desatendido de Análisis de vulnerabilidades Web

Se podrá a disposición del grupo atendido por AndalucíaCERT un servicio de análisis desatendido de vulnerabilidades web con objeto de que puedan analizar sus aplicativos de manera autónoma.

Para ello el adjudicatario deberá implementar sobre infraestructura de virtualización existente de AndalucíaCERT una plataforma central de escaneo de vulnerabilidades web basada en herramientas de seguridad de tipo proxy, ya sean opensource (p.e. OWASP Zed Attack Proxy, Burp Suite CE, …) y/o comerciales (p.e. Burp Suite Enterprise).

Correrá por cuenta del adjudicatario el despliegue, mantenimiento, operación y explotación 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.

Modelo económico estimado

Cuota mensual de servicio fija.

3.3.3. Servicio autónomo de Análisis de vulnerabilidades

La plataforma de escaneo que se despliegue para la prestación del servicio debe permitir la ejecución periódica de escaneos de vulnerabilidades de manera automatizada.

Uno de estos escaneos recurrentes a realizar será sobre la superficie expuesta a Internet descubierta en el servicio anterior (ver apartado 3.2.), si bien se contemplará igualmente la posibilidad de realización de los mismos sobre otras infraestructuras internas a la Red Corporativa de la Junta de Andalucía (p.e.. direccionamientos de CPDs concretos de Organismos del grupo atendido).

A título orientativo, y a efectos del dimensionamiento inicial del servicio, se estiman necesarios contemplar para este servicio escaneos de vulnerabilidades autónomos para 1.000 IPs y 100 URLs.

Modelo económico estimado

Cuota mensual de servicio fija, con ampliación opcional por tramos (mayor número de IPs o de URLs).

3.4. Servicio de Inteligencia de Amenazas

El servicio pretende complementar las capacidades de consulta y enriquecimiento de la información de seguridad y contexto de AndalucíaCERT en su operación diaria.

Se deberá poner a disposición de AndalucíaCERT una serie de herramientas y servicios (propios y de terceros) de consulta y recopilación de indicadores de compromiso, amenazas de seguridad publicadas por fuentes externas (fabricantes de tecnología TIC, proveedores de servicios, servicios de alertas tempranas de seguridad, otros CERTS, etc.), feeds de reputación de dominios/IP/URLs, repositorios OSINT…

Dado que AndalucíaCERT tiene acceso a REYES, del CCN-CERT, y ésta ya integra inteligencia proveniente de distintas fuentes, a la hora de elaborar la propuesta técnica se deberá prestar especial atención a no redundar estas en la oferta.

Deberá contemplarse, al menos, la puesta a disposición durante todo el período de vigencia del contrato) de membresías en las siguientes plataformas:

- Shodan.io (Small Bussiness)
- Censys.io
- Pastebin
- Otras a proponer por el ofertante para una mejor prestación del servicio

Correrá por cuenta del adjudicatario el suministro y gestión de las licencias comerciales o de servicios de terceros que puedan ser necesarias para la prestación del servicio.

Modelo económico estimado

Cuota mensual de servicio fija.

3.5. Servicio de Vigilancia Digital

El servicio de vigilancia digital e identificación de amenazas deberá prestarse como una solución integral dirigida a la detección temprana de posibles amenazas de seguridad desde la perspectiva de una visión externa ajena a la Junta de Andalucía.

Objetivos

Se contempla una monitorización continua en tiempo real estimada de 100 objetivos. Dichos objetivos serán establecidos al inicio del servicio, pudiendo estos ser:

- Nombre de Organismo/marca
- Dominios
- Direccionamiento IP
- Términos específicos
- Aplicaciones móviles
- …, etc

AndalucíaCERT realizará una propuesta inicial de objetivos. El adjudicatario completará y mantendrá actualizada dicha propuesta en base a su experiencia y conocimiento y de acuerdo a los casos de uso de aplicación. Igualmente, AndalucíaCERT podrá solicitar altas/bajas de objetivos a vigilar durante todo el período de duración del contrato.

Fuentes

El licitador deberá presentar un listado exhaustivo de fuentes que serán monitorizadas dentro del alcance del servicio, debiendo contemplarse 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.

Alcance

Dicho listado de objetivos será actualizado a lo largo de la ejecución del servicio y deberá al menos permitir identificar y recolectar información sobre:

- Detección de ataques potenciales: Hacktivismo, campañas de malware, amenazas directas realizadas, …
- Filtración de datos: Fugas de información, credenciales, ….
- Posibles fraudes online, presencia de app's maliciosas, …
- Dominios y webs fraudulentas
- Posibles noticias falsas con implicaciones tecnológicas (no políticas) en nombre de la Junta de Andalucía que estén teniendo especial repercusión y que pueden tener consecuencias negativas para los públicos objetivo de esta.
- Etc

Generación de alertas

Ya sea de manera automatizada en base a las herramientas de trabajo, o bien de manera manual por el propio equipo de trabajo asignado al servicio, se deberán generar alertas instantáneas y trasladarlas a AndalucíaCERT. Dichas alertas tendrán como mínimo la siguiente información:

- Resumen de la información encontrada y análisis de la misma.
- Justificación de la alerta y un análisis del impacto y de las posibles consecuencias de esta información, que deberá estar contextualizada estableciendo enlaces con casos precedentes o con cualquier otra información previa que pueda estar relacionada

Generación de informes

Será preceptiva la elaboración y remisión a AndalucíaCERT de informes con periodicidad mensual que recojan el detalle de las campañas, fugas de información, aplicaciones maliciosas, y resto de amenazas detectadas durante el período.

Modelo económico estimado

En el plano económico se deberá aportar un modelo de costes mensual del servicio medido en bloques/saltos de 10 objetivos sobre los que se preste el servicio.

3.6. Servicio de Red Team

Como parte de la mejora de la defensa activa y resiliencia de la ciberseguridad, y para poder evaluar la preparación y capacidades de detección y respuesta en la Junta de Andalucía, se deberá prestar un servicio de Red Team que realice simulaciones de intrusiones reales y controladas sobre sus sistemas de información y comunicaciones. Tendrá como objetivos:

- Identificar vulnerabilidades en personas, procesos o tecnologías
- Evaluar las capacidades de detección, contención y respuesta ante ciberataques
- Mostrar los potenciales impactos de los ataques exitosos
- Identificar qué acciones de respuesta son efectivas en el contexto y singularidades de la Junta de Andalucía y su Red de Comunicaciones (RCJA).

El servicio deberá simular un agente externo que realice accesos no autorizados a los sistemas de información de la Junta de Andalucía, con la particularidad de que no se llegue a comprometer la operación normal de ningún Organismo.

Para ello se consensuará con la Dirección de los Servicios en la ADA una planificación por ejercicios atendiendo a diversos factores: temporalidad, naturaleza de los sistemas objetivo, capacidades de detección de AndalucíaCERT sobre los mismos, capacidad de detección/respuesta del organismo titular, …, etc.

En función de la naturaleza de los sistemas objetivo de los distintos ejercicios, cuando aplique se deberá contemplar, además de la intrusión clásica, la persistencia a lo largo del tiempo, el escalado de privilegios en sistemas corporativos y la alteración y robo de información confidencial o estratégica.

Sin entrar en el detalle en el procedimiento de prestación del servicio (que cada ofertante deberá definir en su propuesta), las campañas acciones de evaluación sobre los distintos objetivos se realizarán de la siguiente manera:

- Preparación de la campaña: definición de objetivos, elección de herramientas, documentación previa y planificación, …
- Acción técnica: período en el cual se llevan a cabo las acciones de ataque.
- Jornadas de puesta en común: donde se procederá a compartir conocimiento entre el equipo de Red Team del adjudicatario y AndalucíaCERT.
- Documentación final de la campaña, con especial atención a las lecciones aprendidas y recomendaciones a acometer, por parte de AndalucíaCERT y por el Organismo titular de los activos.

Se valorará positivamente el empleo de herramientas de emulación de adversarios, ya sean licenciadas y/o de software libre (p.e. Caldera, Infection Monkey, Atomic Red Team, Cobalt Strike, Attack-IQ, …, etc.), corriendo por cuenta del adjudicatario los costes de gestión y licenciamiento de las distintas herramientas comerciales que utilice para la prestación del servicio.

Se deberán contemplar, al menos, el abordaje de 6 campañas/objetivos anuales.

Modelo económico estimado

Cuota mensual de servicio fija.

3.7. Servicio de gestión de programa de Bug Bounty

Deberá ser prestado como servicio la gestión integral de un programa público de recompensa por reporte de errores/vulnerabilidades/amenazas (Bug Bounty) para la Junta de Andalucía a lo largo del plazo de ejecución del contrato.

El alcance del programa estará conformado por cualquier servicio o aplicativo publicado directamente en Internet por la Junta de Andalucía, o bien en repositorios públicos oficiales (p.e. Google Play, Apple Store, …).

Quedarán excluidos del programa de recompensas el personal trabajador de la empresa adjudicataria, de la administración de la Junta de Andalucía, así como toda aquella persona con vínculos personales o familiares con éstos.

El flujo de trabajo asociado a dicho servicio deberá incluir, al menos:

- Recepción, filtrado y verificación de reportes.
- Recompensa al investigador que ha reportado error/vulnerabilidad/amenaza válida.
- Notificación a AndalucíaCERT.
- A petición de AndalucíaCERT, asesoramiento técnico experto (con carácter exclusivamente consultivo) para la remediación/mitigación por parte del Organismo titular del servicio afectado.
- Publicación y actualización de las bases y condiciones del programa, Hall of Fame, …, etc, tanto hospedadas en infraestructura propia de la Junta de Andalucía, como en la(s) plataforma(s) públicas que puedan utilizarse en paralelo (p.e. Open Bug Bounty).

Modelo económico estimado

Cuota mensual de servicio fija. Gestión por la empresa de las recompensas en base a dicha cuota.

4. Acuerdos de nivel de servicio

Al menos, se está pensando introducir en la licitación el siguiente conjunto de ANS:

- Disponibilidad (software) de las plataformas
- Resolución de incidencias
- Atención a peticiones
- Respuesta a consultas

5. Dimensionamiento

En la descripción de cada servicio se incluye el dimensionamiento inicial/estimado de los servicios de cara al modelado de los mismos.

El ámbito de actuación de la posible contratación sería la Administración de la Junta de Andalucía y sus entidades instrumentales, así como los consorcios a los que se refiere el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía. Esto suma aproximadamente 85 organismos que forman el grupo atendido principal de AndalucíaCERT.

La duración del contrato sería de cuatro (4) años.