Informe sobre la Consulta Preliminar de Mercado para recabar información de los operadores económicos, especialistas en el sector, relativa a la Infraestructura, operación y servicios para AndalucíaCERT, 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

Contenido

1. Introducción....4

2. Resultado de la consulta....4

2.1. Consideraciones generales....4

2.2. Lote I....5

2.2.1. Observaciones....5

2.2.2. División en lotes....5

2.2.3. Servicios adicionales....6

2.2.4. Productos y servicios que podrían aportar poco valor o ser redundantes....6

2.2.5. Otros cambios en los servicios....6

2.2.6. Plataforma de monitorización....7

2.2.7. Otras consideraciones....9

2.2.8. Requisitos de personal....9

2.2.9. Plazos....14

2.2.10. Coste de la electrónica de red....15

2.2.11. Importes de los servicios....16

2.2.12. Modelos de facturación....20

2.3. Lote II....20

2.3.1. Observaciones realizadas....20

2.3.2. Herramientas....21

2.3.3. Guías, estándares, buenas prácticas y certificaciones....22

2.3.4. Otras consideraciones....22

2.3.5. Necesidades de personal....22

2.3.6. Requisitos exigibles al personal utilizado para la prestación de los servicios....24

2.3.7. Costes....25

2.4. Lote III....30

2.4.1. Observaciones....30

2.4.2. Otros servicios propuestos....31
2.4.3. Servicios que aportan poco valor y podrían suprimirse....32
2.4.4. Necesidad de servicios notariales en los procesos de adquisición de prueba....32
2.4.5. Necesidad de visado colegial en los informes forenses....32
2.4.6. Uso de eGarante o similar o de servicios notariales....32
2.4.7. Tiempos de asignación y desplazamiento de personal para Análisis forense / DFIR....33
2.4.8. Tiempos de certificación de evidencias....33
2.4.9. Cualificación exigible a las personas que realicen las peritaciones forenses e DFIR....34
2.4.10. Tiempos para la asignación de pentester....34
2.4.11. Cualificaciones exigibles al personal de pentesting....35
2.4.12. Informes....36
2.4.13. Análisis de malware....36
2.4.14. Ciberejercicios....37
2.4.15. Consultoría....39
2.4.16. Cualificaciones para consultoría....40
2.4.17. Respuesta in situ....42
2.4.18. Costes adicionales....43
2.4.19. Costes....44

1. Introducción

La Agencia Digital de Andalucía estudia la posibilidad de contratar suministros y servicios relativos a la infraestructura, operación y servicios de AndalucíaCERT.

Con el fin de recabar información de los operadores económicos relativa al objeto de dicha contratación y para ayudar en la posible elaboración futura de los pliegos correspondientes a un expediente de contratación, se abrió con fecha 20 de diciembre de 2022 una consulta preliminar de mercado, que puede ser accedida en la siguiente dirección:

https://www.ceh.junta-andalucia.es/haciendayadministracionpublica/apl/pdc_sirec/perfiles-licitaciones/consultas-preliminares/detalle.jsf?idExpediente=58

Este documento constituye el informe contemplado en el artículo 115.3 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.

2. Resultado de la consulta

2.1. Consideraciones generales

La consulta exponía las necesidades de suministros y de servicios de AndalucíaCERT, divididos en tres posibles lotes, y se solicitaba de los agentes participantes la remisión de un formulario por cada uno de dichos lotes con:

- Observaciones sobre la adecuación de los suministros y servicios previstos.
- Productos para la implementación del sistema de Gestión de Información y Eventos de Seguridad (SIEM – Security Information and Event Management).
- Herramientas y servicios para la operación de AndalucíaCERT.
- Herramientas y servicios con los que implementar los servicios de AndalucíaCERT.
- Características y modelos de prestación de los servicios.
- Modelos de facturación.
- Precios de los productos y servicios.

Durante el periodo entre la publicación de la consulta y el final del plazo, varias empresas contactaron por correo electrónico el Servicio de Ciberseguridad con consultas, que fueron respondidas.

Finalizado el plazo de remisión, se recibieron respuestas formales de quince empresas:

- Accenture, S.L. Sociedad Unipersonal
- Babel Sistemas de Información S.L.
- Capgemini España S.L.

- Evolutio Cloud Enabler, S.AU.
- GMV Soluciones Globales Internet, S.A.U.
- Ibermatica S.A.
- Entelgy Innotec
- Mnemo Evolution & Integration Services, S.A.
- Grupo Oesía
- PWC
- S2 Grupo de Innovación en Procesos Organizativos S.L.U.
- Grupo SIA (Sistemas Informáticos Abiertos)
- Telefónica Soluciones de Informática y Comunicaciones de España S.A.
- Viewnext S.A.
- Vodafone España, S.A.U.

Las respuestas incluyeron los cuestionarios rellenos para los distintos lotes, si bien algunas empresas sólo cumplimentaron algunos de ellos

Del análisis realizado por el Servicio de Ciberseguridad cabe extraer las conclusiones que se exponen en los siguientes apartados.

2.2. Lote I

2.2.1. Observaciones

La mayor parte de las empresas indicaron que era necesaria información adicional a la incluida en la Consulta Preliminar para poder responder a varias de las preguntas, incluyendo las orientaciones sobre precios.

Una de las empresas señaló la conveniencia de requerir a los diferentes participantes un nivel de partnership con el fabricante de la solución presentada que acredite los conocimientos necesarios para el despliegue de la tecnología y garantice la colaboración, así como que dispongan de aceleradores (activos, metodologías) específicas para la prestación de servicios de monitorización.

2.2.2. División en lotes

En algunas respuestas se propuso la unificación de los tres lotes en uno con objeto de aprovechar sinergias y optimizar la gestión.

También hubo otras en las que se alegó la imposibilidad para la empresa de ofrecer algunos de los servicios de un lote o en las que no se respondió a las preguntas referidas a algunos de los lotes.

2.2.3. Servicios adicionales

Algunas empresas propusieron la inclusión de servicios adicionales, como:

- Data Loss Prevention.
- Endpoint Protection.
- Insider Threat Program.
- Identity & Access Management.
- Privileged & Access Management.
- Cloud Security.
- Threat Hunting.
- Uso de servicios de VirusTotal.
- Uso de técnicas de Deception.
- Uso de servicios de Seguridad gestionada.

2.2.4. Productos y servicios que podrían aportar poco valor o ser redundantes

Algunas respuestas manifestaron que algunos de los productos y servicios incluidos en la consulta podrían aportar poco valor, ser redundantes o no encajar adecuadamente en la licitación:

- Administración de sistemas y redes.
- Electrónica de red.

También se indicó en uno de los casos que se consideraba que el requerimiento de integración y/o uso de diferentes soluciones de ticketing (ITSM) podría incrementar la complejidad de la prestación de los servicios, recomendando el uso de una única herramienta.

2.2.5. Otros cambios en los servicios

Algunas respuestas propusieron modificaciones en la prestación de los servicios, como:

- Dividir el servicio de Administración de sistemas y redes en dos servicios, uno para sistemas y otro para redes, por tratarse de áreas muy especializadas.
- Definir como de prestación deslocalizada, desde el SOC del proveedor, los servicios de operación de Nivel 1 y Nivel 2 de AndalucíaCERT y el Servicio Experto de la Plataforma de Monitorización.
- Definir como de prestación deslocalizada, desde el SOC del proveedor, todos los servicios incluidos en el Lote 1, con excepción de la figura de un Service Manager que actúe como punto focal la para gestión del servicio.

- Integrar los servicios de operación de la plataforma de monitorización localizado y deslocalizado y asignarle sus tareas dentro del servicio “Servicio de gestión de incidentes de seguridad de Nivel 2 (N2)”.
- Que el despliegue, gestión y operación de la infraestructura de Sensores de red y Electrónica de red sean realizados por el actual equipo de Infraestructura de comunicaciones de la ADA.
- Que el servicio Experto de la plataforma de monitorización se preste de forma deslocalizada (la propuesta incluía un SIEM en modalidad SaaS), evitando tener que incrementar el número de efectivos de este servicio en la fase 2.
- En un caso se indicó que algunas de las responsabilidades incluidas no son propias de un servicio SOC y, por lo tanto, serían derivadas a los departamentos de IT (soporte hardware, gestión de cambios, gestión de parches, aplicación de actualizaciones) y que en otras organizaciones son gestionadas por el Departamento de IT.
- En otro, se señaló que se podrían solapar los servicios de Soporte Experto de la Plataforma de Monitorización, Operación de la Plataforma de Monitorización (localizado) y Gestión de Incidentes de Seguridad de Nivel 1.

2.2.6. Plataforma de monitorización

Las distintas respuestas propusieron las siguientes soluciones SIEM:

- Microsoft Sentinel (4 respuestas)
- Splunk (5 respuestas)
- IBM Qradar (5 respuestas)
- Google Chronicle (1 respuesta)
- Gloria (1 respuesta)
- RSA NetWitness (1 respuesta)

Debe señalarse que una de las respuestas incluía varias propuestas de SIEM. Por otro lado, mientras Netwitness y Qradar, así como la propuesta de Gloria presentada, son soluciones desplegadas on premise, el resto son ofrecidas como SaaS basado en la nube. Como norma general, se puede establecer que mientras los instalados on premise presentan mayores requisitos de hardware y electrónica de red, los basados en la nube exigen un mayor ancho de banda en la conexión a Internet.

Además de esta diferencia de arquitectura, los distintos SIEMs cuentan con distintos modelos de licenciamiento que van desde la ingesta de datos al número de personas empleadas en la organización, pasando por el consumo de potencia de cálculo. La ventaja de los modelos de licenciamiento no basados en ingesta de datos es que no limitan la cantidad de datos almacenados en el SIEM.

Los precios orientativos para los distintos SIEM presentan también grandes diferencias: desde 6,6 millones hasta 14 millones de euros (para cuatro años).

En cuanto a las sondas NIDS, las diferencias de precio son también significativas, estando por debajo del millón de euros, e incluso de los 100.000 euros, en algunos casos y por encima de los 4 millones en otros. Esto viene motivado por las distintas características de los equipos propuestos.

En varias de las propuestas se evaluó el coste de la solución ejecutada en la nube frente a la equivalente alojada en instalaciones (*on-premise*), determinándose que el precio para cuatro años sería aproximadamente el mismo, ofreciendo la solución en la nube mayor flexibilidad, escalabilidad, disponibilidad y facilidad de gestión.

Varias respuestas a la Consulta Preliminar de Mercado incluyeron comentarios en los que se realizaban observaciones o se proponían características a exigir al SIEM:

- Requerir la existencia de un Marketplace para descargar apps o addons para el SIEM.
- Requerir que las sondas sean capaces de analizar el tráfico en bruto hasta capa 7 y procesar los metadatos
- Requerir que se realice en las sondas análisis de flujos.
- Requerir que las sondas dispongan de un asistente basado en Inteligencia Artificial.
- Requerir que se disponga de un SDK.
- Requerir que se soporte alta disponibilidad de forma nativa.
- Incluir capacidades de orquestación y automatización de la respuesta.
- Requerir que las sondas tengan funcionalidades IPS para mejorar la seguridad en tiempo real y que se realice una gestión centralizada.
- Requerir que las sondas tengan capacidades NDR.
- Posibilidad de complementar las sondas con capacidades de HIDS y de escaneo de vulnerabilidades de los activos de los segmentos monitorizados.
- Conveniencia de considerar que el procesado de las reglas SNORT se lleve a cabo en el SIEM y no en los NIDS.
- Conveniencia de no limitar a la capacidad de generar flujos de red de los NIDS al formato Netflow e incluir otros estándares de mercado que puedan proporcionar capacidades adicionales como Jflow, Cflow, sFlow, etc.
- Requerir el análisis de comportamiento de usuarios/as y entidades.
- Requerir la capacidad de crear modelos propios de Machine Learning.
- Requerir la realización del filtrado de eventos en destino.
- Requerir la alineación con MITRE ATT&CK.
- Necesidad de establecer el tiempo de retención de datos.

- Se indica que es difícil encontrar soluciones comerciales que incorporen la compatibilidad nativa con las herramientas del CCN-CERT.
- Se indica la posible conveniencia para la ADA de desplegar capacidades de detección de amenazas en entornos OT.

Todas las soluciones propuestas permiten la ingesta de eventos procedentes de diversas fuentes, dan soporte a la inteligencia de amenazas y, en general, se destaca en las respuestas su escalabilidad.

En algún caso se señaló que podría ser difícil encontrar una solución comercial que cumpla todos los requisitos establecidos en la consulta.

En cuanto a la certificación relativa al Esquema Nacional de Seguridad, para todos, salvo uno se indica que han obtenido o están en vías de obtener la correspondiente al nivel alto. En el caso de dicho producto se señala fecha esperada para su inclusión en la guía CCN-STIC 105..

2.2.7. Otras consideraciones

Las empresas manifestaron como sigue a distintas preguntas relativas a sus SOC, las certificaciones que han obtenido y su pertenencia a grupos. incluyendo:

- Red Nacional de SOC: 8 respuestas.
- ENS nivel alto: 4 respuestas.
- ENS nivel medio: 4 respuestas, una de las cuales señalaba que se encontraba en proceso de obtener nivel alto.
- ENS (sin indicar cuál): 2 respuestas.
- En proceso de obtención de ENS nivel alto: 1 respuesta.
- Foros de seguridad (CSIRT.es, FIRST, TI TF-CSIRT): 11 respuestas
- Además, indicaron poseer ISO 27001: 4 respuestas

2.2.8. Requisitos de personal

2.2.8.1. Dimensionamiento

En uno de los casos se propuso prestar el servicio desde el SOC del proveedor de forma totalmente deslocalizada.

En varios otros se consideró insuficiente el personal indicado en la Consulta Preliminar para la operación deslocalizada de la plataforma y se propuso realizar la operación de forma conjunta con el EDR que se encontraba próximo a ser licitado.

Se realizaron diversas propuestas de configuraciones alternativas de personal para la prestación de los servicios:

- De 5 a 6 personas para el turno de mañana de atención de Nivel 1, de 4 a 5 en horario de tarde y de 2 a 3 en horario de noche (estos últimos, trabajando tanto en el SIEM como en el EDR). Todo ello se complementaría con 4 a 5 personas para el Nivel 2.
- Otra propuesta incluyó:
    - Servicio de coordinación de actividades: 1 FTE
    - Servicio de soporte experto de la plataforma de monitorización: 1,5 FTEs para la Fase 1
    - Servicio de operación de la plataforma de monitorización (localizado): 4 FTEs para la Fase 1
    - Servicio de gestión de incidentes de seguridad de Nivel 1 (N1): 8 FTEs para la Fase 1
    - Servicio de gestión de incidentes de seguridad de Nivel 2 (N2): 3 FTEs para la Fase 1
    - Servicio de administración de sistemas y redes: 2,5 FTEs
- Una tercera consistió en:
    - Atención de Nivel 1: En modalidad 24x7x365, como mínimo 8 personas: 2 personas por turno con refuerzo por la mañana
    - Para la guardia de Nivel 2 no considera viable dedicar sólo una persona.
    - Atención de Nivel 2: En modalidad 8x5, 3-4 personas, con servicio de guardia fuera de horario no viable (2 de mañana y 1 de tarde).
    - Se añadiría 1 persona perfil de N3 en modalidad 8x5, siendo posible una dedicación del 50% para las tareas de malware engineering, forensics, etc. (ver Lote III)
- Finalmente, otra incluyó:
    - En la fase de aprovisionamiento/implantación, que conllevaría 103 jornadas para el servicio inicial, 17 jornadas para una ampliación con sede grande, 34 si la sede es mediana y 53 si es grande.:
        - 1 Consultor con dedicación del 50% (formación profesional o universitaria, con experiencia de 42 meses)
        - 1 Experto con dedicación completa (formación profesional o universitaria, con experiencia de 30 meses y dos certificaciones)
    - En la fase de operación:
        - 1 Security Manager con dedicación del 50% (formación profesional o universitaria, con experiencia de 5 años y dos certificaciones)
        - Los siguientes FTE de perfil de Experto:
            - Para el Servicio Central: 6, con desborde al SOC 24x7
            - Para sede grande: 2, con desborde al SOC 24x7

- Para sede mediana: 1, con desborde al SOC 24x7
- Para sede pequeña: 0,5, con desborde al SOC 24x7

- Para la atención a incidentes de Nivel 1: 8 FTE más uno adicional en la fase 2 en modalidad 24x7.
- Para la atención a incidentes de Nivel 2: 4 FTE más uno adicional en la fase 2 en modalidad 12x5 y guardias adicionales.

También se recomendó en algún caso que la persona encargada de la Coordinación de actividades tuviera dedicación del 100%.

Varias empresas propusieron que las guardias previstas en la Consulta Preliminar se gestionaran como un servicio y no como una asignación de un recurso humano concreto.

2.2.8.2. Características

Algunas propuestas incluyeron perfiles profesionales para la prestación de los distintos servicios.

Así, para el puesto responsable de la Coordinación de Actividades se recibieron las siguientes propuestas:

- Grado de Ingeniería o equivalente en Informática o Telecomunicaciones con 5 años de experiencia y al menos una certificación de las siguientes: CISM, CISA, CISSP, Iso 27001 L/LA.
- 5 años de experiencia y certificaciones ITIL/PMP, sin indicar titulación.
- 10 años de experiencia.
- 8 años experiencia con idioma inglés B1-C1, certificaciones CISSP/CISA/ITIL
- 4 años de experiencia, con grado universitario (asociado a IT o gestión) Recomendable máster, con certificaciones: CISM, ITIL/PRINCE2/PMP o similar, y al menos una de las siguientes certificaciones: MS-900 (Microsoft 365 Fundamentals), AZ-900 (Microsoft Azure Fundamentals) o SC-900 (Microsoft Security, Compliance, and Identity).
- 5 años de experiencia, titulación superior y certificaciones en el área de gestión.
- Una respuesta incluía dos figuras de coordinación:
    - De área de negocio: 5 años de experiencia, con grado, máster, ingeniería o ingeniería técnica y certificación en ITIL y seguridad
    - General: 10 años de experiencia, con grado, máster, ingeniería o ingeniería técnica y certificación en ITIL

Para el personal de atención de Nivel 1 se recibió las siguientes propuestas:

- FP Grado Superior en la especialidad de Informática y/o Telecomunicaciones con 1 año de experiencia y conocimientos en gestión y soporte de productos y plataformas implantadas

- Formación en la herramienta utilizada y en respuesta a incidentes
- 3 años de experiencia
- 1-3 años experiencia, con Ingeniería en Informática y similares y nivel B1 de inglés
- 2 años de experiencia, con grado universitario y certificaciones: SC-900: (Microsoft Security, Compliance, and Identity Fundamentals), SC-200 (Microsoft Certified: Security Operations Analyst Associate), QUALYS -Vulnerability Management
- 1 año de experiencia, con Formación Profesional y certificaciones en Gloria (la plataforma propuesta por la empresa)
- 1 año de experiencia en ciberseguridad
- 6 meses de experiencia y formación profesional

Y el personal de atención de Nivel 2:

- FP Grado Superior en la especialidad de Informática y/o Telecomunicaciones con 2 años de experiencia, certificación CompTIASecurity+ y conocimientos en gestión y soporte de productos y plataformas implantadas.
- 2 años de experiencia y formación en respuesta a incidentes
- Ingenieros de Ciberseguridad Sénior con más de 5 años de experiencia.
- 3-6 años experiencia, con Ingeniería en Informática y similares y nivel B1-C1 de inglés
- 3 años de experiencia, con grado universitario (asociado a IT/Seguridad) y certificaciones: SC-200 (Microsoft Certified: Security Operations Analyst Associate), AZ-500 (Microsoft Certified: Azure Security Engineer Associate), QUALYS -Vulnerability Management, CEH - Certified Ethical Hacker.
- 2 años de experiencia, con grado, máster, ingeniería o ingeniería técnica y certificaciones en Gloria (la plataforma propuesta por la empresa)
- Hubo dos respuestas que distinguían entre niveles. La primera de ella consistía en:
    - Senior: 5 años de experiencia con soluciones basadas en la herramienta o similar
    - Junior: 2-4 años de experiencia con soluciones basadas en la herramienta o similar
- Y la segunda:
    - Técnico: con 18 meses de experiencia, formación profesional o universitaria y una certificación relacionada con la materia
    - Experto: con 30 meses de experiencia, formación profesional o universitaria y dos certificaciones relacionadas con la materia

En una respuesta se propuso personal técnico de Nivel 3:

- 3 años de experiencia, con grado, máster, ingeniería o ingeniería técnica y certificaciones en Gloria (la plataforma propuesta por la empresa)

Para el servicio Experto de la Plataforma de Monitorización:

- FP Grado Superior en la especialidad de Informática y/o Telecomunicaciones con 3 años de experiencia y certificaciones CompTIASecurity+/SSCP y de los fabricantes de los productos.
- 3 años de experiencia, con formación profesional II y certificaciones en Gloria (la plataforma propuesta por la empresa)
- 5 años de experiencia y altos conocimientos de la herramienta utilizada.
- Una respuesta incluyó dos perfiles:
    - N1: 1-3 años experiencia, titulación de Ingeniería en Informática y similares, nivel de inglés B1-C1 y certificaciones en tecnologias de fabricantes
    - N2: 5 años experiencia, titulación de Ingeniería en Informática y similares, nivel de inglés B1-C1 y certificaciones en tecnologias de fabricantes
- Otra planteó tres:
    - Cloud Security Consultant: 2 años de experiencia, con grado universitario (asociado a IT/Seguridad) y certificaciones: SC-200 (Microsoft Certified: Security Operations Analyst Associate), AZ-500 (Microsoft Certified: Azure Security Engineer Associate), MS-500 (Microsoft 365 Certified: Security Administrator Associate)
    - Cloud Security Analyst: Con experiencia pero sin indicar cuánta y grado universitario.
    - SIEM Security Expert: 4 años de experiencia, con grado universitario (asociado a IT/Seguridad) y certificaciones: SC-200 (Microsoft Certified: Security Operations Analyst Associate), AZ-500 (Microsoft Certified: Azure Security Engineer Associate).

Para el servicio de administración de sistemas y redes:

- Experto en SIEM con 5 años de experiencia y certificación en la herramienta SIEM utilizada.
- 3 años de experiencia con grado, ingeniería técnica o formación profesional II y certificaciones de fabricantes
- 5 años de experiencia con entornos de virtualización, almacenamiento de virtualización, electrónica de red, cortafuegos, sistemas operativos y servidores web

Para el servicio de Operación de la Plataforma de Monitorización:

- 2 años de experiencia y formación en la herramienta SIEM utilizada.
- Una respuesta propuso utilizar dos niveles:
    - Senior: 5 años de experiencia y altos conocimientos de la herramienta utilizada.
    - Junior: 2-4 años de experiencia y altos conocimientos de la herramienta utilizada.

Para el servicio de Administración de sistemas y redes:

- FP Grado Superior en la especialidad de Informática y/o Telecomunicaciones, con conocimientos de Windows, Linux, Comunicaciones y Virtualización y certificaciones de fabricantes.
- 5 años de experiencia y certificaciones de los fabricantes

Para el servicio de formación:

- 2 años de experiencia, con grado universitario (asociado a IT/Seguridad) y certificaciones: SC-200 (Microsoft Certified: Security Operations Analyst Associate), AZ-500 (Microsoft Certified: Azure Security Engineer Associate), MS-500 (Microsoft 365 Certified: Security Administrator Associate)

Finalmente, una empresa expuso en su respuesta su modelo de carrera profesional, con tres grados de especialización:

- Grados A:1-2 años de Experiencia con Ingeniería o FP en Informática.
- Grados B: 3-5 años de Experiencia con Ingeniería o FP en Informática y certificaciones enSeguridad Defensiva, Networking, Endpoint Protection así como de Atutomatización
- Grados C: 6-10 años de Experiencia con Ingeniería o FP en Informática y certificaciones en Seguridad Defensiva-Ofensiva, Automatización nivel experto para SIEM/SOAR así como con grandes conocimientos en Inteligencia de Amenazas y respuesta ante incidentes

2.2.9. Plazos

Los tiempos de suministro y de instalación y configuración básica también presentan importantes diferencias dependiendo no sólo de si la instalación se realiza on-premise o en la nube sino de las distintas empresas.

Tiempos de suministro: oscilan entre los 0 hasta los 60 días (pasando por valores de 5, 10, 30, 45 días o hasta 6 semanas para iinstalaciones on-premise).

Tiempos de instalación y configuración básica (fase 1): oscilan entre los 15 y los 180 días.

Cabe señalar que el suministro podrá incluir elementos adicionales al SIEM (NIDS, swithces, etc.) en los casos de despliegues en la nube

2.2.10. Coste de la electrónica de red

Los precios reportados para la electrónica de red variaron significativamente:

- Precio único para adquisición, despliegue y mantenimiento: 77.478 €
- 121.355,15 €:
    - Suministro: 79.852,00
    - Servicios: 5.741,00
    - Mantenimiento: 35.762,15
- 214.486,00 €.
    - Suministro: 145000
    - Servicios: 38.772,00
    - Mantenimiento: 30.714,00
- 121.129,04 €.
    - Suministro: 103.327,40
    - Servicios: 1.423,50
    - Mantenimiento: 16.378,14
- 256.858,00 €.
    - Suministro: 161.858,00
    - Despliegue: 15.000,00
    - Mantenimiento: 80.000,00
- 274.500,00 €
    - Suministro: 225.000,00
    - Despliegue: 13.500,00
    - Mantenimiento: 36.000,00
- 23.101,63 €
    - Suministro: No lo incluye
    - Despliegue: 6.761,45

- Mantenimiento: 16.340,18

- 114.998,82 €
  - Suministro 18.000,00
  - Despliegue 13.252,34
  - Mantenimiento 83.746,48
- 319.025,79 €.
  - Suministro 265.435,72
  - Despliegue 11.540,15
  - Mantenimiento 42.049,92
- 274.500,00 €.
  - Suministro 225.000,00
  - Despliegue 13.500,00
  - Mantenimiento 36.000,00

2.2.11. Importes de los servicios

Para el servicio de Coordinación de actividades, el precio por año varió entre 50.849,28 y 264.000 €. Seis de las orientaciones pertenecían al rango 50.000 – 65.000 €:

- 50.849,28 €
- 56.953,02 €
- 57.388,25 €
- 60.000 €
- 61.811,23 €
- 65.000,00 €
- 83.616,50 €
- 120.000 €
- 196.181 €
- 219.274,82
- 264.000 € (Incluye la formación)
- 264.000 €

Para el servicio Experto de la Plataforma, los importes anuales variaron aún más: entre 28.806,37 y 480.000 €, encontrándose seis de ellos entre 90.412,80 y 186.403 €.

- 28.806,37 €
- 90.412,80 €
- 116.319,50 €
- 135.000,00 €
- 136.250,00 €
- 179.749,5€
- 186.403 €
- 201.942,11 €
- 352.000,00 €
- 352.000,00 €
- 480.000 €

Para el servicio de operación de la Plataforma (localizado), el importe por año varió entre 57.388,25 y 1.200.000 €, estando en cinco casos comprendido en el rango 356.696 - 660.000 €:

- 57.388,25 €
- 356.696 €
- 383.156,00 €
- 540.309,82 €
- 660.000 €
- 660.000 €
- 738.946,39 €
- 1.200.000 €

Para el servicio de operación de la Plataforma (deslocalizado), por año los importes variaron entre 28.036,66 y 784.060,29 €. Seis propuestas estaban en el rango 28.036,66 - 55.000 €:

- 28.036,66 €
- 37.462,50 €
- 37.500 €

- 54.500,00 €
- 55.000,00 €
- 55.000 €
- 127.951,50 €
- 720.000 €
- 784.060,29 €

Para el servicio de atención a incidentes de Nivel 1, por año, el importe varió entre 253.314 y 2.160.000 €, estando 8 propuestas en el rango 452.044,8 - 657.718,25 €:

- 253.314 €
- 452.044,8 €
- 473.065,48 €
- 504.659,73 €
- 567.000,00 €
- 594.000 €
- 594.000,00 €
- 600.000 €
- 657.718,25 €
- 1.053.669,20 €
- 2.160.000 €

Para el servicio de atención a incidentes de Nivel 2, por año, el rango de respuestas fue 69.661,50 – 960.000,00 €, con seis de ellas entre 350.000 y 436.000 €:

- 69.661,5 €
- 350.000 €
- 386.181,75 €
- 415.348,23 €
- 423.500,00 €
- 423.500 €

- 436.000,00 €
- 531.949,95 €
- 608.803,20 € (incluye aquí toda la operación de la plataforma, tanto localizada como no localizada)
- 960.000 €

Una respuesta reunió en un precio único toda la operación y atención a incidentes a un precio anual de entre 1.613.161 y 2.021.759 €

Otra agregó los servicios Experto en la Plataforma de Monitorización, Operación de la Plataforma de Monitorización (localizado) y Operación de la Plataforma de Monitorización (deslocalizado) en uno sólo que se aplica por separado a cada despliegue:

- Despliegue principal: 632.982,48/ año
- Sede pequeña: 37.254,54/ año
- Sede mediana: 62.639,70/ año
- Sede grande: 113.410,02/ año

Para el servicio de administración de sistemas y redes, por año, el rango de importes fue 90.000 - 720.000 €. Cinco de las propuestas estuvieron entre 90.000 y 149.000 €:

- 90.000 €
- 90.250,00 €
- 100.951 €
- 142.363,00 €
- 148.949,37 €
- 221.649,75 €
- 275.000 €
- 275.000,00 €
- 720.000 €

Para el servicio de Formación, para todo el tiempo del proyecto, los precios variaron de forma muy significativa: desde gratuita hasta 271.412,5 €.

- Gratis

- 8.000 €
- 11.600,00 €
- 11.601,00 €
- 15.043,05
- 25.000 €
- 40.000 €
- 41.617,96
- 96.960,00 €
- 191.748,20 €
- 143.168,38 €
- 271.412,5 €

2.2.12. Modelos de facturación

Tres respuestas propusieron que los despliegues y suministros deberían ser abonados por proyecto. Una indicaba que la facturación debería hacerse tras la recepción de petición de suministro por el proveedor. Otra, que un 50% debería ser abonado al inicio y otro 50% al final.

Una respuesta propuso una facturación anual para el conjunto de servicios.

Seis propusieron facturación mensual. En tres casos, no se añadió más detalles. En dos, se indicó que la facturación sería según los recursos consumidos. Otra más señaló que se proponía una facturación mensual plana para los servicios recurrentes.

Una respuesta indicó que los servicios bajo demanda o de cadencia larga podrían ser abonados con periodicidad mayor a la mensual.

2.3. Lote II

2.3.1. Observaciones realizadas

Varias respuestas propusieron incorporar capacidades o subcapacidades adicionales o introducir modificaciones en los incluidos en la consulta, como:

- Data Loss Prevention
- Endpoint Protection
- Insider Threat Program
- Identity & Access Management

- Privileged & Access Management
- Cloud Security
- Propuesta de incluir dentro del servicio de Red Team
    - Pruebas de ingeniería social (phishing, vishing, smishing, USB cebo,…)
    - Pruebas de intrusión física
    - Pruebas de fortaleza de contraseñas
    - Pruebas en edificios inteligentes o sobre dispositivos IoT.
- Campañas de deception.
- Breach assessment.
- Gestión de vulnerabilidades en el directorio activo
- Integrar el servicio de inteligencia de amenazas con las soluciones de seguridad existentes
- Añadir un servicio avanzado de alerta temprana
- Threat Hunting

Tres respuestas cuestionaron el alcance y la utilidad del servicio de Bug Bounty.

En otra se manifestó la necesidad de más información para poder dar respuesta detallada.

Una recomendó la unificación de los tres lotes de la licitación en uno.

Otra propuso que este lote disponga de la figura de Coordinación de Actividades.

Finalmente, otra expuso la imposibilidad de que los clientes accedan a su plataforma de alerta temprana de forma directa, que su servicio no incluye hospedaje de máquinas virtuales y propuso una única herramienta Cloud en la que se centralice el análisis de vulnerabilidades.

2.3.2. Herramientas

Siete respuestas propusieron la prestación de varios de los servicios mediante herramientas de la empresa Tenable: Tenable ASM, Tenable WAW, Tenable.sc, Tenable.io., Nessus, etc.

Dos propusieron usar Qualys VMDR y Qualys WAS.

Una propuso la implementación de una tecnología en formato SaaS encargada al equipo dedicado para varios de los servicios.

Otras herramientas propuestas fueron Recorded Future, CyberSprint, Rapid7 o BugCrowd, Qualys CSAM, Expanse y Cycognito, así como otras de propósito más específico.

En la respuesta que usaba Gloria para el SIEM se indicaba que emas®, el módulo para la gestión de eventos, peticiones y activos de GLORIA, incorpora un módulo de gestión integral de activos (CMDB) en el que se recopila la información de los activos.

Varias respuestas manifestaron utilizar, entre otras, herramientas propias o exclusivas.

Para el servicio de Monitorización de la Superficie de Exposición, una respuesta propuso la creación de dos máquinas virtuales en la infraestructura propia del proveedor con acceso a la red y con escáneres y

herramientas configurados como son Nessus, Netscan y nmap. Los resultados podrían ser incorporados a su plataforma de gestión.

Una respuesta propuso unificar el servicio con el de análisis de vulnerabilidades.

Para el servicio de Bug Bounty, varias de las respuestas apuntaban al uso de plataformas de terceros preexistentes. Por contra, una de ellas sugirió una herramienta autohospedada.

2.3.3. Guías, estándares, buenas prácticas y certificaciones

Distintas empresas mencionaron el valor de aplicar conjuntos de guías, estándares y buenas prácticas en la prestación de los servicios, tales como:

- OSSTMM
- OWASP
- PTES

Del mismo modo, se señaló la conveniencia de alinear la información proporcionada por los servicios con MITRE ATTA&CK

También se mencionaron certificaciones que podrían ser relevantes, como:

- CEH
- OSCP
- ECSA
- ICPP

Y, con respecto a los SOC, las más mencionadas fueron:

- ISO 27001
- ISO 22301
- ISO 20000

2.3.4. Otras consideraciones

Las empresas hicieron numerosas referencias a sus fuentes de información y las metodologías con las que consideran oportuno que se realice la prestación de los servicios, que en general se alineaban con lo indicado en la Consulta Preliminar.

2.3.5. Necesidades de personal

Varias respuestas incluyeron estimaciones de necesidades de personal:

- Usar perfiles medios con horario 8x5.
- Para el servicio de Alerta Temprana de Vulnerabilidades, una propuesta consistió en
    - 1 Coordinación de respuesta frente a vulnerabilidades con dedicación del 15%
    - 2 Especialistas de Gestión de Vulnerabilidades al 60%
- Para el análisis de la superficie de exposición
    - 1 analista de seguridad al 100%
- Para análisis de vulnerabilidades se recibieron dos propuestas
    - La primera consistía en:
        - 1 Coordinación de respuesta frente a vulnerabilidades con dedicación del 10%
        - 1 Especialista de Gestión de Vulnerabilidades al 80%
    - Y la segunda, en
        - Analista de seguridad senior para la gestión de vulnerabilidades: 440 horas
        - Analista de seguridad junior para mantenimiento correctivo de la herramienta de gestión de vulnerabilidades: 440 horas
        - Analista de seguridad para servicio de análisis de vulnerabilidades y soporte en mitigación de riesgos: 440 horas
- Las dos propuestas para Inteligencia de amenazas fueron
    - 1 Especialista en Threat Intelligence al 100%
    - 1260 Horas /Año de Analista Senior de Inteligencia y 1.320 horas de pentester
- Para Vigilancia digital
    - 1 Especialista en Deep Web, Dark Web y alerta temprana al 100%
    - 900 Horas Analista VD Advance, con Certificado CTIA y 900 Horas Analista VD Intermediate, con Certificado CTIA
- Para Red Team
    - 2 Ingenieros de Ciberseguridad ofensiva al 50%
    - 1.560 horas de pentester senior
- Para Bug Bounty:
    - 1 Especialista en hacking ético al 75%
    - 440 horas de pentester

Una respuesta propuso un equipo común con las siguientes dimensiones en FTE:

- 4 Penetration & Vulnerability Testers (2 de ellos senior)
- 2 Threat intelligence Specialist (1 de ellos senior)
- 1 Service Manager

Finalmente, otra propuso entre 5 y 7 perfiles dedicados con responsabilidades separadas por cada subservicio y 1 perfil de coordinación, este último con dedicación al 50%.

2.3.6. Requisitos exigibles al personal utilizado para la prestación de los servicios

Para los puestos asociados a la realización de pruebas de seguridad (Red Team, Análisis de vulnerabilidades, etc) se recibieron dos propuestas:

- Propuesta primera:
    - Pentration & Vulnerability Tester: 2 años de experiencia y certificaciones CEH, OSCP y ECSA
    - Pentration & Vulnerability Tester Senior: 7 años de experiencia y certificaciones CEH, OSCP y ECSA
- Propuesta segunda:
    - Experto en hacking ético: 3 años de experiencia, titulación de Ingeniería Informática o similares, nivel de inglés B1-C1 y certificaciones CEH/OCSP
    - Experto en red team: 5 años de experiencia, titulación de Ingeniería Informática o similares, nivel de inglés B1-C1 y certificaciones CEH/OCSP/OSCE

Para los puestos relacionados con la inteligencia de amenazas se recibieron otras dos propuestas

- Propuesta primera:
    - Threat Intelligence Specialist: 2 años de experiencia y certificaciones Cybersecurity Foundation Professional Certificate y Certified Cyber Intelligence Investigator
    - Threat Intelligence Specialist Senior: 7 años de experiencia y certificaciones Cybersecurity Foundation Professional Certificate y Certified Cyber Intelligence Investigator
- Propuesta segunda:
    - Operadores de inteligencia: 1 año de experiencia, titulación de Ingeniería Informática o similares, nivel de inglés B1
    - Analista de inteligencia: 3-6 años de experiencia, titulación de Ingeniería Informática o similares, nivel de inglés B1-C1 y certificaciones ITIL, criminología y ciberinteligencia

- Analista de malware: 5 años de experiencia, titulación de Ingeniería Informática o similares, nivel de inglés B1-C1.

También se recibió una propuesta para los puestos de gestión de equipos y proyectos: Service Manager: 10 años de experiencia y certificaciones ITIL y PMP

Una propuesta recomendaba que el servicio se prestara con personal de cualificación equivalentes a los grados B y C de su modelo de carrera profesional, conforme a lo indicado en el apartado correspondiente al lote I.

Finalmente, una de las respuestas distinguía entre dos tipos de servicios:

- Alerta Temprana/Análisis de la Superficie de Exposición/Análisis de vulnerabilidades/Triaje del servicio Bug Bounty
  - Técnico: con formación profesional o universitaria, 1 certificación y experiencia de 18 meses.
  - Experto: con formación profesional o universitaria, 2 certificaciones y experiencia de 30 meses.
- Red Team/Digital Risk Protection
  - Experto: con formación profesional o universitaria, 2 certificaciones y experiencia de 30 meses.

2.3.7. Costes

Los modelos de servicio, de facturación y el dimensionamiento que propusieron las empresas que respondieron a la consulta no siempre coincidieron con lo señalado en la consulta, lo que hace difícil una comparación directa.

Para la plataforma de Alerta Temprana, los importes variaron entre 21.710,88 y 3.223.200 €:

- 21.710,88
- 25.000
- 50.500
- 116.253
- 240.000
- 340.000
- 200.740
- 930.610,66
- 2.312.575,00
- 3.223.200

Las orientaciones de importe para la Consultoría para Alerta Temprana oscilaron entre 29.009,76 y 2.521.440 €. La franja comprendida entre 200.740 y 407.345,92 € acumuló la mitad de las propuestas.

- 29.009,76
- 60.000
- 90.000
- 108.183,27
- 200.740
- 223.092,73
- 240.000
- 355.200
- 384.000,00
- 407.345,92
- 2.521.440

Para el Análisis de la Superficie de Exposición se obtuvo un rango entre 36.000 y 1.297.632 €, estando la mitad de las respuestas comprendidas entre 396.968,89 y 650.000 €.

- 36.000
- 240.960,00
- 396.968,89
- 465.601,64
- 400.000
- 555.366
- 650.000
- 707.208,52
- 1.297.632

Las ampliaciones de Análisis de la Superficie de Exposición difirieron también en alcance y precios estimados, entre 4.500 y 240.000 €, estando en la mitad de los casos comprendida entre 22.080 y 50.000 €.

- 4.500
- 22.080
- 23.721,31
- 47.299,53
- 50.000
- 158.400
- 240.000

Para el Servicio Atendido de Análisis de Vulnerabilidades - Servicio atendido, el rango estuvo entre 19.000 y 4.365.600 €:

- 19.000
- 138.000,54
- 240.000
- 334.330,08
- 400.000
- 724.555
- 805.746,20
- 1.344.000,00
- 2.529.450,73
- 4.365.600

Para el Servicio Desatendido de Análisis de Vulnerabilidades Web, el rango de precios estimado fue 999,84 – 724.555 €. Cuatro de los nueve casos estuvo comprendido entre 138.000 y 340.000 €.

- 999,84
- 8.000
- 26.300
- 66.3932,04
- 138.000,54
- 200.000
- 240.000
- 339.845,48
- 724.555

La base para el Servicio Autónomo de Análisis de Vulnerabilidades estuvo comprendida en el rango 25.920 – 8.989.978,08 €. Más de la mitad de los casos estuvieron comprendidos entre 132.399,84 y 400.000 €.

- 25.920
- 43.200
- 48.000
- 132.399,84
- 138.000,54
- 240.000
- 263.215,12
- 315.788,80
- 400.000
- 8.980.978,08

Las ampliaciones del Servicio Autónomo de Análisis de Vulnerabilidades oscilaron entre 270 y 898.097,76€:

- 270
- 2.000

- 4.000
- 13.239,84
- 30.947,30
- 43.200,00
- 164.000,00
- 898.097,76

Para el Servicio de Inteligencia de Amenazas se recibieron precios orientativos entre 19.339,68 y 800.000 €. Más de la mitad de los casos estuvieron comprendidos entre 280.000 y 495.000 €.

- 19.339,68
- 50.400,00
- 91.000
- 281.504,48
- 358.437,95
- 400.000
- 416.000
- 422.736,00
- 434.864
- 492.643
- 618.181,82
- 864.000
- 800.000

La base del Servicio de Vigilancia Digital recibió estimaciones de entre 118.000 y 924.000 €. Cinco de los once casos estuvieron comprendidos entre 393.000 y 655.000 €.

- 118.000
- 133.632
- 240.000
- 393.584
- 400.000
- 598.785,60
- 620.818
- 654.665,28
- 676.800,00
- 744.000
- 924.000

Las ampliaciones del Servicio de Vigilancia Digital oscilaron entre 9.670,08 y 200.000 €. La mitad de los casos estuvieron comprendidos entre 53.000 y 75.000 €.

- 9.670,08
- 12.000
- 20.000
- 53.367,27
- 57.483,42
- 62.400
- 74.400
- 200.000

Las estimaciones para el Servicio de Red Team oscilaron entre 73.323,98 y 1.636.220 €. Seis de los trece casos estuvieron comprendidos entre 439.000 y 762.000 €.

- 73.323,98
- 115.000
- 319.678,86
- 354.320
- 439.636,16
- 573.600
- 600.000
- 600.000
- 604.444,40
- 761.878
- 888.480
- 1.488.000
- 1.636.220

Para el Servicio de gestión de programa de Bug Bounty se obtuvieron estimaciones desde 65.000 hasta 768.000 €. Tres de los siete valores estuvieron en el rango 223.000 – 400.000 €.

- 65.000
- 100.000
- 118.400
- 223.574,84
- 369.600
- 397.636,07
- 768.000

A modo de resumen, la suma de las estimaciones de precio de todos los servicios ofertados para 4 años osciló entre 605.000 y 15.051.791 €, estando más de la mitad de los valores comprendidos entre 3.000.000 y 4.630.000 €.

- 605.500,00

- 986.688,34
- 2.413.390,00
- 3.070.000,00
- 3.437.451,26
- 3.822.000,00
- 4.219.642,84
- 4.371.531,00
- 4.431.840,00
- 4.628.384,22
- 5.816.427,97
- 11.245.769,58
- 15.051.791,52

2.4. Lote III

2.4.1. Observaciones

Tres respuestas alegaron que en la consulta faltaba información relevante para poder hacer una propuesta coherente. En general, manifestaron la dificultad para hacer presupuestos a priori conforme al modelo de facturación indicado en la consulta.

Dos de las respuestas propusieron incluir la figura de un coordinador de seguridad, que podría ser transversal a todos los lotes.

En otra se señaló que, como requerimiento adicional, podría añadirse que toda la gestión de las evidencias debería basarse en marcos y normativas como la ISO/IEC 27037.

Otra apuntó que, dependiendo del equipo de trabajo de AndalucíaCERT, para poder llevar a cabo todas las tareas relacionadas con todos los servicios descritos, podría darse el caso de que no tuviera suficiente personal cualificado o con suficiente disponibilidad en su jornada laboral por lo que fuera necesario la contratación de un equipo de trabajo especializado en formato “oficina técnica remoto o insitu” para poder abordarlo de manera conforme.

Y hubo una respuesta que recomendó unificar los tres lotes de la licitación en uno.

A la pregunta de si un único proveedor podría atender todos los servicios del lote, las respuestas fueron variadas.

- No: Dos respuestas. En una de ellas se adujo que la empresa que elaboró la respuesta no podría prestar asesoramiento legal.
- Sí: Nueve respuestas.
    - Tres, sin añadir más.
    - Señalando que posiblemente necesitaría contratar servicios o nuevo personal: Seis respuestas. Una de ellas respondía inicialmente que no, pero, posteriormente, señalaba

que, llegado el caso, subcontrataría algunos de los servicios a un tercero. Otra apuntó que no tenía medios para prestar el servicio de informes técnicos

En cuanto al análisis forense y DFIR se señaló que:

- La obligatoriedad de garantizar la disponibilidad del perito que ha realizado el informe incluso habiéndose finalizado la relación laborar puede conllevar implicaciones no totalmente beneficiosas y a la empresa que elaboró la respuesta no le era posible garantizarla.
- En DFIR hay una parte de respuesta al incidente que termina con el cierre de este.
- Propuesta de una metodología para análisis forense y DFIR basada en ISO 27037:2012 (Tecnología de la información - Técnicas de seguridad - Guías para la identificación, recopilación, adquisición y preservación de evidencias digitales).
- Comentario relativo a que debe establecerse un procedimiento de entrega y eliminación de evidencias.

En relación con las pruebas sobre código de aplicaciones, una respuesta propuso que las pruebas se debían realizar en el "propio pipeline de desarrollo del cliente".

Finalmente, una respuesta apuntó que cada servicio debería de incluir un proceso de mejora continua; y otra, que sería recomendable un modelo de contratación por suscripción.

2.4.2. Otros servicios propuestos

Los servicios adicionales a los incluidos en la consulta que fueron propuestos incluyeron:

- Creación de una oficina de apoyo a la gestión y coordinación de la ciberseguridad, en apoyo de la Estrategia Andaluza de Ciberseguridad.
- Servicios de Gestión del Riesgo y Gobierno y de Awareness y Gestión del Conocimiento.
- Servicio de Formación y Concienciación en Seguridad.
- Revisión y actualización de procedimientos de Gestión de Crisis y de Continuidad Operativa.
- Servicio de inteligencia.
- Ingeniería Social.
- Deception.
- Breach Assessment.
- Gestión de Vulnerabilidades en el Directorio Activo.
- Rating o Benchmarking.
- Entrenamiento de respuesta a incidentes de ciberseguridad.

- Evaluación activa de amenazas.
- Evaluación o creación del plan de respuesta a incidentes de ciberseguridad.
- Evaluación de la preparación actual para responder a ciber incidentes.
- Acceso a base de datos de inteligencia de amenazas.

En un caso se señaló que los servicios de DFIR, Certificación y preservación de evidencias digitales, respuesta rápida in situ, y peritaje informático deberían prestarse de forma conjunta por un mismo equipo e incluso se podría incluir en esta lista el de consultoría tecnológica en protección, detección y respuesta. Y también que, para lograr mayor eficiencia, se podría cubrir toda la gestión de incidentes mediante la adición de un servicio continuo con tarificación mensual.

2.4.3. Servicios que aportan poco valor y podrían suprimirse

En varias respuestas se señaló la conveniencia de considerar la eliminación de los siguientes servicios:

- Análisis de código DAST e IAST.
- Servicio de elaboración de informes divulgativos.

Una respuesta indicó que el servicio de pentesting y hacking ético debería de proporcionarse por el equipo del Lote II y que el servicio de análisis de código fuente debería considerarse como un Lote separado debido a las características del mismo.

2.4.4. Necesidad de servicios notariales en los procesos de adquisición de prueba

En 3 de las respuestas se indicó que esta figura no sería necesaria, gracias al uso de metodologías, servicios adicionales o garantías técnicas.

En 4 casos se señaló que la figura es necesaria.

Cinco respuestas apuntaron que depende de las circunstancias.

2.4.5. Necesidad de visado colegial en los informes forenses

En 9 respuestas se indicó que este visado no es necesario. Una señaló que sí. Y otra, que depende de las circunstancias.

2.4.6. Uso de eGarante o similar o de servicios notariales

Para los casos de uso indicados, 3 respuestas indicaron que bastaba con eGarante . Otras 8, que depende de las circunstancias. Y una, que ambos servicios se complementan.

2.4.7. Tiempos de asignación y desplazamiento de personal para Análisis forense / DFIR

Los tiempos de asignación y desplazamiento de este personal oscilaron entre 4 horas y, en un caso, más de una semana. Lo más habitual fue que la intervención pudiera realizarse en 24 o 48 horas.

Las orientaciones recibidas fueron:

- Asignación en remoto en 1 hora con desplazamiento en, como máximo, 24 horas.
- Inicio de los trabajos en el día, con un máximo de 4 horas, según gravedad del incidente.
- Disponibilidad en 4 horas y desplazamiento a cualquier punto de Andalucía en 24 horas.
- En los casos en que sea necesaria una intervención rápida, las tareas de recopilación de evidencias deberá ser realizada por el personal de la Agencia Digital de Andalucía. En cuanto a los tiempos ofrecidos, se establece un máximo de 1 hora para triaje y desplazamiento a instalaciones en 24-48 horas.
- Desplazamiento en 10 horas en caso de no tratarse de un incidente grave y 6 horas y media en otro caso, con soporte telefónico durante el desplazamiento, que habrá de realizarse en el medio más rápido posible.
- Primer contacto en menos de 12 horas, reducible a 4 si se contrata un paquete adicional, con informe inicial de situación en 24 horas. La asistencia sobre el terreno debería realizarse en menos de 12 horas en territorio español, si bien este tiempo puede verse afectado por diversas caudas o circunstancias. La asistencia para forense se ofrecería en menos de 24 horas tras el inicio de la asistencia.
- 1 día laborable.
- Asignación de forense en 24 horas. Disponibilidad 24x7 con tiempo de primera respuesta inferior a 15 minutos, inicio de la intervención en 30 minutos y tiempo de intervención remota de 2 horas e insitu para España de 12 horas.
- 48 horas como máximo tras la petición con el objetivo de hacerlo en el siguiente día.
- 48 horas para desplazamientos a cualquier punto de Andalucía.
- 7 días naturales para que la persona esté lista para encargarse de los trabajos. Desplazamientos en 1 a 3 días.

2.4.8. Tiempos de certificación de evidencias

Las estimaciones de tiempo oscilaron entre minutos y 5 días laborables, no pasando de las 12 horas en la mitad de los casos.

Las orientaciones recibidas fueron;

- Si es realizable con eGarante, minutos.
- Media hora para contenidos de la web, pudiéndose certificar más de una evidencia.
- Si no se requiere presencialidad, 2 horas. En otro caso, 12 horas. La primera respuesta se dará en un máximo de 15 minutos, iniciándose las actuaciones en 1 hora.
- Al siguiente día laborable.
- Dependerá de la evidencia. Las que puedan realizarse mediante eGarante se podrán certificar en menos de 24 horas.
- 5 días laborables.

2.4.9. Cualificación exigible a las personas que realicen las peritaciones forenses e DFIR

Las propuestas recibidas fueron:

- Debería exigirse según normativa de referencia.
- Experiencia de al menos 5 años en trabajos similares, y certificaciones vinculadas con la Respuesta ante Incidentes y Análisis Forense Digital.
- Ingeniería en Telecomunicaciones o Informática, con entre 2 y 3 años de experiencia y sugieren las certificaciones GIAC Certified Forensic Analyst (GCFA) y GIAC Mobile Device Security Analyst (GMOB).
- Experiencia superior a 3 años y la conveniencia de contar con la certificación IRCP (DFIR). Se señala que, aunque certificaciones como CEH, CHFI puedan ser válidas, tiene mayor peso la experiencia profesional.
- Acreditación de experiencia previa y, opcionalmente, certificación similar a CHFI (Computer Hacking Forensic Investigator) o un máster relacionado.
- Certificaciones GIAC, CISA y GCFA.
- Ingeniería, 5 años de experiencia y certificaciones certificaciones CHFI o similares.
- Formación Profesional o Universitaria, experiencia de 2 años y certificaciones como OSCP, CEH, GIAC, CREST, CESG o CHECK.
- Además de experiencia, alguna de las certificaciones GIAC Certified Forensic Examiner (GCFE) y GIAC Certified Forensic Analyst (GCFA).

2.4.10. Tiempos para la asignación de pentester

Las estimaciones oscilaron entre 1 jornada y menos de 3 semanas. En 6 de los 10 casos se mencionó valores comprendidos entre 10 y 15 días.

Las orientaciones recibidas fueron:

- 1 jornada.
- 24 horas.
- 4 días.
- 10 – 15 días.
- 14 días naturales.
- 15 días.
- 15 días.
- 15 días naturales, incluyendo planificación de trabajos.
- Al menos 15 días.
- Menos de 3 semanas.

2.4.11. Cualificaciones exigibles al personal de pentesting

Las recomendaciones incluyeron:

- Certificaciones CEH / OSCP / PortSwigger Burp Suite Certified Practitioner Certification (PBCPC) / Otras equivalentes
- Experiencia de 5 años y certificaciones CEH / OSCP
- Certificaciones Offensive Security Certified Professional (OSCP) / Offensive Security Web Expert (OSWE) / Offensive Security Wireless Professional (OSWP) / Offensive Security Experienced Professional (OSEP) / Practical Network Penetration Tester (PNPT).
- Experiencia de 1 año y certificaciones CEH / OSCP. Se podría valorar OSEP.
- Sería necesario alguno de los siguientes certificados en alguno de los auditores asignados al proyecto: CISA, CISSP, GIAC-GPEN, GIAC-GICSP o ITIL Foundation. Así mismo, el jefe de proyecto debería poder contar con alguno de las siguientes certificaciones o experiencia, además de las mencionadas para los auditores: GIAC – GSE, más de 6 años de experiencia en test de intrusión o hacking ético
- Titulación de Ingeniería con como mínimo con 5 años de experiencia y alguna de las siguientes certificaciones: CEH (Certified Ethical Hacker), LPT (Licensed Penetration Tester), OSCP (Offensive Security Certified Professional), CHFI (Computer Hacking Foresnsic Investigator) o GPEN: GIAC Certified Penetration Tester.

- Formación Profesional o Unviersitaria, dos años de experiencia y certificaciones como Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH), Global Information Assurance Certification (GIAC) Certifications (p.e.: GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), o GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)), CREST Penetration Testing Certifications, o Communication Electronic Security Group (CESG) IT Health Check Service (CHECK) .certification.
- Certificaciones CEH / OSCP.

2.4.12. Informes

La estimación de costes y tiempos de entrega para los informes se resume en la siguiente tabla:

COSTE	TIEMPO
2.981,23 euros	1 semana
1.730	5 días laborables
5.000	Estándar 4 semanas, fast-track 2 semanas y media
14.000	4 semanas
3.200	2 semanas
3.200	1-2 semanas
1.860,64	40 horas por informe
	2 semanas
3.000	2 semanas
Indica coste anual de 82.461,22	7-10 días para guía técnica, 15-20 días para un estudio más complejo

El precio típico ronda los 3.000 € y los tiempos más habituales están entre 1 y 2 semanas.

2.4.13. Análisis de malware

La estimación de costes y tiempos de entrega para este servicio se resume en la siguiente tabla:

COSTE	TIEMPO
14.193 euros	7 – 15 días laborables
430	3 días laborables
3.000	1,5 semanas. Fast-track (mínimo esfuerzo) en 1

	semana
1.000	Primera respuesta en 15 minutos, inicio de actividades en 1 hora. Si se trata de una intervención remota, 2 horas; en otro caso, hasta 12 horas
7.900	15 jornadas
2.516,04	Despliegue inmediato en horario de trabajo. Fuera de ese horario, según urgencia, en un máximo de 2 jornadas. Entregable en 2 jornadas tras el análisis
10.000	10 días
Coste dependiendo de la complejidad del malware	Para malware de baja complejidad, 8 horas. Para malware de complejidad media, el informe de hallazgos iniciales se podría entregar en 24 horas, pero variará según los hallazgos. El reporte final se podría entregar en un máximo de 120 horas.

A modo de resumen, los tiempos más habituales estuvieron comprendidos entre 1 y 2 semanas. En cuanto a los precios, el rango que acumuló más casos fue el comprendido entre 1.000 y 3.000 €.

En uno de los casos, se remitió a las estimaciones para DFIR.

2.4.14. Ciberejercicios

Para los ciberejercicios Table-top se recibieron estimaciones entre 2.698,24 y 15.000 €, estando la mayor parte de los casos alrededor de los 10.000 €. Las orientaciones fueron:

- 2.698,24
- 4.846,00
- 8.160,79
- 8.500
- 9.781
- 12.000
- 12.525,00
- 10.000 a 20.000
- 15.000

Una respuesta propuso consumir 40 horas de una bolsa común para el lote.

Para los ciberjercicios de Escenario Real, algunas respuestas indicaron estimaciones de precios genéricas mientras otras indicaron precios según tipo de ejercicio.

Los casos de precio genérico estuvieron típicamente alrededor de los 10.000-15.000 € e incluyeron las siguientes orientaciones:

- 10.000
- 2.681,00
- 13.500
- 10.000
- 3.570,56
- 15.000 a 35.000

En cuanto a los casos con precios según tipo de ejercicio, muchos estuvieron en el rango 2.000 – 4.500 €, mientras otros rondaron con frecuencia los 10.000 €:

- Phishing simple: 4.200
- Phishing complejo: 9.000
- USB Drop simple: 6.000
- USB Drop complejo: 9.000
- Falso servicio técnico: 9.000
- Simulación: 8.960
- Ingeniería social: 12.019
- Phishing Testing 1 fake website genérico, hasta 2,500 empleados Remoto: 3.137,04
- Phishing Testing 1 fake website genérico, hasta 50,000 empleados Remoto: 3.659,88
- Phishing Testing 1 fake website personalizado, hasta 2,500 empleados Remoto: 4.705,56
- Phishing Testing 1 fake website personalizado, hasta 50,000 empleado Remoto: 6.274,08
- Phishing Testing 1 campaña adjuntos maliciosos, hasta 2,500 empleados Remoto 5.228,40
- Phishing Testing 1 campaña adjuntos maliciosos, hasta 50,00 empleados Remoto: 6.274,08
- Vishing Testing 1 campaña, hasta 15 empleados Remoto: 2.091,36
- Vishing Testing 1 campaña, hasta 30 empleados Remoto: 3.137,04
- USB Drop Attack Testing 10 standard USB, por localización Remoto + Onsite: 2.091,36
- USB Drop Attack Testing 10 fake USB, por localización Remoto + Onsite: 2.091,36

- USB Drop Attack Testing 10 standard USB + 10 fake USB por localizacion Remoto + Onsite: 3.137,04
- Rogue Tecnician 1 localización Onsite: 2.091,36

En una de las propuestas se añadía una cuota de alta de servicio de 485,02 euros.

Y otra, basada en bolsa de horas, indicaba un consumo de 80 horas de bolsa para ejercicio de baja complejidad, señalando que tenían algunos ejercicios en catálogo en los que el consumo podría reducirse a 40 horas.

Los tiempos para la preparación oscilaron entre 48 horas y 4 meses, si bien se señaló en repetidas ocasiones que dependería de la complejidad y naturaleza del ejercicio. Más de la mitad de las estimaciones incluyeron datos comprendidos entre 2 semanas y 1 mes.

Las orientaciones recibidas fueron:

- 48 horas
- Entre 5 días y 2-3 semanas, según complejidad, para ejercicios de escenario real.
- 1 semana de gestión y planificación, las necesarias para la ejecución técnica, 1 semana para entrega de documentación, 1 semana para entrega de resultados, 1 semana para entrega de la documentación y 1 semana para presentación de los resultados.
- 14 días naturales
- 1-3 semanas, según complejidad
- 3 semanas
- 4 semanas
- Table-top en 1 mes mínimo para preparación.
- 1 mes para ejercicios Table-top.
- Entre 2 y 4 meses, según complejidad

Una respuesta propuso establecer precios según número de personas participantes. Para 1.000 personas el coste es 10.070 € y para 50 sería 4.940 €.

2.4.15. Consultoría

Los precios por hora estimados para Consultoría Senior oscilaron entre 47,67 y 90 €, siendo valores típicos los comprendidos entre 65 y 75 €.

- 47,67

- 60,55
- 65
- 67,72
- 70
- 72,37
- 75
- 75
- 90
- 90

Los precios por hora estimados para Consultoría Junior oscilaron entre 32,89 y 65 €, siendo valores típicos los comprendidos entre 45 y 55 €:

- 32,89
- 35
- 45
- 47,78
- 54
- 55
- 55
- 56,61
- 60
- 65

Una respuesta propuso usar el mismo sistema de precios que para DFIR y forense.

2.4.16. Cualificaciones para consultoría

Las propuestas de cualificaciones para Consultoría Senior fueron:

- Certificaciones CISA, CISM, CDPP, CRISC y 27001 Lead Auditor

- Ingeniería en Telecomunicaciones o Informática, experiencia de 5 a 7 años, Indicent Response Fundamentals e ITIL Fundamentals.
- Offensive Security Certified Professional (OSCP) / Certified Red Team Professional (CRTP) / Certificacion forense digital movil.Cellebrite Certified Physical Analyst (CCPA) / Certificacion forense Profesional (CPAIF) / eLearnSecurity Web Application Penetration Tester (eWPT) / Foundations of Operationalizing MITRE ATT&CK (AttackIQ) / Check Point Certified Security Administrator (CCSA) / Radware Certified Security Specialist (RCSS)
- 5 años de experiencia
- Formación Profesional o Universitaria y 5 años de experiencia.
- Grado en TI p Ingeniería y master, 5años de experiencia y certificaciones como CISA, CISM o IRCP, por ejemplo.
- Más de 4 años de experiencia
- 5 años de experiencia y certificaciones GIAC Certified Forensic Examiner (GCFE) y GIAC Certified Forensic Analyst (GCFA)

Y, para Consultoría Junior:

- CISA, CISM y CSX
- Ingeniería en Telecomunicaciones o Informática, experiencia de 1 a 3 años, Ethical Hacking, Indicent Response Fundamentals e ITIL Fundamentals.
- CISCO CCNA SECURITY Microsoft IT Center / CISCO CCNA at Microforum school / Malicious software and botnets (Royal Holloway, University of London) / CEHv8 Certified Ethical Hacker . ECC981930 (2016) / CNO: 3820. Gestión de incidentes de seguridad (mód. MF0488_3) / CNO: 3820. Gestión de servicios en el sistema informático (MF0490_3) / Auditor interno ISO27001 Bureau Veritas. Certificación Nº 82617 / Integración de procesos ISO27001 Bureau Veritas. Certificación Nº 82617 / Ciberseguridad: Ataques y contramedidas. Universidad Rey Juan Carlos
- 2 años de experiencia
- Formación Profesional o Universitaria y 2 años de experiencia.
- Grado en TI p Ingeniería y master y 2 años de experiencia.
- 1-4 años de experiencia
- 1 año de experiencia y certificaciones GIAC Certified Forensic Examiner (GCFE) y GIAC Certified Forensic Analyst (GCFA)

Una respuesta propuso establecer los mismos requisitos que para DFIR y forense.

2.4.17. Respuesta in situ

La siguiente tabla resume los datos relativos a precios y tiempos de asignación para el servicio de Respuesta in situ:

Precio hora personal técnico de respuesta in situ	Precio hora personal técnico de respuesta in situ especialista en tecnología	Tiempo de asignación
55	65	5 días laborables
50,00	60,55	1 semana para plan de acción. Desplazamientos en 48 horas
90€/hora (horario laboral) / 120€ (horario extendido)	90€/hora (horario laboral) / 120€ (horario extendido)	Dependerá de la tarea. Desplazamiento en incidente crítico: menos de 4 horas.
		En caso de estar programado, entre 2 y 3 semanas. Para respuesta in situ, entre 24 y 48 horas. Desplazamiento a sedes, 1 día
75	80	Plan de acción en 2 semanas. Respuesta rápida in situ: 1 a 3 días
47,67	53,78	Plan de acción en 2 jornadas y desplazamientos en entre 6 y 24 horas
50	50	
80	100	Para el plan, al menos 1 o 2 días. Desplazamientos en al menos 1 día. En total, tres días como mínimo
120	159	Para el plan de acción dependerá de cada caso. Para la respuesta rápida in situ, como máximo, 48 horas
		Primer contacto en 4 horas si se contrata un pack, información preliminar en 24 horas y

		desplazamiento en menos de 12 horas
		Tiempo de desplazamiento a sedes menor de 48 horas. La llamada inicial de triaje se realizará en, como máximo, 1 hora.

En una respuesta se propuso usar la misma tabla de precios que para DFIR / forense. En otra, se remitió al consumo de horas realizadas conforme a una bolsa.

2.4.18. Costes adicionales

2.4.18.1. Desplazamientos

Las orientaciones recibidas respecto a las cuantías correspondientes a los desplazamientos variaron de forma significativa:

- 150 Euros por día de desplazamiento, incluyendo el transporte, las dietas y el alojamiento en caso de ser necesario pernoctar.
- 450 euros por jornada más los trenes o vuelos necesarios
- El coste de los desplazamientos dependerá del destino y los tiempos de respuesta exigidos.
- 0,21 euros/km, entendiendo que las empresas licitantes deberían ser capaces de integrarlo en sus presupuestos de forma previa.
- 661 euros para desplazamientos de ida y vuelta más 198,41 en concepto de dietas. En el caso de los desplazamientos locales, el coste sería de 80 euros.

2.4.18.2. Testificación

Las orientaciones recibidas respecto a las cuantías correspondientes a las testificaciones correspondientes al análisis forense variaron entre 300 y más de 1.000 €, estando típicamente entre 750 y 1.000 €:

- 750 euros por Jornada de testificación, incluyendo el desplazamiento, la dietas, el alojamiento y la dedicación de la persona que tenga que testifique en el juicio.
- 900 euros por jornada
- Solo la testificación supondría 1.000 euros, a los que habría que añadir otros costes.
- 300 euros más desplazamientos
- 900 euros por jornada y persona.

- Coste de una jornada in-situ (aplica recargos) más desplazamientos.

Dos respuestas propusieron que debía usarse un modelo de coste por horas.

2.4.19. Costes

En general, las respuestas proponen modelos alternativos.

- Algunos incluyen todos o alguno de los siguientes elementos:
    - Análisis previo inicial.
    - Bolsa de horas, que podría estar compartida entre los servicios.
- Otros se basan en precios por jornada y analista.

Una propuesta propone un perfil dedicado en instalaciones de cliente con un coste de 387.114,84 euros para los 4 años. Además, sería necesario adquirir, como equipamiento adicional, una clonadora (4.715,57 euros) y software forense con licencia perpetua y 4 años de soporte (5.738,52 euros) y una bolsa de horas bajo demanda a un precio de 1.414,81 euros o, si son pre-pagadas. 1.061.11. horario laboral (8x5 GMT+1) e incluyen disponibilidad y primera asistencia siempre 24x7x365. Si debido a la criticidad, urgencia o a petición del cliente es necesaria la asistencia in situ o las operaciones fuera del horario laboral (24x7), se aplicará un multiplicador equivalente al doble de la tarifa estándar al precio de las jornadas de trabajo DFIR pre-pagadas. También aplica recargos según las condiciones en que se realice el trabajo.

Otra propone un servicio por suscripción con un coste de 102.956,77 €/año.

Para el peritaje forense, según el objeto del mismo, se obtuvieron las siguientes orientaciones. En algunas de ellas se da un precio cerrado, mientras que en otras se asigna un precio por hora:

- Puesto de trabajo
    - 4.560,00
    - 3.500
    - 6.924,00
    - 100€/hora
- Servidor
    - 6.081,00
    - 5.000
    - 300€/hora
- Terminal móvil
    - 3.040,00
    - 2.500
    - 4.772,00
    - 200€/hora

- Electrónica de red
  - 3.040,00
  - 4.000
  - 4.772,00
  - 100€/hora
- Sistemas empotrados e IoT
  - 4.560,00
  - 4.000
  - 4.772,00
  - 200€/hora

Los datos correspondientes al análisis DFIR son:

- Puesto de trabajo
  - 3.800,00
  - 5.000
  - 3.177,00
  - 200€/hora
- Servidor
  - 5.321,00
  - 6.000
  - 3.600,00
  - 500€/hora
- Terminal móvil
  - 2.280,00
  - 5.000
  - 1.772,00
  - 400€/hora
- Electrónica de red
  - 2.280,00
  - 5.500
  - 1.772,00
  - 200€/hora
- Sistemas empotrados e IoT
  - 3.800,00
  - 5.500
  - 1.772,00
  - 200€/hora

Para la certificación de evidencias:

- Perfil en redes sociales (Twitter, Facebook, Instagram, TikTok, etc.)
    - 250 €
    - 3.000
    - 300€
    - 1.855,42
- Publicación en redes sociales (twit, post, foto, etc.)
    - 250 €
    - 3.000
    - 300€
    - 1.855,42
- Contenido de una web, foro o blog
    - 250 €
    - 3.000
    - 250 €
    - 1.855,42
- Documento alojado en una web, foro o blog (PDF, Word, Excel, etc.)
    - 250 €
    - 3.000
    - 250 €
    - 1.855,42
- Email, SMS, MMS, mensaje de aplicación de mensajería (WhatsApp, Telegram, Signal, etc.)
    - 300 €
    - 3.000
    - 500 €
    - 1.855,42

Para el pentesting (caja negra – caja gris – caja blanca):

- Página web

- 3.615,00 - 3.034,00 - 3.034,00
- 6.435,00 - 4.290,00 - 5.362,00
- 14.000 - 16.000 - 16.000
- 150€/h - 100€/h - 75€/h
- 4.000 - 7.000 - 13.000
- 4.371,46
- N/A - 42.000 - Sin datos
- En dos casos se realizaron estimaciones según complejidad:
  - La primera indicó:
    - Complejidad baja: 1.800,00 - 3.000,00 –
    - Complejidad media: 3.000,00 - 4.200,00 -
    - Complejidad alta: 4.800,00 - 6.000,00 –
  - Y, la segunda:
    - Estándar: 1.568,52 - 2.614,20 - 2.614,20
    - Compleja: 3.659,88

- App móvil (caja negra – caja gris – caja blanca):
  - 3.615,00 - 3.034,00 - 3.034,00
  - 3.753,00 - 4.290,00 - 5.362,00
  - 8.000 - 10.000 - 12.000
  - 250€/h - 200€/h - 100€/h
  - 3.000 - 5.000 - 10.000
  - 4.371,46
  - N/A - 62.500 - Sin datos
  - En un caso se hizo estimaciones según complejidad:
    - Complejidad estándar: 3.000,00 - -
    - Complejidad alta: 4.200,00 - -
  - Y en otro se distinguió entre análisis para una plataforma o para dos:

- IOS o Android: 2.614,20
- IOS y Android: 4.182,72

- Servidor de aplicaciones (caja negra – caja gris – caja blanca):
  - 3.615,00 - 3.034,00 - 3.034,00
  - 2.145,00 - 1.608,84 - 4.290,00
  - 7.000 - 9.000 - 10.000
  - 150€/h - 100€/h - 75€/h
  - Análisis de vulnerabilidades: 1.200,00 - 1.800,00 –
  - Test de intrusión: 1.200,00 - 2.400,00 -
  - 2.000 - 3.000 - 4.00
  - 1.258,02
  - 3.659,88
  - 18.350 - 18.350 - N/A

- Dominio (DC) (caja negra – caja gris – caja blanca):
  - 5.422,00 - 4.841,00 - 3.938,00
  - 2.145,00 - 4.290,00 - 6.435,00
  - 4.000 - 5.000 - 7.000
  - 100€/h - 75€/h - 50€/h
  - 4.000 - 7.000 - 13.000
  - 4.371,46 (los tres tipos)
  - 18.350 - 18.350 - N/A

- WiFi (caja negra – caja gris – caja blanca):
  - 3.938,00 - 3.938,00 - 2.454,00
  - 3.753,00 - 4.290,00 - 5.362,00
  - 4.000 - 5.000 - 6.000

- 25€/h - 20€/h - 10€/h
- 1 SSID: 1.200,00 - -
- 3 SSID: 3.000,00 - -
- 2.000 - 3.000 - 5.000
- 3.113,44 (los tres tipos)
- 3.137,04 (hasta 5 SSID)
- N/A - 9.000 - N/A

- Segmento de red (caja negra – caja gris – caja blanca):
  - 3.034,00 - 2.454,00 - 2.454,00
  - 2.681,00 - 2.681,00 - 4.290,00
  - 3.000 - 3.500 - 4.000
  - 100€/h - 75€/h - 50€/h
  - Clase C Externo: 1.800,00 - -
  - Clase C Interno: 3.000,00 - -
  - Clase C Externo/Interno: 6.000,00 - -
  - 4.000 - 7.000 - 13.000
  - 4.371,46 (los tres tipos)
  - 2.614,20 (hasta 50 direcciones IP)
  - 25.500 - 25.500 - N/A

En una de las respuestas se añade a los precios indicados una cuota de alta de 485,02 euros.

Pruebas de aplicaciones (SST – DAST – IAST)

- Web
  - 6.132,15 - 6.461,97 - 8.329,25 (Completa: 8.329,25)
  - 3.795,00 - 8.295,00 - 8.295,00
  - 3.500 - 4.500 - 4.500

- 3.700 - 3.000 - 3.900
- 3.710,84 - 3.278,60 - 1.258,02
- 100 €/hora para los tres tipos
- Una respuesta establece diferencias según complejidad:
  - SAST
    - Menos de 50.000 líneas de código: 3.500
    - 50.000 – 100.000 líneas: 5.300
    - 100.000 – 250.000 líneas: 8.200
    - 250.000 – 500.000 líneas: 11.200
  - DAST: Según pentesting.
  - IAST: proponen facturación mensual.

- App móvil
  - 6.981,16 - 6.651,34 - 8.853,36 (Completa: 8.853,36)
  - 3.795,00 - 8.295,00 – 6.295,00
  - 3.500 - 4.500 - 4.500
  - 3.500 (solo SAST)
  - 100 €/hora para los tres tipos
  - 3.710,84 - 3.278,60 - 1.258,02
  - Igual que para la web

En un caso se propone que la Agencia Digital de Andalucía licencie software y pague según número de líneas.

EL JEFE DEL SERVICIO DE CIBERSEGURIDAD

Eloy Rafael Sanz Tapia