

En relación con el expediente en tramitación denominado “**SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE MADRID DIGITAL - 4 LOTES**”, a adjudicar por procedimiento abierto mediante pluralidad de criterios, nº de expediente **ECON/000237/2023**, se han recibido las siguientes **consultas** referidas al PLIEGO DE CLÁUSULAS ADMINISTRATIVAS y de PRESCRIPCIONES TÉCNICAS por parte de empresas interesadas en la licitación. Estas preguntas se transcriben tal y como han sido redactadas por el licitador, y son las siguientes:

97. PPT. Apartado 4.1.1.2. ¿Podrían proporcionar más detalle sobre las actividades a realizar que se esperan en el requisito “Auditorías técnicas específicas de sistemas críticos (correo, directorio activo, etc.)” del apartado 4.1.1.2 y qué diferencia habría con el requisito de “auditorías específicas de sistemas concretos como servicios de directorio activo” del apartado 4.1.1.3?

**Respuesta:**

Como se menciona en el PPT: “*este servicio se prestará en modalidad de servicio continuo, en base a las solicitudes de análisis de infraestructuras o sitios web que solicite Madrid Digital, o planificaciones acordadas*”. Con carácter general, la planificación de estos análisis, que son de tipo automático mediante el uso de herramientas, se viene realizando trimestralmente e incluye el conjunto de los activos de Madrid Digital; aunque por necesidades del servicio, enlazando con la pregunta, se puede requerir, además, de una auditoría específica puntual de algún sistema crítico.

En cuanto a las auditorías solicitadas en el *apartado 4.1.1.3* del PPT, éstas igualmente se pueden requerir a demanda por necesidades del servicio y se circunscriben al tipo de análisis manuales por parte de los analistas de seguridad definidos en el propio servicio.

98. PPT. Apartado 4.1.1.2. En relación con la explotación controlada de las vulnerabilidades detectadas, y dado que no es viable la explotación manual de todas ellas: ¿qué criterio sigue Madrid Digital para la selección de las vulnerabilidades a explotar?

**Respuesta:**

El criterio aplicado actualmente es por criticidad de la vulnerabilidad (CVE/CVSS), si bien queda a criterio del licitador proponer otro modelo que amplíe o mejore el existente.

99. PPT. Apartado 4.1.1.3. En relación a las pruebas antiDDoS ¿Se trata de pruebas de capa 3 o de capa 7? ¿Podrían indicar el nivel de intensidad/duración de las pruebas a realizar en cada capa? ¿Tienen identificado el tipo de pruebas a realizar?

**Respuesta:**

El licitador deberá proponer la tipología de pruebas a realizar y metodología de realización, cubriendo cualquier capa del modelo OSI susceptible de poder ser atacado mediante técnicas de denegación de servicio. Como se recoge en el PPT, estas pruebas deberán siempre ser aprobadas por Madrid Digital.

100. PPT. Apartado 4.1.1.3. ¿Podrían proporcionar información sobre la aplicación ITSM-FARO? ¿Tiene API para poder interactuar? ¿Está basada en alguna plataforma comercial?

**Respuesta:**

Está basado en BMC Helix ITSM y dispone de API para poder interactuar.

101. PPT. Apartado 4.1.1.3. ¿Podrían proporcionar información sobre la volumetría de análisis de aplicaciones a realizar, calendario establecido, periodicidad, pruebas bajo demanda?

**Respuesta:**

Para el servicio de análisis de vulnerabilidades de seguridad de aplicaciones, que se realiza de forma manual por parte de los analistas de seguridad, se consensuará con estos analistas los objetivos a cumplir para cada uno de los análisis. Con carácter estimativo, se viene realizando, de media, un análisis web por semana pudiendo incrementarse la demanda en función de las necesidades que tenga en ese momento Madrid Digital.

102. PPT. Apartado 4.1.1.3. ¿Se trata de un servicio que requiere de un equipo dedicado o se espera que se absorban los diferentes análisis con el equipo pool de XXXX?

**Respuesta:**

El equipo de trabajo (número de personas, porcentaje de dedicación y horas estimadas) se especifica en el apartado 4.2.3 del PPT.

103. PPT. Apartado 4.1.1.4. Dentro del alcance de los ciberejercicios en el alcance de "Entrenar a la organización" ¿Podrían detallar si se refieren a la capa directiva o también al equipo SOC o respuesta ante incidentes? ¿Se requiere que el adjudicatario realice ejercicios de simulación para el entrenamiento del equipo técnico?

**Respuesta:**

Tal y como se indica en el PPT, el alcance general se refiere al personal de Madrid Digital que asciende a 660 usuarios, en previsión de crecimiento hasta unos 700. En cualquier caso, en la definición de cada ciberejercicio, bajo la supervisión y aprobación de Madrid Digital, se definirá el alcance explícito del mismo.

104. PPT. Apartado 4.1.1.4. ¿Podrían indicarnos el número de usuarios y dominios para las simulaciones de phishing al año? ¿Todas las campañas de phishing estarán dirigidas a los mismos destinatarios o se prefiere establecer campañas de phishing por lotes de usuarios?

**Respuesta:**

Tal y como se indica en el PPT, las simulaciones de phishing controlados alcanza a todo el personal de Madrid Digital que asciende a 660 usuarios, en previsión de crecimiento hasta unos 700. El licitador deberá proponer las simulaciones propuestas y su alcance. En cualquier caso, en la definición de cada ciberejercicio, bajo la supervisión y aprobación de Madrid Digital, se definirá el alcance explícito del mismo.

105. PPT. Apartado 4.1.2.1. ¿Podrían proporcionar información sobre la volumetría de alertas mensuales gestionadas actualmente por el equipo de operaciones N1?

**Respuesta:**

Por motivos de confidencialidad y de ciberseguridad no es posible revelar este tipo de información.

106. PPT. Apartado 4.1.2.1.1. Solicitan el mantenimiento de la plataforma SIEM actualmente instalada hasta su sustitución por la nueva. ¿Podrían especificar a qué se refieren con mantenimiento hardware? ¿Mantenimiento y actualización del servidor a nivel de parches y sistema operativo o mantenimiento hardware de sustitución de piezas?

**Respuesta:**

Tal y como se especifica en el apartado 4.1.2.1.1 del PPT: *“El adjudicatario estará obligado a su mantenimiento operativo hasta su sustitución por la nueva propuesta. Este mantenimiento operativo incluirá el mantenimiento hardware de toda la plataforma actual y mantenimiento de licencias asociadas [...] Madrid Digital no asumirá ningún coste adicional por esta actividad [...] En este escenario, todos los costes derivados del mantenimiento operativo de los componentes (hw, sw) irán por cuenta del adjudicatario.”*

Por tanto, este mantenimiento deberá incluir todos los elementos necesarios que hagan que la plataforma siga plenamente operativa a todos los niveles hasta su completa sustitución por la nueva.

107. PPT. Apartado 4.1.2.2. ¿Cuál es el número de equipos Fortinet que tiene actualmente desplegados en Madrid Digital?

**Respuesta:**

4

108. PPT. Apartado 4.1.1.1. Respecto al servicio de ciberinteligencia, ¿Se puede facilitar una estimación de volumetrías aproximadas bajo alcance relativa a los siguientes parámetros? IPs públicas, Número de marcas a monitorizar, Número de dominios bajo alcance, Número de dominios de correo electrónico, Número de VIPs a monitorizar, Número de Aplicaciones Móviles, Número estimado de takedowns anual.

**Respuesta:**

La volumetría actual del servicio es la siguiente:

- Número de marcas: 2 marcas principales: Comunidad de Madrid y Madrid Digital, Agencia para la Administración Digital de la Comunidad de Madrid.
- Dominios y direcciones IP: 10
- Personas de interés: 0
- Número de CPEs: 5 (a nivel de “vendor” según la estructura de CPE del NIST)

En cuanto al número estimado de takedowns anual, el número de dominios maliciosos a cerrar por cada periodo es un dato muy variable difícilmente estimable, depende en muchos casos de factores externos no controlables por la organización, como pueden ser entre otros, las campañas de ataques realizadas por actores maliciosos de todo tipo, y también depende de las medidas de detección que el adjudicatario implemente.

109. PPT. Apartado 4.1.4.2. Respecto a la Plataforma MISP: ¿Podrían especificar si por mantenimiento de la plataforma se refieren al mantenimiento de la máquina (servidor) y el aplicativo (MISP)? Además del mantenimiento operativo de la plataforma y de la ingesta de IOC relevantes, ¿es necesario la operación de la misma tanto en lo que se refiere a la compartición con terceros, como a la diseminación de inteligencia a otras áreas operativas de Madrid Digital?

**Respuesta:**

En el apartado 4.1.4.2 del PPT se especifica: *“Será responsabilidad del adjudicatario garantizar la plena operatividad de esta plataforma, el mantenimiento operativo de esta plataforma, así como de su evolución, durante la vigencia del contrato. Se exigirá la consolidación de toda la información de inteligencia de amenazas puesta a disposición del contrato en esta plataforma.”*

Por tanto, la plena operatividad de la plataforma, que siempre se realizará bajo la supervisión y aprobación de Madrid Digital, incluye todos los elementos necesarios para su ejecución y operación: tanto lo que respecta

al mantenimiento de los servidores, al aplicativo como a la compartición con terceros y áreas operativas de Madrid Digital.

110. PPT. Apartado 4.1.4.4. ¿Podrían indicarnos si Madrid Digital ya dispone del entorno controlado y seguro de pruebas, Sandbox? ¿En caso afirmativo podrían especificar de qué producto se trata, tipo de licenciamiento, si es solución on-premise o cloud, y quien es el propietario de la licencia?

**Respuesta:**

No, actualmente Madrid Digital no cuenta con un entorno de pruebas Sandbox.

111. PPT. Apartado 4.1.4.4. ¿Se podría separar el entorno de malware/forense del entorno de pruebas?

**Respuesta:**

La arquitectura del entorno de pruebas Sandbox queda a criterio del licitador.

112. ¿Podrían proporcionar más información sobre a lo que se refieren cuando indican que el adjudicatario deberá operar y mantener las herramientas? ¿Se refieren a mantener la infraestructura o también a realizar las diferentes actividades identificadas como por ejemplo creación de maquetas, análisis forense, análisis de compatibilidad de aplicaciones...? En el segundo caso ¿Podrían proporcionar más información sobre el requerimiento de análisis de compatibilidad de aplicaciones?

**Respuesta:**

Según se recoge en el PPT, el licitador debe operar y mantener la solución de sandbox que ofrezca, así como ejecutar todas aquellas actividades relacionadas con el análisis de posible código malicioso y su impacto en las infraestructuras de Madrid Digital. La solución debe permitir desplegar aplicaciones en condiciones análogas a las desplegadas en el entorno de Producción.

113. En el anexo I del PCAP se indica que el importe máximo de ejecución es de 11.406.123,20 €. ¿En qué escenario se llegaría a este importe con el descuento que se haga? ¿Sería por prestación de más servicios variables para completar el importe de licitación?

**Respuesta:**

Respondido en la publicación de la resolución 502/2024, de 6 de agosto, de corrección de errores del Pliego de Cláusulas Administrativas (PCAP).

*“...La baja que pueda obtenerse en la adjudicación dará lugar a la ampliación a un mayor número de unidades de los servicios objeto del contrato, sin que pueda en ningún caso sobrepasarse el importe del presupuesto base de licitación...”*

114. ¿Podrían clarificarnos la fecha final para la entrega de preguntas? Se refiere a 12 días antes de la entrega, ¿se refiere a días naturales o laborales?

**Respuesta:**

La cláusula 10 del PCAP, en relación con lo establecido en el artículo 138 de la LCSP, establece que “Los licitadores podrán solicitar información adicional sobre los pliegos y sobre la documentación complementaria con una antelación mínima de **doce días** a la fecha límite fijada para la recepción de ofertas en el anuncio de licitación.” La fecha límite para la recepción de ofertas es el **3 de septiembre**

de 2024, como consta publicado en el perfil de contratante del Portal de la Contratación Pública de la CM.

La Disposición adicional duodécima de la LCSP, en relación con el cómputo de plazos, establece que *“Los plazos establecidos por días en esta Ley se entenderán referidos a **días naturales**, salvo que en la misma se indique expresamente que solo deben computarse los días hábiles”*.

115. PPT. Apartado 4.1.5. ¿Podrían indicar si el contenido de la propuesta formativa y el coste de cada sesión de formación es necesario incluirlo en la propuesta técnica o se podría proporcionar una vez se comience con el servicio?

**Respuesta:**

Tal y como se recoge en el PPT, es necesario que se aporte en la propuesta técnica. El coste de cada sesión formativa será siempre a título informativo. Madrid Digital no asumirá ningún coste adicional por este plan de formación.

116. ¿Las diez páginas del sumario ejecutivo forman parte de la documentación de 100 páginas o son a más?

**Respuesta:**

En el PPT en el punto 9.1. *CONTENIDO DE LAS OFERTAS PARA EL LOTE 1*, se indica que la oferta no debe exceder en ningún caso las 100 páginas, lo que incluye el resumen ejecutivo que debe tener un número máximo de 10 páginas.

117. PPT 4.1.2.1.1. En el primer semestre de contrato, si la ingesta es menor de 3TB/día (por ejemplo, 2TB/día), ¿se abonarán los 3TB/día mínimos requeridos en pliego o se facturará la ingesta real consumida?

**Respuesta:**

La facturación de la plataforma de gestión de eventos de seguridad – SIEM está descrita en la *cláusula 1, Apartado 22. REGIMEN DE PAGOS*. El importe semestral consignado de suscripción de herramienta SIEM contempla el pago en el primer semestre de 3TeraBytes/día. Esta ingesta será revisada semestralmente, de forma que las ampliaciones/reducciones posteriores se realizarán en base al valor de referencia indicado de 500 GigaBytes/día; por tanto, el pago aumentará o decrecerá según la ingesta aumente o disminuya respecto al coste del valor de referencia de 500 Gigabytes/día. Todo ello, considerando que estos importes se verán decrementados por el porcentaje de baja que resulte de aplicación debido a la adjudicación del contrato.

118. PPT 4.1.2.1.1. A partir del primer semestre, si la certificación semestral concluye que la ingesta es inferior a 3TB/día (por ejemplo, 2TB/día), ¿se abonarán los 3TB/día mínimos requeridos en pliego o puede ser que se abone una factura de licenciamiento de SIEM semestral por ejemplo de 2TB/día?

**Respuesta:**

La facturación de la plataforma de gestión de eventos de seguridad – SIEM está descrita en la *cláusula 1, Apartado 22. REGIMEN DE PAGOS*. El importe semestral consignado de suscripción de herramienta SIEM contempla el pago en el primer semestre de 3TeraBytes/día. Esta ingesta será revisada semestralmente, de forma que las ampliaciones/reducciones posteriores se realizarán en base al valor de referencia indicado de 500 GigaBytes/día; por tanto, el pago aumentará o decrecerá según la ingesta aumente o disminuya respecto



al coste del valor de referencia de 500 Gigabytes/día. Todo ello, considerando que estos importes se verán decrementados por el porcentaje de baja que resulte de aplicación debido a la adjudicación del contrato.

119. PCAP 22. ¿Será posible certificar las licencias en el mes 1 de contrato o la primera certificación se realizará como mínimo en el mes 6 del contrato?

**Respuesta:**

En la cláusula 1. Apartado 22 REGIMEN DE PAGOS del PCAP se indica que el pago de las suscripciones de herramientas incluidas en el lote 1 que se efectuarán mediante certificaciones **semestrales**.

En consecuencia, el pago de estas licencias se hará semestralmente, y se abonará en el momento que se certifique que las licencias están a disposición de Madrid Digital.

120. En el apartado 4.1.2.2.2 "Análisis avanzado de tráfico – NDR", se menciona que la solución analizará el tráfico en dos CPDs de Madrid Digital y dos CPDs de la Consejería de Sanidad. Sin embargo, también se menciona la protección de servidores en el CPD principal de EducaMadrid. ¿Podrían aclarar si debemos capturar tráfico en 4 o en 5 CPDs en total?

**Respuesta:**

Tal y como se recoge en el PPT 4.1.2.2.2 Análisis avanzado de tráfico – NDR, [...] *la solución estará dimensionada para proteger como mínimo los siguientes activos: [...], 4.000 servidores, alojados en los dos CPD's de Madrid Digital, 3.000 servidores alojados en los dos CPD's de la Consejería de Sanidad – SERMAS y en el CPD principal de EducaMadrid.*

121. En la página 83 del pliego técnico se mencionan 6 sondas IDS en los CPDs de Madrid Digital y 4 en los CPDs de Sanidad. Sin embargo, en la página 25 se indica que será responsabilidad del ofertante dimensionar el número de sondas. ¿Podrían confirmar si el número de sondas mencionado (6 en Madrid Digital y 4 en Sanidad) es el mínimo requerido, dado que están ubicadas en segmentos y áreas distintas que no pueden consolidarse?

**Respuesta:**

Como se menciona en el punto 4.1.2.2.1 *Análisis de tráfico para detección de intrusiones – sondas IDS* del PPT, Madrid Digital considera que este servicio debe ser sustituido por el servicio de análisis avanzado de tráfico, toda vez que la detección de anomalías a través de firmas se ha visto ampliamente superado por los sistemas NDR, mucho más avanzado.

En el caso específico de sondas IDS ubicadas en los centros hospitalarios, los licitadores deberán indicar en su propuesta técnica de sustitución, si consideran necesario instalar algún equipamiento adicional, en modo local como complemento a los equipamientos centrales a instalar en los CPD's, detallando ventajas e inconvenientes. Madrid Digital se reserva el derecho de aceptar o no la propuesta de equipos locales a instalar que realicen los licitadores.

122. En la página 25 del pliego técnico se especifica que el tráfico a analizar en cada CPD será como mínimo de 20 Gb/seg. ¿Esto implica que se debe ofertar una capacidad mínima de 80 Gb/seg de tráfico agregado entre todos los CPDs, o se puede considerar la posibilidad de sobresuscripciones, dado que no todos los CPDs generan simultáneamente ese volumen de tráfico debido a configuraciones en Activo-Pasivo? Queremos confirmar si se permitirá gestionar el tráfico con una capacidad mínima garantizada de 20 Gb/seg por CPD, pero con la posibilidad de manejar picos de tráfico no constantes.

**Respuesta:**

Tal y como se recoge en el PPT, apartado 4.1.2.2.2 Análisis avanzado de tráfico – NDR, *El dimensionamiento del equipamiento a instalar en los CPD's (sensores) será responsabilidad del adjudicatario, estimándose que el tráfico generado en cada CPD a analizar será como mínimo de 20 Gbit/seg.*

123. En el pliego se especifica que la capacidad del SIEM debe medirse en eventos por segundo (EPS). ¿Podrían proporcionarnos la cantidad actual de EPS generados que el SIEM deberá ser capaz de ingerir y procesar? Esto nos permitirá dimensionar correctamente la solución propuesta.

**Respuesta:**

Tal y como se recoge en el PPT, apartado 4.1.2.1.1 Plataforma de gestión de eventos e información de seguridad – SIEM, *Dimensionamiento de la plataforma: La plataforma deberá estar dimensionada y correctamente licenciada para cumplir los siguientes requisitos [...] Capacidad mínima de ingesta diaria total de 3 TeraBytes, ampliable bajo demanda (y reducible) de eventos, flujos y alertas de seguridad.*

124. En la página 8 (Cláusula 1 Apartado 3) del PCAP se indica que el importe total para los servicios de cuota fija para el lote 1 es de 2.533.499,20€. No obstante, y según la tabla de número de perfiles, % dedicación y horas estimadas indicadas en el PPT página 38 (Apartado 4.2.3 Equipo de Trabajo) si se realiza el producto de las horas estimadas para cada perfil por los importes hora indicados en la página 9 del PCAP (Cláusula 1 Apartado 3), este importe total no coincide con el importe total previamente indicado. ¿Podrían por favor dar más detalle sobre cómo se ha realizado esta estimación?

**Respuesta:**

Los importes base de licitación indicados en la *Cláusula 1 Apartado 3* del PCAP identificados como *Cuota fija – servicios* no solo incluyen el número de personas, % de dedicación y horas estimados para el equipo de trabajo indicados en el Apartado 4.2.3 del PPT, sino también los servicios de cuota fija sin perfiles, pago mensual.

125. En el pliego, se menciona que el proyecto técnico inicial de implantación deberá contemplar la integración de las fuentes operadas actualmente, recogidas en el apartado 10.3 Plataforma SIEM actual de Madrid Digital, así como las alertas generadas por el sistema EDR corporativo (Watchguard) y las generadas por el ecosistema Office 365, que actualmente no están gestionadas de forma centralizada por el SIEM.

Asimismo, entendemos que el entorno incluye 1.500 sistemas de información con 5.700 módulos técnicos asociados, de los cuales 320 sistemas están clasificados como oro, 126.000 endpoints (PC's de sobremesa y portátiles), 4.000 servidores alojados en los dos CPD's de Madrid Digital y 3.000 servidores alojados en los CPD's de la Consejería de Sanidad (SERMAS) y en el CPD principal de EducaMadrid.

Además de las siguientes plataformas y servicios: Cortafuegos de red, balanceadores de tráfico, Routers, Switches, Proxies de navegación, Servicios de nombres de dominio (DNS), • Servicios de acceso remoto RADIUS, Servicios de directorio LDAP y DA, Sistemas de VPN y acceso remoto, Sistemas de correo corporativo, Sistemas antispam y antimalware de correo, Servidores web Apache y Nginx, Servidores de aplicaciones (Weblogic, Tomcat, etc.), Bases de datos Oracle, MySQL y PostgreSQL, Sistemas operativos Linux y Windows, Sistemas EDR corporativos, de puesto de trabajo y de servidor, Servicios de ofimática en la nube, Office 365, Sistema NDR.

No obstante, no se detalla en el pliego el número de eventos mensuales que estas infraestructuras y plataformas generan, dato que resulta esencial para dimensionar adecuadamente la solución propuesta. Por lo tanto, agradeceríamos si pudieran proporcionarnos la información específica sobre el volumen de eventos mensuales generados por las infraestructuras mencionadas.

**Respuesta:**

Tal y como se recoge en el PPT, apartado 4.1.2.1.1 Plataforma de gestión de eventos e información de seguridad – SIEM, *Dimensionamiento de la plataforma: La plataforma deberá estar dimensionada y correctamente licenciada para cumplir los siguientes requisitos [...] Capacidad mínima de ingesta diaria total de 3 TeraBytes, ampliable bajo demanda (y reducible) de eventos, flujos y alertas de seguridad.*

126. Indicar cuántos dominios principales (no subdominios) son los que se quiere proteger y de esos dominios a proteger cuantos incluyen redes sociales.

**Respuesta:**

Tal y como se recoge en el PPT, apartado 4.1.1.1 Identificación de amenazas externas y vigilancia digital, *Al inicio de la ejecución del contrato, Madrid Digital definirá en colaboración con el adjudicatario, la relación completa de activos a vigilar. Esta relación podrá ser modificada a instancias de Madrid Digital en cualquier momento de vigencia del contrato.* Como referencia actualmente se están protegiendo los 10 dominios principales, ninguno de ellos relacionado con redes sociales.

127. Acorde a las respuestas del documento "237-23-nota\_informativa-aclaraciones\_pliegos-2\_fdo\_censurado" recibidas desde Madrid Digital sobre el Throughput para dimensionar la solución NDR, hemos llegado a una estimación del dimensionamiento del throughput total en las redes. Pero nos gustaría una confirmación técnica.

Dado que, en el mismo documento, en las respuestas 73 y 74 se indica que Madrid Digital dispone de Packet Brokers en su red, solicitamos amablemente que Madrid Digital lo confirme mirando en los Packet Brokers que tiene actualmente.

Por otra parte se puede filtrar el tráfico que no es necesario ser analizado, por ejemplo imágenes de resonancias magnéticas y otro tipo de ficheros pesados que no son fácilmente manipulables. Si Madrid Digital hace filtrado en los Packet Brokers, nos gustaría saber qué tipo de tráfico

**Respuesta:**

Tal y como se recoge en el PPT, apartado 4.1.2.2.2 Análisis avanzado de tráfico – NDR, *El dimensionamiento del equipamiento a instalar en los CPD's (sensores) será responsabilidad del adjudicatario, estimándose que el tráfico generado en cada CPD a analizar será como mínimo de 20 Gbit/seg.*

Este valor de throughput es una estimación basada en análisis previos realizados por una muestra de fabricantes de este tipo de soluciones; por tanto, no es un dato de medición real ya que gran parte del tráfico este-oeste está contenido en los hosts físicos que dan soporte a nuestra infraestructura de máquinas virtuales. En consecuencia, el ancho de banda estimado de 20 Gbit/seg incluye tráfico entre máquinas físicas y el tráfico interno en dichos hosts.

Actualmente no se realiza ningún tipo de filtrado de tráfico en los Packet Broker instalados.

128. Nos pueden aclarar si de acuerdo con el PCAP modificado hay que utilizar el modelo de equipo de trabajo de acuerdo con la cláusula 10.4 del PPT y en que sobre se debería incluir.

**Respuesta:**

Tal y como se recoge en el PCAP modificado (7-237-23-pcap-3\_fdo\_censurado.pdf) cláusula 15.8, los *Currículos de los miembros del Equipo prestador del servicio, que deberán presentar, siguiendo el modelo de la cláusula 10.4 del Pliego de Prescripciones Técnicas, [...] el licitador propuesto como adjudicatario, deberá aportar los documentos acreditativos de la Titulación y las Certificaciones de los recursos que forman parte del Equipo de trabajo, a efectos de acreditar el cumplimiento de los requisitos exigidos en el Pliego de Prescripciones Técnicas y de los valorados en los criterios de adjudicación.*



Por tanto, los currículos sólo los presenta el licitador propuesto como adjudicatario, siguiendo el formato especificado en el apartado 10.4 del PPT.

129. En el apartado 8.2 CONDICIONES GENERALES APLICABLES A LOS EQUIPOS DE TRABAJO del Pliego de Prescripciones Técnicas, se especifica en la pag. 71 el siguiente párrafo:

“Los licitadores deberán aportar, un documento de compromiso en el que señalen, que, de resultar adjudicatarios del contrato, pondrán a disposición del servicio un equipo de trabajo, con un número de integrantes adecuado, que cumpla los requerimientos mínimos exigidos, y de estabilidad del equipo, recogidos en el presente pliego de prescripciones técnicas.”

¿Podrían aclarar en que sobre tiene que ir este documento de compromiso? En caso que sea en el sobre 2  
¿Puede ir como anexo para que no compute en las 25 páginas de la oferta técnica?

**Respuesta:**

En el SOBRE Nº 1 - DOCUMENTACIÓN ADMINISTRATIVA, en relación con el ANEXO III: *MODELO DE DECLARACIÓN RESPONSABLE MÚLTIPLE*, concreción de la solvencia requerida.

130. ¿El packet broker actual tiene una limitación a solo interfaces de 10 gig o puede enviar a 25gig/40gig)?  
¿Es por eso que necesitan enviar múltiples interfaces desde el packet broker?

**Respuesta:**

El Network Packet Broker (NPB) actual tiene puertos /10/25Gb (SFP28) y 40/100Gb (QSFP28). La utilización de un tipo de puerto u otro viene marcada por la electrónica de red que se conecta al propio NPB.

131. ¿Qué opciones de reenvío de paquetes a los sensores de NDR hay disponibles actualmente en el datacenter de EducaMadrid?

**Respuesta:**

En el CPD de EducaMadrid no hay Network Packet Broker (NPB).

132. ¿Entre los data centers de Madrid Digital o SERMAS hay algún tipo de conectividad en capa 2, como VLANs extendidas?

**Respuesta:**

Técnicamente existe la posibilidad de tener conectividad de capa 2 entre los dos CPDs mediante la extensión de VLANs. Actualmente dicha posibilidad solo se hace efectiva en casos muy justificados ya que no está recomendada por criterios de operación de comunicaciones.

133. ¿En la infraestructura virtual tiene desplegados VDS con la capacidad de configurar ERSPAN?

**Respuesta:**

Si.

134. En el Lote 1, se valoran como criterios cualitativos cuya cualificación depende de un juicio de valor, con diferentes puntos, la completitud e idoneidad de las soluciones y plataformas propuestas para: el análisis de vulnerabilidades de seguridad de redes y sistemas; La monitorización; La orquestación, automatización y respuesta de incidentes de seguridad; La información relativa a estos criterios debe incluirse en el Sobre 2.

También se valoran como criterios cualitativos evaluables de forma automática por aplicación de fórmulas, con dos puntos cada uno, la inclusión en la propuesta de: (Criterio 3) Una solución para analizar y auditar la postura de seguridad de los servicios en nube; (Criterio 4) Una solución para la revisión de la explotabilidad de vulnerabilidades identificadas en sistemas internos y en sistemas expuestos a Internet (superficie de exposición); (Criterio 5) Una solución para reducir los eventos que se envían al SIEM; (Criterio 6) Una solución SOAR on prem, o en caso de nube, independiente de otros clientes. La respuesta debe ir, como SI o como NO, en el sobre 3.

Hemos entendido que no se puede incluir en el Sobre 2 nada relacionado con los criterios objetivos del Sobre 3, siendo motivo de exclusión, caso de hacerse. Por tanto, no se puede describir en el Sobre 2 el detalle concreto de las soluciones o plataformas que tuvieran relación con esos criterios objetivos porque, de hacerlo, se estaría diciendo implícitamente que SI se incluye la solución o plataforma que responde a este criterio objetivo de valoración y seríamos excluidos del proceso.

Por ejemplo, si se incluyera en nuestra oferta un SOAR (Criterio 6), responderíamos SI en el Sobre 3. Pero no podríamos describir en el Sobre 2 la completitud e idoneidad de la solución SOAR que propusiéramos, viéndonos afectados en la valoración del criterio 7.5.

¿Debemos describir en profundidad en el Sobre 2 el detalle de las soluciones y plataformas que propongamos, aunque eso signifique que estaríamos respondiendo implícitamente que SI a los criterios objetivos del Sobre 3?

**Respuesta:**

No se puede incluir en el Sobre 2 ninguna información relacionada con los aspectos concretos valorados en los criterios cualitativos evaluables de forma automática por aplicación de fórmulas, información que única y exclusivamente ha de contenerse en el Sobre 3.

En los criterios evaluables de forma automática por aplicación de fórmulas, se valoran capacidades específicas que complementan la solución, por lo que se puede describir la solución en el Sobre 2 sin necesidad de hacer referencia a estos puntos concretos que, si se ofertan, deben incluirse en el Sobre 3.

135. Hablando de la fase de implantación de los servicios, (página 26 del PCAP), se indica que la plataforma del SIEM debe estar plenamente operativa en el mes 7. Es decir, hay seis meses para implantar el nuevo SIEM. También se indica así en los SLAs (página 48 del PPT), donde el ANS-11 tiene un tiempo máximo de 180 días naturales.

Sin embargo, en la página 18 del PPT se indica lo siguiente:

La solución propuesta será en nube, preferiblemente pública tipo SaaS, y no debe requerir la instalación de ningún elemento físico o virtual en los Centros de Proceso de Datos (CPD's) de Madrid Digital, salvo los elementos imprescindibles para la recolección de eventos. En todo caso, si durante la fase de implantación del SIEM, antes de la finalización del tiempo previsto de esta fase (tres meses) el adjudicatario declarase la imposibilidad técnica de prestar el servicio requerido en nube ya sea de forma total o parcial, estará obligado a prestar el servicio con solución on-premise en los CPD's de Madrid Digital de forma completa, o bien, mediante solución hibridada en nube y on-premise en los CPD's de Madrid Digital.

Entendemos que el plazo de implantación del SIEM debe ser 6 meses, pero este párrafo nos confunde. ¿Lo podrían aclarar por favor?

**Respuesta:**

El plazo de implantación del SIEM es de 6 meses.

136. Una vez leído el pliego y según nuestra interpretación del mismo.

Entendemos que ahora no es necesario aportar la documentación acreditativa referentes a la capacidad y solvencia económica y técnica (cláusula 1 apartado 6) sino que en el sobre administrativo se debe aportar:

- Declaración responsable del licitador sobre el cumplimiento de los requisitos previos para participar en este procedimiento de contratación. Anexo II DEUC indicando "SI" que se cumplen los requisitos en la sección IV criterios apartado genérico alfa
- Declaración responsable -Declaración responsable múltiple Anexo III
- Compromiso de adscripción a la ejecución del contrato

Y en caso de UTE - Declaración compromiso constitución UTE

Sólo será el adjudicatario o cuando sea requerido por ustedes, el que tendrá que presentar/acreditar todo lo referido a la cláusula 1 apartado 6 del pliego.

¿es correcta nuestra interpretación?

**Respuesta:**

La cláusula 12 del PCAP, recoge la documentación a aportar en el sobre 1.

Será el propuesto como adjudicatario el que tendrá que presentar/acreditar todo lo requerido en la cláusula 1 apartado 6 del PCAP (solvencia económica y técnica), a excepción de las certificaciones y compromisos exigidos en los apartados 2.2 y 2.3 de dicha cláusula, en relación con la solvencia técnica, que deberán aportar todos los licitadores en el sobre 1.

**Por considerar de interés las aclaraciones y en virtud de lo establecido en el *Pliego de Cláusulas Administrativas Particulares*, se remite para su publicación en el perfil de contratante del Portal de la Contratación Pública de la Comunidad de Madrid.**

**El Subdirector General de Servicios a Consejerías**

Firmado digitalmente por: GARCIA LOMBARDIA FRANCISCO RAMON  
Fecha: 2024 08 23 15:33

**Fdo.: Francisco García Lombardía**