

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:

61. PCAP. Pág. 23. Por favor confirmar la fecha inicio del servicio de cada uno de los lotes porque entendemos que existe una errata en el pliego ya que se establece que "el plazo de ejecución del presente contrato será de, 24 meses comprendidos entre 1 de julio de 2024 a 30 de junio de 2026"

Respuesta:

El plazo de ejecución es de veinticuatro (24) meses. Posteriormente en la adjudicación del contrato se reajustará fecha de inicio, y demás aspectos relacionados.

62. PCAP. Pág. 26. En la página 25 se establece que los servicios recogidos en el lote 2, 3 y 4 estarán disponibles desde el inicio de ejecución del contrato, es decir, desde el MES 1. Y por otro lado, afirma que la fase de operación de los servicios tendrá una duración de 23 MESES, desde la finalización de la fase de implantación ¿Confirmar la duración de la fase de implantación para los lotes 2, 3 y 4 será de 1 mes y que será facturable?

Respuesta:

Los servicios del lote 1 se facturan desde el mes 1 y deben cumplir el calendario de fases de implantación, operación y devolución indicados en el PCAP para cada servicio.

Los servicios de los lotes 2, 3 y 4 se facturan desde el mes 1 y deben estar disponibles desde ese mes, la fase de implantación dura un mes.

63. PTT. Pág. 59. Según la página 59 “Los ejercicios contemplarán como mínimo ataques desde Internet, a través de acceso físico la red, a través de conexiones inalámbricas y simulando un atacante interno.” ¿Será necesario desplazar un técnico in situ para la ejecución de los ejercicios de acceso físico y conexión inalámbrica? ¿Cómo se gestionarán el acceso y los permisos a las instalaciones de cada organismo?

Respuesta:

Para las pruebas de acceso físico y/o conexión inalámbrica a la red se requerirá, en principio y salvo indicación en contra por parte de Madrid Digital, la presencia física de las personas del Red Team que se consideren oportunas, por parte de Madrid Digital y del responsable del equipo Red Team, para el buen desarrollo del ataque concreto acordado. Los accesos y permisos serán gestionados por el personal de Madrid Digital según los procedimientos de acceso físico a los edificios requeridos por cada una de las sedes de cada uno de los organismos.

64. PTT. Apartado 9.3.2. En la Página 77 se dice que en la propuesta técnica se debe incluir una "Propuesta de ejercicios de Red Team a ejecutar a lo largo del contrato, detallando equipo de trabajo dedicado, esfuerzo estimado en horas/hombre, vectores de ataque utilizados, tácticas y técnicas de la matriz de MITRE ATT&CK aplicadas." ¿En la propuesta técnica hay que incluir una planificación plurianual de los ejercicios a ejecutar? En la fase 1 de diseño para la cobertura y priorización de la mayor superficie de ataque posible para las diferentes entidades/organismos ¿Los objetivos, los target y la planificación final será revisada conjuntamente con el "white team" de Madrid Digital?

Respuesta:

Según indica el PPT, el alcance de este documento se ajusta a la propuesta de ejercicios de Red Team a realizar a lo largo del contrato. Esta propuesta incluirá el equipo de trabajo dedicado, el esfuerzo estimado en horas/hombre, los vectores de ataque utilizados y las tácticas y técnicas de la matriz de MITRE ATT&CK aplicadas.

Respecto a la segunda pregunta, con carácter general, todos los servicios serán siempre revisados y aprobados por Madrid Digital previo a su ejecución.

65. PTT. Apartado 9.3.2. En la página 59 explica que "deben diferenciarse claramente de los análisis de vulnerabilidades de seguridad de aplicaciones, redes y sistemas (test de intrusión)". Según se solicita en el pliego, el alcance de los ejercicios de Red Team se basarán en los TTPs del framework MITRE ATT&CK que no se establece la distinción por aplicaciones, redes y sistemas ¿se definirán y diferenciarán estos target en la fase de diseño conjuntamente con el White Team de Madrid Digital?

Respuesta:

Tal y como se menciona expresamente en el PPT: *"FASE 1 - Diseño del ejercicio: con el asesoramiento del adjudicatario, se fijarán los parámetros globales del mismo: autorizaciones, comunicaciones, miembros de los distintos equipos (White Team, Red Team), alcance y duración, límites aceptables, objetivos específicos, tareas a realizar, etc. En la definición del ejercicio deberá asegurarse que no se pone en peligro el servicio analizado, ni se producen daños en las infraestructuras o aplicaciones."*

Por tanto, el objetivo del ejercicio, que cuenta con el asesoramiento y aprobación por parte de Madrid Digital, será el que deba diferenciarse del propio objetivo de los análisis de vulnerabilidades de seguridad de aplicaciones, redes y sistemas que es otro servicio independiente circunscrito al LOTE 1.

66. PTT. Pág. 60. En la página 60 se recoge en la revisión de auditoría que el adjudicatario participará en "la revisión de la efectividad de las mismas". Dado que la verificación de las contramedidas/remediación puede tener impacto en la planificación inicial aprobada ¿Se trataría como una gestión del cambio para la revisión de la planificación y del alcance inicial?

Respuesta:

Respecto a este punto, como se menciona en la FASE 6 del PPT, Madrid Digital podrá solicitar al adjudicatario la revisión de las medidas de corrección de los problemas detectados, por lo que el licitador debería considerarlo al planificar el ejercicio.

67. PTT. Pág. 60. En la FASE 2 de Ejecución del ejercicio establece que como mínimo deberá aplicar un 20% de las técnicas y tácticas recogidas en la matriz para empresas MITRE ATT&CK ¿la cobertura mínima de TTPs de MITRE es para la duración del contrato (24 meses) y no para cada uno de los ejercicios? Por ejemplo, si se quiere realizar ejercicios de phishing es imposible ejecutar el 20% de TTPs durante este ejercicio

Respuesta:

El compromiso del 20% mínimo es para el total de ejercicios que se realicen durante el contrato.

68. PTT. Apartado 8.1. Sería posible aclarar la participación de la Oficina Técnica (Lote 4) en los Comités de Dirección y Operación del resto de lotes. ¿Quién será responsable de convocarlos y organizarlos (elaboración de las órdenes del día y actas de reunión)?

Respuesta:

En el punto 8. *MODELO DE GESTIÓN COMÚN A TODOS LOS LOTES* del PPT se indica el modelo de seguimiento y control de la ejecución del contrato de aplicación para cada lote. Con respecto a la elaboración de las actas, corresponde a cada adjudicatario de cada lote elaborarlas. Se espera de la Oficina Técnica que participe en estos comités y desarrolle su servicio según lo que se indica en el punto 7. *LOTE 4: OFICINA TÉCNICA DE SEGUIMIENTO Y CONTROL DE LOS SERVICIOS GESTIONADOS DE CIBERSEGURIDAD*

69. PTT. Pág. 60. En la página 60 en la FASE 3 donde se indica que se incluirá un reporte de auditoría, sería bueno saber qué gestor de vulnerabilidades tienen para saber si tenemos que hacer además del informe, algún fichero que luego se pueda importar por ejemplo en ServiceNow, Jira, etc, y así en los seguimientos poder priorizar por criticidad, también que se pueda llevar a los KPIs....

Respuesta:

Actualmente, Madrid Digital cuenta con la plataforma Rapid7 como gestor de vulnerabilidades. En cualquier caso, la integración de los resultados obtenidos en los ejercicios de Red Team en este, u otro gestor considerado por el licitador, queda a criterio de la oferta técnica que realice.

70. ¿Existe conectividad interna a nivel 3 de red, entre los cuatro (4) CPDs, es decir, los dos de Madrid Digital y los dos de la Consejería de Sanidad?

Respuesta:

Sí.

71. ¿Existe conectividad interna a nivel 3 de red entre los 37 Centros Hospitalarios y 22 Centros Sanitarios con el CPD Principal?

Respuesta:

Sí.

72. ¿Se puede proporcionar una estimación del Ancho de Banda de Entrada/Salida que localmente tienen los 59 Centros Sanitarios/Hospitalarios o los sensores IDS actuales objetos de sustitución?

Respuesta:

Todos los centros tienen líneas de 1 Gbps excepto 5 hospitales, que tienen líneas de 10 Gbps (aunque de momento con caudales contratados de 2 Gbps). Estos hospitales son:

H. Clínico San Carlos

H. GUGM

H. H12O

H. La Paz

H. Ramón y Cajal

73. ¿MADRID DIGITAL dispone en sus 4 CPDs (2 de Madrid Digital / 2 de la Consejería de Sanidad) con tecnología para redirigir el tráfico de los segmentos de red objeto de inspección a los futuros Sensores NDR que se desplegarán? Es decir, ¿cuenta con tecnología del tipo NETWORK PACKET BROKER o NETWORK TAPs?

Respuesta:

Sí, se disponen de Network Packet brokers y sus correspondientes Network TAPs, en los 4 CPDs (2 de Madrid Digital y 2 de la Consejería de Sanidad).

74. ¿MADRID DIGITAL dispone en sus 59 centros Hospitalarios/Sanitarios tecnología para redirigir el tráfico de los segmentos de red objeto de inspección a los futuros Sensores NDR que se desplegarán? Es decir, ¿cuenta con tecnología del tipo NETWORK PACKET BROKER o NETWORK TAPs?

Respuesta:

Actualmente, no se dispone de NPB o TAPs en ninguno de los 59 centros sanitarios indicados.

75. En caso de proponer un producto alternativo a Rapid7 para la parte de análisis de vulnerabilidades, ¿se podrá disponer de la máquina on-premise que se esté actualmente utilizando en MD para instalar la sonda del nuevo producto? ¿tendrá algún coste para el proveedor disponer de esa máquina?

Respuesta:

Respecto a este punto, tal y como se menciona en el PPT, *los licitadores deberán indicar en su oferta si proponen la continuidad de la plataforma de análisis de vulnerabilidades basada en Rapid7 o su sustitución, debiendo tener en cuenta la obligación de renovación por parte del adjudicatario del contrato, de las licencias de producto correspondientes.* Así mismo, en este apartado, se menciona *que los licitadores deberán indicar en su oferta el conjunto de herramientas utilizadas para el servicio (bien sea Rapid7 o no), considerándose dentro del coste del servicio todos los gastos derivados de las mismas (licencias, mantenimientos, actualizaciones, etc.)*

En otro punto, en el último párrafo de la página 23 del PPT, se indica que *queda a criterio de los licitadores la reutilización total o parcial de la infraestructura actual.* En este escenario, todos los costes derivados del mantenimiento operativo de los componentes (hw, sw) irán por cuenta del adjudicatario. Por tanto, Madrid Digital no asumirá ningún coste adicional de despliegue de la nueva solución.

76. En la descripción de los criterios Cualitativos "Número Adicional de horas de recursos asociados a los ejercicios de red team", dice "las horas adicionales ofertadas como mejora serán las primeras que se consuman". Entendemos que se trata de incrementar las horas del equipo adicionalmente al equipo mínimo solicitado (1 JP 40h/mes y 2 Analistas de seguridad 80h/mes) desde el inicio hasta que se agoten las horas ofrecidas sin que esto tenga repercusión sobre la facturación establecida en la pagina 37 del PCAP, es decir, trimestralmente se facturaran las horas del equipo establecidas para cada ejercicio de Red Team y adicionalmente, sin coste, los ejercicios adicionales con las horas sin coste ofertadas. Es decir, primera factura la correspondiente a los meses 1 2 y 3 de proyecto.

Respuesta:

En la *cláusula 1, Apartado 8 CRITERIOS OBJETIVOS DE ADJUDICACIÓN DEL CONTRATO del PCAP*, respecto al LOTE 3 se indica que esas horas son adicionales y deben permitir ejecutar un mayor número de ejercicios, sin coste adicional. En caso de ser necesario ampliar servicios, estas horas adicionales serán las primeras en consumirse sin coste.

77. En la descripción de los criterios Cualitativos "Número Adicional de horas de consultores especializados en ciberseguridad y seguridad de la información". Entendemos que se trata de incrementar las horas del equipo adicionalmente al equipo mínimo solicitado (2 consultores) desde el inicio hasta que se agoten las horas ofrecidas sin que esto tenga repercusión sobre la facturación establecida en la pag 37 del PCAP, es decir, pago recurrente trimestral desde el inicio del proyecto (primera factura la correspondiente a los meses 1 2 y tres de proyecto)

Respuesta:

En la *cláusula 1, Apartado 8 CRITERIOS OBJETIVOS DE ADJUDICACIÓN DEL CONTRATO del PCAP*, respecto al LOTE 4 se indica que esas horas son adicionales y deben permitir reforzar el equipo humano de la oficina, sin coste adicional. En caso de ser necesario ampliar servicios, estas horas adicionales serán las primeras en consumirse sin coste.

78. En la CLÁUSULA 15.- ACREDITACIÓN DE LA CAPACIDAD PARA CONTRATAR Y PROPUESTA DE ADJUDICACIÓN, se especifica la documentación a presentar, y , entre ella, en la pág. 61, 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. ¿Se entiende que no hay que presentar los modelos de CVs en la propuesta en ninguno de los sobres sino sólo en caso de ser adjudicatarios, es así?

Respuesta:

Consultar la nueva versión publicada y corregida del Pliego de Cláusulas Administrativas (PCAP), los CVs los presenta el licitador propuesto como adjudicatario, según se indica en la cláusula 15 del PCAP.

79. ¿Habría algún inconveniente en caso de que algunas de las sedes del grupo no se encuentren en estos momentos unificadas en el registro mercantil de España para acreditar la solvencia que solicitan? Ya que estaríamos interesados en acudir de forma conjunta contando con todas las sedes de XXXX en forma de unión temporal, pero dos de las empresas/sedes del grupo se encuentran fuera del territorio español.

Respuesta:

Se deberá tener en cuenta lo establecido en los Artículos 69 y 75 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP).

80. En referencia al punto 4.1.2.1.1 Plataforma de gestión de eventos e información de seguridad – SIEM en la página 23 del PPT se indica “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 a Elastic – SIEM-DATALAKE”. Para poder asumir el mantenimiento de estas licencias, ¿podrían indicarnos si existe un acuerdo de tarifas asociadas en la devolución del servicio y a cuanto importe asciende? ¿tendrá obligación del adjudicatario de realizar un acuerdo con el actual proveedor?

Respuesta:

En el apartado 4.1.2.1.1 *Plataforma de gestión de eventos e información de seguridad – SIEM* del PPT en su último párrafo se indica de forma textual que: *El adjudicatario estará obligado a su mantenimiento operativo hasta su sustitución por la nueva propuesta*. Corresponde al adjudicatario asumir este mantenimiento, dejando a su criterio la forma y condiciones para hacerlo.

81. En referencia al requerimiento incluido en 4.1.1 Servicios de prevención, más concretamente 4.1.1.1 Identificación de amenazas externas y vigilancia digital, descrito en la página 11 del PPT, para poder dimensionar correctamente dicho servicio, sería necesario conocer el número de dominios de búsqueda. ¿Podrían facilitarnos esta información?

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)

82. En todo documento de PPT se solicitan una serie de servicios que posteriormente están adscritos a una valoración en base a criterios evaluables de forma automática por fórmulas, como por ejemplo aportar de una solución de CPSM. Dado que es un criterio evaluable por fórmula, ¿se debería describir técnicamente en la Memoria Técnica la solución aportada y como permitiría abordar el requisito expresado por Madrid Digital o por el contrario no se puede realizar ninguna referencia a la solución propuesta para abordar dicho requisito? Al no poder hacer referencia en el documento técnico a ningún requisito adscrito a criterios evaluables de forma automática, en la memoria técnica no se podría describir ninguno de esos servicios. ¿es correcto?

Respuesta:

Los criterios evaluables por fórmula se complementan según el *anexo V* del PCAP.

83. En referencia al punto 4.1.2.1.1 Plataforma de gestión de eventos e información de seguridad – SIEM del PPT, dónde se hace describe el requisito sobre las líneas de comunicaciones dedicadas para poder enviar los logs tanto de plataformas on-premise como en cloud y, con el fin de poder realizar el correcto dimensionamiento de las mismas, queríamos formular dos preguntas relativas a las tecnologías cloud actualmente en uso o en fase de implantación. En lo referente a la integración del servicio de correo Exchange online, ¿es necesario o se valorará positivamente integrar estos usuarios con la plataforma SIEM/SOAR propuesta? En caso afirmativo sería interesante conocer cuántos usuarios han sido migrados a Exchange online.

Respuesta:

En su oferta, el adjudicatario deberá mantener como mínimo la relación de fuentes de logs indicada en el punto 10.3 PLATAFORMA SIEM ACTUAL DE MADRID DIGITAL, así como proponer nuevas fuentes de logs bajo su criterio y conocimiento que refuercen la seguridad global del Organismo.

A fecha de agosto de 2024 se ha migrado entorno al 35 % de las cuentas de los usuarios a Exchange online.

84. En referencia al punto 4.1.2.1.1 Plataforma de gestión de eventos e información de seguridad – SIEM del PPT, dónde se hace describe el requisito sobre las líneas de comunicaciones dedicadas para poder enviar los logs tanto de plataformas on-premise como en cloud y, con el fin de poder realizar el correcto dimensionamiento de las mismas, queríamos formular dos preguntas relativas a las tecnologías cloud actualmente en uso o en fase de implantación. Considerando que puede resultar interesante integrar las alertas e incidentes de la solución de CASB y de los procesos de autenticación de Azure AD en la plataforma SIEM/SOAR propuesta, ¿qué solución de CASB se utiliza actualmente en Madrid Digital? ¿Cómo se protegen los procesos de autenticación en Azure AD?

Respuesta:

Respecto al CASB, actualmente, Madrid Digital está en proceso de evaluación de las funcionalidades ofrecidas por las posibles tecnologías ofrecidas por Microsoft en este tipo de soluciones.

En cuanto a la protección de los procesos de autenticación, Madrid Digital dispone de autenticación reforzada por doble factor además de políticas de detección de anomalías en autenticación.

85. ¿Cómo está actualmente integrada la fuente InfoBlox en elastic?, ¿está desplegado un Infoblox Data Connector?

Respuesta:

Actualmente, Infoblox no es una de las fuentes integradas en Elastic.

86. PPT. Pág. 36. La concienciación con píldoras, cursos online o videos divulgativos ¿será para los 126.000 usuarios o sólo para el personal técnico de Madrid Digital?

Respuesta:

Se circunscribe al personal de Madrid Digital que asciende a 660 usuarios, en previsión de crecimiento hasta unos 700.

87. Lote 4. En la página 65 afirma que la oficina técnica se encargará de la organización de la documentación de seguimiento, entre ellos, los "Cuadros de mando, informes agregados que reflejen toda la actividad realizada, que deberán realizarse en PowerBI" ¿Está PowerBI actualmente integrado con las soluciones corporativa de ticketing (ITSM-FARO)?

Respuesta:

No.

88. Lote 4. En la página 77 afirma que en la propuesta técnica se deberá proporcionar un "contenido y estructura de cuadro de mando de prestación del servicio de la OTSC-Ciber, considerando que PowerBI es la herramienta corporativa". Y por otro lado, los adjudicatorios del resto de lotes también deben proponer cuadros de mando para seguimiento de KPIs y ANS en PowerBI ¿Quién será responsable de la definición de las métricas y la configuración de cuadros de mando de cada uno de los lotes?

Respuesta:

El alcance de cada lote y servicios incluidos en los mismos queda perfectamente definido en el PPT. El adjudicatario de cada lote será responsable, exclusivamente, de los objetivos marcados para tal fin. Madrid Digital se reserva el derecho de aceptar o no la definición de las métricas y la configuración de los cuadros de mando propuestos, y proponer nuevas métricas y cuadros de mando.

89. Para el Lote 1, revisando el número de personas, % de dedicación y horas estimados para el equipo de trabajo indicados en el apartado 4.2.3 Equipo de trabajo (servicios cuota fija y servicios cuota variable) del PPT, los importes hora (IVA no incluido) para los perfiles de ambos servicios y el presupuesto base de licitación indicados en la Cláusula 1 Apartado 3 del PCAP, se ha identificado que al realizar el cálculo de las horas del equipo de trabajo por las tarifas (sin IVA) de los diferentes perfiles, no coincide con los importes base de licitación para los servicios de cuota fija y cuota variable. ¿Se trata de un error o los cálculos son correctos? Si la respuesta es el segundo caso, ¿Podrían por favor darnos más de detalle de como se ha realizado la estimación del presupuesto base para estos servicios?

Respuesta:

Los importes base de licitación indicados en la *Cláusula 1 Apartado 3* del PCAP 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 el resto de los conceptos facturables como, por ejemplo, el número de activos para los análisis de vulnerabilidades de sistemas y redes, NDR y el número de Terabytes dimensionados para la plataforma de gestión de eventos - SIEM.

90. Revisando el pliego, para el Lote 1, la proposición económica que se indica en el Anexo 1 del PCAP, considera únicamente el porcentaje general de baja a aplicar sobre el presupuesto base de licitación (servicios cuota fija, cuota variable y subscripciones). De cara a la facturación trimestral o semestral de servicios y subscripciones, ¿el mismo porcentaje de baja general se aplica a los tres conceptos individualmente?

Respuesta:

Sí.

91. Revisando el PPT del Lote 1 se especifica que en los CPDs de MADRID DIGITAL se disponen de 6 Sondas IDS. Se deduce que están instaladas 3 Sondas en cada CPD de Madrid Digital ¿es correcto? Se podría especificar ¿cuántos Segmentos de Red monitoriza cada Sonda IDS? Y ¿Cuántos Puertos Físicos utiliza cada Sonda?

Respuesta:

Actualmente, están desplegadas 4 sondas en un CPD y 2 en el otro. No obstante, 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. Por tanto, la propuesta de solución no tiene porqué observar dicha relación de 4:2.

En cuanto a segmentos se monitorizan todos los segmentos troncales de entrada salida a internet, en total 6 en el CPD principal y 5 en el secundario, y los segmentos que implementan los accesos a los servicios públicos como a los privados, siendo en este caso, 10 segmentos de red en el CPD principal y 2 en el secundario .

Los puertos que están previstos para dar conectividad a las sondas son:

8 puertos de 10 Gbs (4 activos y 4 en backup) en el CPD principal

4 puertos de 10 Gbps (2 activos y 2 en backup) en el CPD de secundario

92. Revisando el PPT del Lote 1 se especifica que en los CPDs de la Consejería de Sanidad se disponen de 4 Sondas IDS. Se deduce que están instaladas 2 Sondas en cada CPD de Madrid Digital ¿es correcto? Se podría especificar ¿cuántos Segmentos de Red monitoriza cada Sonda IDS? Y ¿Cuántos Puertos Físicos utiliza cada Sonda?

Respuesta:

Sí, existen 2 sondas en cada CPD de la Consejería de Sanidad.

Los segmentos de red que se monitorizan son las conexiones troncales entre los routers de operadora y los switches principales de sede.

En cuanto a la última pregunta, está previstos para dar conectividad a las sondas de 4 puertos de 10 Gbps por CPD.

93. En la página 61 del PPT se menciona que el Jefe de Proyecto será responsable de la coordinación e interlocución con los equipos de Madrid Digital (White Team y Blue Team). ¿Cuántos equipos hay en Madrid Digital y qué roles específicos tendrán el White Team y el Red Team? Además, ¿serán los equipos White Team los encargados de definir el alcance y limitaciones, y gestionar las autorizaciones correspondientes, como por ejemplo, para realizar pruebas en el CPD de Madrid Digital, CPD Sermas, CPD EducaMadrid o pruebas onsite en los diferentes organismos?

Respuesta:

Los equipos, roles y alcance de los objetivos y responsabilidad de cada servicio recogido en el PPT están perfectamente definidos en cada uno de ellos.

Para las pruebas acceso físico y/o conexión inalámbrica a la red se requerirá, en principio y salvo indicación en contra por parte de Madrid Digital, la presencia física de las personas del Red Team que se consideren oportunas, por parte de Madrid Digital y del responsable del equipo Red Team, para el buen desarrollo del ataque concreto acordado. Los accesos y permisos serán gestionados por el personal de Madrid Digital según los procedimientos de acceso físico a los edificios requeridos por cada una de las sedes, de cada uno de los organismos.

94. Se ruega confirmación de que, a efectos de las incompatibilidades previstas, al no indicar nada en contrario los Pliegos aplicará lo establecido en el art. 99.4 LCSP y, por tanto, a efectos de las limitaciones en las uniones de empresarios serán éstas y no sus componentes las consideradas candidato o licitador.

Respuesta:

Sí.

95. Para la solución de análisis de vulnerabilidades de seguridad de sistemas y redes que se solicita en el Lote 1, ¿Madrid Digital tiene preferencia por una solución de análisis on-premise o en Nube?

Respuesta:

La propuesta de solución de análisis de vulnerabilidades de seguridad de sistemas y redes queda a criterio del licitador, observando el resto de los servicios definidos en el pliego, las características particulares de cada uno de ellos y la arquitectura actual de sistemas y redes desplegada en Madrid Digital.

96. Para el lote 4, hay acceso a datos personales? Entendemos que en los lotes 1 2 y 3 sí lo hay, pero en el 4 no puesto que solo se realizan tareas de gobierno y seguimiento

Respuesta:

Sí, existe acceso a datos de carácter personal también en el lote 4.

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.

**La Subdirectora de la Subdirección General de Ciberseguridad,
Protección de Datos y Privacidad**

Firmado digitalmente por: MUÑOZ FUENTES ESTHER
Fecha: 2024 08 14 12:32

Fdo.: Esther Muñoz Fuentes