SERVICIO INTEGRAL DE CIBERSEGURIDAD GESTIONADA DE IFEMA MADRID

Expediente 26/033 – 2000028564

-. RESPUESTAS A CONSULTAS .-

CONSULTAS REALIZADAS

Les informamos de las consultas realizadas por las empresas interesadas y de las respuestas facilitadas por IFEMA MADRID, relacionadas con el expediente de referencia:

1. Buenas tardes. Se indica en el pliego la necesidad de presentar el ANEXO X: Modelo de Documento de Compromiso de Confidencialidad para poder acceder al anexo Situación Actual Exp 26_033 CONFIDENCIAL. No obstante, entre la documentación publicada no se localiza ningún anexo con dicha denominación. El Anexo X disponible corresponde a una declaración de confidencialidad de la información aportada por el licitador y no a un compromiso de confidencialidad para el acceso a información técnica restringida. Rogamos indiquen dónde puede obtenerse el modelo referido o, en su defecto, si será facilitado por IFEMA una vez solicitada la documentación técnica confidencial. Gracias.

   Respuesta IFEMA.

   - Se ha realizado la publicación del documento "FE DE ERRATAS_Exp 26 033", en el cual se rectifica el nombre del anexo que corresponde a la solicitud de documentación confidencial.
   - Adicionalmente, se ha realizado la publicación del documento "Anexo XXIII Compromiso de Confidencialidad_Exp 26 033".

2. Buenas tardes. En el PPT, pág. 28 (entre otros), se habla de un documento denominado SLA_Exp 26 033_Servicio Ciberseguridad, pero el mismo no parece estar disponible en su portal. ¿Podrían indicarnos cómo conseguirlo? Muchas gracias.

   Respuesta IFEMA.

   - Es parte de la documentación confidencial, por tanto, no está disponible en el portal.

3. 7.1.- ADSCRIPCIÓN DE MEDIOS OBLIGATORIA A LA EJECUCIÓN DEL CONTRATO (SERVICIOS OPERATIVOS DE CIBERSEGURIDAD Y GESTIÓN DE LICENCIA): Se especifica que el perfil de Service Manager requiere Dedicación Exclusiva pero en la documentación técnica no se hace referencia a ello y tampoco se identifica una partida presupuestaria específica asignada, se requiere aclaración de este punto.

Respuesta IFEMA.

El perfil debe estar incluido en el servicio, como tal. No hay partida presupuestaria específica para este perfil puesto que se considera que está embebido dentro del coste del servicio.

4. 3.1.2. Análisis de vulnerabilidades (sistemas y redes): Actualmente se dispone de herramienta de escaneos ?? Indicar cual, en caso de respuesta negativa confirmar que debemos incluirla dentro del servicio de Gestión de vulnerabilidades

Respuesta IFEMA.

Actualmente IFEMA MADRID, no cuenta con una herramienta de escaneo de vulnerabilidades.
Sí deberá incluirla dentro del servicio de vulnerabilidades.

5. 3.1.2. Análisis de vulnerabilidades (sistemas y redes): La herramienta de escaneos (si disponen de ella) actual incluye el módulo de escaneos App-Web ??

Respuesta IFEMA.
IFEMA MADRID, actualmente no dispone de herramienta de escaneos

6. 3.1.2. Análisis de vulnerabilidades (sistemas y redes): Número total de vulnerabilidades aproximado gestionado en el último año ??

Respuesta IFEMA.

Se considera que esta información no es necesaria para la elaboración de la oferta.

7. 3.1.2. Análisis de vulnerabilidades (sistemas y redes): Dentro de las tareas del Servicio de Gestión de Vulnerabilidades se requiere Gestión con las áreas resolutoras hasta que se parchea las vulnerabilidades o esa responsabilidad recaera sobre IFEMA ??

Respuesta IFEMA.

No se requiere la gestión con las áreas resolutoras pero sí la colaboración, soporte y apoyo tal y como se indica en el punto **3.1.2 Análisis de vulnerabilidades (sistemas y redes)** del ppt

"Aunque IFEMA MADRID es responsable de aplicar las correcciones en los sistemas afectados, el adjudicatario apoyará y dará soporte en las tareas necesarias para facilitar la resolución de las vulnerabilidades"

8. 3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad: Qué tecnología SIEM se dispone actualmente ??

Respuesta IFEMA.

Se considera que esta información no es necesaria para la elaboración de la oferta.

.

9. 3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad: Cual es el tiempo de retención que se aplica actualmente ?? Y cual es el mínimo requerido ??

   Respuesta IFEMA.

   Actualmente está en vigor un periodo de retención de eventos de seguridad de 3 meses. Por lo tanto y como mínimo debería mantenerse el mismo tiempo

10. 3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad: Cuantos Casos de Uso se dispone actualmente en Producción ?? En caso de que se realice un cambio de tecnología, se requiere la migración de los Casos de Uso en Producción ?? En tal caso confirmar de que se transferirá la lógica de detección (query) para su migración ??

    Respuesta IFEMA.

    IFEMA MADRID tiene actualmente 63 casos de uso en Producción.

    Sí, se confirma. En el contrato actual se contempla que el proveedor saliente transfiera el servicio al proveedor entrante

11. 3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad: Actualmente se disponen de Playbooks Automatizados de contención/remediación vía SOAR ?? Se contempla como evolución del servicio su implementación ??

    Respuesta IFEMA.

    "*Se disponen de Playbooks Automatizados de contención/remediación vía SOAR*?". Esta cuestión no es determinante para la elaboración de la oferta.

    Tal y como se indica en el ppt en el punto **3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad.** el proveedor deberá aplicar las medidas y herramientas para cumplir con el objeto del servicio

    "*En consecuencia, IFEMA MADRID requiere que el adjudicatario disponga de un* ***Centro de Operaciones de Seguridad (SOC)*** *con capacidad* ***24x7x365****, orientado a la prevención, detección, análisis y respuesta ante eventos e incidentes de seguridad que puedan afectar a sus infraestructuras y servicios. El SOC deberá monitorizar y correlacionar la actividad de las redes, infraestructuras y sistemas, identificar y priorizar riesgos y vulnerabilidades, y coordinar una respuesta ágil que permita la contención y neutralización de ataques, incluyendo la gestión y aplicación de indicadores de compromiso (IoC) y otras medidas preventivas que resulten necesarias*".

12. 3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad: Qué tecnología de Ticketing se dispone actualmente ??

    Respuesta IFEMA.

    IFEMA MADRID cuenta con la herramienta de **ticketing ServiceNow**

13. 3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad: Se requiere integración entre ambos Sistemas de Ticketing de forma bidireccional (SOC a IFEMA y viceversa) para que en ambos entornos se transfiera la misma información o un flujo de comunicación vía correo electrónico unidireccional (SOC a IFEMA) es válido ??

    Respuesta IFEMA.

    Tal y como se indica en el ppt para el Servicio Integral de Ciberseguridad Gestionada de IFEMA MADRID, en los diferentes apartados, todas las acciones que se realicen dentro del objeto del servicio deben quedar registradas en la herramienta de ticketing ITSM de IFEMA MADRID.
    Mientras que esté reflejado en la herramienta de IFEMA MADRID, la vía establecida por el contratista no es relevante.

14. 3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad: Se hace referencia a la información del nº de fuentes y consumo de EPS recogido en el documento Situación Actual Exp 26_033 CONFIDENCIAL/Apartado 5. Información relativa al SOC SIEM y EPS. No obstante, podrían por favor compartir información del nº medio de alertas mensuales que reciben, discriminando si incluyen o no el nº de falsos positivos?

    Respuesta IFEMA.

    Toda la información de volumetría se encuentra en el "Documento de Situación Actual Confidencial" indicado en el ppt.

15. 3.3.1. Gestión de respuesta ante incidentes (DFIR): Se requiere de cadena custodia Legal que posteriormente pueda ser utilizado en un proceso Judicial ??

    Respuesta IFEMA.

    En algún caso, puede ser requerido Cadena de Custodia Legal

16. 3.5. Certificaciones, riesgos y cumplimiento norNo mativo: Podría confirmar la dedicación reuqerida en número de jornadas/horas por semana, y si se requiere combinar presencial y remoto? A modo de ejemplo, podrían especificarlo como han hecho en el apartado 3.4. Consultoría experta en ciberseguridad?

    Respuesta IFEMA.

    No podemos confirmar la dedicación. Esta irá en función de los objetivos del servicio, de manera estructurada y lógica.

17. 3.6. Servicio de Administración de infraestructura de seguridad y plataformas de ciberseguridad: Número total de intervenciones fuera de horario laboral ejecutadas en el último año ??

    Respuesta IFEMA.

    No han superado las 20 h.

18. 3.6. Servicio de Administración de infraestructura de seguridad y plataformas de ciberseguridad: En el punto 4. (Horario) se especifica que la su cobertura es en 8x5, pueden confirmar que no se requiere disponibilidad adicional 24x7 en modalidad de guardia ??

    Respuesta IFEMA.

    El horario indicado corresponde a la dedicación del técnico que operará con las infraestructuras de ciberseguridad **on premise**.
    En caso de necesidad de interacción con los sistemas de ciberseguridad objeto del servicio, el SOC deberá cubrirla tal y como se indica en el ppt. **3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad**

    *"En consecuencia, IFEMA MADRID requiere que el adjudicatario disponga de un **Centro de Operaciones de Seguridad (SOC)** con capacidad **24x7x365**, orientado a la prevención, detección, análisis y respuesta ante eventos e incidentes de seguridad que puedan afectar a sus infraestructuras y servicios. El SOC deberá monitorizar y correlacionar la actividad de las redes, infraestructuras y sistemas, identificar y priorizar riesgos y vulnerabilidades, y coordinar una respuesta ágil que permita la contención y neutralización de ataques, incluyendo la gestión y aplicación de indicadores de compromiso (IoC) y otras medidas preventivas que resulten necesarias."*

    Es responsabilidad del SOC llevar a cabo cualquier acción para la mitigación de incidentes en los sistemas de ciberseguridad objeto del contrato.

19. 3.6. Servicio de Administración de infraestructura de seguridad y plataformas de ciberseguridad: Se indican como plataformas a administrar (mínimo) las siguientes: FWs y seguridad perimetral, Seguridad del correo electrónico, protección de endpoint (EDR) y herramientas de seguridsd en MS 365 y Azure. No obstante se indica más adelante que tienen micro CLAUDIA. Pueden confirmar si es obligado gestionar o administrar esta herramienta? o es algo que se puede ofertar de forma opcional?

    Respuesta IFEMA.

    Sí. es obligatorio gestionar la herramienta tal y como se indica en el ppt **3.6. Servicio de Administración de infraestructura de seguridad y plataformas de ciberseguridad,** se indica lo siguiente:

    *"En el marco del presente contrato, IFEMA MADRID requiere un servicio de **administración y operación técnica** de carácter **presencial** sobre las plataformas y sistemas de ciberseguridad objeto del contrato, a prestar en la sede corporativa de IFEMA MADRID."*

20. Buenos días. En las págs. 32 y 33 del PPT se indica un límite de 20 páginas para la documentación técnica (contenido obligatorio y contenido valorable). Dicho límite, ¿aplica de forma separada a cada bloque (pudiendo entregar hasta 40 páginas entre los dos documentos descritos en los puntos 11 y 12) o es la extensión máxima de todo el contenido del Sobre 2? Muchas gracias.

    Respuesta IFEMA.

Se admiten 20 páginas por cada bloque, de acuerdo como se indica en el ppt de los siguientes apartados.

11. Documentación técnica (contenido obligatorio) para entregar por el ofertante. Sobre 2.

La información para incluir en este sobre, NO DEBERÁ EXTENDERSE EN MÁS DE 20 PÁGINAS (1 cara) y deberá seguir estrictamente el guion indicado a continuación:

12. Documentación técnica para entregar por el ofertante (contenido sujeto a valoración). Sobre 2.

La información para incluir en este sobre, NO DEBERÁ EXTENDERSE EN MÁS DE 20 PÁGINAS (1 cara) y deberá seguir estrictamente el guion indicado a continuación:

21. Buenos días. En la página 6 del Cuadro de Características del PCAP, se piden certificaciones oficiales del personal adscrito al servicio, indicándose que es obligatoria al menos una certificación en vigor de cada punto listado (4 en total). Entendemos entonces que se deben presentar, como mínimo, una certificación de FW/perimetral, otra de seguridad de correo, otra de EDR y otra de O365/Azure, y que dichas certificaciones podría tenerlas cualquier persona del equipo dedicado al proyecto (un perfil concreto podría tener 2, otro ninguna, etc., pero el equipo al completo debe disponer en global de esas 4 certificaciones). ¿Es correcto este planteamiento? Muchas gracias.

Respuesta IFEMA.

Sí, deben presentarse las certificaciones indicadas. Las certificaciones solicitadas deberán presentarse por cada perfil de acuerdo a lo indicado en ANEXO I AL PLIEGO DE CLÁUSULAS ADMINISTRATIVAS PARTICULARES CUADRO DE CARACTERÍSTICAS , en el apartado 7 – SOLVENCIA

[X] Así mismo, se requiere al licitador que haya presentado la mejor oferta que presente, junto con el anterior compromiso, la siguiente documentación complementaria para su acreditación:
- Certificaciones oficiales de los perfiles mencionados, **siendo obligatoria**:
  Certificación de Check Point.
  CV con experiencia igual o superior a 5 años al objeto del contrato.

- Certificaciones oficiales del personal adscrito al servicio, **siendo obligatoria al menos una** certificación en vigor:
  Firewalls y seguridad perimetral.
  Seguridad de correo electrónico.
  Protección de endpoint (EDR).

22. Buenos días. En la página 29 del Cuadro de Características del PCAP se indica que no hay plazo de garantía. Sin embargo, en el PPT, pág. 32 (ap. 10), se indica un mínimo de 6 meses. ¿Pueden decirnos qué opción prevalece? Muchas gracias.

Respuesta IFEMA.

Prevalece lo indicado en el PPT, apartado 10. Garantía de los trabajos y titularidad.

En cuanto a lo indicado en el Anexo I al PCAP, apartado 25.- PLAZO DE GARANTÍA (Cláusula 42), esto se refiere a otra tipología de proyectos (obras, suministros, proyectos con entregas parciales), por lo tanto, en este caso no aplica este literal sino lo que indica en el ppt por la naturaleza del servicio.

23. Buenos días. En la página 6 del Cuadro de Características del PCAP, se indica que el Consultor Experto en Ciberseguridad debe tener dedicación exclusiva. Sin embargo, en la página 18 del PPT, se establecen para este servicio 104 jornadas anuales (2 jornadas a la semana, una presencial y otra remota). Entendemos que prevalece esto último y que, por tanto, la dedicación al 100% sería solamente en esos dos días de dedicación al proyecto, ¿correcto? Por otro lado, respecto de los Administradores de Sistemas, ¿qué dedicación total se requiere? Entendemos que, aunque solo se pide dedicación exclusiva durante las jornadas presenciales, como el servicio es totalmente presencial, solo podría haber dedicación a otros proyectos si las jornadas a cubrir se reparten entre 2 o más perfiles, ¿es así?. Muchas gracias

Respuesta IFEMA.

- La dedicación exclusiva del Consultor Experto en Ciberseguridad será durante las jornadas de prestación del servicio a IFEMA MADRID.

-la dedicación del perfil de administrador de sistemas será del 100% cuando preste servicio a IFEMA de forma presencial o remota.
De acuerdo lo que se indica en el apartado 3.6 del ppt :

"*La dedicación del/los administrador/es será* ***exclusiva*** *para IFEMA MADRID durante la jornada presencial, no pudiendo dedicarla a otros servicios o actividades ajenas al objeto del contrato*".

24. Buenos días. En la página 22 del PPT, se habla de una bolsa de horas fuera de horario de oficina, para el servicio de Administración de la infraestructura. ¿Qué partida presupuestaria corresponde a este concepto, de las indicadas en la Ficha de Oferta Económica del Anexo IX? ¿Cuántas intervenciones fuera de horario se estima que podria haber al año? Muchas gracias.

Respuesta IFEMA.

No corresponde a ninguna partida de la ficha económica. En caso de necesidad se ejecutará bajo la vía de modificado de contrato.

En el contrato actual no se han superado las 20 horas.

25. Buenos días. En relación al contenido del apartado 3.1.1 del PPT (pág. 6). ¿Se debe incluir servicio de take down? Si es así ¿cuántos anuales? Muchas gracias.

Respuesta IFEMA.

Tal y como se indica en el punto 3.1.1 **Servicio de Vigilancia Digital y gestión de alertas**, del ppt las actividades a desarrollar, entre otras, incluyen:

"*Ejecución de las tareas necesarias de cierre técnico de dominios maliciosos detectados que suplanten dominios legítimos de IFEMA MADRID, y apoyo en las acciones legales que puedan derivarse de esta detección.*"

Por lo tanto, sí está incluido el Take Down. No es posible establecer una cantidad exacta de acciones anuales referente a este punto.

26. Buenos días. En relación al contenido del apartado 3.2.1 del PPT (pág. 11). ¿Es posible el despliegue de colectores de logs virtualizados en la infraestructura de virtualización de IFEMA (en caso de ser necesario) o en ese caso el adjudicatario debe suministrar HW para tal fin? Muchas gracias.

    Respuesta IFEMA.

    Sí es posible IFEMA MADRID, puede suministrar entornos de virtualización. No obstante, el adjudicatario será el responsable de cumplir con los objetivos del servicio.

27. Buenos días. En relación al contenido del apartado 3.3 del PPT (pág. 15). ¿Cuál es el volumen actual de incidentes gestionados por el servicio, distribuido según la severidad? Muchas gracias.

    Respuesta IFEMA.

    En el anexo Situación Actual Confidencial, vienen indicadas volumetrías del servicio actual

28. Buenos días. Respecto al Modelo de Gobierno y Relación (pág. 23 del PPT) y la figura del Service Manager. Vemos que se solicita dedicación exclusiva, ¿se requiere entonces que el perfil esté al 100% en el proyecto (es decir, 1 FTE)? ¿Debe ser esta figura obligatoriamente diferente a la del Administrador de Sistemas? ¿Se permite compatibilizar la tarea de Service Manager con otras, como la consultoría o la gestión de certificaciones? Muchas gracias.

    Respuesta IFEMA.

    No se requiere que esté al 100% . Este perfil debe ser diferente al perfil de Administrador de Sistemas y al Consultor Experto en Ciberseguridad,

    La compatibilidad será permitida siempre y cuando se preserve las dedicaciones en cada uno de los perfiles cumpliendo los requisitos del perfil y las indicaciones del ppt.

29. Buenos días, ¿Podrían, por favor, darnos respuesta a las siguientes preguntas? ¿Los anexos técnicos y diagramas computan dentro del límite de 20 páginas del Sobre 2? ¿Las referencias a procedimientos corporativos pueden incluirse mediante anexos o enlaces externos? ¿La dedicación presencial del administrador debe ser continua durante toda la jornada laboral o puede complementarse con operación remota? ¿La certificación Check Point debe estar asociada al recurso presencial o es válida a nivel de equipo del servicio? ¿Se admite un modelo de respaldo con dos administradores alternos previamente validados? ¿Las 104 jornadas anuales de consultoría son una previsión máxima de consumo o se siempre se empleará la totalidad de las mismas? ¿Qué alcance esperan para la vigilancia digital: marca, dominios, empleados VIP, activos expuestos o todos ellos? ¿Se prevé operación sobre herramientas existentes o se permite incorporar herramientas del adjudicatario? ¿Cuántos activos aproximados forman parte del alcance inicial de gestión de vulnerabilidades? ¿Las herramientas de análisis de vulnerabilidades deberán ser propiedad de IFEMA o pueden prestarse en modalidad servicio? ¿Los cinco ejercicios anuales previstos serán de tamaño homogéneo o podrán variar significativamente? ¿Qué nivel de madurez ENS e ISO 27001

mantiene actualmente IFEMA? ¿Las renovaciones se limitarán a fabricantes actualmente implantados? ¿La plataforma debe estar certificada por CCN/CPSTIC en el momento de la oferta o puede acreditarse durante la transición? ¿Se requiere presencia física inmediata en incidentes críticos o se admite respuesta remota inicial? ¿Cuántos usuarios deben recibir concienciación? Gracias, saludos

a. ¿Los anexos técnicos y diagramas computan dentro del límite de 20 páginas del Sobre 2?

Respuesta IFEMA.

Sí computan.

b. ¿Las referencias a procedimientos corporativos pueden incluirse mediante anexos o enlaces externos?

Respuesta IFEMA
A efectos de valoración de la propuesta, únicamente se considerará la información contenida en la documentación aportada en la oferta de acuerdo con lo indicado en el sobre, sin considerar en la valoración documentos anexos adicionales no solicitados en el pliego. No se accederá ni se valorará información incluida mediante hipervínculos o referencias a fuentes externas, por lo que la ausencia de la información en los documentos presentados podrá dar lugar a que el aspecto correspondiente no sea objeto de valoración.

c. ¿La dedicación presencial del administrador debe ser continua durante toda la jornada laboral o puede complementarse con operación remota?

Respuesta IFEMA.

La dedicación presencial debe ser continua toda la jornada laboral

d. ¿La certificación Check Point debe estar asociada al recurso presencial o es válida a nivel de equipo del servicio?

Sí. La certificación de CheckPoint debe estar asocial al recurso presencial

e. ¿Se admite un modelo de respaldo con dos administradores alternos previamente validados?

No. El recurso presencial debe tener la certificación de CheckPoint y cumplir todos los requisitos que se indica en el ppt.

¿Las 104 jornadas anuales de consultoría son una previsión máxima de consumo o se siempre se empleará la totalidad de las mismas?

Respuesta IFEMA.
Siempre se empleará la totalidad de las mismas

f. ¿Qué alcance esperan para la vigilancia digital: marca, dominios, empleados VIP, activos expuestos o todos ellos?

Respuesta IFEMA.

Tal y como se indica en punto 3.1.1. Servicio de Vigilancia Digital y gestión de alertas del pliego

"El servicio se prestará sobre los diferentes activos públicos de IFEMA MADRID, como pueden ser entre otros: nombres de directivos, marcas asociadas a IFEMA MADRID, direccionamiento IP público de servicios, aplicaciones, webs y dominios publicados, cuentas de correo electrónico corporativas, etc".

g. ¿Se prevé operación sobre herramientas existentes o se permite incorporar herramientas del adjudicatario?

Respuesta IFEMA.

IFEMA MADRID plantea un servicio integral de ciberseguridad gestionada. El proveedor deberá ser capaz de dar cobertura a todos los servicios incluidos en el servicio con las herramientas que consideren.

h. ¿Cuántos activos aproximados forman parte del alcance inicial de gestión de vulnerabilidades?

Respuesta IFEMA.

Tal y como se indica en el punto **3.1.2. Análisis de vulnerabilidades (sistemas y redes)** del ppt

"Las IP incluidas en el alcance de este servicio se detallan en el anexo "Situación Actual Exp 26_033 CONFIDENCIAL". A efectos de dimensionamiento inicial, se considera un alcance aproximado de 50 IP externas y 100 IP internas. Durante la vigencia del contrato, IFEMA MADRID podrá ampliar dicho alcance, sin coste extra, cuando existan necesidades justificadas, sin que el incremento del alcance supere el 30% sobre el alcance inicial. Con carácter ordinario, se realizarán ejercicios de análisis con periodicidad trimestral.Adicionalmente, IFEMA MADRID podrá solicitar escaneos bajo demanda en ejercicios acotados",

i. ¿Las herramientas de análisis de vulnerabilidades deberán ser propiedad de IFEMA o pueden prestarse en modalidad servicio?

Respuesta IFEMA.

IFEMA MADRID solicita un servicio de análisis de vulnerabilidades. Es responsabilidad del proveedor de disponer de las herramientas necesarias para el correcto desempeño de este servicio.

j. ¿Los cinco ejercicios anuales previstos serán de tamaño homogéneo o podrán variar significativamente?

Respuesta IFEMA.

No podemos hacer una estimación de tamaño ni su homogeneidad.

k. ¿Qué nivel de madurez ENS e ISO 27001 mantiene actualmente IFEMA?

Respuesta IFEMA.

IFEMA MADRID está actualmente certificado en ISO 27001 y ENS nivel medio.

l. ¿Las renovaciones se limitarán a fabricantes actualmente implantados?

Respuesta IFEMA.

Tal y como se indica en punto **3.7. Renovación anual de licencias de los productos de ciberseguridad** del pliego

*"La finalidad de este servicio consiste en la **gestión, renovación, soporte y mantenimiento** de las licencias asociadas a los productos y soluciones de ciberseguridad utilizados por IFEMA MADRID, tanto los actualmente desplegados como aquellos que puedan incorporarse durante la vigencia del contrato. El inventario y alcance vigente se detalla en el anexo "Situación Actual Exp 26_033 CONFIDENCIAL". La incorporación de nuevas soluciones durante el contrato implicará, cuando proceda, la inclusión de sus licencias y mantenimientos en este servicio, de conformidad con las modificaciones contractuales que resulten aplicables".*

m. ¿La plataforma debe estar certificada por CCN/CPSTIC en el momento de la oferta o puede acreditarse durante la transición?

Respuesta IFEMA.

La plataforma debe de estar certificada en el momento de la oferta.

n. ¿Se requiere presencia física inmediata en incidentes críticos o se admite respuesta remota inicial?

Respuesta IFEMA.

Tal y como se indica en el punto 3.3.1. **Gestión de respuesta ante incidentes (DFIR)** del pliego

*"Una vez activado el servicio, el adjudicatario pondrá en marcha los mecanismos necesarios para apoyar y coordinar la respuesta, actuando en modalidad **remota y/o presencial** según la naturaleza del incidente y lo requerido por IFEMA MADRID. El adjudicatario colaborará con los responsables designados por IFEMA MADRID para definir y ejecutar, entre otras, medidas de aislamiento, contención y mitigación, así como para coordinar la recuperación del servicio cuando proceda".*

o. ¿Cuántos usuarios deben recibir concienciación? Gracias, saludos

Respuesta IFEMA.

Todos los empleados de la compañía reciben concienciación en ciberseguridad

30. Buenos días: Para la solvencia que piden en la página 10 del cuadro de características hay un concepto que parece repetido (el E y el G es el mismo): E. Estar dado de alta en la Plataforma de concienciación en ciberseguridad validada por el CCN e incluida en el catálogo CPSTIC F. Tener Servicio de SOC de ámbito nacional deberá formar parte de la red G. Plataforma de concienciación en ciberseguridad deberá encontrarse incluida y vigente por el CCN e incluida

en el catálogo CPSTIC Por favor, indiquen si ambos se refieren a lo mismo: a que tengamos la posibilidad de ofrece una plataforma de concienciación que esté en el catálogo CPSTIC. Gracias

Respuesta IFEMA.

Sí, se refieren a lo mismo.

31. Buenas, realizamos varias consultas para poder avanzar en la oferta: Consulta 1: Licenciamiento e infraestructura Respecto al alcance de la necesidad de renovación de licenciamiento/mantenimiento, ¿podrían confirmar si únicamente se requiere la renovación de los elementos indicados en el apartado 1 del documento de "Situación Actual" (asumiendo que la plataforma de concienciación se cubre mediante otra solución)? CISCO IronPort: Service Contract 206400993. Check Point Maestro (Account ID 5716162). Fortigate (601E): Serial Numbers FG6H1ETB21909382 y FG6H1ETB21909776. Fortigate (201E): Serial Numbers FG201ETK20903802 y FG201ETK20903632. Fortigate (2500E): Serial Numbers FG2K5ETB19900355 y FG2K5ETB19900356. Asimismo, en relación con los equipos (FWs) que conforman la infraestructura de seguridad de IFEMA y tomando como referencia el esquema de red incluido en el apartado 2 del documento de "Situación Actual", ¿sería posible identificar con mayor detalle los modelos y la cantidad de equipos asociados a cada uno de los firewalls representados en dicho esquema? Adicionalmente, ¿la solución/herramienta Cisco ISE forma parte de las plataformas que deben ser administradas por el adjudicatario? En caso afirmativo, ¿podrían facilitar información adicional sobre el licenciamiento actualmente disponible?

    a. Licenciamiento e infraestructura Respecto al alcance de la necesidad de renovación de licenciamiento/mantenimiento, ¿podrían confirmar si únicamente se requiere la renovación de los elementos indicados en el apartado 1 del documento de "Situación Actual" (asumiendo que la plataforma de concienciación se cubre mediante otra solución)? CISCO IronPort: Service Contract 206400993. Check Point Maestro (Account ID 5716162). Fortigate (601E): Serial Numbers FG6H1ETB21909382 y FG6H1ETB21909776. Fortigate (201E): Serial Numbers FG201ETK20903802 y FG201ETK20903632. Fortigate (2500E): Serial Numbers FG2K5ETB19900355 y FG2K5ETB19900356.

Respuesta IFEMA.

Tal y como se indica en el punto 3.7. Renovación anual de licencias de los productos de ciberseguridad del pliego

En el alcance actual, IFEMA MADRID dispone, entre otros, de licencias/mantenimientos de: Cisco IronPort firewalls Check Point y FortiGate, sin perjuicio de los elementos adicionales incluidos en el anexo "Situación Actual Exp 26_033 CONFIDENCIAL". Este apartado comprende la **gestión administrativa**, la **renovación** de licencias y soporte y mantenimientos con los respectivos fabricantes.

En el anexo "Situación Actual Exp 26_033 CONFIDENCIAL" se detalla la relación completa de productos y licencias incluidos en el ámbito de este contrato. El licitador deberá disponer de la capacidad de interlocución y gestión con los fabricantes correspondientes (por ejemplo, en calidad de partner/distribuidor autorizado), en los términos que resulten necesarios para asegurar la correcta renovación y soporte de las licencias.

    b. Asimismo, en relación con los equipos (FWs) que conforman la infraestructura de seguridad de IFEMA y tomando como referencia el esquema de red incluido en el apartado 2 del documento de "Situación Actual", ¿sería posible identificar con mayor detalle los

modelos y la cantidad de equipos asociados a cada uno de los firewalls representados en dicho esquema?

Respuesta IFEMA.

Con la información que se aporta en el documento "Situación Actual Confidencial", y siendo partner del producto mencionado, podrán obtener la información solicitada.

c. Adicionalmente, ¿la solución/herramienta Cisco ISE forma parte de las plataformas que deben ser administradas por el adjudicatario?

Respuesta IFEMA.

Sí, así es.

d. En caso afirmativo, ¿podrían facilitar información adicional sobre el licenciamiento actualmente disponible?

Respuesta IFEMA.

Con la información que se aporta den el documento Situación Actual Confidencial, y siendo partner del producto mencionado, podrán obtener la información solicitada.

32. Consulta 2: Alcance de operación y administración de plataformas En relación con la solución SIEM, no nos queda claro si el adjudicatario debe asumir la monitorización y operación integral de la herramienta o únicamente determinadas tareas y actividades específicas, coordinándose con un tercero para la prestación del servicio. ¿Podrían ampliar el alcance previsto e indicar qué solución SIEM se encuentra actualmente implantada? Por otra parte, en el Pliego de Prescripciones Técnicas, apartado 3.6 (página 19), se indica que las soluciones o plataformas a administrar, como mínimo, son las siguientes: Firewalls y seguridad perimetral. Seguridad de correo electrónico. Protección de Endpoint (EDR). Servicios y herramientas de seguridad en Microsoft 365 y Azure. Sin embargo, en el documento de "Situación Actual" se indica que determinadas plataformas no están incluidas dentro del alcance de administración y gestión, aunque sí deban ser conocidas por su posible impacto en las decisiones de seguridad y en la integración con otros sistemas. ¿Podrían aclarar expresamente si los productos y servicios de seguridad de Microsoft 365 y Azure deben ser administrados por el adjudicatario? En caso afirmativo, agradeceríamos que se identificaran las soluciones concretas incluidas en el alcance del servicio. Por último, respecto a la herramienta microCLAUDIA, se indica que será gestionada por el administrador de los sistemas de ciberseguridad. ¿Debemos entender que su administración queda fuera del alcance del contrato y, por tanto, no correspondería al adjudicatario?

a. Alcance de operación y administración de plataformas En relación con la solución SIEM, no nos queda claro si el adjudicatario debe asumir la monitorización y operación integral de la herramienta o únicamente determinadas tareas y actividades específicas, coordinándose con un tercero para la prestación del servicio. ¿Podrían ampliar el alcance previsto e indicar qué solución SIEM se encuentra actualmente implantada?

Respuesta IFEMA.

IFEMA MADRID no tiene herramienta SIEM y contrtista debe asumir toda la monitorización, tal y como se indica en el punto 3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad del ppt

"En el anexo "Situación Actual Exp 26_033 CONFIDENCIAL", se amplía información sobre las fuentes, EPSs y la infraestructura híbrida de IFEMA MADRID susceptible de ser monitorizada con las sondas SIEM que el **proveedor designe** para el correcto funcionamiento del servicio.

El SOC debe usar la herramienta SIEM de manera eficiente con el objetivo de alertar y prevenir las situaciones que requieran atención y no llamar nuestra atención frente falsos positivos sin dejar que las amenazas reales a la seguridad se queden sin detectar. Por lo tanto, se debe realizar una gestión adecuada de los eventos con su correcta correlación, priorización y triaje. A su vez se investigará el alcance y la gravedad de la información, así como la clasificación de los posibles incidentes."

b. Por otra parte, en el Pliego de Prescripciones Técnicas, apartado 3.6 (página 19), se indica que las soluciones o plataformas a administrar, como mínimo, son las siguientes: Firewalls y seguridad perimetral. Seguridad de correo electrónico. Protección de Endpoint (EDR). Servicios y herramientas de seguridad en Microsoft 365 y Azure. Sin embargo, en el documento de "Situación Actual" se indica que determinadas plataformas no están incluidas dentro del alcance de administración y gestión, aunque sí deban ser conocidas por su posible impacto en las decisiones de seguridad y en la integración con otros sistemas. ¿Podrían aclarar expresamente si los productos y servicios de seguridad de Microsoft 365 y Azure deben ser administrados por el adjudicatario?

Respuesta IFEMA.

Sí deben ser administradas por el contratista.

c. En caso afirmativo, agradeceríamos que se identificaran las soluciones concretas incluidas en el alcance del servicio.

Respuesta IFEMA.

Herramientas estándar de seguridad de Microsoft365 y elementos estándar de seguridad de Azure.

d. Por último, respecto a la herramienta microCLAUDIA, se indica que será gestionada por el administrador de los sistemas de ciberseguridad. ¿Debemos entender que su administración queda fuera del alcance del contrato y, por tanto, no correspondería al adjudicatario?

Respuesta IFEMA.

La administración de esta plataforma está dentro del alcance del contrato.

33. Buenas, necesitamos aclarar las siguientes cuestiones para seguir avanzando en la oferta: 1. ¿Cuál es el número actual y máximo previsto de personas usuarias nominativas que deberán licenciarse en la plataforma, diferenciando personal interno, temporal, colaboradores y

terceros? ¿Debe considerarse que los aproximadamente 800 puestos indicados en la Situación Actual equivalen a la población licenciable? 2. Además de los perfiles generales, técnicos y mandos mencionados en el pliego, ¿qué colectivos y áreas deberán contemplarse, cuántas personas integran cada itinerario y qué idiomas y requisitos de accesibilidad serán obligatorios? 3. Respecto de la instancia actual de CyberGuru, ¿cuál es la edición y versión contratada, el número y tipo de licencias, los módulos habilitados y las principales parametrizaciones e integraciones existentes? 4. ¿El concepto de "campañas" incluye simulaciones de phishing? En caso afirmativo, ¿cuántas campañas ordinarias anuales deberán incluirse, sobre qué poblaciones y con qué niveles de complejidad y personalización? 5. ¿Cuántas campañas específicas adicionales están incluidas en el precio base? ¿Qué unidad de medida o umbral determinará que deban tramitarse mediante modificación contractual? 6. Dado que el pliego exige migrar campañas, usuarios, históricos, métricas, plantillas, grupos y parámetros de reporting, ¿qué información puede exportarse efectivamente desde la instancia actual, con qué granularidad, formatos y API? ¿Qué asistencia prestará el proveedor saliente y se exigirá convivencia temporal entre plataformas? 7. ¿Los honorarios de las entidades certificadoras y de los auditores externos serán contratados y abonados directamente por IFEMA MADRID o deberán incluirse en el precio ofertado por el adjudicatario? 8. ¿El servicio comprende la evaluación de riesgos o cumplimiento de proveedores y terceros? En caso afirmativo, ¿cuántos deberán evaluarse anualmente, con qué frecuencia, metodología y profundidad? Gracias.

1. ¿Cuál es el número actual y máximo previsto de personas usuarias nominativas que deberán licenciarse en la plataforma, diferenciando personal interno, temporal, colaboradores y terceros? ¿Debe considerarse que los aproximadamente 800 puestos indicados en la Situación Actual equivalen a la población licenciable?

Respuesta IFEMA.

Al no especificar la plataforma a la que se refiere, no es posible facilitar respuesta a la consulta realizada

2. Además de los perfiles generales, técnicos y mandos mencionados en el pliego, ¿qué colectivos y áreas deberán contemplarse, cuántas personas integran cada itinerario y qué idiomas y requisitos de accesibilidad serán obligatorios?

Respuesta IFEMA.

Al no especificar la plataforma a la que se refiere, no es posible facilitar respuesta a la consulta realizada

3. Respecto de la instancia actual de CyberGuru, ¿cuál es la edición y versión contratada, el número y tipo de licencias, los módulos habilitados y las principales parametrizaciones e integraciones existentes?

Respuesta IFEMA.

Esta información no es relevante para la preparación de la oferta.

4. ¿El concepto de "campañas" incluye simulaciones de phishing? En caso afirmativo, ¿cuántas campañas ordinarias anuales deberán incluirse, sobre qué poblaciones y con qué niveles de complejidad y personalización?

Respuesta IFEMA.

Sí, incluye campañas. Se estima realizar una campaña trimestral sobre toda la población y la complejidad y la personalización dependerá de la necesidad identificada por IFEMA MADRID en el momento de la realización de la campaña.

5. ¿Cuántas campañas específicas adicionales están incluidas en el precio base? ¿Qué unidad de medida o umbral determinará que deban tramitarse mediante modificación contractual?

Respuesta IFEMA.

Está incluido en el alcance. En caso de excepcionalidad IFEMA MADRID revisará.

6. Dado que el pliego exige migrar campañas, usuarios, históricos, métricas, plantillas, grupos y parámetros de reporting, ¿qué información puede exportarse efectivamente desde la instancia actual, con qué granularidad, formatos y API? ¿Qué asistencia prestará el proveedor saliente y se exigirá convivencia temporal entre plataformas?

Respuesta IFEMA.

El pliego no exige la migración de la herramienta. La plataforma actual permite un nivel amplio de granularidad con diferentes formatos. El proveedor saliente colaborará durante el proceso de transición de la plataforma si fuera necesario. La convivencia de plataformas dependerá de la solución propuesta por el contratista y posterior validación por parte de IFEMA MADRID:

7. ¿Los honorarios de las entidades certificadoras y de los auditores externos serán contratados y abonados directamente por IFEMA MADRID o deberán incluirse en el precio ofertado por el adjudicatario?

Respuesta IFEMA.

Esto no está incluido en el alcance del servicio.

8. ¿El servicio comprende la evaluación de riesgos o cumplimiento de proveedores y terceros? En caso afirmativo, ¿cuántos deberán evaluarse anualmente, con qué frecuencia, metodología y profundidad? Gracias.

Respuesta IFEMA.

No los comprende

34. Buenas tardes, Por ultimo, en relación con el apartado del PPT 3.6. Servicio de Administración de infraestructura de seguridad y plataformas de ciberseguridad, ¿aceptará IFEMA modelos de prestación basados en equipos especializados por tecnología, combinando presencia planificada en sede y soporte remoto, siempre que se garantice el cumplimiento de los acuerdos de nivel de servicio, la continuidad operativa y la disponibilidad requerida? En caso afirmativo, ¿deberá mantenerse necesariamente la figura de un administrador residente y de dedicación exclusiva o podrán proponerse modelos organizativos alternativos de servicio gestionado? Gracias de antemano.

Respuesta IFEMA.

No se acepta prestación de este servicio basados en equipos

EL PRESENTE DOCUMENTO PASA A FORMAR PARTE INTEGRANTE DEL PLIEGO DE BASES, QUEDANDO AFECTOS EN LOS TÉRMINOS PREVISTOS EN EL CITADO PLIEGO.

Dirección de Compras y Logística
13 agosto 2026