Pliego de Prescripciones Técnicas para el Servicio Integral de Ciberseguridad en Formato Híbrido

Exp.: 23/031

Sol. Ped.: 2000022463

Versión	Fecha	Descripción	Autor/es
1	28-01-2023	Pliego de Prescripciones Técnicas para el Servicio Integral de Ciberseguridad en Formato Híbrido	Área de Sistemas de la Información y Ciberseguridad

Aprobado por	Rol	Fecha Aprobación

Cajetín de firma/s

1. Objeto

Vivimos en un momento en el que el acceso a la información debe ser ágil y los datos, que antes solo estaban en la sede corporativa, se distribuyen cada vez más entre las diferentes nubes existentes. Esto requiere que los recursos de IFEMA MADRID deban estar defendidos de forma cada vez más robusta frente a amenazas tales como malware, ransomware, phishing, los ataque DDOS, los ataques de fuerza bruta, etc. Por lo tanto, IFEMA MADRID necesita un servicio de ciberseguridad integral que cubran los entornos en Cloud, en sede corporativa (On Premise) y en situación de hosting. Este servicio debe anticipar, prevenir, detectar y reaccionar mejor ante las amenazas, con el objetivo de hacer la información de IFEMA MADRID más segura. Dicho servicio debe conseguir los objetivos establecidos en materia de integridad, confidencialidad, trazabilidad y disponibilidad de la información, sistemas, servicios, diseños y dispositivos de IFEMA MADRID.

En los últimos meses, hemos sido testigos de la sofisticación de los ataques informáticos a empresas, administraciones públicas y gobiernos que han provocado innumerables daños económicos y de imagen. Para 2023, se prevé un incremento y un aumento de la sofisticación de estos ciberataques, por lo que, además de hablar de ciberseguridad modular y distribuida, será fundamental contar con soluciones y el esfuerzo de personas expertas que permitan detectar y neutralizar ciberamenzas cada vez más sofisticadas y propongan diseños seguros capaces de integrase con herramientas y plataformas sin poner en riesgo los datos de la compañía.

IFEMA MADRID también acoge eventos muy importantes y de gran repercusión mundial, por ejemplo: la CUMBRE de La OTAN 2022 y la celebración de la COP25. Estos eventos, hacen que IFEMA MADRID sea el foco mediático para ciberdelincuentes sometiendo a la compañía a todo tipo de ataques.

La respuesta a estos desafíos es el objeto del presente contrato: dotar a IFEMA MADRID de un servicio híbrido de ciberseguridad para la protección de los datos y servicios de IT de IFEMA MADRID. Será un servicio híbrido desde el punto de vista que la ubicación material de los recursos a proteger es diversa: tanto en la sede corporativa de IFEMA MADRID como en proveedores de hosting, de servicios cloud, de SaaS, PaaS, IaaS, etc. Es decir, el objeto es la seguridad de los datos de IFEMA MADRID cualquiera que sea su ubicación o su tratamiento.

Este servicio híbrido estará gobernado por acuerdos de nivel de servicio (ANS en adelante), **estará dotado tanto con la dedicación completa y presencial de personas competentes del adjudicatario en la sede corporativa de IFEMA MADRID**, como con la dedicación en remoto parcial o bajo demanda de otras personas de los equipos de expertos del adjudicatario.

Por último, incluirá la renovación de las licencias de productos de ciberseguridad de IFEMA MADRID con sus respectivos fabricantes.

2. Alcance

Este contrato incluye todas las actividades necesarias para cubrir las necesidades de ciberseguridad de IFEMA MADRID con objeto de proteger los servicios de tecnologías de la información, los datos y sus tratamientos dondequiera que se encuentren.

Se solicita un servicio de ciberseguridad integral, que comprenda la administración de los elementos de ciberseguridad, registro de sucesos y su retención, monitorización básica, correlación basada en reglas de seguridad, análisis en tiempo real e histórico de sucesos de seguridad, detección, alertas, gestión y respuestas ante incidentes, detección proactiva, análisis profesional avanzado,

automatización, interlocución con proveedores y otras áreas de la compañía, diseño de nuevas soluciones seguras, consultoría y asesoramiento en cuestiones de ciberseguridad, etc.

Dentro del alcance del servicio, enumeramos los puntos clave que IFEMA MADRID estima y necesita para cubrir la ciberseguridad de la compañía. No obstante, en el anexo de "Situación Actual CONFIDENCIAL", se amplía información sobre infraestructura, redes, fuentes a monitorizar por el SOC, servicios y otros elementos para tener en cuenta para que el licitante comprenda el alcance del servicio.

El proveedor centrará sus esfuerzos en el cumplimiento de los procedimientos por parte del equipo de trabajo, así como en la gestión de los recursos dedicados al contrato. Esto incluye el control, seguimiento y evaluación del servicio prestado, en cada una de sus fases y actividades, mediante interlocución con los responsables de IFEMA MADRID persiguiendo siempre la orientación a la mejora continua y la calidad en el servicio. Para ello se realizará la gestión de las incidencias, peticiones y proyectos de forma continua y correcta, haciendo el seguimiento de estas evitando que se descontrolen, se paren o se desvíen de sus objetivos principales y que se resuelvan en modo y forma adecuada. Se realizarán informes de actividad, de control de calidad y de facturación, así como la recogida y el seguimiento de los ANS establecidos, gestión de la calidad, etc. La empresa adjudicataria presentará mensualmente un informe de actividad del servicio que será remitido a IFEMA MADRID. El proveedor pondrá los medios necesarios para que se preste un servicio óptimo, sin embargo, desde IFEMA MADRID se solicita la figura del service manager para la gestión del servicio prestado.

El horario de prestación del servicio para IFEMA MADRID será 24x7x365.

El servicio debe contar como mínimo con las siguientes características:

2.1 Descripción del Servicio de SOC 24x7x365

La seguridad se debe entender como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relativos a la información y los sistemas que la sustenta.

Consciente de estos principios, IFEMA MADRID necesita contar con las herramientas necesarias capaces de monitorizar el estado de la seguridad de los recursos informáticos para gestionar los riesgos y garantizar un alto nivel de seguridad de los sistemas y su información.

IFEMA MADRID tiene implementadas medidas de seguridad y métodos de protección en su organización, pero debido a la complejidad de los sistemas, los riesgos existentes y su creciente actividad es esencial contar con el asesoramiento de expertos en seguridad y ciberseguridad para establecer y consolidar una adecuada gestión de la seguridad para la información y los sistemas de IFEMA MADRID que permita responder lo antes posible y en cualquier momento ante cualquier amenaza.

En definitiva, el objetivo principal es, garantizar la seguridad y calidad de las infraestructuras de TI disminuyendo las vulnerabilidades y riesgos que comprometan el funcionamiento de los sistemas y servicios, reaccionando de forma eficiente ante cualquier evento de seguridad y por ello, el adjudicatario dispondrá de un Centro de Operaciones de Seguridad (SOC) capaz de garantizar las infraestructuras y servicios de IFEMA MADRID a través de la prevención y la monitorización de las redes y de internet, capaz de diagnosticar vulnerabilidades, respuesta ágil frente a incidentes, neutralización de ataques, implementando entre otros, programas de prevención, IoCs, etc. IFEMA MADRID requiere un servicio 24x7x365.

El proveedor, dentro la función de vigilancia y asesoramiento continuo mantendrá alerta a IFEMA MADRID de las amenazas e incidentes de TI relevantes que se encuentren presentes para poder gestionarlos conjuntamente. Alertas con el fin de identificar y prevenir amenazas, mitigar riesgos, dar soluciones y proponer mejoras continuas en aspectos de ciberseguridad. Por ejemplo, alertas de nuevas ciberamenazas, nuevas campañas de ciberfraude, nuevos ramsonware que se extienden con rapidez, emails masivos que suplantan a bancos legítimos, boletines de IOCs, etc. junto con la propuesta de solución a dichas amenazas.

La forma de llevar a cabo lo anteriormente expuesto, debe realizarse mediante avisos, boletines informativos a través de correo electrónico, apertura y gestión de tickets en el Service Desk de IFEMA MADRID relativos a seguridad y ciberseguridad, etc., tan pronto como sean detectadas dichas amenazas. Siguiendo en todo momento los procesos y procedimientos que se establezcan desde IFEMA MADRID.

Actualmente IFEMA MADRID dispone de un servicio de SOC 24x7x365 con el proveedor actual monitorizando cinco fuentes con una herramienta SIEM, que se necesitan seguir monitorizando:

- Firewalls CheckPoint objeto del contrato
- Directorio Activo
- Proxy Inverso
- Sistema de filtrado de correo Cisco CES (en la nube) objeto del contrato
- Endpoint (Consola en nube)

En el anexo "Situación Actual CONFIDENCIAL" se indica la volumetría de EPSs (menos de 500 EPSs) y detalles de los sistemas a monitorizar.

El proveedor saliente entregará al nuevo adjudicatario la situación actual y las reglas casos de uso de su recolector de eventos.

Tal y como se menciona en el objeto del servicio, IFEMA MADRID requiere de un servicio híbrido de ciberseguridad donde se proteja los servicios de la compañía y todos sus datos, independientemente de su ubicación sean en la sede de IFEMA MADRID o cualquiera de sus nubes.

Teniendo en cuenta los datos actuales, estas fuentes no superan los 500 EPSs, por lo tanto, IFEMA MADRID podrá incrementar todas las fuentes necesarias y que considere de interés para la seguridad de los sistemas, hasta completar estos 750 EPSs.

Estas fuentes podrán estar ubicadas en función de su necesidad y de la implementación de los nuevos servicios, en cloud y On Premise y deberán conectarse de forma segura al colector de datos que el proveedor designe para el servicio, instalando en todas las fuentes las sondas necesarias para el correcto desempeño del servicio. Por ejemplo, IFEMA MADRID cuenta con servicios cloud desplegados en nubes como Azure, AWS y GCP o productos en nube como Salesforce (Sales, Service, Marketing Cloud y Anypoint Mulesoft), Office 365, Marketing Cloud, SAP Hana Cloud Integration que pueden ser objeto de esta monitorización.

IFEMA MADRID podrá solicitar, durante la vigencia del contrato, la incorporación de nuevas fuentes que deban ser monitorizadas por el SOC. Con el fin de prever esta situación, el licitante indicará en su oferta el precio de los 750 EPSs base y paquetes de 250 EPSs adicionales a estos 750 EPSs incluidos inicialmente con el fin de que, en caso de necesidad, IFEMA MADRID pueda adquirir mediante las previstas modificaciones al contrato esta posible ampliación.

El adjudicatario indicará el precio de esta parte del servicio en su oferta de forma individual, siendo este acorde al precio de mercado. En ningún caso se admitirán ofertas cuyo importe del servicio sea anormalmente bajo, que pueda generar dudas acerca su sostenibilidad.

En el anexo "Situación Actual 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.

El objetivo del SOC, en función de las amenazas que detecte, será el responsable de aplicar las medidas correctivas necesarias para mitigar el riesgo en los elementos de ciberseguridad objeto del servicio, Cisco CES IronPort, Checkpoint y Fortinet, bien a través del Administrador de sistemas de ciberseguridad o del propio SOC, si dicha detección se realiza fuera del horario de oficina. El proveedor además deberá aplicar los IOCs en los elementos objetos del contrato en un tiempo máximo de 4 horas desde su comunicación.

Las acciones por realizar en las demás fuentes monitorizadas y cuya gestión y mantenimiento no son objeto del presente contrato, por ejemplo, acciones a tomar en Directorio Activo, serán notificadas a los responsables del área de Sistemas y Ciberseguridad de la Dirección de Tecnologías de la Información de IFEMA MADRID a través de la herramienta de ticketing destinada para el servicio, con el fin de mediar y aplicar las medidas necesarias en dichas fuentes. Estas acciones serán llevas a cabo por el personal adecuado.

Todos los incidentes que el SOC registre, así como todas las tareas que el administrador de sistemas de ciberseguridad que presta sus servicios de forma presencial deberá quedar registrados en la herramienta de ticketing que IFEMA MADRID dispone para el servicio.

El SOC también será el responsable de administrar los elementos de ciberseguridad objeto del contrato que IFEMA MADRID dispone fuera del horario habitual o de oficina (lunes a jueves de 09.00 – 18.30 y viernes de 09.00-15.00h.)

El servicio de SOC, debe formar parte de la empresa adjudicataria.

2.2 Renovación anual de licencias de los productos de ciberseguridad

Los productos de ciberseguridad que IFEMA MADRID tiene contratados corresponden a los fabricantes Cisco Ironport CES en nube como filtro de correo, firewalls Checkpoint On Premise para la seguridad perimetral corporativa, Fortigate para la red IoT, y para la gestión de la red comercial y sólo está incluida la renovación de las licencias estando fuera del alcance de este contrato otras tareas como su administración.

En el anexo, "Situación Actual CONFIDENCIAL", se detalla la relación completa de productos de seguridad empleados por IFEMA MADRID en el ámbito de este contrato y que el licitante, como distribuidor autorizado, puede consultar con los respectivos fabricantes.

Este contrato incluye el coste y las gestiones de renovación de las licencias de los productos de ciberseguridad actuales de IFEMA MADRID ante sus fabricantes respectivos para un año desde la fecha del fin de los mantenimientos actuales de Checkpoint, Cisco y Fortinet. Actualmente, IFEMA MADRID tiene pagadas las licencias de estos productos hasta unas fechas dadas (ver anexo "Situación Actual CONFIDENCIAL" para el detalle). A partir de estas fechas, el adjudicatario será el responsable de su renovación y gestión. No se debe imputar a IFEMA MADRID el coste de las licencias desde la adjudicación del servicio hasta la renovación de las licencias mencionadas. Las licencias serán siempre propiedad de IFEMA MADRID.

Hasta llegar a la fecha de renovación de las licencias de estos productos, el adjudicatario tendrá que realizar los trámites necesarios para ser el interlocutor entre el fabricante e IFEMA MADRID y prestar el servicio asociado a las mismas.

Las renovaciones se realizarán en tiempo y en forma, sin costes adicionales para IFEMA MADRID, es decir, si el proveedor se retrasase en el pago de las licencias al fabricante, debe responsabilizarse del posible recargo. También están incluido el mantenimiento evolutivo y correctivo de los productos en las condiciones actuales, es decir se debe seguir manteniendo el mismo de tipo de licenciamiento que IFEMA MADRID posee para poder tener acceso a parches, nuevas versiones de productos, etc.

El adjudicatario será el interlocutor de IFEMA MADRID ante los respectivos fabricantes de los productos de ciberseguridad. Consultará y hará seguimiento de todas las cuestiones que sean necesarias en los servicios de atención al cliente de los fabricantes de productos de seguridad, para su solución satisfactoria.

El Soporte de los productos, estará disponible a cualquier hora todos los días del año, es decir, disponibilidad 24x7x365, para la recuperación inmediata del servicio.

El adjudicatario indicará el precio de esta parte del servicio en su oferta de forma individual, siendo este acorde al precio de mercado. En ningún caso se admitirán ofertas cuyo importe del servicio sea anormalmente bajo, que pueda generar dudas acerca su sostenibilidad.

2.3 Administración de sistemas de ciberseguridad presencial

En el ámbito de este contrato, **IFEMA MADRID necesita un administrador de sistemas de ciberseguridad en la sede corporativa**. El/los administrador/es designado/s, prestarán el servicio de forma presencial en nuestra sede, sólo, se podrá contemplar el teletrabajo de las personas designadas, a discreción de IFEMA MADRID y sin perjuicio de su disponibilidad y dedicación. Para poder dar cobertura al requisito de presencialidad, anteriormente solicitado, se admite también que, el perfil de administración de sistemas de ciberseguridad sea prestado por dos personas, que puedan alternarse y deberán ser siempre las mismas personas. Todos los administradores que se destinen al servicio de Administración de los sistemas de ciberseguridad de IFEMA MADRID deben contar con certificaciones oficiales de los productos objeto del contrato. Todos los administradores deben contar con un mínimo de 3 años de experiencia en puestos similares al del objeto del contrato (en los últimos 5 años)..

Las vacaciones, permisos y bajas deberán estar siempre cubiertos, de tal forma que, haya siempre alguien presencial en la sede corporativa de IFEMA MADRID y no impacte desfavorablemente en el avance y estado de los asuntos encomendados. Siempre que cuando se prevea esta casuística los administradores que vayan a cubrir la suplencia del administrador, deben tener los conocimientos y contextualización que el servicio requiere.

La dedicación del/los administrador/es será exclusiva para IFEMA MADRID, no pudiendo dedicar su jornada a otros servicios ni actividades que no sean objeto de este contrato, durante la presencialidad.

El horario habitual será de lunes a jueves de 9.00h a 18.30h con una hora de comida y los viernes de 9.00h a 15.00h En caso de un incidente de ciberseguridad o una circunstancia crítica que pueda poner en riesgo los sistemas de la compañía, la jornada podrá demorarse hasta que el incidente quede resuelto o la circunstancia baje de criticidad.

Por otro lado, IFEMA MADRID planifica con antelación intervenciones de mejora en materia de ciberseguridad. El coste de este tipo de intervenciones fuera de horario laboral es un extra que no está incluido en la jornada ordinaria. Se estima que estas horas tengan un precio por hora entre 1,5 y 1,7 veces del de hora ordinaria en horario laboral. Por lo tanto, el licitante debe indicar en su oferta el precio de una bolsa de 50 horas extras de pago por uso destinadas a estas intervenciones. Esta bolsa de 50 horas debe facturarse contra la partida presupuestaria variable del contrato y se facturarán en el mes en el que se hayan realizado.

El adjudicatario indicará el precio de esta parte del servicio en su oferta de forma individual, siendo este acorde al precio de mercado. En ningún caso se admitirán ofertas cuyo importe del servicio sea anormalmente bajo, que pueda generar dudas acerca su sostenibilidad.

Se solicita disposición por parte de la persona designada para acordar con IFEMA MADRID su disponibilidad para la planificación de las intervenciones fuera de horario laboral, así como el esfuerzo de atender las urgencias que pudieran sobrevenir fuera del horario laboral, si bien este caso no es habitual en absoluto.

El administrador dispondrá de acceso preferente al Consultor Experto en Ciberseguridad (ver apartado 2.4) de la empresa adjudicataria que se define en el siguiente apartado del presente documento, para acometer y resolver los asuntos de ciberseguridad que requieran conocimientos o experiencia profundos en materia de ciberseguridad. Este Consultor Experto en Ciberseguridad debe contar con los conocimientos técnicos avanzados para resolver todo lo referente a las necesidades de IFEMA MADRID en el ámbito de la ciberseguridad.

IFEMA MADRID facilitará a la persona designada la normativa interna y la persona designada se compromete a conocerla y respetarla.

El adjudicatario proveerá al administrador de ciberseguridad los elementos y dispositivos necesarios para desempeñar su trabajo tales como teléfono móvil, ordenador portátil, software, accesorios, medidas de seguridad, dirección de email, acceso remoto, VPN, formación, documentación, etc.

Será exclusiva responsabilidad del adjudicatario la organización, formación, control, dirección, selección, aseguramiento, retribución, disciplina y cuantas facultades y obligaciones atribuya la legislación laboral a los empresarios, y en particular, respecto de los retrasos, ausencias, sustituciones, enfermedad o cualquier otra situación similar en que pudieran incurrir sus empleados.

El personal del adjudicatario deberá estar dirigido y controlado por el/los responsable/s pertenecientes al adjudicatario, quién, como interlocutor de dicha empresa, coordinará la prestación del servicio y sus diferentes aspectos con IFEMA MADRID, actuando de acuerdo con las indicaciones que reciba de IFEMA MADRID.

Se espera que la dedicación presencial proporcione al administrador un conocimiento cercano, valioso y extenso de las circunstancias de las tecnologías de información en IFEMA MADRID, de modo

que pueda aportar soluciones seguras y conformes a los intereses y necesidades efectivas para el negocio.

Con objeto de prestar un servicio a IFEMA MADRID de calidad y con continuidad, el adjudicatario protegerá al/los administrador/es con las condiciones contractuales y económicas acordes al mercado y a su experiencia, para promover su implicación con el servicio, su satisfacción, su dedicación y su permanencia indefinida, desalentando de este modo su salida inesperada.

El/los administrador/es contarán con conocimientos, capacitación y experiencia en los productos de ciberseguridad objeto del contrato y en asuntos de ciberseguridad.

Para ello, el ofertante incluirá en su oferta las certificaciones del/los administrador/es de los sistemas de ciberseguridad objeto del servicio.

Será este administrador de sistemas de ciberseguridad el encargado de:

- Operar, administrar y gestionar los productos de ciberseguridad objeto del servicio
- Realizar las actualizaciones de los productos de ciberseguridad
- Utilizar herramientas para solución de incidencias
- Interlocutor con los fabricantes de los productos objeto del servicio
- Interlocutor con proveedores y otras áreas de la compañía de IFEMA MADRID que requieran propuestas en materia de ciberseguridad general y básica e interactuar con otros proveedores y áreas de IFEMA MADRID sobre temas de ciberseguridad
- Representar y mediar entre su empresa e IFEMA MADRID para cualquier necesidad propia del servicio y escalado a otros niveles técnicos. Recopilar información para escalarla a los consultores expertos en ciberseguridad.
- Realizar recomendaciones sobre diferentes aspectos de ciberseguridad básicos y elementales
- Análisis de impactos y riesgos asociados a elementos de ciberseguridad básicos y elementales
- Diseñar y proponer soluciones en lo referente a la ciberseguridad de los sistemas objeto del contrato
- Otras funciones/necesidades que IFEMA MADRID requiera y que estén relacionadas con el puesto.

IFEMA MADRID tiene una suscripción propietaria de microCLAUDIA del CCN-CERT desplegada en sus dispositivos y servidores Windows que será gestionada por el administrador de los sistemas de ciberseguridad.

El administrador priorizará las actividades de ciberseguridad proporcionalmente a su riesgo y a su interés para IFEMA MADRID. Realizarán las tareas dentro sus competencias y escalarán las actividades de niveles superiores a los técnicos correspondientes de su empresa. Hará seguimiento de las actividades escaladas para que avancen adecuadamente y poder indicar la progresión de su avance a IFEMA MADRID. Preverá el consumo de las actividades escaladas y controlará que no se produzcan consumos desmesurados por encima de los previstos.

El administrador asistirá a las reuniones de IFEMA MADRID a las que se le convoque para tratar las cuestiones en el ámbito de ciberseguridad y de los productos objeto del contrato y relacionadas con el asunto principal de la reunión. Dichas reuniones contarán con interlocutores de IFEMA MADRID y de terceros. Ante el tercero, en dichas el administrador prestará su asesoría con el criterio de la mejor seguridad para los sistemas, datos y tratamientos de IFEMA MADRID dentro del asunto que trate. Comprobará que las actas recogen las cuestiones de ciberseguridad tratadas y registrará, priorizará y acometerá de acuerdo con el Área de Sistemas de la Dirección de Tecnologías de la Información de IFEMA MADRID las actividades de ciberseguridad surgidas en las reuniones.

El administrador no realizará funciones de gestor, coordinador, services manager, etc. (estas funciones serán realizadas por el Service Manager) necesarias para el correcto funcionamiento del servicio. Es de prever que las actividades de operación y administración de los productos de ciberseguridad de IFEMA MADRID ocupen de forma recurrente toda su dedicación.

La administración de los sistemas de ciberseguridad se realizará previendo el posible impacto en los servicios de IFEMA MADRID, celebración de Ferias y Congresos, afectación a otros sistemas, escogiendo el momento más adecuado, en particular las operaciones con impacto en la disponibilidad de las comunicaciones seguras lo que podría suponer en algún caso, realizar acciones fuera del horario de servicio.

En el anexo "Situación Actual CONFIDENCIAL", se adjunta un gráfico con la volumetría de acciones realizadas en el contrato actual.

2.4 Consultoría experta en Ciberseguridad

IFEMA MADRID está inmersa en un proceso de transformación digital abarcando diversos escenarios y proyectos que implican integraciones con diversas infraestructuras y servicio tanto en cloud como On Premise, despliegue de soluciones, adquisición de nuevas herramientas de ciberseguridad adicionales, etc.

Dentro del objeto de contrato, se requiere la dedicación de un Consultor Experto en Ciberseguridad para realizar tareas de consultoría relacionadas con los nuevos proyectos asociados al proceso de transformación digital, emisión de dictámenes de seguridad, diseños de soluciones de ciberseguridad, asistir a reuniones con otras áreas de la compañía y empresas colaboradoras de IFEMA MADRID para la toma de decisiones en el ámbito de la ciberseguridad y otras tareas que no estén incluidas en el ámbito de la administración de los sistemas de ciberseguridad objeto del contrato.

Se requiere una dedicación en modo presencial de una jornada a la semana, que puede ser repartida en dos medias jornadas para asistir a reuniones para prestar asesoría con el criterio de la mejor seguridad para los sistemas, datos y tratamientos de IFEMA MADRID dentro del asunto que trate, coordinación con los responsables del área de Sistemas y Ciberseguridad de IFEMA MADRID en el diseño y toma de decisiones en el ámbito de la ciberseguridad, toma de requisitos para la emisión de dictámenes, etc.

El adjudicatario indicará el precio de esta parte del servicio en su oferta de forma individual, siendo este acorde al precio de mercado. En ningún caso se admitirán ofertas cuyo importe del servicio sea anormalmente bajo, que pueda generar dudas acerca su sostenibilidad.

También se estima una jornada semanal, que podría ser no presencial para realizar tareas de su responsabilidad dentro del objeto del contrato.

En definitiva, se estima una dedicación anual de 104 jornadas (832 horas) anuales de las cuales, como mínimo, 52 serán presenciales.

En caso de que esta dedicación se supere, se facturará contra el modificado del contrato.

El adjudicatario, también indicará el precio por jornada extra del Consultor experto en Ciberseguridad por si fuese necesario contratar más jornadas de este servicio, siendo este acorde al precio de mercado. En ningún caso se admitirán ofertas cuyo importe del servicio sea anormalmente bajo, que pueda generar dudas acerca su sostenibilidad.

Se requiere un titular del servicio de Consultoría experto en Ciberseguridad para que pueda entender las necesidades de la compañía. Sin embargo, en algunos momentos, durante la vigencia del contrato, podrá asistir otro experto en ciberseguridad para algún requerimiento específico, que el titular no cuente con la experiencia requerida o el conocimiento para realizarlo.

A continuación, se citan algunos ejemplos, sin que esto excluya a otras situaciones que puedan producirse:

- Asistirá a reuniones para la toma de decisiones y asesoramiento con el criterio de la mejor seguridad para los sistemas, datos y tratamientos de IFEMA MADRID dentro del asunto que trate.
- En caso de solicitar un informe sobre un producto novedoso o de reciente aparición en el mercado y que IFEMA MADRID necesite desplegar en la compañía y que tenga afectación sobre la seguridad de la información y que el administrador con dedicación presencial no sea capaz de resolver en tiempo y forma
- En caso de necesitar la validación de una solución de ciberseguridad compleja y ante una situación nueva y con un impacto importante en la compañía que afecte tanto a la infraestructura On Premise como a nuestra infraestructura cloud y que el administrador con dedicación presencial no sea capaz de validar
- Ante la necesidad de integración de servicios o plataformas de forma segura cuya complejidad se escape al conocimiento del administrador con dedicación presencial
- Conformidad a normativas de seguridad
- Integraciones entre sí de servicios y tratamientos en ubicaciones diversas como en sede corporativa de IFEMA MADRID, Hosting gestionado, Clouds Públicas y otros servicios SaaS, Paas, IaaS, etc. de terceros
- Directrices de seguridad a incorporar en otros contratos de IFEMA MADRID con terceros
- Diseños de seguridad
- Campañas de concienciación de usuarios
- Campañas con señuelos de ransomware a empleados
- Acompañamiento y asesoría para la Certificación en el Esquema Nacional de Seguridad (ENS). Durante la duración de este contrato IFEMA MADRID podría iniciar el proceso de certificación en el Esquema Nacional de Seguridad. Dentro de esta certificación surgirán actividades dentro de las competencias de la persona con dedicación presencial, incluidas por tanto en este contrato, y actividades que deberán escalarse a personas de nivel superior del adjudicatario.

- Seguridad y consultoría avanzada para actividades DevOps
- Avanzar de Devops a Devsecops para integrar la seguridad en los flujos de trabajo de los desarrollos y de los despliegues de IFEMA MADRID
- Consultoría en asuntos RGPD. IFEMA MADRID tiene contrato en vigor con una empresa colaboradora encargada de aspectos jurídicos, reglamentarios y organizativos de la protección de datos de carácter personal, dotando a IFEMA MADRID de un Delegado de Protección de Datos. Pero dicho contrato no comprende asuntos de tecnología. Por lo tanto, puede requerirse complementar a dicho contrato jurídico en los asuntos de tecnológicos de la protección de los datos de carácter personal
- Acompañamiento para la implantación de un Plan de continuidad de Negocio, planes de contingencia, Disaster Recovery y gestión de crisis
- Análisis de dependencias tecnológicas.
- Acompañamiento y diseño en la implementación de herramientas de análisis de código seguro
- Diseño de implantación estratégica de la seguridad en redes IoT
- Análisis de impactos y riesgos
- Análisis de aplicaciones de mercado desde el punto de vista de la ciberseguridad
- Analizar junto con el equipo de Sistemas y Ciberseguridad de IFEMA MADRID las necesidades del negocio en materia de ciberseguridad ayudando a minimizar los riesgos
- Definir estrategias y proponer soluciones para ayudar a la prevención de incidentes de ciberseguridad y la recuperación de estos
- Otras funciones/necesidades que IFEMA MADRID requiera y que estén relacionadas con el puesto.

2.5 Cibervigilancia digital

Dentro del alcance del servicio, IFEMA MADRID necesita monitorizar cualquier actividad relacionada con la ciberseguridad relativa al desempeño principal de la compañía que son las Ferias, Convenciones y Eventos con el fin de detectar amenazas y mitigar los posibles riesgos relativos a sus sistemas e infraestructuras. A su vez puede requerir este servicio de monitorización para personajes VIP o compañías participantes en los diferentes eventos que se celebren en IFEMA MADRID. Por lo tanto, se trata de poder detectar las amenazas externas basándose en el análisis de varias fuentes de información como por ejemplo Deep y Dark Web, análisis de reputación, redes sociales, etc.

Por este motivo, IFEMA MADRID estima que realizará la cibervigilancia de 10 eventos durante la vigencia del contrato a determinar en tiempo y forma y que se ejecutarán bajo demanda o necesidades de la compañía, con lo cual se facturará contra la parte variable del contrato.

El adjudicatario indicará el precio de cada cibervigilancia en su oferta de forma individual, siendo este acorde al precio de mercado. En ningún caso se admitirán ofertas cuyo importe del servicio sea anormalmente bajo, que pueda generar dudas acerca su sostenibilidad.

En caso de que por circunstancias IFEMA MADRID necesite ampliar el servicio de cibervigilancia por encima de los 10 eventos incluidos en la oferta, los podrá solicitar al proveedor en tiempo y forma y se podrá adquirir mediante las modificaciones previstas al contrato. Por este motivo, el ofertante deberá presentar una propuesta económica por cada cibervigilancia adicional de cualquier evento.

IFEMA MADRID indicará al proveedor como mínimo con diez días de antelación a la celebración de la Feria, Congreso o Evento que desea vigilar, con el fin de puedan ponerse en marcha los mecanismos necesarios para desarrollar el trabajo solicitado.

Los trabajos se basarán en la monitorización de los ataques de los siguientes ámbitos, siendo estos los mínimos aceptables:

- Oportunismo cibercriminal (Basado en la monitorización de la Deep Web).
- Activismo/Hacktivismo social (Basado en el comportamiento y redes sociales).
- Activismo político (Basado en el contexto geopolítico).

La cibervigilancia deberá comenzar a realizarse unos tres días antes del inicio del evento. La emisión de informes diario comenzará con el primer día de celebración del evento y el proveedor emitirá el informe diario, al cierre de la jornada, con toda la información relevante en cualquiera de los tres ámbitos mencionados. Si los días antes del inicio del evento se detectase alguna alarma o riesgo, el proveedor deberá informar a IFEMA MADRID de dicha situación para poder tomar las medidas necesaria para mitigar el problema.

Al final del evento, el proveedor entregará también un informe con la valoración general de la cibervigilancia del evento, riesgos detectados, acciones realizadas, notas emitidas, etc. con el fin de tomar las medidas necesarias para mitigar los riesgos de este y otros eventos de IFEMA MADRID.

A su vez, el proveedor también deberá emitir durante el periodo de cibervigilancia del evento, cualquier nota informativa que considere relevante y pueda poner en riesgo dicho evento, informando a IFEMA MADRID, de la amenaza detectada, la fecha y hora de detección, nivel de criticidad, referencia y los actores implicados en el suceso, así como las medidas y recomendaciones a tener en cuenta para mitigar el riesgo detectado.

En caso de que IFEMA MADRID no haga uso de la cibervigilancia de algunos eventos incluido en la oferta y sí se produjese la renovación del servicio, estos podrán ser usados en el año siguiente, es decir, si de los 10 eventos incluidos en la oferta, IFEMA MADRID no hiciese uso de alguno de ellos podrán acumularse a los 10 eventos del año siguiente.

2.6 Análisis de vulnerabilidades

Dentro del alcance del contrato, IFEMA MADRID necesita un servicio de gestión de vulnerabilidades con el fin de monitorizar e investigar el uso inadecuado de sus sistemas o actividades sospechas que puedan poner en peligro los activos de la compañía.

Aun disponiendo de herramientas de seguridad adecuadas, resulta difícil encontrar y eliminar todas las vulnerabilidades del entorno IT. IFEMA MADRID cree en un enfoque proactivo sobre la situación de la ciberseguridad.

Por lo tanto, este servicio debe detectar información detallada sobre las amenazas reales y explotables para identificar la criticidad de estas y priorizar su resolución.

Para ello se establece el estudio de vulnerabilidades como máximo de 30 IPs internas y 10 IPs externas con la herramienta adecuada y con periodicidad de escaneo trimestral. También se requiere el estudio de vulnerabilidades de 10 aplicaciones Web como máximo con periodicidad trimestral.

El adjudicatario indicará el precio de esta parte del servicio en su oferta de forma individual, siendo este acorde al precio de mercado. En ningún caso se admitirán ofertas cuyo importe del servicio sea anormalmente bajo, que pueda generar dudas acerca su sostenibilidad.

El adjudicatario debe entregar un informe a la finalización de cada tarea indicando las vulnerabilidades encontradas e implementando las medidas oportunas en los elementos de ciberseguridad objeto del servicio. Será responsabilidad de IFEMA MADRID la mitigación del resto de las vulnerabilidades de los sistemas afectados.

2.7 Pentesting

IFEMA MADRID, siendo consciente de los riesgos actuales y con el objetivo de conocer el nivel de eficiencia de sus defensas y poder determinar el alcance de los fallos de seguridad de los sistemas de la compañía, podrá solicitar el servicio de dos pentesting por cada año de contrato de los servicios de IFEMA MADRID sean On Premise o de cualquiera de sus servicios cloud.

Estos pentesting podrán ser interno y/o externo, siendo la Dirección de Tecnologías de la Información quien determine el tipo y las fechas a realizar, comunicándolo con suficiente antelación al proveedor para que este pueda preparar las acciones necesarias a realizar.

En el momento de activar esta petición, se le comunicará al proveedor, el tipo de pentesting a realizar, así como la modalidad de este, pentesting de “caja blanca” o pentesting de “caja negra”. IFEMA MADRID escuchará la recomendación del proveedor a este respecto.

El adjudicatario indicará el precio de esta parte del servicio en su oferta de forma individual servicio con el fin de que IFEMA MADRID pueda solicitar pentesting adicionales a los incluidos en la oferta en caso de ser necesario, siendo este importe acorde al precio de mercado. En ningún caso se admitirán ofertas cuyo importe del servicio sea anormalmente bajo, que pueda generar dudas acerca su sostenibilidad.

El ofertante, indicará en su propuesta el valor económico de este servicio con el fin de que IFEMA MADRID pueda solicitar pentesting adicionales a los incluidos en la oferta en caso de ser necesario.

2.8 Gestión y respuesta ante incidentes

Dentro del alcance del contrato, se incluye la activación de un servicio de respuesta ante incidentes, con una duración de como mínimo 100 horas. Se podrá activar este servicio en cualquier momento (24x7x365).

Una vez activado el servicio, el proveedor pondrá en marcha los mecanismos adecuados para tomar el control y asumiendo el liderazgo de la situación in situ ante el incidente, asignando el personal adecuado y realizando todas las acciones, mecanismos y medidas para aislar, contener y mitigar la brecha de seguridad o el problema detectado.

El proveedor, en esta situación, también será el interlocutor con otras áreas o proveedores implicados en la resolución de la brecha de seguridad, compartiendo información y colaborando de forma estrecha con las personas o equipos que IFEMA MADRID designe para este escenario.

Se solicita también la recolección de los datos cruciales del origen y alcance del incidente de seguridad en los dispositivos y programas e infraestructuras implicados ya sea de los servicios On Premise, cloud e IoT de la compañía.

En caso de que IFEMA MADRID no haga uso del servicio DFIR incluido en la oferta, el excedente de horas no consumidas se sumará a las horas del servicio del año siguiente en caso de renovación de este. También se podrán cambiar las horas de ese servicio para otros servicios objeto del contrato como la bolsa de horas extras del Administrador de sistemas de ciberserguridad, horas de consultor experto en ciberseguridad, EPSs adicionales, cibervigilancias adicionales y pentesting adicionales.

El adjudicatario indicará el precio de esta parte del servicio en su oferta de forma individual, siendo este acorde al precio de mercado. En ningún caso se admitirán ofertas cuyo importe del servicio sea anormalmente bajo, que pueda generar dudas acerca su sostenibilidad.

3. Situación actual

La situación de IFEMA MADRID con respecto a la ciberseguridad goza de buena salud, es estable y afortunadamente no ha sufrido incidentes graves en los últimos 12 meses.

En este momento IFEMA MADRID se haya en fase de expansión de sus infraestructuras y la integración segura de estas infraestructuras On Premise y cloud está latente, y son los retos a los que nos debemos enfrentar en el futuro más cercano.

También, IFEMA MADRID es objeto mediático y de interés para los ciberdelicuentes por lo tanto, somos conscientes del peligro que esto entraña, destinando medios y aplicando medidas para mitigar los riesgos que impactan en este escenario.

Concienciamos a los empleados de la compañía de los riesgos actuales, phishing, ransomware, etc., realizando campañas de concienciación, desplegando herramientas para mitigar los peligros que acechan y estableciendo protocolos de actuación en caso de posibles incidentes.

La Dirección de IFEMA MADRID está concienciada con los riesgos relacionados con la Ciberseguridad.

En el anexo Situación Actual CONFIDENCIAL que el licitante podrá solicitar, siguiendo las indicaciones pertinentes, se detalla con amplitud la situación con respecto a la ciberseguridad en la que IFEMA MADRID se encuentra. En este anexo se enumeran también los elementos de ciberseguridad de la compañía.

También se detallan todos los elementos para tener en cuenta para la correcta prestación del servicio y datos de volumetría para que el licitante puede valorar y conocer la situación de IFEMA MADRID.

Las empresas interesadas en retirar la documentación confidencial relativa al "Anexo Situación Actual CONFIDENCIAL", deberán facilitar el modelo de compromiso de confidencialidad que se adjunta en el Anexo XX "*MODELO DE DOCUMENTO DE COMPROMISO DE CONFIDENCIALIDAD*", junto con la escritura de poder y los certificados Partner que se detallan a continuación, y remitirlo a

los siguientes correos electrónicos: igomez@ifema.es; aticas@ifema.es para hacerles entrega de la documentación.

a. Partner 4 estrellas o superior y CCSP de Checkpoint.

b. Partner Select Integrator o superior de Cisco.

c. Partner Select o superior de Fortinet

4. Modelo de Gobierno y Relación

El modelo de Gobierno y Relación estará basado en la consecución de los ANS contratados y pretende conseguir la resolución de las incidencias y peticiones en el momento oportuno, atendiendo a las necesidades y prioridades planificadas por IFEMA MADRID y de un modo que, en todo momento, las personas implicadas de IFEMA MADRID y del proveedor estén informadas regularmente sobre el responsable y estado de todas las actividades del servicio.

El actor fundamental para este modelo de relación es el descrito en el apartado "2.3 Administrador de los sistemas de Ciberseguridad presencial", del presente pliego de prescripciones técnicas. Gestionará las solicitudes de la herramienta de ticketing de IFEMA MADRID tanto para su creación, seguimiento, gestión y cierre de las mismas que IFEMA MADRID tiene destinada para el seguimiento del servicio y en la que se basará el cálculo de ANS. Se requiere por parte de proveedor, una profunda contextualización, ofreciendo soluciones adaptadas a IFEMA MADRID para las distintas tareas, no solo basadas en "libros blancos" sino aplicándolas al marco de necesidades y circunstancias de IFEMA MADRID.

Habrá reuniones de seguimiento del servicio e informes con periodicidad mensual.

Se requiere que por parte del adjudicatario exista el rol de service manager, el cual deberá asistir y liderar las reuniones de seguimiento del servicio, exponiendo el informe de servicio y realizando un acta de la reunión en donde se recogerán los acuerdos alcanzados con respecto al servicio y/o facturación, y tareas o actividades a realizar definiendo responsabilidades y fechas de compromiso.

El objeto de la gestión de solicitudes es la atención correcta de las solicitudes en materia de ciberseguridad dentro de los Acuerdos de Nivel de Servicio ANS acordados y priorizándolas en proporción al riesgo que mitigan y a su interés para IFEMA MADRID.

Diariamente, el equipo de Sistemas de la Información y Ciberseguridad se reúne con el objeto de identificar y poner en común las actividades del área a realizar acordando prioridades en todos los ámbitos y en la que también se incluyen los aspectos de ciberseguridad, con el fin de relacionar y conocer el impacto de nuestras tareas con las del resto del equipo.

Todas las actividades de ciberseguridad tienen que estar registradas en el software de tickets de IFEMA MADRID. Por tanto, todas las actividades de ciberseguridad contarán con su identificador de ticket. El ticket también registrará la información relacionada con la actividad que sea útil como base de datos de conocimiento y para determinar el estado de ejecución y de la resolución.

Se denomina incidencia a toda interrupción o reducción de la calidad no planificada del servicio. Pueden ser fallos reportadas por el SOC, el equipo de Sistemas Corporativos y Seguridad de la Información de IFEMA MADRID, por alguna herramienta de monitorización de eventos, por otro proveedor de servicios tecnológicos como resultado de su monitorización de los sistemas de IFEMA MADRID, por el CAU (Centro de Atención al Usuario) de IFEMA MADRID, etc. El objetivo principal ante las incidencias es restaurar cuanto antes la operativa normal del servicio minimizando el impacto negativo en el negocio.

Las peticiones podrán ser de diversa índole como asesoramiento, consultoría, diseño de soluciones de ciberseguridad, análisis de viabilidad, informes, etc.

Es decir, se trata de acometer todas las acciones necesarias para un óptimo funcionamiento de los sistemas de IFEMA MADRID. Dichas acciones (incidencias y peticiones) estarán sujetas a esta clasificación:

- **Incidencia crítica**: Aquella que afecta significativamente al nivel de servicio prestado. El servicio esta indisponible lo que impide la operativa básica del sistema, afecta a un número elevado de usuarios o puede afectar económicamente a IFEMA MADRID. También es una incidencia crítica el incumplimiento de los ANS contratados.

- **Petición urgente**: Aquella que afecta parcialmente al servicio, produciendo una degradación de este, pero sin estar el servicio indisponible y afectando a un número moderado de usuarios pero que requiera una solución urgente. Se podrá realizar una petición urgente porque sea de interés prioritario para IFEMA MADRID.

- **Incidencia grave**: Aquella que afecta parcialmente al servicio, produciendo una degradación de este, pero sin estar el servicio indisponible y afectando a un número reducido de usuarios.

- **Incidencia o petición leve**: Aquella que no afecta al nivel de servicio prestado, aunque existe riesgo potencial de degradación/perdida de este.

La criticidad asignada a una incidencia o petición será determinada por IFEMA MADRID en el momento de su apertura, pudiendo ser recalificada a petición del proveedor con el acuerdo de Sistemas Corporativos y Seguridad de la Información de IFEMA MADRID.

No llegarán tickets indiscriminadamente y sin filtrar a la bandeja de entrada de tickets del Servicio de Ciberseguridad, porque los usuarios finales de IFEMA MADRID no abren tickets de ciberseguridad directamente. Los tickets de ciberseguridad ya vienen filtrados y pueden proceder del escalado por parte de otras áreas de IFEMA MADRID, como el CAU (Centro de Atención de Usuarios) que ya han filtrado según procedimiento qué tickets debe atender el servicio de Ciberseguridad. Los tickets también proceden de personas adscritas al Área de Sistemas y Ciberseguridad de IFEMA MADRID.

El administrador de los sistemas de ciberseguridad también abrirá los tickets necesarios de las actividades que no se hayan registrado en el sistema de ticketing. Por ejemplo, las actividades derivadas de acuerdos en reuniones de ciberseguridad. El objeto es poder priorizarlas, atenderlas correctamente y hacer su seguimiento.

5. Acuerdos Mínimos de Nivel de Servicio

En este apartado se presenta el sistema de evaluación de la calidad del servicio que el adjudicatario debe cumplir.

La empresa adjudicataria deberá garantizar la prestación y cumplimiento adecuados de los servicios solicitados dentro del ámbito del presente pliego. No obstante, lo anterior, hay ciertas prestaciones que se regularan por el sistema de "Acuerdo de Nivel de Servicio" (ANS).

El sistema de evaluación tiene como objetivo la determinación del índice de calidad de la prestación del servicio o ICS (Índice de Calidad del Servicio), basado en los acuerdos de nivel de servicio (ANS) mínimos imprescindibles, que el adjudicatario debe cumplir en la ejecución de los servicios a prestar.

Los acuerdos de nivel de servicio se van a materializar en una serie de "Indicadores de nivel de servicio (INS)" y unos "valores objetivos" (VO) que deben cumplir y que van a permitir evaluar los distintos ámbitos de servicios prestados por la empresa adjudicataria.

El incumplimiento de los acuerdos definidos será penalizable y dicha penalidad será determinada en base al % de penalización asociado a cada indicador.

El adjudicatario deberá proponer los mecanismos necesarios para el tratamiento de desviaciones, garantizando que estas se corrigen en los informes del mes siguiente.

Será en la fase inicial de la prestación del servicio en la que se deberán definir y poner en marcha los indicadores que inicialmente constituirán las medidas de calidad del servicio.

El conjunto de indicadores puestos en marcha inicialmente podrá ser revisado durante el periodo de prestación del servicio como consecuencia de la evolución del servicio o de las necesidades de IFEMA MADRID. Se podrán entonces acordar modificaciones en el sistema de ANS que deberán respetar las siguientes condiciones:

- Los nuevos indicadores o las modificaciones deberán contar con el acuerdo de ambas partes, reflejados en un acta de reunión expresa para dicha gestión.
- Una incidencia podría incumplir varios ANS a la vez.

En caso de discrepancia entre lo dispuesto en el presente ANS y en la oferta presentada o cualesquiera documentos aportados por el adjudicatario en el marco de la presente contratación, siempre prevalecerá lo dispuesto en el presente ANS, salvo aceptación en contrario, de forma expresa y por escrito, por parte de IFEMA MADRID.

Condiciones de aplicación de los ANS

Con el cumplimiento de las prestaciones reguladas por los ANS se pretende que el adjudicatario garantice una calidad mínima en la prestación del servicio.

Por este motivo, los INS y VO definidos van a tener carácter de mínimos. El adjudicatario podrá ampliar los indicadores INS y los valores objetivos VO a establecer de común acuerdo con IFEMA MADRID, siempre respetando los mínimos.

Los factores principales que inspiran este modelo tienen como objetivo último la garantía de la calidad de los servicios prestados, el incentivo a la mejora continua del adjudicatario en la provisión de estos y la consecuente mejora en la satisfacción tanto de los usuarios como de la Dirección de Tecnologías de la Información de IFEMA MADRID.

En relación con los Acuerdos de Nivel de Servicio, el adjudicatario se obliga a:

- Enviar de forma mensual un informe detallado de los indicadores obtenidos, que serán revisados en la reunión mensual del seguimiento del servicio.
- Es obligación del proveedor del servicio la recogida, tratamiento y documentación de estos.
- Recoger y calcular fielmente, de acuerdo con las definiciones establecidas, todos los indicadores y sus valores mes a mes. Aunque los datos obtenidos deberán ser validados por IFEMA MADRID, la recogida errónea de los indicadores y sus valoraciones será sancionada económicamente, según lo indicado en el apartado de penalidades de este anexo.

- El adjudicatario es responsable de comunicar a IFEMA MADRID cualquier anomalía que pueda existir en los datos utilizados para el cálculo, o en los propios cálculos, en un periodo máximo de 15 días naturales tras la emisión de cada informe.

- El adjudicatario debería mejorar los resultados de los indicadores mes a mes. Deberá prestar especial atención a aquellos indicadores cuyo incumplimiento se repita o bien a aquellas situaciones que provoquen una bajada de la calidad del servicio. El adjudicatario deberá proponer planes y acciones de mejora y recuperación del nivel de cada indicador que repetidamente se incumpla o tengan bajada de calidad de forma continua.

- Dentro del ámbito de las prestaciones que se regulen por el sistema de ANS, será responsable del cumplimiento de todos los VO establecidos, con independencia de los recursos materiales o humanos que para ello tenga que incorporar en cada momento.

- El incumplimiento continuo del nivel de calidad establecido en el servicio en función de los niveles exigidos en el pliego de bases y los ofertados expresamente por el adjudicatario será motivo suficiente para la extinción del contrato de forma unilateral por parte de IFEMA MADRID.

Modelo de cálculo de los ANS

En este apartado se describe el modelo de cálculo de los ANS.

El sistema de ANS evaluará no solo las distintas prestaciones del servicio, sino que concederá un papel destacado a las no conformidades.

Se producirá una No Conformidad en toda aquella situación en la que IFEMA MADRID no esté satisfecha con la actuación realizada por el proveedor, así como para indicar el grado de cumplimiento de aspectos formales del servicio, como por ejemplo, una estimación a la que no se llega a un acuerdo, un análisis de impacto no satisfactorio, una documentación no adecuada, un requisito no cubierto, una cláusula del pliego no cumplida, una resolución no satisfactoria de una tarea, de un proyecto, una transferencia de conocimiento no adecuada, un recurso no adecuado en capacidad técnica y experiencia, etc.

IFEMA MADRID indicará el motivo y la posible subsanación de la no conformidad. El proveedor está obligado a registrar las no conformidades, recogiendo toda esta información más la que considere oportuna y dispondrá de un plazo de tiempo fijado en cada caso para proceder a su subsanación. Si transcurrido el plazo de tiempo establecido no se ha subsanado, o bien, si el proveedor desestima su subsanación, contabilizará como una no conformidad no resuelta que aplicará en el mes que corresponda y en meses sucesivos hasta su subsanación.

La criticidad de la incidencia/petición va a determinar los distintos valores de los acuerdos de nivel de servicio (ANS) aplicables.

Además de la criticidad de las incidencias/peticiones, se va a medir el nivel de cumplimiento de aspectos como:

- **Disponibilidad:** Compromisos de disponibilidad de herramientas, sistemas, comunicaciones necesarias para la prestación de los servicios

- **Plazos:** Cumplimiento de los plazos acordados en la prestación de los servicios

- **No conformidades**: Numero de incumplimientos y desacuerdos

- **Calidad:** Evaluación de la calidad de las entregas realizadas por el proveedor

Para finalizar con el modelo, también se determina la criticidad de cada uno de los indicadores, con ponderación mayor de los críticos respecto de los no críticos para el cálculo del índice de calidad (ICS).

Peso de los indicadores (Peso índice de calidad):

- **Muy críticos**: 3 puntos
- **Críticos**: 2 puntos
- **No críticos**: 1 puntos

La suma de todos los indicadores que corresponde al ICS solicitado es de 35 puntos. Documento Excel *"SLA_Exp 23 031_Ciberseguridad"*.

Penalidades

Tal y como se indica anteriormente, el incumplimiento de los acuerdos será penalizable. La naturaleza de las penalidades por incumplimiento de los acuerdos será de carácter económico. Se persigue con esta medida que el servicio se preste adecuadamente y con la calidad exigida durante todo el período de contratación.

La obtención de la penalidad económica de carácter mensual será aplicable en la facturación de cada mes correspondiente al Componente Fijo.

Se aplicará, como penalidad, la suma de las penalidades de los indicadores que no hayan alcanzado el % de cumplimiento definido para cada uno de ellos. Por Ejemplo:

- Si se incumpliera "INC01_Tiempo de Resolución de Incidencias Críticas" (5% de Penalidad sobre factura mensual fijo) y el "INC03_Tiempo de Resolución de Incidencias Graves" (3% de Penalidad sobre factura mensual fijo) la penalidad total a aplicar en la facturación del mes será del 8% sobre el importe del Componente Fijo del mes correspondiente al incumplimiento.

El valor de penalidad obtenido se aplicará como porcentaje a descontar de la facturación del mes correspondiente.

La renovación anual de licencias de los productos de ciberseguridad está exenta de la aplicación de penalidades.

Cláusula de recurrencia: puesto que el objetivo de este planteamiento es ir mejorando mes a mes el servicio, aquellos indicadores cuyo incumplimiento se repita tres meses consecutivos sin causa justificada y aceptada por IFEMA MADRID, automáticamente el % de penalidad asociado se duplicará en el cuarto mes consecutivo de incumplimiento.

La recogida errónea de los valores de los INS o su no recogida en el informe mensual conlleva una penalidad del 1% de la facturación mensual del Componente Fijo y acumulable a las otras penalidades que pudieran corresponder.

6. Dotación de medios

El adjudicatario deberá disponer de la infraestructura de conectividad para materializar las comunicaciones necesarias para la prestación del servicio. Dispondrá de los elementos físicos y lógicos adicionales para garantizar la calidad en la comunicación tanto con los sistemas como con los aplicativos, utilidades y servicios implicados en las actividades propias del servicio de soporte para la ciberseguridad de IFEMA MADRID. Se compromete además a cumplir los estándares de comunicación en que se basa la arquitectura de red de IFEMA MADRID, por ejemplo, adaptándose a la configuración de los elementos de seguridad tales como firewalls, proxys, etc.

El modo de comunicación debe ser ágil y seguro usando para ello las distintas posibilidades adecuadas para cada caso. Por ejemplo, entre otras, VPNs LAN to LAN, línea dedicada, etc. El adjudicatario desplegará las líneas y método de comunicación más adecuado para el servicio que se está prestando. Será en la fase I de la prestación del servicio donde se establecerá la conexión con IFEMA MADRID. En caso de elegir comunicación VPN LAN to LAN el adjudicatario dispondrá de una VPN compatible con el terminador VPN de IFEMA MADRID. No se habilitará ningún acceso adicional a los sistemas de IFEMA MADRID que no sea a través del medio de comunicación elegido. El proveedor del servicio deberá poseer un plan de contingencia de las comunicaciones que debe aplicar en caso de problemas para no dejar de prestar el servicio. Durante esta fase, el adjudicatario deberá definir los parámetros para la conexión junto con IFEMA MADRID y llevará a cabo todas las tareas necesarias para que la conectividad esté plenamente operativa y comprobada.

A partir de la fase II el adjudicatario deberá además proporcionar el soporte técnico necesario para un correcto funcionamiento de las comunicaciones entre las dependencias desde las que el equipo realice los servicios.

El adjudicatario es responsable del cumplimiento de los ANS relacionados con las comunicaciones, sus herramientas y sus equipos.

El adjudicatario permitirá la conexión a IFEMA MADRID únicamente a los sistemas autorizados, no pudiendo acceder a otros que se escapen del objetivo de este contrato y exclusivamente para las tareas relacionadas con el mismo.

El adjudicatario deberá proporcionar y actualizar periódicamente una lista de usuarios autorizados por IFEMA MADRID para acceder a la plataforma, además de auditar y controlar quien accede, en qué momento y con qué objetivo. A su vez, también deben identificar los equipos clientes que se vayan a conectar usando los medios necesarios para que se garantice que sólo se permite el acceso desde los equipos autorizados.

Los equipos desde los que el adjudicatario se vaya a conectar con IFEMA MADRID deben cumplir ciertos requisitos de seguridad como tener un endpoint actualizado y operativo, un nivel de parches de sistema operativo que no permitan explotar bugs, etc. Deben poseer una password segura y su acceso debe ser restringido.

Como ya se ha mencionado, para IFEMA MADRID la seguridad de la información es un aspecto muy importante. En lo relacionado con las actuaciones, decisiones, planificaciones, etc. en que están involucrados los sistemas de IFEMA MADRID siempre se deben tener en consideración la seguridad en todas sus vertientes, tanto en la confidencialidad como en la integridad y disponibilidad de datos y sistemas.

El adjudicatario deberá aprovechar y preservar los recursos de IFEMA MADRID puestos a su disposición, sin desviarlos de sus objetivos sustanciales ni se desviarán hacia actividades que no se hallen directamente relacionadas con la prestación del servicio.

El empleo de estos recursos informáticos debe ser siempre acorde con el prestigio y la imagen corporativa de IFEMA MADRID, especialmente si se proyecta al exterior.

La instalación y el mantenimiento del servicio de comunicaciones correrán por cuenta del adjudicatario.

7. Fases de la prestación del servicio

El servicio global requerido, constará de las siguientes fases. La duración de las 4 fases es de 1 año (facturable), siendo las dos primeras fases dentro de las primeras 2 semanas.

- Fase I: Preparación y Constitución del Servicio. **Duración máxima 1 semana.**
- Fase II: Fase de transición. **Duración mínimo 2 semanas, máximo 1 mes**. **Inicio simultaneo a Fase I.**
- Fase III: Prestación completa del Servicio.
- Fase IV: Traspaso del Servicio. Durante las 2 últimas semanas del contrato.

Fase I - Preparación y Constitución del Servicio

En la fase I - Preparación y Constitución del Servicio los objetivos son:

- Preparar el equipo designado por el proveedor para poder comenzar con el servicio.
- Preparar la infraestructura técnica y organizativa necesaria para la prestación del servicio.

Así mismo, se establecerá la conectividad con IFEMA MADRID del equipo de trabajo del adjudicatario, se realizarán reuniones de coordinación con IFEMA MADRID, se definirán los procedimientos de trabajo y de gestión del servicio, los de la gestión de tareas, y todos aquellos que resulten necesarios para que el servicio se pueda comenzar a prestar con la calidad necesaria de acuerdo con las especificaciones de este pliego.

Para evitar retrasos indeseados, es muy importante que desde el momento de la adjudicación del servicio se pongan en marcha, rápidamente, todas las tareas necesarias para el cumplimiento de los objetivos indicados. El adjudicatario será responsable de los posibles perjuicios que se puedan producir en el arranque del servicio, derivados del retraso tanto de la disponibilidad del equipo como de la puesta en marcha de las comunicaciones necesarias, aun cuando ello sea achacable a otras empresas que tengan que proporcionar o instalar alguno de los recursos/elementos necesarios.

El adjudicatario deberá poner en marcha todos los medios técnicos y organizativos necesarios para garantizar la seguridad de la plataforma. Es decir, se establecerán los mecanismos necesarios para que el acceso a la red de IFEMA MADRID esté disponible únicamente para los usuarios autorizados y solamente para realizar las tareas autorizadas por este contrato. Una vez finalizada la fase se pasará a la fase de transición.

Fase II: Fase de transición.

En la fase II – Transición, se realizará el traspaso de conocimiento de los sistemas de IFEMA MADRID objeto del contrato. El proveedor tendrá que estudiar la documentación técnica existente, así como

realizar entrevistas con los responsables del Área de Sistemas Corporativos y Seguridad de la Información de IFEMA MADRID y con el actual adjudicatario contratado. Es posible que esas reuniones se celebren presencialmente en IFEMA MADRID, hasta garantizar que el proveedor ha alcanzado un nivel de autonomía suficiente (seguimiento de los procedimientos establecidos, conocimiento técnico, etc.), para la elaboración de las tareas descritas en este pliego.

Al final de esta fase se pasará a la fase de prestación completa del servicio. La facturación del servicio será desde la fase II en adelante.

Fase III: Prestación completa del Servicio.

La fase III - Prestación Completa del Servicio lleva implícito el objetivo principal del proyecto, esto es, alcanzar el máximo nivel de servicio posible a través del análisis y resolución de las tareas que se generen en tiempo y forma.

El servicio de soporte para ciberseguridad debe recoger todas las actividades descritas en este pliego encaminado a asegurar el aprovechamiento de los sistemas, su disponibilidad, su seguridad y su evolución ante los cambios, todo dentro de un marco metodológico que garantice un máximo de calidad y eficiencia en este servicio.

Durante este periodo se pondrán en marcha tanto los ANS determinados como mínimos en estas especificaciones técnicas (ver apartado "5. Acuerdos Mínimos de Nivel de Servicio" con estas especificaciones).

Todos los aspectos de Seguridad relacionados con la prestación del servicio estarían indicados en el anexo *"ANEXO XIII: 076 Anexo para contratos de bienes y servicios con elementos relacionados con TI"*.

Fase IV: Traspaso del Servicio.

La fase IV - Traspaso del servicio se producirá en caso de cese o finalización de contrato. El adjudicatario del servicio queda obligado a transferir el conocimiento técnico, así como el concerniente a herramientas, procedimientos, procesos y documentación, casos de usos etc. a la entidad que sea designada por IFEMA MADRID para que, en el menor tiempo y las mejores condiciones posibles, dicha entidad pueda ofrecer con garantías la continuidad en el servicio.

Deberá, además, generar toda la documentación necesaria para que este traspaso sea lo más efectivo y ágil posible, sin penalizar el objeto del contrato.

Con anticipación suficiente al inicio de la fase de devolución del servicio, se hará una evaluación y planificación de todas estas actividades, obteniéndose un Plan de Reversión del servicio.

El proveedor deberá realizar el proceso de reversión, asegurando que se mantiene el servicio de ciberseguridad en IFEMA MADRID durante el traspaso del control de servicios y deberá colaborar activamente con IFEMA MADRID y con el futuro proveedor, durante este proceso, para facilitar la transición de los servicios sin causar perjuicios.

El proveedor entregará, al final del contrato, toda la documentación del servicio actualizada hasta dicho instante, que deberá ser validada por el personal de IFEMA MADRID. Así mismo, el proveedor deberá borrar y destruir de su instalación todos los datos, ficheros, programas, documentos, etc. utilizados para la prestación del servicio que sean propiedad de IFEMA MADRID.

8. Garantía de los trabajos y titularidad

Con independencia de la duración prevista en el contrato, el proveedor debe a IFEMA MADRID, a partir de la aceptación por parte de esta de cada uno de los trabajos y actividades realizadas y por un periodo no inferior a seis meses, el correcto funcionamiento de todos los servicios prestados. Se compromete a subsanar, sin coste adicional y sin impacto en la prestación normal del servicio, cualquier error que pudiera aparecer durante dicho periodo.

En ningún caso el proveedor podrá hacer uso, dar acceso o divulgar la información, programas y materiales a los que haya tenido conocimiento y acceso en virtud del presente contrato de mantenimiento, para cualesquiera asuntos que no estén directamente relacionados con las actividades y tareas descritas en este documento.

Todos los derechos sobre los estudios, análisis, documentación y materiales relacionados obtenidos al amparo del presente contrato quedan íntegramente bajo la propiedad de IFEMA MADRID.

9. Personas de contacto

El adjudicatario deberá proporcionar a la Dirección de Tecnologías de la Información, los contactos de soporte del presente pliego para cualquier gestión que IFEMA requiera.

Les recordamos que, para cualquier consulta o aclaración de carácter administrativo, técnico o económico sobre este expediente, deben proceder conforme a lo previsto en los apartados 5.- CONSULTAS y 6.- PRESENTACIÓN DE LAS PROPOSICIONES. NOTIFICACIONES Y COMUNICACIONES- del Cuadro de Características-.

Igualmente, les recordamos que, para aquellas cuestiones que puedan afectar a la operativa / funcionalidad del portal de licitación electrónica de IFEMA MADRID, existe un área de soporte y consulta a licitadores dentro de la web:

- Preguntas frecuentes: https://licitaciones2.ifema.es/html/preguntas-frecuentes
- Manual de uso de la plataforma: https://licitaciones2.ifema.es/resources/Guia_Licitadores.pdf
- Soporte y contacto con plataforma: https://pixelware.com/servicios-soporte-licitadores/

El contacto telefónico con el encargado de la gestión del expediente perteneciente a la Dirección de Compras y Logística de IFEMA MADRID, que se cita a continuación, se limitará a cuestiones meramente informativas no vinculantes sobre el propio proceso de licitación: Amy Ticas, 676.132.048.

10. Visita a las instalaciones de los ofertantes

En caso de considerarlo necesario, el personal de IFEMA MADRID podrá visitar las instalaciones de las ofertantes propuestas para la ejecución del servicio.

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

Se deberá aportar la documentación técnica que se requiere en este apartado, para la validación de su oferta técnica.

La documentación que debe presentar el ofertante tendrá el objetivo concretar su propuesta para el servicio solicitado. Es decir, debe explicar como pretende acometer el servicio que requiere IFEMA MADRID explicando cada parte del mismo. Esta documentación seré descriptiva, exacta, pertinente, breve y concisa, abarcando los elementos de la solución ofertada por el licitador.

Serán descartados aquellos licitadores que técnicamente no presenten un servicio bajo los estándares y requerimientos exigidos en el presente pliego. Igualmente, IFEMA MADRID descartará aquellas propuestas que no incluyan información sobre los aspectos que se citan.

La información para incluir en este sobre, NO DEBERÁ EXTENDERSE EN MÁS DE 10 PÁGINAS (1 cara) y deberá seguir estrictamente el guion indicado a continuación:

1. **Índice**

2. **Descripción detallada de los puntos incluidos en el apartado "2. Alcance" del presente documento**

   2.2 Renovación anual de licencias de los productos de ciberseguridad
   2.3 Administrador de sistemas de ciberseguridad presencial
   2.4 Consultoría experta en ciberseguridad

3. **Otra documentación**
   3.1 Otra documentación que el ofertante considere de interés

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

Se deberá aportar la documentación técnica que se requiere en este apartado, para la validación de su oferta técnica.

La documentación que debe presentar el ofertante tendrá el objetivo concretar su propuesta para el servicio solicitado. Es decir, debe explicar como pretende acometer el servicio que requiere IFEMA MADRID explicando cada parte del mismo. Esta documentación seré descriptiva, exacta, pertinente, breve y concisa, abarcando los elementos de la solución ofertada por el licitador.

Serán descartados aquellos licitadores que técnicamente no presenten un servicio bajo los estándares y requerimientos exigidos en el presente pliego. Igualmente, IFEMA MADRID descartará aquellas propuestas que no incluyan información sobre los aspectos que se citan.

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:

1. **Índice**

1. **Organización y gestión del servicio**

1.1 Planteamiento del servicio

a. Descripción detallada de la disposición de elementos de control y gestión. Se valorará el nivel de detalle de los elementos de control y gestión que se proponen para el servicio, el nivel de adaptación y acople de estos elementos de control y gestión a las características del negocio de IFEMA MADRID, el nivel de implicación en el control y gestión del servicio por parte del proveedor, así como la acciones que se propongan para la mejora continua del servicio.
b. Descripción de mejoras a la propuesta de los ANSs, con respecto a los niveles de compromiso.

1.2 Descripción de la gestión del servicio/Modelo de relación

a. Descripción de la estructura organizativa de gestión y herramientas utilizadas. Se valorará el nivel la idoneidad de la estructura organizativa y herramientas propuestas a la estructura de IFEMA MADRID y el nivel de madurez en cuanto a la gestión de los servicios y nivel de sencillez, eficacia y claridad de las herramientas utilizadas para la gestión.
b. Descripción detallada de los recursos, tanto humanos como técnicos, que se ponen a disposición de IFEMA MADRID para la correcta prestación y gestión del servicio. Se valorará la idoneidad de los recursos propuestos para cada uno de los servicios solicitados, así como el nivel de detalle en cuanto a certificaciones y formación en el ámbito de la Ciberseguridad.
c. Descripción de nuevas herramientas y tecnologías innovadoras que pueden incorporarse al servicio para que la gestión y operación sea más eficiente y eficaz, indicando cómo se realizará la mejora continua del servicio a través de estas herramientas. Se valorará el nivel de innovación de las herramientas que se proponen para la provisión del servicio, así como las nuevas que pueden implantarse asociadas a la mejora continua, valorando el impacto positivo que pueden ofrecer al servicio si se adoptan.
d. Descripción detallada del modelo de relación que se establecerá con IFEMA MADRID para el control y seguimiento del servicio prestado. Se valorará el detalle con el que se presente el modelo de relación, en base a la efectividad y eficacia del modelo de comunicación que se plantee.

1.3 Descripción de los procedimientos y metodología para la prestación del servicio

- Descripción de las metodologías que se aplicarán en el servicio. Se valorará la descripción de los procesos y procedimientos asociados al servicio en base a la claridad, sencillez y efectividad en su ejecución, así como las herramientas y planes de trabajo que se desarrollarán durante el servicio (Plan de Calidad, Plan de Gestión del Conocimiento, …) en base a la precisión y elementos de relevancia que se identifiquen para la correcta ejecución y seguimiento de dichos planes.

1.4 Descripción de responsabilidades (matriz RACI)

- Descripción detallada y clara de la asignación de roles para el servicio y proceso IT, determinando quién es el responsable de cada tarea/actividad específica asociada a cada tipo de servicio solicitado y proceso IT implicado. Se valorará la distribución coherente de dichos roles a las tareas/actividades identificadas, que aseguren fluidez y efectividad en los procesos, valorando la eliminación de pérdidas de tiempo o acciones que no generen valor y que no afecten al control efectivo.

1.5 Descripción de la planificación de la fase de transición y traspaso del servicio

- Descripción detallada de la planificación, fases de transición y traspaso del servicio (Plan de Transición). Se valorará el detalle y la identificación clara y concisa de los recursos asignados en cada momento y el nivel de detalle e idoneidad con el que se identifiquen y describan la necesidad de implicación de otros recursos internos de IFEMA MADRID o de otros terceros.

2. Descripción detallada de los puntos incluidos en el apartado "2. Alcance" del presente documento.

2.1 Descripción del Servicio de SOC 24x7x365

a. Descripción de la gestión del SOC, las fuentes y la correlación de eventos. Se valorará el nivel de detalle de las acciones y actividades relacionadas con la gestión del SOC, así como la idoneidad de las fuentes y correlación de eventos presentada.
b. Descripción detallada de la infraestructura del SOC y las herramientas para la monitorización y cómo van a gestionar la vigilancia y la gestión del servicio fuera del horario del administrador de sistemas de ciberseguridad presencial. Se valorará el nivel de eficacia y efectividad de la infraestructura del SOC y herramientas de monitorización, así como correcto ajuste del enfoque de la gestión del servicio fuera del horario con respecto a las necesidades de IFEMA MADRID.

2.2 Cibervigilancia digital

a. Descripción detallada de cómo se proveerá el servicio y soluciones integrales consideradas teniendo en cuenta los tipos de amenaza digital, hacktivismo, activismo y oportunismo criminal teniendo también en cuenta el contexto geopolítico. Se valorará en nivel de coherencia e idoneidad al entorno de IFEMA MADRID.
b. Descripción detallada de las medidas a tomar de forma proactiva y reactiva, así como la mitigación de problemas encontrados relativos a la ciberseguridad, así como del procedimiento ante crisis, valorándose el nivel de efectividad y eliminación de pérdidas de tiempo y nivel de coherencia.

2.3 Análisis de vulnerabilidades

a. Descripción detallada del proceso de análisis de vulnerabilidades, tal y como se solicita en el pliego, valorándose el nivel de eficacia y eficiencia del proceso que se presente.
b. Descripción del contenido de los informes detallados, valorándose la manera de reporte y la coherencia del formato, así como la claridad.
c. Descripción detallada de las medidas a tomar para el detección y seguimiento de problemas e incidentes, así cómo del procedimiento ante crisis, valorándose el nivel de efectividad y eliminación de pérdidas de tiempo y nivel de coherencia.

2.4 Pentesting

a. Descripción detallada de cómo se realizarán los pentesting internos o externos, así como las medidas a tomar y aspectos a cubrir en ambos casos.
b. Descripción del contenido de los informes generados y acciones a realizar.

2.5 Gestión y respuesta ante incidentes

- Descripción detallada de la metodología, procesos y procedimientos, herramientas, disponibilidad y modelo de gestión para el servicio solicitado. Se valorará en nivel de coherencia e idoneidad al entorno de IFEMA MADRID, así como en nivel de detalle de la descripción de las capacidades de reacción y remediación en caso de necesidad de aplicar este servicio.

3. Descripción de la infraestructura, medidas de seguridad y herramientas

3.1 Descripción detallada del SOC y las instalaciones del proveedor

- Descripción detallada de la organización del equipo y la gestión de las alertas, así como las herramientas a usar tanto para la gestión de las incidencias como las herramientas SIEM para la recolección de datos de los elementos objeto del servicio. Se valorará la idoneidad al entorno de IFEMA MADRID, así como la coherencia y claridad con la que se presenta la información solicitada.

3.2 Descripción de las herramientas destinadas para la prestación del servicio (SIEM, Gestión de vulnerabilidades, Pentesting, etc.)

a. Descripción detallada de todas las herramientas que se utilizarán para los diferentes aspectos del servicio. Se valorará el enfoque y acoplamiento de las herramientas para la gestión correcta del servicio.
b. Descripción de herramientas y tecnologías innovadores que puede tener el SOC, dentro de la mejora continua, que permitan tener una gestión más eficiente y eficaz de la ciberseguridad. Se valorará en nivel de innovación de las herramientas y tecnologías que se presenten, valorando la efectividad y eficacia en el entorno de IFEMA MADRID.

3.3 Descripción de las medidas de seguridad que se adaptarán para la prestación del servicio: VPN, aislamiento de la red con acceso a IFEMA MADRID del resto de la red del proveedor, procedimiento de contingencia, etc.
- Descripción de las medidas a tomar para la interconexión de los sistemas para la correcta prestación del servicio, así como las medidas de aislamiento de la red con acceso a IFEMA MADRID del resto de la red del proveedor, procedimiento de contingencia, etc. . Se valorará la idoneidad al entorno de IFEMA MADRID, así como la coherencia y claridad con la que se presenta la información solicitada.

13. Modificaciones del contrato

Los productos y servicios incluidos en este contrato son adecuados para mitigar los riesgos que resultan de las amenazas actuales. Pero las circunstancias cambian con el paso del tiempo y es de prever que cambiarán a lo largo de la ejecución de este contrato y más en todo lo relacionado en el ámbito de la ciberseguridad.

Por un lado, pueden surgir amenazas nuevas que hoy no conocemos. También las amenazas actuales, que ahora son poco probables, pueden incrementar su nivel de riesgo. Es de prever que los productos de ciberseguridad aumenten los tipos de riesgos mitigados, que incorporen tecnologías nuevas de seguridad y que los fabricantes actuales u otros nuevos comercialicen mejoras aparte de la cobertura inicial de los productos actuales que podrían ser necesarias.

Las circunstancias de IFEMA MADRID también cambian. Hay sucesos y eventos, ferias, congresos, etc. que ponen a IFEMA MADRID de forma destacada en el foco mediático y que podrán requerir de servicio de cibervigilancia adicional. También podría necesitarse asesoramiento adicional en materia de ciberseguridad. Pueden presentarse ciberataques generales y específicos dirigidos a IFEMA MADRID.

Es posible que haya cambios en las infraestructuras, como por ejemplo la nueva red de dispositivos IoT, que podrían necesitar la adquisición de soluciones de ciberseguridad específicas de fabricantes de prestigio.

También podrían aparecer servicios nuevos de TI de IFEMA MADRID de terceros proveedores que requerirán decisiones, dictámenes y diseños específicos en materia de ciberseguridad, servicios tales como ERP en cloud, Analítica de datos, Data Driven, Big Data, etc.

También se puede requerir aumentar las fuentes a monitorizar por el SIEM lo que se traduce en EPSs adicionales o cualquier otro servicio relacionado con la ciberseguridad que IFEMA MADRID considere necesario.

Los escenarios anteriores son los que requerirán la ampliación de este contrato para ampliar la cobertura de los productos actuales, para incorporar productos nuevos o para adquirir servicios de ciberseguridad que puedan ser de interés para IFEMA MADRID.

También podría ser necesaria aumentar la presencia de más técnicos con dedicación presencial en temporadas en que la actividad lo requiriese por más actividad propia de IFEMA MADRID como eventos, congresos, ferias, etc.

La realización de las actividades no incluidas en el contrato requerirá la elaboración de un presupuesto y la aprobación explícita del mismo por parte de IFEMA MADRID para llevarse a cabo y poder proceder a su facturación tras finalizarse correctamente y a satisfacción de IFEMA MADRID.

Los presupuestos excluirán las actividades que se puedan encuadrar dentro del ámbito de este contrato, que estén dentro de las competencias de la persona con dedicación presencial y que tengan cabida en su dedicación prevista.

La existencia de productos, soluciones, servicios y actividades adicionales de ciberseguridad así como sus presupuestos de ampliación de ciberseguridad correspondientes no supondrán para IFEMA MADRID compromiso alguno de realizarlos ni de llevar a cabo dichos gastos adicionales.