DIRECCIÓN DE OPERACIONES

Dirección de tecnologías de la información

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL SERVICIO INTEGRAL DE CIBERSEGURIDAD GESTIONADA DE IFEMA MADRID

Exp.: 26/033

Sol. Ped.: 2000028564

Julio 2026

ÍNDICE

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 (pública y privada) y en sede corporativa (On Premise). Este servicio debe anticipar, prevenir, detectar y reaccionar de forma adecuada y con diligencia 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 tiempos se ha observado una evolución en la sofisticación y frecuencia de los ataques informáticos a empresas, administraciones públicas y organismos, con impactos relevantes tanto económicos como reputacionales. En este contexto, resulta imprescindible contar con capacidades técnicas y con personal especializado que permitan detectar, contener y neutralizar amenazas avanzadas, así como proponer diseños seguros que se integren con herramientas y plataformas sin comprometer la información de IFEMA MADRID.

IFEMA MADRID acoge eventos de gran repercusión mediática y participación internacional, lo que puede incrementar su exposición como objetivo de ciberataques. En determinados periodos de alta actividad, la organización puede verse sometida a campañas dirigidas o a intentos de explotación oportunista por parte de actores maliciosos, por lo que resulta necesario disponer de un servicio de ciberseguridad con capacidad de adaptación a picos de riesgo.

El objeto es dotar a IFEMA MADRID de un servicio integral de ciberseguridad en "formato híbrido", orientado a la protección de los sistemas de información, los servicios TIC y los datos de IFEMA MADRID, con independencia de su ubicación o tratamiento. A estos efectos, se entenderá por "formato híbrido" la prestación coordinada de actividades y capacidades de ciberseguridad aplicables tanto a entornos en sede corporativa (on-premise) como a entornos externalizados (hosting) y servicios en la nube (SaaS, PaaS, IaaS) utilizados por IFEMA MADRID.

La prestación del servicio estará gobernada por acuerdos de nivel de servicio (ANS) y combinará:

(i) Dedicación presencial, completa y continuada, de los perfiles que se establezcan en el presente pliego para la operación y administración de las plataformas objeto del contrato en la sede corporativa de IFEMA MADRID;
(ii) Dedicación remota, continua o bajo demanda, de perfiles especializados del adjudicatario para cubrir capacidades avanzadas (por ejemplo, SOC 24x7, análisis avanzado, respuesta, etc.).
(iii) También incluirá el soporte y renovación de las licencias de productos de ciberseguridad de IFEMA MADRID con sus respectivos fabricantes.

2. 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 Exp 26_033 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 "Situación Actual Exp 26_033 CONFIDENCIAL"**", deberán facilitar el modelo de compromiso de confidencialidad que se adjunta en el Anexo X "*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; sramirez@ifema.es para hacerles entrega de la documentación**.

a. Partner nivel mínimo Proffesional y CCSP de Checkpoint.

b. Partner Select Integrator o Superior de Cisco.

c. Partner Select o Superior de Fortinet.

d. Ser miembro de la red nacional de SOCs.(Declaración jurada firmada con persona con capacidad).

e. Estar incluidos todas las plataformas y productos tecnológicos que den soporte al servicio en el catálogo CPSTIC del CCN. (Declaración jurada firmada con persona con capacidad).

3. Alcance

Este lote 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.

El adjudicatario deberá implantar un modelo de gestión del servicio que asegure el control, seguimiento y evaluación de la prestación en todas sus fases, mediante interlocución con los

responsables designados por IFEMA MADRID. Dicho modelo incluirá, como mínimo: gestión de incidencias, peticiones y proyectos; priorización en base a criticidad/riesgo; seguimiento hasta cierre; control de calidad; y reporte periódico.

Dentro del alcance del servicio, enumeramos los puntos clave que IFEMA MADRID estima y necesita para cubrir la ciberseguridad de la institución. No obstante, en el anexo de "Situación Actual Exp 26_033 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 acordados y en la adecuada asignación y gestión de los recursos dedicados al contrato. La gestión de incidencias, peticiones y proyectos se realizará mediante la herramienta de ticketing/ITSM de IFEMA MADRID, asegurando su registro, priorización (por criticidad/riesgo), seguimiento y cierre. La empresa adjudicataria presentará mensualmente un informe de actividad del servicio que incluirá, como mínimo, el estado de los ANS, principales riesgos/incidencias, acciones realizadas y plan de trabajo del mes siguiente, conforme a lo indicado en el apartado "5. Modelo de Gobierno y Relación".

El servicio debe contar como mínimo con las siguientes características:

3.1. Servicio de prevención

El objetivo fundamental de los servicios de prevención requeridos será obtener un diagnóstico global del estado de la seguridad de los sistemas TIC responsabilidad de IFEMA MADRID que permita una detección temprana de las vulnerabilidades y una actuación proactiva en el despliegue de medidas de seguridad preventivas.

Dentro del servicio de Prevención, estarán incluidas las siguientes tareas:

3.1.1. Servicio de Vigilancia Digital y gestión de alertas

Este servicio facilitará una visión externa de las diferentes amenazas de seguridad que puedan afectar a la organización fuera de su perímetro, permitiendo el desarrollo de una defensa proactiva de ciberseguridad, una mejor gestión de los riesgos, la orquestación y automatización de acciones en base a una priorización de amenazas, y un mejor conocimiento de los atacantes y de sus tácticas y técnicas de ataque.

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.

Al inicio de la ejecución del contrato, IFEMA MADRID definirá en colaboración con el adjudicatario, la relación completa de activos a vigilar. Esta relación podrá ser modificada a instancias de IFEMA MADRID en cualquier momento de vigencia del contrato.

Las actividades a desarrollar entre otras, serán las siguientes:

- Alerta temprana de amenazas de seguridad, que puedan afectar a la seguridad de los servicios, sistemas e infraestructuras TIC gestionadas por IFEMA MADRID.
- Información de vulnerabilidades de seguridad, en base a los CPE (Common Platform Enumeration) de los activos corporativos.

- Monitorización de la superficie de exposición de IFEMA MADRID para la identificación de los recursos activos, cambios en resoluciones IP-dominio, creación de nuevos subdominios, apertura de puertos/servicios en IP's monitorizadas, etc.
- Monitorización de fuentes diversas de información para la detección temprana de, entre otros:
    - Suplantaciones de identidad.
    - Actividades relacionadas con el fraude.
    - Campañas de malware.
    - Exposición de credenciales.
    - Venta de accesos/credenciales en mercados de la DeepWeb.
    - Hacktivismo y ataques organizados.
    - Abuso de marca.
    - Dominios ilegítimos de reciente creación.
- Recopilación y análisis de indicadores de compromiso (IOC's).
- 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.

El servicio realizará una gestión completa del ciclo de vida de las amenazas detectadas, contemplando desde la identificación, recopilación y almacenamiento de los datos obtenidos, su procesamiento inteligente, clasificación y evaluación, la generación de alertas en base a peligrosidad de la amenaza y probabilidad de materialización, elaboración de informes, registro en los sistemas de seguimiento de IFEMA MADRID y propuestas para mitigación y/o eliminación de la amenaza.

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 **5 eventos anuales** durante la vigencia del contrato a determinar en tiempo y forma y que se ejecutarán bajo demanda.

El adjudicatario deberá incluir en su oferta económica el **precio unitario** aplicable a la realización de ejercicios de ciber vigilancia, con el fin de permitir a IFEMA MADRID solicitar, cuando sea necesario, ejercicios adicionales.

En caso de que por circunstancias IFEMA MADRID necesite ampliar el servicio de ciber vigilancia por encima de los 5 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 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 ciber vigilancia, con carácter general, deberá comenzar a realizarse unos tres días aproximadamente antes del inicio del evento. La emisión de informes diarios 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 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 ciber vigilancia 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 ciber vigilancia 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.

El alcance inicial de este servicio incluye:

- 10 dominios.
- 50 IP’s públicas.
- 20 emails VIP
- 5 marcas
- 5 eventos anuales
- 100 CPE´s

3.1.2. Análisis de vulnerabilidades (sistemas y redes)

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 de tecnologías de la información (TI) de 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.

Este servicio tendrá como objetivo identificar las vulnerabilidades existentes en los activos que dan soporte a los servicios y sistemas de información de IFEMA MADRID, con el objetivo de adoptar medidas orientadas a disminuir los riesgos de explotación de una vulnerabilidad, el número de incidentes de seguridad asociados y su posible afectación.

El servicio gestionará de forma completa el ciclo de vida de las vulnerabilidades de Seguridad de todos los activos, ya estén desplegados en infraestructura on-premise o en infraestructura en nube (pública o privada), facilitando una priorización de cada vulnerabilidad e información suficiente que permita conocer el grado real de riesgo asociado al contexto de IFEMA MADRID, así como planificar las acciones para minimizar dicho riesgo.

Las principales actividades a desarrollar en este servicio serán las siguientes:

- Descubrimiento de activos, ya sea on-premise o en nube, detallando nombre, IP, sistema operativo, puertos abiertos, aplicaciones en ejecución, etc.
- Generación de una **base de datos de los activos encontrados,** clasificados por criticidad para el negocio y nivel de seguridad. Esta base de datos será la fuente de información posterior para el reporte de la postura de seguridad y priorización de las actividades de mitigación.
- Identificación y análisis de la superficie de exposición de IFEMA MADRID y construcción de la estrategia de protección correspondiente. Análisis de las distintas redes/activos descubiertos para búsqueda de vulnerabilidades, en las franjas y horarios aprobados por IFEMA MADRID.
- Auditorías técnicas específicas de sistemas críticos (correo, directorio activo, etc.).
- Clasificación de las vulnerabilidades por CVE (Common Vulnerabilities and Exposures). Registro de cada vulnerabilidad encontrada, criticidad y recomendaciones de mitigación.
- Priorización del tratamiento de cada vulnerabilidad en base a factores como criticidad del activo para el negocio, nivel de exposición, facilidad de explotación, interés del atacante, facilidad de descubrimiento de la vulnerabilidad o contexto del negocio. Evaluación del impacto de nuevas vulnerabilidades, ya sean notificadas por el servicio de vigilancia digital o por terceros, en los activos de IFEMA MADRID, determinando a qué activos afecta, en qué grado, qué medidas de remediación hay que aplicar, etc.
- Notificación y gestión del ciclo de vida de las vulnerabilidades identificadas a las áreas internas de IFEMA MADRID responsables de su tratamiento.

Este servicio se prestará en base a las solicitudes de análisis de infraestructuras o sitios web que solicite IFEMA MADRID planificadas trimestralmente de manera ordinaria y pudiendo solicitar puntualmente ejercicios acotados sobre infraestructuras específicas.

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, que se ejecutarán en las ventanas y horarios previamente aprobados por IFEMA MADRID.

El adjudicatario deberá entregar un informe a la finalización de cada ejercicio, indicando al menos: activos y alcance analizado, metodología y herramientas utilizadas, vulnerabilidades encontradas (con su CVE/CVSS cuando aplique), evidencias, priorización y nivel de riesgo contextualizado para IFEMA MADRID (considerando exposición, criticidad del activo y explotabilidad), y una propuesta de plan de remediación. El servicio no se limitará a la entrega de un informe estándar, sino que deberá incluir conclusiones y recomendaciones adaptadas al contexto real de IFEMA MADRID. Se realizará seguimiento trimestral del estado de mitigación, registrando las acciones y acuerdos en la herramienta de ticketing. 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.

3.1.3. Análisis pentesting o Análisis de vulnerabilidades de seguridad de aplicaciones

Con el objetivo de evaluar la eficacia de las medidas de seguridad implantadas y conocer el alcance de posibles vulnerabilidades, IFEMA MADRID podrá solicitar la realización de pruebas de penetración (pentesting) sobre los sistemas y servicios de la organización durante la vigencia del contrato. Estas

pruebas podrán efectuarse, a criterio de IFEMA MADRID, sobre entornos *on-premise* y/o sobre servicios en la nube (cloud).

Este servicio tendrá por objeto la realización de auditorías de seguridad sobre las aplicaciones y sistemas de información gestionados por IFEMA MADRID en el entorno de producción, ya sean desarrollos propios o productos comerciales, mediante la ejecución de pruebas de penetración por parte de personal técnico experto.

Las auditorías de seguridad se realizarán indistintamente en modalidad de caja negra, gris o blanca, en los horarios acordados con IFEMA MADRID.

Podrán solicitarse auditorías específicas de sistemas concretos como por ejemplo servicios de directorio activo.

Con carácter general, las actividades de análisis no comprometerán la integridad de los datos objeto de revisión, ni la disponibilidad de los servicios analizados, si bien IFEMA MADRID se reserva la posibilidad de solicitar pruebas específicas de denegación de servicio para sistemas concretos, con el objetivo de valorar adecuadamente las protecciones anti DDoS instaladas.

El alcance inicial de este servicio contempla 5 ejercicios anuales, sin perjuicio de que IFEMA MADRID podrá solicitar adicionalmente análisis de vulnerabilidades para aplicaciones específicas en base a las necesidades de Negocio, operativas, etc.

Las pruebas de penetración (pentesting) podrán ser internas y/o externas. La Dirección de Tecnologías de la Información de IFEMA MADRID determinará, para cada solicitud, el tipo de prueba y la fecha de ejecución, comunicándolo al adjudicatario con la antelación suficiente para la correcta planificación y preparación de los trabajos.

En el momento de activar cada solicitud, IFEMA MADRID indicará al adjudicatario la modalidad de ejecución (caja negra, caja blanca o caja gris), así como el alcance y las condiciones de la prueba. IFEMA MADRID podrá considerar la recomendación técnica del adjudicatario respecto de la modalidad más adecuada en función de los objetivos del ejercicio.

El adjudicatario deberá incluir en su oferta económica el **precio unitario** aplicable a la realización de ejercicios de pentesting, con el fin de permitir a IFEMA MADRID solicitar, cuando sea necesario, ejercicios adicionales.

A efectos de dimensionamiento, se estima un consumo de **5 ejercicios anuales**.

3.1.4. Concienciación en Ciberseguridad

El adjudicatario elaborará y entregará una **píldora formativa mensual** (formato PDF) lista para su publicación directa en la intranet corporativa de IFEMA MADRID. Cada píldora deberá ser breve, clara y orientada a la acción, e incluir, como mínimo: objetivo del mes, explicación del riesgo, buenas prácticas, ejemplos (p. ej., correos fraudulentos), "qué hacer si ocurre", y un apartado de recordatorio de canales de notificación internos.

Asimismo, el adjudicatario deberá poner a disposición de IFEMA MADRID una **plataforma de concienciación en ciberseguridad** validada por el CCN e incluida en el catálogo CPSTIC, en modalidad *SaaS* o equivalente, que permita la gestión centralizada de campañas y contenidos. La plataforma deberá incorporar, como mínimo:

(i) **Plan anual** de formación y concienciación para todo el personal interno
(ii) Itinerarios por perfiles (p. ej., usuarios generales, perfiles técnicos y mandos)
(iii) Contenidos actualizables y alineados con amenazas habituales (phishing, ransomware, uso de contraseñas, MFA, navegación segura, tratamiento de información, trabajo remoto, etc.)
(iv) EValuaciones y refuerzo (tests, recordatorios, microcontenidos)
(v) **Cuadros de mando** con métricas (participación, finalización, resultados, evolución y comparativas por áreas), exportables para su seguimiento por IFEMA MADRID

Actualmente, IFEMA MADRID dispone de una plataforma de concienciación en ciberseguridad con vigencia hasta **abril de 2027,** descrita en el apartado "2. Situación actual". El adjudicatario podrá (i) dar continuidad a dicha plataforma a partir de esa fecha, o (ii) proponer una solución alternativa de características equivalentes o superiores, garantizando en todo caso la continuidad del servicio y la **migración** de campañas, usuarios, históricos y métricas, así como la configuración de plantillas, grupos y parámetros de reporting.

La adquisición de licencias, la implantación, la parametrización, la administración y el soporte anual de la plataforma durante toda la vigencia del contrato correrán a cargo del adjudicatario. El servicio incluirá, como mínimo: alta y mantenimiento de usuarios/grupos, asistencia funcional, resolución de incidencias, actualización de contenidos, y soporte a la explotación de métricas. La plataforma y el servicio deberán cumplir los requisitos de seguridad y privacidad aplicables (incluida la protección de datos personales), y permitir el control de accesos y la trazabilidad de actividad.

Como entregables, el adjudicatario presentará para aprobación de IFEMA MADRID:

(i) **Plan anual** de concienciación y formación (calendario, temáticas, públicos objetivo y objetivos de aprendizaje);
(ii) Calendario y contenidos de las **píldoras mensuales**; y
(iii) **Informe trimestral** de seguimiento con resultados, conclusiones y propuestas de mejora (incluyendo acciones correctoras ante baja participación o resultados insuficientes). IFEMA MADRID podrá solicitar campañas específicas adicionales en periodos de mayor exposición o ante la aparición de amenazas relevantes.

3.2. Servicio de Detección y monitorización

La monitorización de eventos de seguridad tendrá como objetivo fundamental la recolección de los eventos de seguridad de los diferentes componentes tecnológicos que sustentan las aplicaciones y sistemas de información, para que, analizados de forma conjunta, correlados y enriquecidos con el contexto tecnológico y la información de amenazas disponible, puedan convertirse en alertas de seguridad. La confirmación tras su análisis de estas alertas de seguridad podrá derivar en la apertura de un incidente de ciberseguridad a gestionar.

3.2.1. SOC as a Service 24x7 Monitorización de eventos de seguridad

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.

Aunque IFEMA MADRID dispone de medidas de seguridad y mecanismos de protección implantados, la complejidad del entorno tecnológico, la evolución de las amenazas y el crecimiento de la actividad de la organización hacen necesario contar con el apoyo continuado de especialistas en seguridad y ciberseguridad. Este apoyo deberá permitir establecer y consolidar un modelo de gestión de la seguridad de la información y de los sistemas de IFEMA MADRID, asegurando la capacidad de anticipación, coordinación y respuesta con la máxima inmediatez y en cualquier momento ante amenazas o incidentes.

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.

En el marco de las funciones de vigilancia y asesoramiento continuo, el adjudicatario mantendrá informada a IFEMA MADRID, de forma proactiva, sobre amenazas y eventos/incidentes relevantes de TI que puedan afectarle, con el fin de facilitar su valoración y gestión conjunta. Estas comunicaciones deberán orientarse a la identificación y prevención de amenazas, la mitigación de riesgos, la propuesta de medidas de contención/remediación y la mejora continua de la postura de ciberseguridad. A título enunciativo, podrán incluirse avisos relativos a nuevas ciberamenazas, campañas de ciberfraude, familias de ransomware con alta propagación, campañas masivas de suplantación (p. ej., entidades bancarias) y boletines de indicadores de compromiso (IoC), acompañados de la recomendación de actuación correspondiente.

La comunicación de dichas alertas se realizará tan pronto como sean detectadas, mediante los canales que IFEMA MADRID establezca, incluyendo, cuando proceda: avisos puntuales o boletines informativos por correo electrónico; y apertura, clasificación, seguimiento y cierre de tickets en el Service Desk / herramienta corporativa de ticketing/ITSM de IFEMA MADRID, garantizando la trazabilidad de las actuaciones y recomendaciones. En todo caso, el adjudicatario actuará de acuerdo con los procesos, procedimientos y ventanas de actuación definidos por IFEMA MADRID.

Actualmente IFEMA MADRID dispone de un servicio de SOC 24x7x365 con el proveedor actual monitorizando fuentes (descritas en "Situación Actual Exp 26_033 CONFIDENCIAL") con una herramienta SIEM, que se necesitan seguir monitorizando:

- Firewalls Check Point/Fortinet (objeto del contrato).
- Directorio Activo (fuente a monitorizar; la administración/cambios no forman parte del objeto del contrato salvo que se indique expresamente en otro apartado).
- Proxy inverso (fuente a monitorizar).
- Sistema de filtrado de correo Cisco CES (en la nube) (objeto del contrato en lo relativo a su operación/gestión según los apartados aplicables).
- Endpoint/EDR (consola en nube) (fuente a monitorizar y, cuando aplique, administrar según el alcance del apartado **"**3.6. Servicio de Administración de infraestructura de seguridad y plataformas de ciberseguridad").
- Salesforce
- M365

En el anexo "Situación Actual Exp 26_033 CONFIDENCIAL" se indican volumetrías 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 integral 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.

En el anexo "Situación Actual Exp 26_033 CONFIDENCIAL" se incluyen las volumetrías y el dimensionamiento actual del servicio. A efectos de esta licitación, el adjudicatario deberá dimensionar el servicio de SIEM y la capacidad de ingesta/correlación para cubrir, como mínimo, el volumen actualmente monitorizado y permitir ampliaciones durante la vigencia del contrato. Cualquier cifra concreta de EPS que se establezca en el contrato (base y ampliaciones) deberá quedar alineada con el anexo citado; en caso de discrepancia, prevalecerá lo indicado en dicho anexo y/o lo que se acuerde en fase de transición, dejando trazabilidad documental del ajuste.

Las fuentes a monitorizar podrán estar ubicadas en función de su necesidad y de la implementación de los nuevos servicios, en clouds (públicas o privadas) 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 a monitorizar por el SOC y/o incrementos de volumetría que permita a IFEMA MADRID, si fuera necesario, tramitar una modificación contractual. La necesidad concreta de ampliación (métrica aplicable, volumen base y unidades de incremento) se definirá con referencia a las volumetrías del anexo "Situación Actual Exp 26_033 CONFIDENCIAL" y quedará documentada durante la fase de transición para evitar discrepancias.

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.

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 incluidos en el documento "Situación Actual Exp 26_033 CONFIDENCIAL", 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 registrado en la herramienta de ticketing que IFEMA MADRID dispone para el servicio.

El servicio de SOC, debe formar parte de la empresa adjudicataria de ámbito nacional. Así mismo deberá formar parte de la red nacional de SOC's Esto también implica la posibilidad de poder integrarse con las herramientas de notificación de incidentes del CCN (Lucía, Reyes, etc).

3.2.2. Servicio de búsqueda proactiva de amenazas - Threat hunting

El servicio de búsqueda proactiva de amenazas (Threat Hunting) tiene por objetivo anticiparse a los incidentes de seguridad mediante la identificación, análisis y validación de actividad potencialmente maliciosa que haya podido pasar inadvertida a los controles preventivos y a la monitorización ordinaria del SOC. El servicio se basará en una búsqueda iterativa y trazable de amenazas persistentes u ocultas, tanto activas como latentes, en las infraestructuras, servicios y sistemas TIC de IFEMA MADRID (on-premise y cloud).

Esta capacidad contribuirá a reducir el tiempo de permanencia del atacante (*dwell time*) y los tiempos medios de detección y respuesta, así como a disminuir la superficie de exposición frente a amenazas internas y externas. Los hallazgos del Threat Hunting deberán traducirse en mejoras operativas medibles (por ejemplo, nuevos casos de uso y reglas de detección en el SIEM/EDR, ajustes de telemetría, endurecimiento de configuraciones y recomendaciones de remediación), evitando que el servicio se limite a análisis puntuales sin retorno a la operación.

El servicio de Threat Hunting se prestará conforme a un **modelo continuo e iterativo**, ejecutando hunts de menor duración de forma recurrente (por ejemplo, con periodicidad **mensual o quincenal**) sobre telemetría actual e histórica, y garantizando capacidad de **activación bajo demanda** ante, entre otros: campañas activas, explotación masiva de vulnerabilidades, alertas críticas del SOC, aparición de nuevos TTP relevantes o cambios significativos en el entorno. El adjudicatario deberá asegurar que los resultados del hunting se integran en la operación del SOC, transformándose en mejoras verificables (casos de uso, reglas de detección, ajustes de telemetría, playbooks y automatizaciones) y quedando registradas y trazables mediante tickets.

Como parte del servicio, el adjudicatario realizará sesiones periódicas de *purple teaming* (o actividades equivalentes de validación) para comprobar que las hipótesis, técnicas y comportamientos identificados se convierten en detecciones eficaces y accionables en las herramientas de IFEMA MADRID (SIEM/EDR/XDR y fuentes asociadas). El servicio incluirá, como mínimo, un **reporte mensual consolidado** con: hipótesis ejecutadas, técnicas MITRE evaluadas, evidencias, activos potencialmente afectados, conclusiones, recomendaciones priorizadas y detalle de las mejoras incorporadas al SOC (incluyendo fecha, responsable y ticket asociado), así como un resumen ejecutivo orientado a riesgos y tendencias.

Entregables y métricas del servicio

Como mínimo, el adjudicatario deberá proporcionar los siguientes entregables, dejando trazabilidad en la herramienta de ticketing/ITSM de IFEMA MADRID:

- Registro y trazabilidad de los hunts (planificados o bajo demanda) mediante ticket, incluyendo hipótesis/alcance, periodo analizado y evidencias principales.

- Reporte mensual consolidado (técnico y ejecutivo) con resultados, tendencias, riesgos relevantes y recomendaciones priorizadas.
- Relación de mejoras incorporadas al SOC derivadas del hunting (p. ej., reglas/casos de uso/playbooks), con su referencia de ticket y estado.

El adjudicatario reportará mensualmente un conjunto de métricas para evidenciar la actividad y el valor aportado por el servicio:

- **Actividad**: número de hunts/hipótesis ejecutadas (planificadas y bajo demanda).
- **Hallazgos relevantes**: número de hallazgos confirmados y su criticidad (alta/media/baja).
- **Mejora operativa**: número de mejoras implantadas en el SOC derivadas del hunting (reglas/casos de uso/playbooks).
- **Tiempo de comunicación**: tiempo medio desde la identificación de un hallazgo crítico hasta su notificación a IFEMA MADRID.

3.3. Servicio de Respuesta

Los servicios de análisis y respuesta ante incidentes de seguridad constituyen el primer punto de notificación y coordinación para los incidentes relacionados con las infraestructuras y servicios bajo responsabilidad de IFEMA MADRID. Este servicio recibirá notificaciones provenientes de los equipos de IFEMA MADRID, del SOC (apartado 3.2.1), del servicio de búsqueda proactiva de amenazas (apartado 3.2.2) y de cualquier otro canal acordado, con el fin de analizar, confirmar y gestionar el incidente hasta su contención, mitigación y erradicación.

Será responsabilidad de este servicio coordinar los incidentes de ciberseguridad que: requieran la actuación de varios equipos (internos o proveedores) de IFEMA MADRID, y/o cuya peligrosidad/criticidad estimada sea **ALTA, MUY ALTA o CRÍTICA**. Cuando proceda, este servicio coordinará asimismo la comunicación y colaboración con el CERT de referencia (CCN-CERT, CNPIC) o con otros organismos/terceros autorizados, de acuerdo con los procedimientos de IFEMA MADRID y la normativa aplicable.

El servicio recibirá y consolidará la información de amenazas, alertas e incidentes identificados por los distintos servicios del SOC de IFEMA MADRID, con objeto de asegurar una visión unificada, evitar duplicidades y garantizar la correcta trazabilidad del tratamiento del incidente.

Con carácter general, el servicio realizará un análisis profundo de las notificaciones recibidas para: confirmar o descartar el incidente; determinar su alcance, activos afectados e impacto potencial; definir y coordinar las acciones de contención, mitigación y erradicación; y proponer medidas preventivas y de mejora para reducir recurrencias.

Para cumplir lo anterior, el adjudicatario deberá realizar, como mínimo, las siguientes actividades:

- Recepcionar y analizar las alertas y/o incidentes escalados por el SOC y por otros canales acordados, aplicando los procedimientos y playbooks vigentes.
- Atender los canales de notificación establecidos (al menos: correo electrónico, teléfono, herramienta corporativa de ticketing/ITSM, y canales de notificación del CCN-CERT tales como LUCIA u otros que apliquen), garantizando trazabilidad.
- Registrar, gestionar y coordinar el ciclo de vida de los incidentes en la herramienta de ticketing/ITSM y, cuando proceda, en las plataformas externas de notificación/seguimiento que resulten aplicables.

- Coordinar la respuesta con los equipos de IFEMA MADRID y, en su caso, con terceros/proveedores implicados (por ejemplo, para contención, cambios, bloqueos, recuperación, etc.).
- Determinar, proponer y coordinar estrategias de contención, mitigación y erradicación.
- En los casos que proceda, activar el procedimiento corporativo de gestión de incidentes críticos (gestión de crisis) y apoyar la coordinación de comunicaciones internas/externas según lo indicado por IFEMA MADRID.
- Elaborar un informe de cierre por cada incidente relevante, incluyendo cronología, alcance, evidencias clave, impacto, acciones realizadas, estado final, recomendaciones y un apartado de lecciones aprendidas.
- Proponer mejoras continuas sobre procesos, casos de uso, automatizaciones y capacidades de respuesta, derivadas de la experiencia operativa (lecciones aprendidas).

3.3.1. Gestión de respuesta ante incidentes (DFIR)

Este servicio proporcionará capacidades avanzadas de **respuesta ante incidentes y análisis forense digital** (DFIR), activables a demanda, para la gestión de incidentes de ciberseguridad de elevada criticidad y situaciones de cibercrisis. Su objetivo es apoyar la toma de decisiones, acelerar la contención y recuperación, y reducir el impacto sobre las operaciones y los activos de IFEMA MADRID, en coordinación con los equipos internos y el SOC.

Tras su activación, el adjudicatario atenderá el servicio de forma prioritaria, asignando los recursos especializados necesarios y manteniendo la dedicación requerida hasta la **estabilización** del incidente y, cuando así se determine, hasta su **cierre**, de acuerdo con la dirección y prioridades establecidas por IFEMA MADRID.

Dentro del alcance del contrato se incluye una **bolsa de 100 horas** de servicio DFIR, **activable en cualquier momento (24x7x365)**. La activación, el seguimiento y el consumo de la bolsa se registrarán en la herramienta de ticketing/ITSM de IFEMA MADRID, indicando al menos: fecha/hora de activación, motivo, severidad/criticidad, recursos asignados, horas imputadas y estado de la intervención.

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.

Cuando intervengan otros equipos o proveedores (internos o externos), el adjudicatario actuará como **coordinador técnico** para la gestión de tareas, intercambio de evidencias y alineamiento de acciones, asegurando una comunicación ordenada y trazable conforme a los procedimientos de IFEMA MADRID.

El servicio incluirá la **recolección, preservación y análisis** de la información necesaria para determinar el origen, la evolución y el alcance del incidente (por ejemplo, logs, artefactos y evidencias digitales) en los sistemas, aplicaciones e infraestructuras implicadas, tanto en entornos *on-premise* como *cloud*. Cuando aplique, se seguirán las buenas prácticas de preservación de evidencias y **cadena de custodia**, de acuerdo con los procedimientos establecidos por IFEMA MADRID.

A título orientativo y sin perjuicio de las necesidades específicas de cada caso, el adjudicatario deberá estar en disposición de prestar actividades DFIR tales como: **triaje avanzado** y validación del incidente; **scoping** (determinación de alcance y sistemas afectados); definición de estrategia de

contención (corto plazo) y **erradicación** (medio plazo); apoyo a **recuperación** y vuelta a operación; y apoyo a la **investigación técnica** (incluida la identificación de TTP y la extracción de IoC/IoA reutilizables para su aplicación en el SOC).

Las tareas mínimas que podrán solicitarse al amparo de este servicio incluyen, al menos, las siguientes:

- Análisis técnico inicial y avanzado para confirmar el incidente, determinar alcance, activos afectados e impacto potencial, e identificar vectores/cadena de ataque cuando sea posible.
- Definición y coordinación de medidas de contención, mitigación y erradicación, incluyendo recomendaciones de hardening y reducción de recurrencia.
- Apoyo a la recuperación del servicio (restauración segura, verificación post-recuperación y criterios de vuelta a operación), coordinando acciones con los equipos de IFEMA MADRID y/o terceros implicados.
- Apoyo a la coordinación operativa durante la crisis (interlocutores, canales, cadencia de actualización y compartición de evidencias), conforme a los procedimientos de IFEMA MADRID.
- Apoyo técnico a las necesidades de comunicación relacionadas con el incidente (interna/externa y, cuando aplique, con CERT/terceros autorizados), bajo directrices de IFEMA MADRID.
- Elaboración de un informe de cierre del incidente y plan de acciones correctivas/preventivas (lecciones aprendidas), incluyendo cronología, evidencias relevantes, alcance, impacto, decisiones adoptadas, IoC/IoA reutilizables y recomendaciones priorizadas.

El servicio se prestará con personal especializado del adjudicatario y podrá requerir intervención remota y/o desplazamiento presencial, en función de la naturaleza del incidente y de las necesidades operativas de IFEMA MADRID.

En caso de que, por necesidades justificadas, IFEMA MADRID requiera una dedicación extra a la indicada, dichas horas adicionales se tramitarán mediante la modificación contractual que corresponda. A tal efecto, el adjudicatario incluirá en su oferta el **precio unitario por hora adicional**.

3.4. Consultoría experta en ciberseguridad

IFEMA MADRID está inmersa en un proceso de transformación digital que abarca diversos escenarios y proyectos (integraciones, despliegue de soluciones y adopción de nuevas herramientas), tanto en entornos *cloud* como *on-premise*. En este contexto, resulta necesario disponer de un servicio de asesoría experta que acompañe la toma de decisiones y asegure la incorporación de criterios de seguridad desde las fases iniciales de diseño.

Dentro del objeto del contrato, se requiere un servicio de **Consultoría Experta en Ciberseguridad** orientado a: asesorar iniciativas y proyectos; emitir **dictámenes** e **informes** de seguridad; elaborar, revisar o validar **diseños y arquitecturas** de ciberseguridad; y participar en reuniones de coordinación con otras áreas de IFEMA MADRID y con terceros para apoyar la definición de requisitos y la toma de decisiones. Los trabajos se materializarán, cuando proceda, en entregables documentados (informes, notas técnicas, recomendaciones y/o requisitos de seguridad). Este servicio no incluye la operación y administración diaria de las plataformas de ciberseguridad, que se regirá por el alcance definido en el apartado "3.6. Servicio de Administración de infraestructura de seguridad y plataformas de ciberseguridad".

La prestación del servicio se realizará con una dedicación estimada de **dos (2) jornadas por semana**, equivalentes a **104 jornadas anuales (832 horas)**:) **una (1) jornada presencial** en la sede corporativa de IFEMA MADRID; y **una (1) jornada en remoto** destinada a la preparación de reuniones y a la elaboración de entregables, análisis y dictámenes.

El adjudicatario indicará en su oferta el **precio unitario por jornada** de este servicio.

En caso de que, por necesidades justificadas, IFEMA MADRID requiera una dedicación superior a la indicada, dichas jornadas adicionales se tramitarán mediante la modificación contractual que corresponda. A tal efecto, el adjudicatario incluirá en su oferta el **precio unitario por jornada adicional**.

El adjudicatario designará un **titular** del servicio de Consultoría Experta en Ciberseguridad, que actuará como referente, interlocutor técnico y responsable de la continuidad del servicio. Cuando se requiera conocimiento altamente especializado para un asunto concreto, el adjudicatario podrá incorporar puntualmente otros perfiles expertos, manteniendo en todo caso la coordinación del titular y la calidad de los entregables.

A título enunciativo, y sin carácter limitativo, el servicio podrá incluir las siguientes actuaciones:

- Asistencia a reuniones para la toma de decisiones, aportando criterios de seguridad aplicables a los sistemas, datos y tratamientos de IFEMA MADRID.
- Evaluación y emisión de informes/dictámenes sobre productos, servicios o soluciones (incluidos productos novedosos) con impacto en la seguridad de la información.
- Revisión y validación de arquitecturas, diseños e integraciones complejas en entornos on-premise, cloud, hosting y/o servicios SaaS/PaaS/IaaS.
- Definición de requisitos y directrices de seguridad para su incorporación en contratos y pliegos de IFEMA MADRID con terceros.
- Análisis de riesgos de iniciativas de negocio/tecnología, y propuesta de medidas de mitigación priorizadas.
- Asesoramiento para la conformidad con normativas y marcos de referencia aplicables en materia de seguridad.
- Acompañamiento en la implantación de prácticas y herramientas de seguridad (por ejemplo, análisis de código seguro), cuando proceda.
- Definición de estrategias y recomendaciones para la prevención de incidentes y la mejora de la capacidad de respuesta y recuperación.
- Otras necesidades relacionadas con el objeto del servicio que IFEMA MADRID requiera durante la vigencia del contrato.

3.5. Certificaciones, riesgos y cumplimiento normativo

El presente servicio tiene por objeto el establecer el marco de **gobierno, riesgos y cumplimiento** del servicio integral de ciberseguridad objeto de este contrato, así como supervisar su correcta ejecución.

Se actuará con **capacidad independiente de supervisión y aseguramiento**, orientada a garantizar el alineamiento de los servicios con la normativa aplicable, los estándares internacionales de seguridad y las buenas prácticas del sector (por ejemplo, ENS, ISO/IEC 27001, ISO/IEC 27035, ISO 22301 y NIST). Esta capacidad deberá proporcionar a IFEMA MADRID una visión objetiva del desempeño, los riesgos y el grado de cumplimiento, así como recomendaciones priorizadas de mejora.

Se requerirá los siguientes servicios:

- **Adecuación a ENS/ISO 27001 y normativas futuras**: asegurar, con la dedicación necesaria, que IFEMA MADRID mantiene durante toda la vigencia del contrato los controles, documentación, procedimientos y evidencias requeridos para conservar las certificaciones **ENS** e **ISO/IEC 27001** (ya vigentes) y para atender nuevas obligaciones normativas y/o certificaciones que resulten aplicables (p. ej., **NIS2**). Se prestará apoyo en auditorías internas previas y en auditorías oficiales/externas (seguimiento/recertificación), incluyendo preparación de evidencias, soporte a entrevistas, gestión de hallazgos/no conformidades y seguimiento de planes de acción hasta cierre.
- **Gestión de riesgos y no conformidades**: identificación, registro, priorización y seguimiento de riesgos, desviaciones y no conformidades, definiendo planes de acción correctores/preventivos (responsables, plazos y estado) y verificando su cierre.
- **Reporting y soporte a comités**: elaboración de informes y cuadros de mando para audiencia ejecutiva y técnica, y apoyo a comités de seguimiento, auditorías y revisiones regulatorias, aportando trazabilidad y evidencias. Como mínimo, se emitirá un **informe trimestral ejecutivo de estado de la seguridad**, con evolución de riesgos, postura de seguridad, tendencias, principales hitos/incidentes relevantes, estado de planes de acción y decisiones requeridas.
- **Mejora continua**: definición, priorización y seguimiento de un roadmap de mejora del servicio (personas, procesos, tecnología y control), incluyendo recomendaciones de evolución de capacidades, automatización y control.

3.6. Servicio de Administración de infraestructura de seguridad y plataformas de ciberseguridad

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. La prestación del servicio será, con carácter general, presencial, pudiendo contemplarse el trabajo en remoto de forma **excepcional** y previa autorización de IFEMA MADRID, sin menoscabo de la disponibilidad, dedicación y cumplimiento de los acuerdos de nivel de servicio (ANS) aplicables. A fin de garantizar la cobertura de la presencialidad, el servicio podrá prestarse por **uno o dos administradores** que se alternen, debiendo tratarse en todo caso de perfiles estables y previamente validados por IFEMA MADRID.

Los administradores asignados deberán acreditar **certificaciones oficiales** de los productos objeto del contrato, siendo **obligatoria** la certificación de **Check Point**. Asimismo, deberán contar con un mínimo de **5 años** de experiencia en puestos similares, adquirida en los últimos 5 años.

Soluciones o plataformas a administrar (mínimo):

- Firewalls y seguridad perimetral.
- Seguridad de correo electrónico.
- Protección de endpoint (EDR).
- Servicios y herramientas de seguridad en Microsoft 365 y Azure.

Las vacaciones, permisos y bajas deberán estar cubiertos de forma que se mantenga, en todo momento, la presencia necesaria en la sede corporativa de IFEMA MADRID y no se vea afectado el avance y estado de las tareas encomendadas. Los perfiles de sustitución deberán contar con el conocimiento, certificaciones y contextualización requeridos para el servicio.

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.

El horario habitual de prestación presencial será de lunes a jueves de **09:00 a 18:30** (con una hora de comida) y los viernes de **09:00 a 15:00**. En caso de incidente de ciberseguridad o circunstancia crítica que pueda poner en riesgo los sistemas o servicios, el adjudicatario deberá mantener la dedicación necesaria hasta su estabilización, de acuerdo con las prioridades establecidas por IFEMA MADRID.

El administrador de este servicio dispondrá de acceso preferente al Consultor Experto en Ciberseguridad (ver apartado "3.4. Consultoría experta en Ciberseguridad") de la empresa adjudicataria, para acometer y resolver los asuntos que requieran conocimientos o experiencia avanzada. Este Consultor Experto en Ciberseguridad deberá contar con conocimientos técnicos suficientes para apoyar al administrador y a IFEMA MADRID en decisiones de arquitectura, diseño seguro, integración y respuesta ante riesgos complejos.

IFEMA MADRID facilitará al personal asignado la normativa interna y procedimientos aplicables. El personal del adjudicatario se compromete a conocerlos y respetarlos en el desempeño del servicio.

El adjudicatario proveerá al personal asignado los medios necesarios para la correcta prestación del servicio (incluyendo, cuando proceda, equipo informático, telefonía, software, credenciales corporativas, acceso remoto y comunicaciones seguras), así como la formación y documentación necesarias para mantener su capacitación en los productos objeto del contrato, según lo indicado en el apartado "9. Dotación de medios".

Será responsabilidad exclusiva del adjudicatario la organización y gestión de su personal (selección, dirección, sustituciones, formación, retribución y cualesquiera obligaciones derivadas de la legislación laboral), garantizando en todo momento la continuidad del servicio conforme a lo establecido en el presente pliego.

El personal del adjudicatario estará dirigido y coordinado por un responsable designado por el adjudicatario, que actuará como interlocutor para la organización interna del servicio y para la coordinación con IFEMA MADRID, de acuerdo al apartado "5. Modelo de gobierno y relación" y los procedimientos establecidos.

La dedicación presencial deberá permitir al administrador adquirir un conocimiento detallado del entorno tecnológico y operativo de IFEMA MADRID, a fin de proponer y ejecutar soluciones seguras, viables y alineadas con las necesidades del negocio, dentro del alcance del contrato.

Con el fin de asegurar la continuidad y calidad del servicio, el adjudicatario deberá adoptar las medidas necesarias para mantener la **estabilidad** de los perfiles asignados y minimizar rotaciones no planificadas, garantizando, en todo caso, una sustitución adecuada y una transferencia de conocimiento efectiva cuando resulte imprescindible.

Será este administrador de sistemas de ciberseguridad el encargado de:

- Operar, administrar y mantener los productos y plataformas de ciberseguridad objeto del servicio, conforme a los procedimientos establecidos.
- Planificar y ejecutar actualizaciones, parches y cambios en los productos de ciberseguridad, evaluando impacto y coordinando ventanas con IFEMA MADRID.
- Utilizar las herramientas necesarias para la resolución de incidencias y peticiones, registrando y actualizando en todo caso los tickets en la herramienta corporativa de IFEMA MADRID.
- Actuar como interlocutor técnico con los fabricantes de los productos objeto del servicio (apertura y seguimiento de casos, soporte y escalados), cuando aplique.
- Coordinarse con otras áreas de IFEMA MADRID y con terceros/proveedores cuando sea necesario para la correcta operación de las medidas de seguridad, aportando recomendaciones técnicas dentro del alcance del servicio.
- Escalar al adjudicatario (incluido el apoyo del apartado "3.4. Consultoría experta en ciberseguridad") aquellos asuntos que requieran conocimiento especializado, realizando seguimiento hasta su resolución y manteniendo informada a IFEMA MADRID.
- Proponer recomendaciones técnicas de mejora en materia de ciberseguridad dentro del ámbito de los sistemas administrados.
- Analizar impactos y riesgos asociados a cambios o configuraciones en los elementos de ciberseguridad administrados, y proponer mitigaciones.
- Diseñar y proponer soluciones de mejora sobre los sistemas objeto del contrato, cuando proceda, en coordinación con IFEMA MADRID y el adjudicatario.
- Otras funciones que IFEMA MADRID requiera relacionadas con el objeto del puesto y dentro del alcance del contrato.

IFEMA MADRID tiene una suscripción propietaria de micro CLAUDIA 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 en función del riesgo y del impacto para IFEMA MADRID, ejecutando aquellas que se encuentren dentro de sus competencias y escalando, cuando proceda, las actuaciones que requieran niveles de especialización superiores dentro del adjudicatario. Asimismo, realizará el seguimiento de las actividades escaladas y mantendrá informada a IFEMA MADRID de su estado, incluyendo previsión de esfuerzo y control de consumos cuando resulte aplicable.

El administrador asistirá a las reuniones a las que sea convocado por IFEMA MADRID cuando el objeto de las mismas esté relacionado con el ámbito de ciberseguridad y/o con los productos objeto del contrato. Cuando participen terceros, aportará criterio técnico orientado a la protección de los sistemas, datos y tratamientos de IFEMA MADRID, dentro del alcance del servicio. Verificará que las actas recojan los aspectos de ciberseguridad tratados y, cuando se deriven acciones, registrará las actividades correspondientes en la herramienta de ticketing/ITSM para su priorización, seguimiento y ejecución conforme a lo acordado con IFEMA MADRID.

Las funciones de gobierno y gestión del servicio (por ejemplo, Service Manager y coordinación contractual) serán desempeñadas por los roles definidos en el apartado "5. Modelo de gobierno y relación". El administrador centrará su dedicación en tareas de **operación y administración técnica** de las plataformas objeto del contrato, sin perjuicio de las actividades de coordinación técnica necesarias para su correcta ejecución.

La administración de los sistemas de ciberseguridad se realizará minimizando el impacto en los servicios de IFEMA MADRID y teniendo en cuenta los periodos de mayor actividad (ferias, congresos y eventos). En particular, las operaciones con impacto en la disponibilidad o en las comunicaciones seguras deberán planificarse en las ventanas acordadas y, cuando sea necesario, ejecutarse fuera del horario habitual conforme a lo previsto en la bolsa de horas fuera de horario.

En el anexo "Situación Actual Exp 26_033 CONFIDENCIAL", se adjunta un gráfico con la volumetría de acciones realizadas en el contrato actual.

3.7. Renovación anual de licencias de los productos de ciberseguridad

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.

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.

El contrato incluye el coste y las gestiones necesarias para la renovación anual de las licencias/mantenimientos de los productos de ciberseguridad actualmente vigentes, por un periodo de **un (1) año** a contar desde la **fecha de vencimiento** de los mantenimientos actuales (según el detalle del anexo "Situación Actual Exp 26_033 CONFIDENCIAL"). IFEMA MADRID dispone de licencias ya abonadas hasta determinadas fechas; en consecuencia, **no deberá imputarse** a IFEMA MADRID coste alguno por renovación antes de dichas fechas de vencimiento. A partir de las fechas indicadas en el anexo, el adjudicatario será responsable de realizar las gestiones de renovación en tiempo y forma. En todo caso, las licencias serán siempre propiedad de IFEMA MADRID.

Hasta la fecha efectiva de renovación, el adjudicatario deberá realizar las gestiones necesarias para actuar como **interlocutor** entre IFEMA MADRID y los fabricantes, incluyendo, cuando proceda, el alta o traspaso de la cuenta, la actualización de datos de contacto, y la verificación de que IFEMA MADRID mantiene el acceso a los portales de soporte, actualizaciones, parches y recursos asociados a las licencias vigentes.

Las renovaciones deberán realizarse en tiempo y forma, sin costes adicionales para IFEMA MADRID derivados de retrasos imputables al adjudicatario. En caso de recargos o penalizaciones del fabricante por retraso en la tramitación o pago atribuible al adjudicatario, estos serán asumidos por el adjudicatario. Asimismo, el adjudicatario deberá garantizar al menos la continuidad del **mismo nivel de cobertura** y del **modelo de licenciamiento** existente, de forma que IFEMA MADRID mantenga el acceso a soporte, actualizaciones, parches y nuevas versiones en condiciones equivalentes a las actuales, salvo que IFEMA MADRID autorice expresamente un cambio.

El adjudicatario actuará como interlocutor de IFEMA MADRID ante los fabricantes de los productos de ciberseguridad incluidos en este apartado, gestionando la apertura, seguimiento y cierre de solicitudes de soporte y/o casos con el fabricante cuando resulte necesario, y manteniendo la trazabilidad mediante la herramienta de ticketing/ITSM de IFEMA MADRID.

El servicio asociado a este apartado deberá asegurar la disponibilidad **24x7x365** para la **gestión y escalado** de solicitudes de soporte con los fabricantes (por ejemplo, apertura de casos críticos, seguimiento y coordinación), cuando sea necesario para restaurar la continuidad de los servicios cubiertos por las licencias. Lo anterior se entiende sin perjuicio de los servicios operativos del SOC y de administración técnica regulados en los apartados correspondientes.

Como mínimo, el adjudicatario deberá mantener actualizado: (i) un **calendario de vencimientos y renovaciones**; (ii) un **inventario** de licencias/mantenimientos incluidos; y (iii) la **evidencia documental** de cada renovación (por ejemplo, confirmación del fabricante, nº de contrato/soporte o documento equivalente), quedando disponible para su revisión por IFEMA MADRID.

El adjudicatario indicará el precio de esta parte del servicio en su oferta de forma individual.

4. Horario de prestación de los servicios

A continuación, se indican los horarios de cada uno de los servicios contemplados.

Servicio	**Horario**
Servicios de prevención	8 x 5 *(*)*
Servicios de detección y monitorización	24 x 7 x 365
Gestión de respuesta ante incidentes	24 x 7 x 365
Consultoría experta en ciberseguridad	8 x 5 *(*)*
Certificaciones, riesgos y cumplimiento normativo	8 x 5 *(*)*
Servicio de administración de infraestructura	8 x 5 (posibilidad de intervenciones fuera de horario)
Renovación anual de licencias	8 x 5 *(*)*

(*) El horario habitual de prestación de servicio será de lunes a jueves de **09:00 a 18:30** (con una hora de comida) y los viernes de **09:00 a 15:00**

5. Modelo de Gobierno y Relación

El modelo de Gobierno y Relación se orienta a asegurar el control, seguimiento y mejora continua de la prestación del servicio, incluyendo: el cumplimiento de los acuerdos de nivel de servicio (ANS); la priorización de incidencias y peticiones en función del riesgo e impacto; y la trazabilidad de las actividades mediante la herramienta de ticketing/ITSM de IFEMA MADRID. Asimismo, establece una

comunicación periódica y estructurada entre IFEMA MADRID y el adjudicatario para disponer de visibilidad sobre estado, responsables, plazos, riesgos y decisiones.

En la operativa diaria, el perfil de Administrador descrito en el apartado "**3.6. Servicio de Administración de infraestructura de seguridad y plataformas de ciberseguridad"** actúa como punto de referencia para la ejecución y seguimiento de tareas técnicas, asegurando que las solicitudes y actuaciones quedan registradas, actualizadas y cerradas en la herramienta de ticketing/ITSM de IFEMA MADRID. Este registro constituye la base objetiva para el seguimiento de ANS, la priorización y la trazabilidad del servicio.

Se establecen, como mínimo, los siguientes foros de seguimiento:

- **Reunión mensual de seguimiento operativo**: revisión del informe mensual del servicio, estado de incidencias/peticiones, cumplimiento de ANS, riesgos operativos, principales acciones realizadas y plan de trabajo del mes siguiente.

El adjudicatario designará el role **Service Manager Operativo** liderará la reunión mensual de seguimiento operativo, presentará el informe mensual del servicio y elaborará el acta con acuerdos, responsables y fechas de compromiso. IFEMA MADRID podrá invitar puntualmente a responsables de la capa operativa, cuando sea necesario para aportar contexto.

La gestión de solicitudes tiene por objeto atender incidencias y peticiones dentro de los ANS acordados, priorizándolas en proporción al riesgo que mitiguen y a su impacto para IFEMA MADRID.

IFEMA MADRID podrá mantener reuniones internas de coordinación para la priorización diaria de actividades. Cuando resulte necesario, el adjudicatario participará en dichas reuniones o facilitará información para asegurar la correcta coordinación de acciones y la alineación con las prioridades de IFEMA MADRID.

Todas las actividades objeto del contrato deberán registrarse en la herramienta de ticketing/ITSM de IFEMA MADRID, de modo que cada actuación disponga de identificador, estado, responsable y trazabilidad asociada. Esta información servirá, entre otros fines, como base de conocimiento, control de ejecución y cálculo de ANS cuando aplique.

Se denomina **incidencia** a toda interrupción o reducción no planificada de la calidad del servicio. Puede ser un fallo reportado por el SOC, por el Área de Sistemas y Ciberseguridad de IFEMA MADRID, por herramientas de monitorización, por el CAU (Centro de Atención al Usuario) o por otros proveedores tecnológicos, entre otros. El objetivo ante una incidencia es restaurar la operativa normal del servicio con la máxima rapidez, minimizando el impacto en el negocio.

Se denomina **petición** a una solicitud planificada o no urgente relacionada con el servicio (por ejemplo, asesoramiento, consultoría, diseño o mejora de soluciones de ciberseguridad, análisis de viabilidad, elaboración de informes, cambios o tareas de mantenimiento), que deberá registrarse, priorizarse y gestionarse conforme al procedimiento establecido.

Las incidencias y peticiones se clasificarán por criticidad conforme a la siguiente tipología, con el fin de facilitar su priorización y la aplicación de los ANS correspondientes:

- **Incidencia crítica**: aquella que afecta significativamente al nivel de servicio prestado. El servicio está indisponible o se impide la operativa básica, afecta a un número elevado de usuarios o puede provocar un impacto económico relevante. También tendrá esta consideración el incumplimiento de ANS cuando aplique.

- **Petición urgente**: aquella que requiere atención prioritaria por su impacto o por interés estratégico para IFEMA MADRID, pudiendo existir degradación parcial del servicio sin indisponibilidad total.

- **Incidencia grave**: aquella que afecta parcialmente al servicio y produce degradación, sin que exista indisponibilidad total, y con impacto limitado a un número reducido de usuarios o procesos.

- **Incidencia o petición leve**: aquella que no afecta de forma apreciable al nivel de servicio prestado, aunque pueda existir un riesgo potencial de degradación o de pérdida de calidad del servicio.

La criticidad asignada a una incidencia o petición será determinada por IFEMA MADRID en el momento de su apertura, pudiendo ser recalificada a propuesta del adjudicatario, previo acuerdo con el Área de Sistemas y Ciberseguridad de IFEMA MADRID.

Los usuarios finales de IFEMA MADRID no abrirán tickets de ciberseguridad directamente. Las solicitudes llegarán filtradas y canalizadas a través de los procedimientos internos (por ejemplo, mediante escalado del CAU u otras áreas), así como desde el Área de Sistemas y Ciberseguridad de IFEMA MADRID y/o desde los servicios del adjudicatario (por ejemplo, SOC), conforme a los flujos acordados.

El administrador de sistemas de ciberseguridad abrirá asimismo los tickets necesarios para registrar actividades que deban quedar trazadas (por ejemplo, acciones derivadas de acuerdos en reuniones de ciberseguridad), con el fin de permitir su priorización, ejecución y seguimiento.

6. Acuerdos 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.

6.1. 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.

6.2. 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 "SLA_Exp 26 033_Servicio Ciberseguridad ".

6.3. 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.

7. Fases de la prestación del servicio

El correspondiente servicio constará solo de las siguientes fases:

- Fase I: Preparación y Constitución del Servicio. **Duración máxima 1 semana. No facturable.**
- Fase II: Fase de transición. Duración mínimo 2 semanas, máximo 1 mes y medio. Inicio simultaneo a Fase I. **No facturable.**
- Fase III: Prestación completa del Servicio.

- Fase IV: Traspaso del Servicio. Durante las 4 últimas semanas del contrato.

7.1. 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.

7.2. 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.

7.3. 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 los correspondientes ANS determinados para este servicio como mínimos en estas especificaciones.

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

7.4. 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. Visita a las instalaciones de los ofertantes

En caso de considerarlo necesario, el personal de IFEMA MADRID podrá visitar las instalaciones que han sido propuestas por parte de los ofertantes para la ejecución de los correspondientes servicios.

9. Dotación de medios

El correspondiente 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 comienzo de la Fase II de prestación completa del servicio 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.

10. Garantía de los trabajos y titularidad

Con independencia de la duración prevista en el contrato, el correspondiente adjudicatario 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.

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 será 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**

2. **Descripción detallada de los puntos incluidos en el apartado "3. Alcance" del presente documento**

   2.1 Servicios de prevención
   2.2 Servicios de detección y monitorización.
   2.3 Servicio de respuesta
   2.4 Consultoría experta en ciberseguridad
   2.5 Certificaciones, riesgos y cumplimiento normativo
   2.6 Servicio de administración de infraestructura y plataformas de ciber seguridad
   2.7 Renovación anual de licencias de los productos de ciberseguridad
   2.8 Administrador de sistemas de ciberseguridad presencial

3. **Herramientas para la prestación del servicio de análisis de vulnerabilidades**
   El licitador deberá indicar en su oferta el conjunto de herramientas utilizadas para el servicio, considerándose dentro del coste del servicio todos los gastos derivados de las

mismas (licencias, mantenimientos, actualizaciones, etc.). El personal técnico de IFEMA MADRID dispondrá de permisos de acceso a todas las herramientas.

4. **Metodologías de análisis, tácticas, técnicas y procedimientos aplicados para la prestación del servicio de análisis pentesting**
   Los licitadores indicarán en su oferta técnica la metodología de análisis, tácticas, técnicas y procedimientos aplicados para la prestación del servicio, los criterios de valoración de las vulnerabilidades encontradas y las herramientas de análisis y explotación utilizadas por el equipo técnico de hacking ético.

5. **Metodologías de análisis, tácticas, técnicas y procedimientos aplicados para la prestación del servicio Threat Hunting**

   Los licitadores deberán describir en su propuesta la metodología y el enfoque de análisis, incluyendo como mínimo: (i) definición y priorización de hipótesis de caza basadas en el contexto de IFEMA MADRID, inteligencia de amenazas y/o riesgos emergentes; (ii) mapeo de técnicas y sub-técnicas conforme a MITRE ATT&CK y orientación a indicadores de ataque (IoA) y comportamientos (TTP) frente a búsquedas exclusivamente basadas en IoC; (iii) fuentes de telemetría empleadas (SIEM, EDR/XDR, logs de identidad, red, cloud, correo, proxy, etc.) y requisitos de retención para permitir análisis histórico; (iv) proceso de investigación y pivoteo (búsqueda, validación, descarte de falsos positivos, determinación de alcance); y (v) criterios de cierre del hunt, evidencias y trazabilidad (registro en ticketing, resultados, acciones recomendadas y acciones implantadas cuando proceda).

6. **Otra documentación**
   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 valoración 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.

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**

2. **Organización y gestión del servicio**

   a. Descripción de la estructura organizativa de gestión del servicio de operación de ciberseguridad, asignación de roles (incluida matriz RACI) y tareas, 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, valorándose el grado de definición, implantación y mejora continua de los procesos de monitorización, detección, análisis y respuesta ante incidentes de ciberseguridad, así como los mecanismos de control, seguimiento y medición de su eficacia y nivel de sencillez, eficacia y claridad de las herramientas utilizadas para la gestión.

b. 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.

3. Descripción detallada de los siguientes servicios

2.1. 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.

2.2 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, así como el nivel de personalización de análisis, tratamiento de resultados y plan de remediación para el contexto de IFEMA MADRID

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 como del procedimiento ante crisis, valorándose el nivel de efectividad y eliminación de pérdidas de tiempo y nivel de coherencia.

2.3 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, valorándose en nivel de eficacia y el nivel de profundidad, así como el nivel de personalización de análisis, tratamiento de resultados y plan de remediación para el contexto de IFEMA MADRID. Descripción del contenido de los informes generados y acciones a realizar, valorándose la manera de reporte y la coherencia del formato, así como la claridad.

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

a. Descripción de herramientas y tecnologías innovadoras 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 y el nivel de aporte de valor añadido al servicio dentro del entorno de IFEMA MADRID.

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.

Los presupuestos asociados a las modificaciones de contrato 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.

14. 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: 645 07 67 13.