SERVICIO DE SOPORTE PARA CIBERSEGURIDAD DE LA INSTITUCIÓN FERIAL DE MADRID

EXP. 19-237 - 2000015111

Pliego de Prescripciones Técnicas

Comisión de Compras
Madrid, Julio 2019

1. OBJETO DEL CONTRATO

El presente expediente tiene por objeto la contratación de un servicio de ciberseguridad enfocado a la protección de la información y de todos los recursos informáticos de IFEMA. Será un servicio para la protección tanto de la información contenida en los sistemas de IFEMA como de la información que circula por las redes de IFEMA junto con la defensa y securización de los propios sistemas de IFEMA. Será un servicio que dará respuesta adecuada a los riesgos actuales y futuros en materia de ciberseguridad.
También está dentro del objeto del contrato la renovación de las licencias correspondientes de los productos de seguridad que IFEMA tiene instalados y que se describen en el punto 2.1 Productos de Seguridad y Licencias así como su mantenimiento, gestión y soporte.

2. SITUACIÓN ACTUAL

La situación actual de la ciberseguridad de IFEMA está compuesta por dispositivos y productos de seguridad con sus licencias de soporte en vigor, su primer nivel de soporte y la realización de tareas de administración de sistemas y asesoramiento por parte del proveedor.

La documentación (ANEXO Productos de Seguridad de IFEMA) será enviada por correo electrónico, cuando el ofertante así lo solicite, debiendo para ello enviar copia de las escrituras al correo electrónico marisa.cruz@ifema.es

2.1. SERVICIOS DE MANTENIMIENTO Y PRIMER NIVEL

El servicio prestado actualmente consiste en el soporte, administración y mantenimiento de los productos de seguridad de IFEMA. Así mismo, se lleva a cabo la investigación y resolución de problemas o bugs de los productos y la respuesta a dudas de uso y configuración, así como proyectos de actualización y modernización de los sistemas de seguridad.

Además, la empresa colaboradora, también presta servicios de administración de sistemas, mantenimiento, asesoramiento. Servicios tales como la elaboración de informes, recomendaciones y consejos. Realiza para IFEMA tareas tales como administración de sistemas, configuraciones, migraciones, comprobaciones y otras actividades, todo ello siempre dentro del ámbito de la ciberseguridad. En la situación actual también la empresa colaboradora pone a disposición de IFEMA un número de jornadas de personas expertas en asuntos de ciberseguridad para la prestación de este tipo de servicios in situ en las propias instalaciones de IFEMA.

3. ALCANCE DEL SERVICIO SOLICITADO

Se solicita un servicio de Ciberseguridad completo para la protección de todos los recursos informáticos de IFEMA.

El servicio solicitado consta de tres partes fundamentales:

- **Servicios Horizontales de Ciberseguridad**: Monitorización, servicios de soporte y mantenimiento preventivo y correctivo prevención de riesgos con *herramientas* **de análisis de eventos de seguridad** en el **SOC** del proveedor, con el fin de identificar y prevenir riesgos, dar soluciones y proponer mejora continua en aspectos de ciberseguridad. Todo ello sujeto a los términos y condiciones que se indican en el punto 3.1 .

- **Proyectos** basado en una bolsa de jornadas para la realización de proyectos evolutivos dentro del ámbito de la ciberseguirdad y en el que se vean involucrados los sistemas de IFEMA relacionados con este área.

- **Las licencias**: la renovación, con sus respectivos fabricantes de los contratos de mantenimiento y soporte en caso de incidencias de los productos de ciberseguridad.

La empresa adjudicataria debe mostrar una visión global del servicio de ciberseguridad con el fin de proponer e impulsar actuaciones de mejora continua del mismo.

También deberá disponer de un SOC (Centro de Operaciones de Seguridad) con el fin de monitorizar, identificar y prevenir riesgos, dar soluciones y proponer mejora continua en aspectos de ciberseguridad.

Los sistemas informáticos que controlan la seguridad de IFEMA y sus comunicaciones tienen un papel fundamental en las actividades de la institución. Por eso es necesario establecer unas comunicaciones modernas, robustas y seguras, además de impedir que las comunicaciones legítimas sean la entrada de amenazas al resto de los sistemas informáticos de IFEMA. Éstos son los cometidos que le corresponden a los sistemas de protección perimetral de IFEMA: interconectar y proteger.

Se trata de sistemas con una configuración que requiere atención profesional. Sistemas siempre actualizados para establecer las interconexiones de IFEMA con internet, con terceros o con otros dispositivos y servicios de IFEMA. Se emplean para ello elementos tales como procedimientos, servicios y dispositivos actualizados y dotados con los estándares más modernos de comunicaciones y seguridad tales como VPNs, certificados digitales, TLS, comunicaciones 802.1x, etc. Todos estos elementos de protección detectan y rechazan las amenazas actuales y se mantienen en evolución y actualización continua para afrontar las amenazas futuras.

Las especificaciones que se muestran se entienden como las mínimas exigibles.

El modelo de los servicios de mantenimiento que se pretende conseguir es el correspondiente a un servicio de ciberseguridad integral, y basado en la consecución de los niveles de servicio acordados. Este servicio permitirá disponer de los recursos necesarios en cada momento para poder dar respuesta a las necesidades de mantenimiento, actualización y mejora de los sistemas de seguridad perimetral de IFEMA, incluyendo la implementación de las correciones, modificaciones y mejoras que sean requeridas en dichos sistemas para que estos puedan seguir respondiendo a las necesidades de seguridad y de comunicaciones de IFEMA.

Ese servicio requiere TÉCNICOS SENIOR EXPERTOS.

El adjudicatario estará normalmente el servicio desde sus instalaciones. El proveedor también podrá presentarse en las instalaciones de IFEMA cuando lo estime oportuno o bien cuando IFEMA lo requiera para la realización de las actividades del servicio, la solución de los problemas o la reparación de los errores en los productos. Cualquier coste adicional por desplazamiento, dietas, pernoctaciones, etc. correrán por cuenta del proveedor del servicio, no siendo imputable de ningún modo al servicio.

En ningún caso el proveedor está autorizado a subcontratar el servicio completo a un tercero, aunque si podrá subcontratar especialistas puntualmente, No obstante la responsabilidad total sobre la prestación del servicio será exclusivamente del adjudicatario.

Será el área de Sistemas Corporativos y Seguridad de la Dirección de Tecnologías de la Información de IFEMA la que coordinará y gestionará el servicio.

Los asuntos de cumplimiento normativo, compliance, normativa de protección de datos de carácter personal, sistemas y servicios alojados en el hosting de IFEMA, no son objeto del presente contrato.

Para ello, el proveedor deberá contar con un **SOC** para la prestación de **Servicios Horizontales de Ciberseguridad** que aumenten la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones de IFEMA, así como la mejora de su capacidad de respuesta ante cualquier ataque. El proveedor, dentro de esta función de vigilancia y asesoramiento continuo, mantendrá informada a IFEMA de las amenazas e incidentes de TI que se encuentren presentes en internet y que pudieran causar impacto en el negocio de IFEMA, para poder gestionarlos juntos, IFEMA con el proveedor. Por ejemplo, nuevos ramsonware que se extienden con rapidez, emails masivos que suplantan a bancos legítimos, etc.
También deberá recopilar información de los sistemas de IFEMA, y del tráfico de red de la Institución ya sea con sondas o herramientas de análisis de eventos de seguridad.

Se requiere el servicio de mantenimiento y asesoramiento continuo de ciberseguridad de los sistemas de seguridad perimetral de IFEMA El servicio de mantenimiento comprende las acciones y tareas correspondientes a mantenimiento correctivo, preventivo y evolutivo que se encuentran dentro de la ciberseguridad, las comunicaciones y las redes.

El servicio de mantenimiento incluye también la resolución de consultas, análisis de impacto, elaboración de informes, diseño de soluciones, etc. de cualquier asunto relacionado con la ciberseguridad. Por ejemplo, responder consultas y elaborar recomendaciones acerca de la seguridad, de los productos descritos en la situación actual, de las comunicaciones seguras, de las redes, las amenazas, los riesgos, los nuevos avances y funcionalidades en materia de seguridad, etc. Por ejemplo, diseño de soluciones de seguridad para la movilidad, la autenticación de usuarios y dispositivos, la interconexión segura con otras empresas colaboradoras, las VPNs, las tecnologías TLS, SSL, los certificados digitales, etc. Todo ello adaptado a los requisitos y circunstancias de IFEMA.

Es un servicio del que se requiere proactividad y está sujeto a la consecución de los Acuerdos de Nivel de Servicio ANS descritos en este documento. Las tareas se llevarán a cabo en base a las necesidades y prioridades planificadas por IFEMA.

El alcance del presente contrato comprende también la renovación de las licencias y condiciones de soporte tanto de los productos de seguridad perimetral de los que dispone IFEMA, descritos en la situación actual, como la de los productos que se vayan incorporando en el futuro de acuerdo con las ampliaciones del contrato que se acuerden, así como el primer nivel de soporte correctivo de los sistemas de seguridad perimetral que se describirá a continuación. Lógicamente, la adquisición de nuevos productos de Checkpoint o Ironport implicará el incremento en el precio de la renovación de las licencias y su mantenimiento, de acuerdo con la estimación reflejada en el apartado 7 – MODIFICACIONES DEL CONTRATO – del pliego de bases.

3.1. SERVICIOS HORIZONTALES DE CIBERSEGURIDAD (SOC)

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

IFEMA tiene implementadas medidas de seguridad y métodos de protección en su organización, pero debido a la complejidad de los sistemas, los riesgos existentes y su creciente actividad es esencial contar con el asesoramiento de expertos para

establecer y consolidar una adecuada gestión de la seguridad para la información y los sistemas de IFEMA que permita responder lo antes posible y en cualquier momento ante cualquier amenaza.

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

Este servicio, también, debe estar orientado a la resolución de incidencias que requieran la realización de actividades de diseño, recomendación, modificación, corrección, adaptación, mantenimiento, asesoramiento o mejora de la seguridad y de los sistemas de seguridad perimetral

El servicio realizará todas estas tareas en tiempo real 24 horas al día por 7 días a la semana.

Los servicios entre otros que deben incluirse, son:

- Instalación de “sondas” y herramientas de análisis de eventos de seguridad herramientas, dispositivos, software, incluida la integración con los dispositivos perimetrales para disponer de información. Logs, eventos en el SOC con el obejtivo de permitir toma de decisiones en el mantenimiento proactivo y reactivo ante cualquier evento de seguridad.-

- Correlación e inteligencia. Revisión logs generados por los sistema de monitorización centralizado de IFEMA y el resto de sistemas que dispongan de logs que aporte valor en el ámbito de la ciberseguridad, más los de la/s sonda/s y herramientas instaladas para el servicio solicitado.

- Detección en tiempo real de amanezcas y actividades anómalas. Informando y estableciendo planes de actuación acordes al nivel de la amenaza.

- Proveer servicios de ciberinteligencia y vigilancia digital capaces de detectar campañas de ataques dirigidos con el fin de anticiparse a estos y ser capaces de bloquearlos.

- Protección de riesgo corporativo. Detección de comportamientos inseguros dentro de la organización. Robo de credenciales, fuga de información, etc.

- Análisis de seguridad orientado al riesgo.

- Prevención y detección de intrusiones y vulnerabilidades de las infraestructuras de IFEMA.

- Protección de marca contra posibles abusos y daños reputacionales a nivel nacional e internacional.

- Investigación y análisis continúo de las alertas de seguridad recogidas por las distintas fuentes para determinar planes de alertas y actuación.

- Capacidad de realizar Análisis Forense en caso de necesidad y con el fin de diagnosticar cualquier incidente de seguridad informática.

- Seguimiento continúo de los planes de prevención de Seguridad Informática establecidos, comprobando la eficacia de las medidas implementadas.

- Participación activa en las situaciones críticas por incidentes relevantes que puedan llegar a producirse durante la vigencia del contrato.

- Diagnosticar y analizar las incidencias recibidas así como sus posibles causas.
- Acometer su resolución con celeridad, prontitud y eficacia realizando el seguimiento de las mismas.
- Acometer tareas que lo requieran con un enfoque que se pueda alargar en el tiempo, como puede ser comprobar si la implementación de una solución ocasiona problemas con el tiempo, etc.
- Actualizar la incidencia correspondiente, donde quedarán reflejadas las tareas desarrolladas por el adjudicatario para su resolución, así como los estados por los que pase esta incidencia hasta su cierre final, la dedicación, etc.

- Mantener actualizada la documentación técnica del sistema, así como los manuales de usuario cuando corresponda, la base de datos de conocimiento, los manuales de operaciones, los documentos de diseño, etc.
- Atención y respuesta a las dudas y consultas del equipo de Sistemas de la DTI sobre la seguridad o sobre el mantenimiento de los sistemas de seguridad perimetral.

- Al realizar las tareas objeto del contrato, generar propuestas para mejorar la seguridad y el mantenimiento de los sistemas de seguridad perimetral. A su vez, si al realizar estas tareas el adjudicatario encontrase errores o problemas, deberá alertar al equipo de Sistemas de la DTI de IFEMA informándole del asunto.
- Colaboración con el resto del equipo de Sistemas de la DTI para el correcto mantenimiento de los sistemas de seguridad perimetral de IFEMA.
- Auditoría perimetral interna y externa.
- Pruebas de penetración, pentesting.
- Resolución de todas las incidencias, mantenimiento correctivo.
- Resolución de todas las peticiones de mantenimiento evolutivo pequeño que tenga un coste inferior a 20 horas.

Todas las actividades tendrán en cuenta las fechas de celebración de ferias, tratándose de evitar la interferencia en el correcto desarrollo de los servicios de la feria. Se deberá calibrar la envergadura: dependiendo del riesgo o magnitud de la actividad, planificar las medidas de seguridad adecuadas, elaborar planes de detalle, extremar las comprobaciones, prever la vuelta atrás en caso de problemas, prever los recursos necesarios para dar respuesta inmediata a una incidencia en la realización de la actividad, etc. Cada actividad debe incluir una fase de seguimiento a posteriori.

Todas las actividades y mantenimientos realizados deberán estar debidamente documentados.

Será también responsabilidad del adjudicatario la entrega, durante el servicio, de informes de seguimiento, actas de reunión y todos los informes de gestión consensuados con IFEMA.

3.2 PROYECTOS

IFEMA está inmersa en un proyecto de transformación digital y debido a esto y otro tipo de proyectos que se acometerán en un futuro y en los que se vean involucrados los sistemas de seguridad implantados en IFEMA o cualquier otro aspecto de ciberseguirdad que esté relacionada la marca IFEMA, podrá solicitar al proveedor la intervención para realizar Proyectos con carácter evolutivo, siempre y cuando dicha intervención supere las 20 horas de dedicación.

Para acometer estos proyectos IFEMA dispone una bolsa de 50 jornadas anuales.

Este servicio parte del servicio deberá disponer de los recursos necesarios en cada momento para poder dar respuesta a las necesidades del proyecto, actualización y mejora de los sistemas de seguridad perimetral de IFEMA,

Podrán existir proyectos paralelos realizados por otros equipos de trabajo (de IFEMA o de terceros) sobre los sistemas de seguridad perimetral de IFEMA. En estas circunstancias, las tareas, funciones y competencias de cada uno de los equipos, incluyendo el del proveedor del servicio que se está solicitando en estas prescripciones técnicas, se determinarán en todo momento según el criterio de IFEMA.

Cada vez que IFEMA solicite este servicio el proveedor tendrá que:

- Asistir a reuniones en las oficinas de IFEMA.
- Ponerse en contacto con clientes y proveedores que intervengan en el proyecto.
- Planificar las tareas necesarias para llevar a cabo el proyecto, indicando las fases del mismo.
- Documentar el proyecto con el suficiente nivel de detalle de las tareas para que puedan llevarse a cabo con exactitud, incluyendo acciones y personas que intervienen.
- Adecuar la ejecución al proyecto de tal manera que impacte lo menos posible en la actividad comercial de IFEMA.
- Consensuar con el Dpto. de Sistemas de la D.T.I. tanto el diseño del proyecto como la ejecución del mismo.
- Analizar y acometer los diferentes análisis para la ejecución del proyecto.
- Identificar dependencias con otros sistemas de IFEMA involucrados en el proyecto.
- Migraciones, actualizaciones de los productos de seguridad desplegados en IFEMA.
- Elaboración de recomendaciones e informes sobre tema de seguridad, para incorporarlos a otros proyectos de IFEMA o incluso al Documento de Política de Seguridad de IFEMA. Por ejemplo, informes de seguridad relacionados con los proyectos de desarrollos previstos en IFEMA
- Implantación de nuevas medidas de seguridad que vayan surgiendo, avances y novedades de la industria, modernizaciones.
- Consultoría de seguridad.
- Colaborar en proyectos que no estén liderados por el adjudicatario pero que requieran de su actuación en los aspecto relacionados con la ciberseguridad y dentro del alcance de este servicio. Por ejemplo, IFEMA podría encargar la

implantación de dispositivos móviles a un tercero necesitando la ayuda y colaboración del adjudicatario.

- Diseño, planificación y/o implantación de nuevas soluciones de seguridad adaptadas a las necesidades y circunstancias de IFEMA.

3.3. LICENCIAS. CONTRATOS DE MANTENIMIENTO DE LOS PRODUCTOS

El alcance comprende la renovación de los contratos de mantenimiento de los productos descritos en el apartado 2.1. Productos de Seguridad y Licencias de la Situación Actual, así como la resolución de cualquier incidente derivado de bugs y problemas con dichos productos.

La relación completa de productos de seguridad empleados por IFEMA en el ámbito de este contrato los puede consultar el ofertante con los fabricantes respectivos de los productos, como distribuidor autorizado suyo que es, haciendo referencia a los contratos de IFEMA con dichos fabricantes:

- "Service Contract 90784688" con Cisco IronPort
- "User Center 5716162" con Check Point.

A continuación se describen algunos ejemplos de elementos que, como mínimo, deben estar incluidos en el primer nivel de soporte relacionado con las licencias.

- Soluciones del fabricante a errores o bugs de los productos en el mínimo tiempo posible.
- Acceso a las actualizaciones del software y sus últimas versiones.
- Actualizaciones de ficheros con datos de configuración que constituyen las listas blancas, listas negras, ficheros de firmas y otros tipos de ficheros necesarios para el funcionamiento de los diferentes componentes de seguridad.
- Acceso a manuales de producto, guías de buenas prácticas, libros blancos de temas de seguridad, uso y configuración de los productos.

El Soporte de los productos, en el caso de incidencias críticas con impacto en el negocio, estará disponible a cualquier hora todos los días del año, es decir, disponibilidad 24x7x365, para la recuperación inmediata del servicio.

4. MODELO DE GOBIERNO Y RELACIÓN

Este modelo de Gobierno y Relación estará basado en la consecución de los ANS contratados y pretende conseguir la resolución de las incidencias y peticiones en el momento oportuno, atendiendo a las necesidades y prioridades planificadas por IFEMA y de un modo que en que en todo momento, las personas implicadas de

IFEMA y del proveedor estén informadas puntualmente del responsable y estado de todas las actividades del servicio.

Todas las acciones se llevarán a cabo en base a las necesidades y prioridades planificadas por IFEMA. Es fundamental atender también al criterio de máxima disponibilidad de los servicios productivos. El adjudicatario será consciente de la actividad del calendario ferial y de la actividad del negocio de IFEMA y lo tendrá en cuenta en las planificaciones y en la realización de actividades que tengan impacto en el funcionamiento normal de los sistemas: Los momentos más oportunos son los de menor actividad de negocio.

Se requiere por parte de proveedor, una profunda contextualización, ofreciendo soluciones adaptadas a IFEMA para las distintas tareas, no solo basadas en "libros blancos" sino aplicándolas al marco de necesidades y circunstancias de IFEMA.

El proveedor será también el responsable de interactuar con el SOC, con el fin de mitigar, eliminar, de forma proactiva o reactiva cualquier incidente de seguridad informática.

Cualquier implementación, solicitud de actuación o configuración en los sistemas de ciberseguridad de IFEMA así cualquier decisión relativa a TI y sus sistemas que pueda provocar alguna brecha de seguridad deben estar consensuada con los especialistas del SOC.

Se denomina incidencia a toda interrupción o reducción de la calidad no planificada del servicio. Pueden ser fallos reportadas por los usuarios, el equipo de Sistemas de IFEMA, por alguna herramienta de monitorización de eventos, por el propio proveedor del servicio de forma proactiva como resultado de su monitorización de los sistemas de IFEMA, por el CAU de IFEMA, etc. El objetivo principal ante las incidencias es restaurar cuanto antes la operativa normal del servicio minimizando el impacto negativo en el negocio.

Las peticiones podrán ser de diversa índole como asesoramiento, consultoría, parametrizaciones, diseño de soluciones de ciberseguridad, realización de tareas de mantenimiento, implantaciones, integraciones, análisis de viabilidad, operaciones, estudios, informes, configuraciones, etc. También habrá tareas que requerirán por parte del proveedor un enfoque de tarea continua, como revisiones diarias de la plataforma, revisión de implantación de soluciones que se alargarán en el tiempo, lo que requerirá un amplio conocimiento de la plataforma de IFEMA por parte del proveedor, haciéndola suya para poder trabajar de forma independiente contextualizándose siempre a las necesidades y requerimientos de IFEMA. Es decir se trata acometer de todas las acciones necesarias para un óptimo funcionamiento de los sistemas de IFEMA. Dichas acciones estarán sujetas a los Acuerdos de Nivel de Servicio.

Una vez abierta la petición, el adjudicatario indicará el tiempo que se tardará en realizar dicha petición. IFEMA evaluará la propuesta. En caso de disconformidad el adjudicatario deberá realizar otra propuesta llegando a un acuerdo.

Para el tratamiento de las incidencias y peticiones, en IFEMA se cuenta con BMC Remedy, herramienta que será utilizada por el proveedor tanto para el alta y actualización como para el seguimiento de incidencias y peticiones a nivel general y la gestión del conocimiento de las mismas.
Cada actividad estará reflejada en su correspondiente tarea en el dicha herramienta La tarea identificará el contenido, la criticidad, los detalles, el estado de realización y, si procede, el consumo de horas previsto y el consumo de horas realizado. Los datos de consumo no proceden en las actividades de primer nivel de soporte.

Los cambios de estado de las incidencias causarán el envío de un email de notificación a los interesados con la identificación de la incidencia y los detalles del cambio.

En la fase de devolución del servicio, el adjudicatario enviará a IFEMA en un formato estandarizado (PDF o MS Word) toda la información contenida en el sistema de helpdesk relacionada con IFEMA.

Cuando en IFEMA tengamos una incidencia de ciberseguridad se realizará una petición al proveedor a través del helpdesk.

Para la realización de tareas que superen las 20 horas de dedicación, el adjudicatario indicará el consumo previsto de la bolsa de jornadas, el tiempo que se tardará en realizar una tarea y el técnico asignado a su resolución. IFEMA evaluará la propuesta. En caso de disconformidad el adjudicatario deberá realizar otra propuesta llegando a un acuerdo. Se procederá a su resolución previa autorización por parte de IFEMA. Una vez concluida la petición se debe remitir a IFEMA un informe con el consumo de jornadas finalmente realizado.

Si la incidencia es crítica o urgente se debe atender de forma inmediata. Se debe trabajar en ella hasta su resolución.

La resolución de las incidencias incluidas en el primer nivel de soporte se atenderá en función de su criticidad sin necesidad de indicar el consumo previsto de la bolsa de jornadas.

En general, las tareas objeto del contrato se van a clasificar según su criticidad (es la importancia de la incidencia en función del impacto que origina sobre el negocio) en:

- Incidencia crítica: Aquella que afecta significativamente al nivel de servicio prestado. El servicio esta indisponible lo que impide la operativa básica del sistema, afecta a un número elevado de usuarios o puede afectar

económicamente a IFEMA. También es una incidencia crítica el incumplimiento de los ANS contratados.

- Incidencia urgente: Aquella que afecta parcialmente al servicio, produciendo una degradación del mismo, pero sin estar el servicio indisponible y afectando a un número moderado de usuarios pero que requiera una solución urgente.
- Incidencia grave: Aquella que afecta parcialmente al servicio, produciendo una degradación del mismo, pero sin estar el servicio indisponible y afectando a un número reducido de usuarios.
- Incidencia leve: Aquella que no afecta al nivel de servicio prestado aunque existe riesgo potencial de degradación/perdida del mismo.

La criticidad asignada a una incidencia será determinada por IFEMA en el momento de su apertura, pudiendo ser recalificada a petición del proveedor con el acuerdo de la D.T.I.

Es importante tener en cuenta que habrá proyectos o evolutivos que requerirán un enfoque con la metodología adecuada, con sus fases de análisis de la necesidad de IFEMA y la planificación de las tareas para una correcta ejecución del mismo.

Para ello el proveedor deberá identificar todas y cada una de las tareas del proyecto con todas las dependencias entre las mismas, su duración y responsable de cada tarea, presentando para ello un documento tipo planning para poder hacer un seguimiento correcto del estado.

En estos proyectos el proveedor tendrá la responsabilidad completa. Además deberá tener especial cuidado en cumplir las planificaciones acordadas, entregando documentación y haciendo una correcta puesta en producción del mismo. Para ello podrá realizar los chequeos que considere oportunos para asegurar la calidad en el trabajo.

La finalización del proyecto tendrá que contar con la aprobación de la DTI.

IFEMA cerrará las incidencias cuando estén resueltas en modo y forma correcta.

5. HORARIO Y DE PRESTACIÓN DEL SERVICIO

La atención del servicio, de forma general, será 24 x 7.

El horario para la atención y resolución de las incidencias críticas detectadas por IFEMA o el SOC, será 365 días con disponibilidad 24x7 con objeto de restablecer la normalidad en el negocio.

IFEMA no abrirá incidencias que no sean críticas fuera del horario de oficina (de lunes a viernes, de acuerdo al horario de oficina y al calendario laboral de IFEMA, en jornadas de ocho horas,)

6. LUGAR DE EJECUCIÓN DEL CONTRATO

De forma general, la prestación de los servicios se realizará en remoto desde la sede del proveedor. Se requerirá, por lo tanto, acceso remoto a IFEMA. No obstante, el proveedor podrá acudir a las instalaciones de IFEMA para resolver las incidencias, configuraciones, ejecución de proyectos cuando, bajo su propio criterio, lo estime oportuno.

En las ocasiones en que se realice el trabajo en las instalaciones de IFEMA los técnicos, con carácter general, se ajustarán al calendario de IFEMA y de forma consensuada con el Departamento de Sistemas de IFEMA. De la misma manera, cualquier coste adicional por desplazamiento, tiempo de desplazamiento, dietas, medios de transporte, etc. correrá por cuenta del proveedor del servicio.

Para más información respecto del acceso remoto revisar Anexo VII "NORMAS PARA EL ACCESO A LOS RECURSOS DE IFEMA Y MEDIDAS DE SEGURIDAD".

7. FASES DE LA PRESTACIÓN DEL SERVICIO

El servicio global requerido, constará de las siguientes fases:

- **Fase I**: Preparación y Constitución del Servicio.
- **Fase II**: Fase de transición.
- **Fase III**: Prestación completa del Servicio.
- **Fase IV**: Traspaso 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 del equipo de trabajo del adjudicatario, se realizarán reuniones de coordinación con IFEMA, 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 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.

En la **fase II – Transición**, se realizará el traspaso de conocimiento de los sistemas de IFEMA objeto del contrato. El proveedor tendrá que estudiar la documentación técnica existente, así como realizar entrevistas con los responsables del Área de Sistemas de IFEMA y con el actual adjudicatario contratado. Es posible que esas reuniones se celebren presencialmente en IFEMA, 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. Únicamente será facturable la fase II. Esta fase tendrá una duración de un mes como máximo.

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

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

Durante este periodo se pondrán en marcha tanto los ANS determinados como mínimos en estas especificaciones técnicas (ver anexo V de estas especificaciones) como los ofrecidos en la oferta del proveedor, siendo posible la precisión, mejora y definición de nuevos indicadores con el acuerdo de ambas partes.

Esta fase se extiende hasta la finalización del período contratado.

Todos los aspectos de Seguridad relacionados con la prestación del servición estarían indicados en el anexo "NORMAS PARA EL ACCESO A LOS RECURSOS DE IFEMA Y MEDIDAS DE SEGURIDAD".

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, a la entidad que sea designada por IFEMA 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 durante el traspaso del control de servicios y deberá colaborar activamente con IFEMA 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. 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.

8. DOTACIONES DE MEDIOS

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

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. En caso de elegir comunicación VPN LAN to LAN el adjudicatario dispondrá de una VPN compatible con el terminador VPN de IFEMA. No se habilitará ningún acceso adicional a los sistemas de IFEMA 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 y llevará a cabo todas las tareas necesarias para que la conectividad esté plenamente operativa y comprobada.

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

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

El adjudicatario permitirá la conexión a IFEMA 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 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 deben cumplir ciertos requisitos de seguridad como tener un antivirus 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.

Desde dichos equipos del proveedor se accederá a escritorios virtuales en IFEMA. El acceso a estos sistemas será a través del cliente de Horizon View. Para acceder a estas máquinas virtuales de Ifema desde las que se realizarán las tareas objeto del contrato, se les proporcionará usuarios del dominio Ifema con una password segura. También se les proporcionará usuarios con privilegios suficientes para poder desempeñar correctamente la prestación del servicio. No se debe revelar esas passwords a nadie y además se deben cumplir las normas referentes al acceso a los sistemas de Ifema.

IFEMA entregará al adjudicatario el documento de normativa interna, perteneciente al Documento de Seguridad de IFEMA, llamado “Normas del Personal externo con acceso a los sistemas” que será de obligado cumplimiento por todos que requieran

algún tipo de acceso a los sistemas de IFEMA, tanto de forma remota como presencial.

Como ya se ha mencionado, para IFEMA 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 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 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 Feria de Madrid, especialmente si se proyecta al exterior.

El adjudicatario es responsable de garantizar con medios técnicos y organizativos que a la red de IFEMA sólo se conectarán los usuarios autorizados para realizar las tareas autorizadas por este contrato.

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

9. RESPONSABLE DEL SERVICIO

El adjudicatario nombrará a un interlocutor único con IFEMA que realizará las actividades de coordinación y gestión del servicio. El personal del adjudicatario estará dirigido y controlado exclusivamente por el interlocutor perteneciente al adjudicatario, quién coordinará la prestación del servicio y sus diferentes aspectos con IFEMA.

Sus actividades están centradas en el cumplimiento de los procedimientos por parte del equipo de trabajo, así como en la gestión de los recursos dedicados al contrato. Incluyen, control, seguimiento y evaluación del servicio prestado, en cada una de sus fases y actividades, mediante interlocución con los responsables de IFEMA o con terceros en su caso, persiguiendo siempre la orientación a la mejora continua y la calidad en el servicio. Debe realizar las gestión las incidencias, peticiones y proyectos de forma continua y correcta, haciendo el seguimiento de las mismas evitando que se descontrolen, se paren o se desvíen de sus objetivos principales y que se resuelvan en modo y forma adecuada. Realizará los informes de actividad, de control de calidad y de facturación, así como la recogida y el seguimiento de los ANS establecidos. La empresa adjudicataria presentará mensualmente un informe de actividad del servicio que será remitido a IFEMA. También debe incluir en el informe mensual de actividad del servicio el consumo de horas del servicio.

El gestor del servicio deberá estar siempre localizable durante la jornada laboral y designará un sustituto por ausencias y periodos vacacionales.

El gestor del servicio realizará las siguientes actividades:

- Responsabilizarse del cumplimiento y ejecución de las tareas relativas a los sistemas de IFEMA, sean oncloud u onpremises, así como gestionar las incidencias y peticiones de forma continua y correcta, haciendo el seguimiento de las mismas evitando que se descontrolen, se paren o se desvíen de sus objetivos principales y que se resuelvan en modo y forma adecuada. Prestará especial atención a las incidencias críticas persiguiendo su rápida resolución

  - Representación del proveedor en la prestación del servicio ante IFEMA.

  - Interlocución con los comités y responsables de IFEMA.

  - Interlocución con la Dirección de Tecnologías de la Información (D.T.I.) de IFEMA a través de un único gestor permanente del servicio por parte de la empresa adjudicataria para los aspectos relativos a procedimientos de trabajo y gestión de recursos.

  - Búsqueda de soluciones adaptadas a las necesidades y contexto de IFEMA.

  - Gestionará y coordinará internamente dentro de su empresa la obtención de los recursos necesarios para la correcta prestación de los servicios.

  - Realizará el control y seguimiento de la asistencia, horario, etc. de los recursos del servicio.

  - Efectuará un control de consumo de horas mensuales de las jornadas de evolutivos que no comprenda el mantenimiento correctivo y pequeño evolutivo todo incluido. En caso de ser sobrepasado, deberá avisar a IFEMA para determinar las prioridades.

  - Deberá realizar la gestión de la Calidad, en cuanto a recursos, procedimientos y resolución de las incidencias y peticiones.

  - Desarrollar planes para mejorar el nivel de satisfacción de IFEMA, incluyendo reducción de problemas, estandarización, etc.

  - Representar a IFEMA dentro de la empresa proveedora, velando por los intereses y necesidades de IFEMA en relación al servicio requerido.

  - Canalizar el asesoramiento del proveedor como partner tecnológico, sobre nuevas tecnologías, productos, plataforma tecnológica, estándares,

herramientas, soporte a la elaboración de pliegos técnicos, establecimiento de procedimientos de gestión, etc

- Elaboración de informes de actividad, de control de calidad y de facturación, así como la recogida y el seguimiento de los ANS establecidos. La empresa adjudicataria presentará mensualmente un informe de actividad del servicio que será remitido a IFEMA. También debe incluir en el informe mensual de actividad del servicio el consumo de horas de la bolsa de jornadas de evolutivos que no comprenda el mantenimiento correctivo y pequeño evolutivo todo incluido, de técnicos junior, senior y consultor en tecnología para poder realizar la facturación de las mismas.

- Se requiere que el gestor esté totalmente involucrado en el servicio, contextualizado con las necesidades de IFEMA. Deberá mantener contacto de primera mano con el equipo de Sistemas de IFEMA. De hecho podría ser necesaria la participación "in situ" del gestor del servicio en las reuniones de trabajo del equipo de Sistema de IFEMA o usuarios, así como en reuniones semanales de coordinación de tal manera que tenga una visión de las prioridades, requerimientos y necesidades.

- Actuará como interlocutor con las distintas empresas que dan soporte a IFEMA y ante otros proveedores, velando por el buen funcionamiento de los sistemas.

- Deberá aglutinar el conocimiento en los procedimientos y operativas propias de los sistemas de IFEMA.

Las tareas realizadas por este gestor para gestionar el servicio no serán objeto de facturación, ya que se considerarán incluidas en el coste horario de los técnicos que prestarán el servicio. Es decir, el adjudicatario debe incorporar el coste de la gestión en el precio de las tarifas de los técnicos. En general, se estima que un máximo del 5% del tiempo imputado en la resolución de las incidencias y peticiones, corresponde a la gestión de la misma por parte del Gestor del Servicio.

10. GARANTÍA DE LOS TRABAJOS Y TITULARIDAD

10.1. Garantía de los trabajos

Con independencia de la duración prevista en el contrato, el proveedor debe a IFEMA, 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.

10.2. Titularidad

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.

11. VISITA A LAS INSTALACIONES DE LOS OFERTANTES

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

12. DOCUMENTACIÓN TÉCNICA A ENTREGAR POR EL OFERTANTE SOBRE Nº2

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 de concretar su propuesta para el servicio solicitado. Esta documentación deberá ser descriptiva, exacta, pertinente, breve y concisa, abarcando los elementos de la solución propuesta.

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

La información a incluir en este sobre, , NO DEBERÁ EXTENDERSE EN MÁS DE 25 PÁGINAS y deberá seguir estrictamente el guion indicado a continuación

1.- Índice

2.- Organización, equipo y gestión del servicio

- Planteamiento general del servicio
- Organización de los trabajos y actividades
- Descripción detallada de la infraestructura de comunicación y modo de conexión
- Descripción de la gestión del servicio
- Descripción detallada y estructura del equipo de soporte para ciberseguridad

- Descripción detallada de las instalaciones del proveedor

3.- Metodología en la prestación de los servicios

- Descripción de los procedimientos de trabajo
- Uso de herramienta de soporte y su adecuación a la prestación del servicio.
- Gestión e interconexión con el SOC (Centro de Operaciones de Seguridad)
- Descripción de sondas y herramientas de análisis de eventos de seguridad destinadas para el servicio.

4.- Plan de Garantía de Calidad

* Medidas dispuestas por el oferente para asegurar la calidad de los trabajos: medios materiales, seguridad y confidencialidad
* Medidas dispuestas por el oferente para vigilar y garantizar el adecuado cumplimiento del contrato

5.- Seguridad

- Descripción de las medidas de seguridad que se adaptarán para la prestación del servicio: VPN, aislamiento de la red con acceso a IFEMA del resto de la red del proveedor, procedimiento de contingencia, etc.

6.- Otra documentación

Otra documentación que el ofertante considere de interés,