Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Suministro de software y licencias Web Application Firewall (WAF) para la Red Corporativa Administrativa (RCA)

Especificaciones de compra / Pliego de condiciones técnicas

Septiembre 2021

Mediterráneo, 14 • 01010 Vitoria-Gasteiz • Posta-kutxatila / Apartado: 809 • 01080 Vitoria-Gasteiz • Tel. 945 01 73 00* • Fax. 945 01 73 01 • www.ejie.eus

Este documento es propiedad de Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, S.A. (EJIE). Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de EJIE. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. EJIE no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.

Versión	Fecha	Resumen de cambios	Elaborado por:	Aprobado por:
1.0	20/09/2021	Versión Inicial	Josu Bagazgoitia	Aritza Iratzagorria

Índice

Contenido

1 Introducción 4
1.1 Perfil de la compañía 4
1.2 Situación actual y necesidad 5
2 Alcance y objeto del contrato 6
2.1 Objeto de la contratación 6
2.2 Descripción del escenario previsto 6
2.3 Requisitos técnicos de los suministros 6
2.4 Justificación cumplimiento de requisitos solicitados 9
2.5 Garantía y soporte del fabricante 9
2.6 Otros servicios de mantenimiento 9
2.6.1 Alcance no incluido 10
3 Requerimientos del servicio 11
3.1 Acuerdos de nivel de servicio 11
3.1.1 Mantenimiento correctivo. Acuerdos de nivel de servicio 11
3.1.2 Mantenimiento preventivo. Acuerdos de nivel de servicio 12
3.1.3 Equipo de trabajo para la ejecución del proyecto 12
3.2 Otros requisitos asociados a la prestación del servicio 12
3.2.1 Medios técnicos y herramientas de apoyo al servicio 12

1 Introducción

1.1 Perfil de la compañía

EJIE, Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, es la Empresa pública de servicios de las tecnologías de la información y las comunicaciones (TIC), cuya razón de existir es contribuir a la consecución de un Sector Público Vasco, moderno y eficiente, en el Marco Legal establecido por el Gobierno, con la seguridad y calidad necesarias y con el debido respeto al medio ambiente.

EJIE tiene como meta final la consecución de la satisfacción de sus clientes, siendo el instrumento común de prestación de servicios TIC en el Sector Público Vasco, y comprometiéndose en:

- Construir y mantener con eficiencia y calidad la infraestructura de los Sistemas de Información, posibilitando su continuidad y seguridad.
- Garantizar la interoperabilidad entre las distintas administraciones.
- Servir de apoyo a las necesidades de planificación y realización de la función informática de los Departamentos y Organismos Autónomos del Gobierno, asegurando la cobertura de sus demandas con el compromiso y profesionalidad adecuados a las relaciones contractuales que se establezcan.

Por tanto, EJIE debe ser, un instrumento común de referencia para la prestación de servicios TIC en el Sector Público Vasco:

- Aportando valor añadido.
- Proporcionando soluciones competitivas.
- Transmitiendo confianza a sus clientes.
- Contando con personas cualificadas y comprometidas.

Se puede obtener información más detallada y extensa en nuestra dirección de Internet http://www.ejie.eus.

En el Consejo de Gobierno de 14 de enero de 2014, el Consejero de Hacienda y Finanzas informó de una iniciativa departamental consistente en el inicio de un proyecto de estudio y análisis de las oportunidades de mejora derivadas del proceso de convergencia en materia de Tecnologías de la Información y de la Comunicación (TIC) en el seno de la Administración Pública y el sector público de la Comunidad Autónoma de Euskadi.

La labor consistía en definir un nuevo modelo basado en el análisis detallado de la situación actual de prestación de servicios en materia de Tecnologías de la Información y de la Comunicación (TIC) en el seno de la Administración Pública y el sector público de la Comunidad Autónoma de Euskadi, comprendiendo la Red Corporativa Administrativa del Gobierno Vasco y las Redes Sectoriales, así como cualquier otra infraestructura informática y de comunicaciones utilizada por las entidades del sector público de la Comunidad Autónoma de Euskadi.

La propuesta elaborada fue aprobada en Consejo de Gobierno de 27 de Julio de 2015, instando a llevar a cabo un proceso de convergencia en materia TIC en principio circunscrito a las infraestructuras y elementos anexos (Infraestructuras, Comunicaciones, Puesto de Trabajo y Servicios Corporativos Unificados), proponía una metodología y gobernanza de trabajo para la implementación del nuevo modelo de convergencia TIC-ICPS articulado a través de EJIE.

En Consejo de Gobierno de 21 de junio de 2016 se aprueba el documento ejecutivo «Plan General de actuación en materia de Convergencia» y se autoriza la implementación del proceso de convergencia, consistente en la puesta en marcha desde EJIE como órgano gestor de un Catálogo de Servicios ICPS a ofrecer a los Entes y Redes del Sector Público vasco, e implementar de forma paulatina.

1.2 Situación actual y necesidad

Este proyecto se enmarca en el contexto presente de ciberataques a webs de instituciones públicas y la repercusión que un ciberataque tiene de cara al ciudadano, al servicio y el impacto económico generado.

La Red Corporativa Administrativa de Gobierno Vasco, en adelante RCA, gestiona una serie de aplicaciones web que cuelgan de los dominios de Gobierno. Estas aplicaciones en la actualidad necesitan de una protección perimetral, dado que se encuentran publicadas en Internet, con acceso desde el exterior y desde la propia Red Corporativa. Además, dan servicio ciudadano y a las propias instituciones públicas. Para ello se ha decidido recurrir a un cortafuegos de aplicaciones web: Web Application Firewall, en adelante WAF.

Un WAF es un elemento intermedio entre las aplicaciones web y los usuarios, que es capaz de detectar ataques a vulnerabilidades conocidas o desconocidas. Analiza todas las comunicaciones antes de que lleguen al servidor web o al usuario y en función de las amenazas detectadas permite desencadenar diferentes acciones para proteger tanto el nivel de aplicación web como el del usuario que consume las aplicaciones.

Todo tráfico malicioso será bloqueado por el WAF y el servidor recibirá sólo tráfico legítimo. Un WAF está situado entre el usuario y la propia aplicación y puede ser un dispositivo hardware o software. En el caso de RCA, este firewall se va a soportar sobre la infraestructura de VMware del CPD de EJIE dotándonos de escalabilidad y una alta disponibilidad, en adelante HA (high availability).

Este tipo de implementación, virtualizada y en las instalaciones de cliente ofrece un mayor control, escalabilidad, flexibilidad y capacidad de aplicar una seguridad más avanzada. Permite a su vez, aplicar protección en aplicaciones Web cuyos servidores están en instalaciones de RCA y EJIE, estén o no publicadas en Internet.

El WAF deberá soportar funciones globales intrínsecas a la protección web de aplicaciones y usuarios:

- Despliegue en modo sencillo de autoaprendizaje.
- Amplio soporte WAF.
- Capacidades de reporte y análisis.
- HA y escalabilidad.
- Soporte e integración con APIs estándar.

Por otro lado, deberá soportar igualmente funciones para la gestión del tráfico inteligente y balanceo de carga de capa 7.

De cara a la integración del WAF para la protección de las aplicaciones web de RCA que cuelgan de los dominios de Gobierno gestionados por RCA, se plantea, por tanto, y a través del siguiente expediente las siguientes necesidades:

- El suministro del software y de 2 licencias en modo subscripción para la instalación de 2 firewall con soporte HA para aplicaciones web sobre un entono virtualizado.
- El hypervisor requerido es VMware por ser la plataforma en uso y estandarizada en el CPD de EJIE.
- Se demanda un modo de licenciamiento por caudal nominal sin límite de aplicaciones y/o FQDNS. En este caso se requiere de 1 Gbps para cubrir las necesidades del conjunto de aplicaciones web bajo los dominios de Gobierno gestionados por RCA.
- Además, se necesita de funcionalidad de gestión del tráfico inteligente y balanceo de carga de capa 7.
- Estas licencias deben acompañarse de un soporte 24x7 de fabricante hasta el 31/12/2022 desde la entrega de las mismas, tras la formalización del contrato.
- Se solicita un servicio de mantenimiento adicional de nivel 3 hasta el 31/12/2022 de acuerdo a los requisitos establecidos en el presente documento (detalle en el apartado 2.6).

2 Alcance y objeto del contrato

2.1 Objeto de la contratación

El objeto del presente Pliego de Condiciones Técnicas es, atendiendo al escenario y requisitos descritos, la contratación de los siguientes suministros y servicios:

CONCEPTO	CANTIDAD
Suministro de software y licencias de subscripción por throughput nominal de 1 Gbps para WAF sin límite de aplicaciones/fqdns, virtualizadas sobre Plataforma VMware y con soporte HA, con funcionalidades de gestión del tráfico inteligente y balanceo de carga de capa 7 con soporte 24x7 de fabricante hasta el 31/12/2022. (*estimado 14 meses)	2
Servicios de mantenimiento adicionales de nivel 3 hasta 31/12/2022, de acuerdo al alcance de servicio expuesto en el presente documento. (*estimado 14 meses)	1

El licitador deberá ofertar el precio para los suministros y servicios solicitados de la anterior tabla, de acuerdo al Modelo Económico incluido en el Anexo I del PCP

Todas licencias y soportes de fabricante asociados deberán ser oficiales y estar garantizadas por el fabricante.

2.2 Descripción del escenario previsto

Con relación a la plataforma la infraestructura y los parámetros previstos sobre los que se va a construir el servicio se establece lo siguiente:

- Entorno de virtualización VMware (entorno actual que se utiliza en EJIE).
- Throughput nominal previsto de 1 Gbps.
- Se requieren 2 licencias para funcionamiento en HA.
- Se contempla además que las licencias y software soporten la escalabilidad a más de 2 equipos para cubrir crecimientos futuros.
- Además, existirá un mecanismo en caso de caída del CPD principal por el cual se moverán las máquinas virtuales del WAF al CPD de Disaster Recovery (DR) de Erandio.
- Se requiere de licencias sin límite de fqdns para disponer de una solución escalable que no impacte y permita abordar escenarios de diversificación.

2.3 Requisitos técnicos de los suministros

Se enumeran una serie de características para las licencias que se requieren para la puesta en marcha de este servicio. Por lo tanto, la solución propuesta debe cumplir con los siguientes requisitos:

- Servicio disponible en máquina virtual VMware (CPD de EJIE).
- Alta disponibilidad, tanto en activo-activo como en activo-pasivo (opción de escalabilidad a más de 2 equipos en función de necesidades futuras)
- Defensa contra las 10 principales vulnerabilidades según OWASP (Open Web Application Security Project).
    - Errores de inyección, particularmente inyección de SQL

  - Inyección de comandos de OS, LDAP y XPath y otros errores de inyección
  - Desbordamiento de buffer (Buffer overflows)
  - Almacenamiento Criptográfico Inseguro
  - Canales [de comunicaciones] inseguros
  - Manejo incorrecto de errores
  - Cross-Site Scripting (XSS)
  - Cross-Site Request Forgery (CSRF)
  - Autenticación y administración de sesión interrumpidas
  - Control de acceso incorrecto (referencias no seguras a objetos directos, fallas en la restricción de acceso a URL).
- Posibilidad de restringir cada uno de los siguientes parámetros:
  - Protocolo y versión utilizada
  - Longitud del método de request
  - Longitud del URI solicitado
  - Número de cabeceras (headers)
  - Longitud del nombre de las cabeceras
  - Longitud del valor de las cabeceras
  - Longitud del cuerpo (body) de la solicitud
  - Longitud del nombre y el valor de las cookies
  - Número de cookies
  - Longitud del nombre y valor de los parámetros
  - Número de parámetros
- Firmas nativas para tecnologías de servidor de mercado.
- Creación de firmas personalizadas.
- Soporte para creación automática de políticas, incluyendo políticas basadas en wildcards con múltiples URLS.
- Firmas de ataques con actualización automática.
- Machine learning.
- Aprendizaje automático de aplicaciones.
- Aceleración de servicios mediante técnicas de caching, multiplexación TCP, reutilización de conexiones, gestión de ancho de banda y aplicación de perfiles TCP optimizados.
- Opción de alimentarse de una base de datos reputación de IPs (aunque sea susceptible de activarse a futuro) que permita bloquear tráfico desde y hacia direcciones IP en categorías como: scanners, Windows exploits, denial of services, proxies de phishing, botnets, proxies anónimos
- Protección DDoS (ataques de DDoS a nivel de aplicación), Mitigación Bot, Mitigación APT
- Validación de Protocolo - cumplimiento RFC HTTP.
- Soporte a modificación de la cabecera y contenido en el payload (función de Proxy inverso), sin necesidad de utilizar terceros equipos ni adquisición de licencias adicionales. Soporte de reescritura de URL y URI incluidas en el GUI de configuración.
- Inspección SSL/TLS
- Posibilidad de modo bloqueo o simulación por aplicación
- Módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones web: latencias y throughput hacia los servidores, latencias en los URLs

- Política de seguridad para API mediante una configuración guiada e importación de un archivo swagger y OpenAPI
- Creación y despliegue de políticas de seguridad, protección antiBots y protección frente a denegación de servicio mediante wizards
- Personalización de las páginas de bloqueo con capacidad de responder a webservices mediante un código HTTP 500.
- Validación de URL-encoded characters
- Mecanismos de identificación y protección avanzados:
  - Escáneres
  - CRAWLERS (programa que analiza los documentos de los sitios web de forma automática)
  - CREDENTIAL STUFFING (inyección automatizada de pares de usuario/contraseña para obtener acceso fraudulentamente a las cuentas de usuarios)
  - Generación de firmas dinámicas de capa 7 en tiempo real para la mitigación de ataques de DDoS incluyendo detección dinámica de latencias del servidor
  - Soporte de análisis de comportamiento para la mitigación de DDoS de nivel 7 en un número ilimitado de servicios
  - Protección frente ataques de DDoS en la negociación de TLS mediante fingerprinting del stack TLS presentado por el cliente
  - Protección mediante cifrado de los campos sensibles de las aplicaciones web en el navegador cliente
  - Garantía de integridad de datos, detectando al menos la manipulación de parámetros en URLs y peticiones AJAX
  - Protección anti-bot con mecanismos de captcha y challenge de javascript para detección e identificación de navegadores y comportamiento de usuario
  - Protección frente a Web Scraping
  - Identificación de URLs con gran consumo en los servidores como vector de ataque de DDoS
  - Verificación de las firmas de ataque en las respuestas del servidor al usuario
  - Enmascaramiento de información sensible enviada por el servidor
  - Bloqueo basado en la ubicación geográfica (base de datos de geolocalización incluida)
  - Descarte de paquetes de una IP sospechosa una vez detectado un ataque
  - Verificaciones de seguridad y validación en protocolos FTP y SMTP
  - Protección a Web Services XML y restricción al acceso mediante métodos definidos vía Web Services Description Language (WSDL)
  - Soporte para prevenir exponer el “OS fingerprinting”
  - Soporte de tecnologías AJAX y JSON
- Gestión.
  - Posibilidad de delegar la administración de forma granular por grupos y usuarios
  - Acceso a la consola con autentificación en AD, LDAP, radius u otros sistemas de gestión de identidades.
  - Interfaz gráfica con dashboard personalizable que permita monitorizar el estado del equipo en tiempo real.
  - Administración de las políticas de seguridad mediante una API.
  - Posibilidad de captura de tráfico con tcpdump en caso de ataque
  - Mecanismos de auditoría de cambios
  - Garantizar la disponibilidad y el buen rendimiento de la aplicación incluso en caso de ataque
  - Integración con SIEM y/o recolectores de Log
  - Integración con SNMP versión.2.0 o superior

- Envío de Alertas (snmp, correo).
- Disponibilidad de REST API para automatización de procesos.

2.4 Justificación cumplimiento de requisitos solicitados

El licitador deberá presentar una descripción detallada de las características de las licencias ofertadas y de forma particular completar la tabla que se adjunta como Anexo XV del PCP como parte del Sobre A, adjuntando la documentación oficial del fabricante que acredite el cumplimiento de las características técnicas y funcionalidades mínimas exigidas en el presente capítulo y haciendo referencia a los puntos correspondientes donde se localice la información de interés.

2.5 Garantía y soporte del fabricante

La empresa adjudicataria deberá incluir junto con los suministros, la garantía y soporte de fabricante de acuerdo a las siguientes condiciones:

- Todas las licencias objeto de suministro deberán disponer de garantía de fabricante hasta el 31/12/2022.
- Se incluye el software necesario para garantizar las diferentes funcionalidades y tecnologías solicitadas, incluyendo el soporte de fabricante hasta el 31/12/2022 desde su entrega, tras la formalización del contrato.
- El soporte de fabricante debe incluir, sin coste adicional, el acceso a las actualizaciones de parches, alertas de seguridad, y nuevas versiones de software durante el periodo de garantía. El suministro de la actualización incluirá tanto las licencias y software como los manuales y la documentación técnica del fabricante asociado.
- El soporte de fabricante será en modalidad 24x7.

Los licitadores deberán presentar justificación de cumplimiento de garantías solicitadas para el suministro, mediante declaración responsable correspondiente (modelo Anexo VIII del PCP), de acuerdo a las condiciones establecidas en el PCP.

2.6 Otros servicios de mantenimiento

Además del servicio propio del fabricante, durante el periodo de garantía ofertado, el contratista adjudicatario se responsabilizará de servicios de mantenimiento adicionales de tercer nivel.

EJIE dispone de soportes adicionales denominados de segundo nivel que serán los encargados de interactuar con el contratista adjudicatario para la prestación de los servicios solicitados, y facilitar el acceso a los equipos requeridos en el ámbito del contrato (caso de que aplique para el desarrollo de sus funciones). El acceso será siempre a través de estos soportes de segundo nivel no existiendo accesos remotos permanentes.

A continuación, se describe el alcance de los servicios solicitados al contratista adjudicatario como parte de los servicios de mantenimiento de tercer nivel.

- Servicio de mantenimiento correctivo para la resolución de incidencias (in situ o en remoto) generadas por problemas o mal funcionamiento del software incluido en contrato, incluyendo las tareas necesarias hasta conseguir la restauración del servicio y otras asociadas a la gestión de incidencias y mejora continua, como pueden ser:

  - Coordinación con los grupos de soporte y resto de proveedores que conforman la solución.
  - Administración de los sistemas objeto del contrato y de los servicios ofrecidos a través de estos sistemas.

- Instalación de software por fallo, vulnerabilidades publicadas, necesidad de actualización detectada en el mantenimiento preventivo o por indicación del fabricante.
- Pruebas para verificación de la reposición del servicio.
- Escalado a fabricante.
- Soporte técnico avanzado propio y soporte especializado experto de fabricante en el ámbito de la incidencia.
- Registro, seguimiento y documentación de la incidencia hasta su resolución.
- Elaboración de informes o partes de intervención o incidencias, a petición de EJIE.

- Servicio de mantenimiento preventivo. A partir de inspecciones y/o mediciones periódicas (como mínimo 2 anuales) se realizarán propuestas orientadas a mejorar el rendimiento y/o disponibilidad del servicio. Se incluye la propuesta de la línea base de monitorización para una detección temprana de problemas, el análisis de las versiones software buscando el reducir el número de incidencias a futuro en la red, obsolescencia tecnológica y fechas de fin de vida, y el health check de la infraestructura para revisar la salud y configuraciones.
- Elaboración de informes mensuales de servicio y estadísticas de incidencias. Se realizarán informes mensuales que reflejen el detalle de los servicios prestados en ese periodo, indicándose al menos datos relativos a incidencias ocurridas, causa de las incidencias, tiempos de respuesta, tiempos de resolución, tareas y/o peticiones cursadas como pueden ser la configuración y optimización de los sistemas, revisión de las vulnerabilidades publicadas en ese periodo… con identificación del cumplimiento o incumplimiento de los niveles de servicio comprometidos. Asimismo, si se considera oportuno, se podrán poner a disposición de EJIE herramientas que faciliten el seguimiento de las incidencias y la monitorización de los niveles de servicio vía Web.
- Alta de las garantías del software y de la suscripción de las licencias. Se darán de alta las garantías del software y la suscripción de las licencias objeto de contrato hasta el periodo de validez del contrato indicado. Todas las altas y mantenimientos deberán ser oficiales y estar garantizadas por el fabricante.
- Asunción de evoluciones sobre la misma plataforma. Si durante la vigencia del contrato, se decidiera actualizar o evolucionar los servicios existentes, el adjudicatario deberá asumir el mantenimiento de esas posibles evoluciones sobre la misma plataforma objeto del presente contrato.
- Intervenciones planificadas. Las operaciones y asistencias que requieran los servicios descritos, por ejemplo, la parada de algún elemento que conforma la plataforma o de alguno de los servicios que presta, se planificarán de acuerdo con el personal técnico de EJIE en un horario convenido y que menos afecte al funcionamiento de dichos servicios.
- Estadísticas de uso de la plataforma. EJIE podrá solicitar al adjudicatario la elaboración de un informe con toda la información relativa al servicio que la plataforma presta. EJIE validará y podrá a su vez requerir la inclusión de más información en el citado informe.
- Servicio de soporte técnico experto, abierto a las necesidades de EJIE en consultas de soporte y en el ámbito de las tecnologías especificadas y horarios de atención solicitados.

2.6.1 Alcance no incluido

No forman parte del alcance del presente contrato los siguientes conceptos:

- La instalación y configuración de las licencias y software objeto del suministro, que será realizado por los equipos de Soporte de EJIE.
- La infraestructura sobre la que las licencias y software objeto del suministro van a instalarse y configurarse, —infraestructura de virtualización VMware—, que será provista por EJIE.

3 Requerimientos del servicio

3.1 Acuerdos de nivel de servicio

En los siguientes capítulos se describen los acuerdos de nivel de servicio que deberá de prestar el adjudicatario del expediente. En caso de incumplimiento, se aplicarían las penalizaciones correspondientes descritas en el PCP.

Asimismo, y de acuerdo a lo especificado en capítulos previos, el adjudicatario deberá presentar informes mensuales de servicio con el objetivo de valorar el correcto cumplimiento de los SLAs acordados.

3.1.1 Mantenimiento correctivo. Acuerdos de nivel de servicio

El adjudicatario proporcionará soporte técnico avanzado con técnicos cualificados y soporte especializado experto de fabricante a través de los canales habituales: correo, web, teléfono y presencial. Cumplimentar el apartado “medios materiales” del Anexo II incluido en el pliego de condiciones particulares con la información relativa al flujo y canales de comunicación.

Durante el periodo objeto de contratación, el adjudicatario se comprometerá a ser el punto de contacto para atender cualquier tipo de incidencia o consulta técnica que pueda surgir en el ámbito del contrato y actuar como intermediario en el escalado al soporte técnico especializado experto de fabricante, es decir, asumir labores de gestión, coordinación e interlocución con los soportes adicionales con los que EJIE cuenta y/o a su vez con el fabricante en el caso de incidencias, actualizaciones de software, consultas y demás circunstancias posibles.

A continuación, se especifican diferentes niveles de servicio requeridos en la prestación del servicio de mantenimiento correctivo:

- Horario de prestación del servicio: 24x7. El adjudicatario deberá disponer tanto de un soporte propio 24x7 como del mantenimiento necesario con el fabricante. Se deberá acreditar la disposición de ambos servicios y que los perfiles profesionales asignados tengan autorización en la apertura de incidentes directamente con el fabricante.

Se deben cumplir los siguientes tiempos de respuesta y resolución según la siguiente clasificación:

- Críticas y graves: incidencias que impidan o degraden el uso del servicio, resultando en incidencias por parte del usuario final.
- Leves: incidencias que no impiden el funcionamiento del servicio, pero que degradan su uso de manera leve, sin suponer incidencias de usuario final.
- Consultas: consultas técnicas en el ámbito de las tecnologías especificadas.

La siguiente tabla muestra los tiempos máximos a cumplir por el adjudicatario:

	Críticas y graves	**Leves**	**Consultas**
Tiempos de respuesta	15 minutos	15 minutos	-
Tiempos de resolución	4 horas (restauración servicio)	24 horas	96 horas

Con el fin de cumplir los acuerdos de nivel de servicio, el adjudicatario dispondrá de los acuerdos y contratos de soporte y mantenimiento necesarios con el fabricante.

La notificación de las diferentes incidencias al adjudicatario correspondiente se realizará por personal de EJIE o por los soportes con los que EJIE cuenta. Teniendo en cuenta lo anterior, se definen los siguientes conceptos:

- Tiempo de respuesta: tiempo transcurrido desde la comunicación de la incidencia hasta el inicio de las actividades encaminadas a su resolución.
- Tiempo de resolución: tiempo transcurrido desde la comunicación de la incidencia hasta el restablecimiento del servicio.

En cualquier caso, deberán entregarse informes mensuales de servicio y cumplimiento de SLAs.

3.1.2 Mantenimiento preventivo. Acuerdos de nivel de servicio

A continuación, se indican los requisitos relativos a los acuerdos de nivel de servicio en el mantenimiento preventivo que serán de aplicación en el presente expediente

El licitador a partir de inspecciones y/o mediciones periódicas (como mínimo 2 anuales) debe realizar propuestas orientadas a mejorar el rendimiento y/o disponibilidad del servicio, incluyendo:

- Propuesta de la línea base de monitorización para una detección temprana de problemas.
- Análisis de las versiones software buscando el reducir el número de incidencias a futuro en la red.
- Obsolescencia tecnológica y fechas de fin de vida
- Health check de la infraestructura para revisar la salud y configuraciones, aplicación de las best practices y las recomendaciones particularizadas a nuestro entorno.

En los informes preventivos, como mínimo dos, uno a final del primer trimestre y otro a final del tercer trimestre, deben de reflejarse las acciones sobre el hardware /software que se consideren necesarias:

- Propuesta.
- Ventajas/inconvenientes de la migración.
- Inconvenientes de la no migración.
- Estimación de esfuerzo e impacto sobre el servicio.
- Observaciones si las hubiera.

3.1.3 Equipo de trabajo para la ejecución del proyecto

El adjudicatario pondrá a disposición el personal técnico adecuado con la preparación y experiencia necesarias, con el dimensionamiento y dedicaciones requeridas, para llevar a cabo las tareas demandadas para la ejecución del contrato y poder cumplir con los niveles de servicio establecidos.

Dichos perfiles y su descripción deberán reflejarse en el Anexo II del PCP (Anexo de Adscripción de Medios), en aquellos casos en que así se solicite de acuerdo a requisitos de solvencia técnica.

3.2 Otros requisitos asociados a la prestación del servicio

3.2.1 Medios técnicos y herramientas de apoyo al servicio

Todo el material técnico necesario para posibilitar la prestación del servicio, de acuerdo al alcance y requisitos solicitados, será responsabilidad del adjudicatario, quedando EJIE exento de cualquier obligación de suministrar dichos elementos.
No obstante, en caso de que EJIE así lo solicite, el adjudicatario deberá hacer uso de aquellas herramientas y medios técnicos dispuestos por EJIE en la prestación y gestión del servicio (sistemas para registro y seguimiento de incidencias, acceso a informes on-line, gestión de inventario…).