Abadiño
Elizateko Udala

Informatika
Informática

SERVICIOS DE GOBIERNO IT, MANTENIMIENTO Y GESTION DE LA INFRAESTRUCTURA INFORMATICA Y TECNOLOGICA DEL AYUNTAMIENTO DE LA ANTEIGLESIA DE ABADIÑO

Abadiño
Elizateko Udala
Informatika
Informática

INDICE

Contenido

1.- OBJETO DEL CONTRATO 3
2.- ALCANCE DEL CONTRATO 3
3.- DEFINICIONES Y CONCEPTOS DE LOS SERVICIOS A REALIZAR 4
4.- FUNCIONES A DESEMPEÑAR 6
4.1.- DataCenter 6
4.2.- Seguridad Perimetral 7
4.3.- Gestión en el Parque de equipos: 8
4.4.- Gestión en el Parque de Equipos Multifunción 8
4.5.- Gestión de las Comunicaciones entre edificios y/o salida de internet. 8
4.6- Gestión Parque Wifi Privado y Público 9
4.7.- Mantenimiento preventivo 9
5.- GOBERNANZA IT. ASISTENCIA TÉCNICA A PROYECTOS Y TAREAS DE EVOLUCIÓN TECNOLÓGICA 10
6.- CENTRO DE ATENCIO DE USUARIOS. CAU 10
6.1.- Resolución de Incidencias. 11
6.2.- Horario de Servicio 12
6.3.- Control de Infraestructuras 12
7.- SEGUIMIENTO DEL SERVICIO. 12
8.- CAMBIOS EN LA COMPOSICION DEL EQUIPO 13
9.- ACUERDO DE NIVEL DE SERVICIO. ANS. 13
10.- MEDIOS TÉCNICOS 14
11.- FASES DE EJECUCION 15
11.1.- Traspaso del Conocimiento. 15
11.2.- Fase de Transición 15
11.3.- Fase de explotación del Servicio. 15
12.- ACCESO A LA INFORMACION NECESARIA PARA LA ELABORACION DE LA OFERTA 17
13.- PROPIEDAD INTELECTUAL Y CONFIDENCIALIDAD 17

1.- OBJETO DEL CONTRATO

El objeto de la presente licitación lo constituye la contratación de los servicios de Gobierno IT, mantenimiento y gestión de infraestructura informática del Ayuntamiento de la Anteiglesia de Abadiño[1], conforme a lo previsto en el presente pliego.

Con carácter general el presente contrato comprenderá los siguientes ámbitos:

- Servicios de Gobernanza IT y Gestión del Sistema Informático[2].
- Mantenimiento global de la Infraestructura Informática y Tecnológica.
- Centro de Atención a Usuarios.[3]
- Gestión de Ciberseguridad

2.- ALCANCE DEL CONTRATO

Este servicio de Gobierno IT, Mantenimiento y Gestión de Infraestructura Informática se responsabilizará del correcto funcionamiento de todos y cada uno de los subsistemas[4] que componen la Infraestructura Informática de AEU.

En concreto:

- Servicios de Gobernanza IT.

  La empresa adjudicataria deberá, junto al Responsable de IT de AEU, definir y supervisar las políticas y necesidades de AEU en el área de Sistemas para los próximos 5 años. Éstas podrán ser realineadas, en función de las necesidades de AEU.

  Definir un modelo de Gobierno IT que permita gestionar el Sistema Informático.

  Definir iniciativas tecnológicas en relación a la implantación de nuevos proyectos y nuevas soluciones departamentales.

  Supervisión de los proyectos IT, en los que este inmerso AEU sean o no implementados la empresa adjudicataria.

  Asesorar al Responsable de IT en la definición de iniciativas y búsquedas de soluciones para dar respuesta a las diferentes necesidades corporativas o departamentales que pudieran surgir en AEU.

[1] En adelante AEU.
[2] En adelante SI.
[3] En adelante CAU.
[4] DataCenter, Seguridad Perimetral, Parque de equipos, Parque de Equipos Multifunción e Infraestructura

- Mantenimiento global de la infraestructura informática.

  La empresa adjudicataria deberá realizar un mantenimiento preventivo, correctivo y evolutivo del SI.

- Centro de Atención a Usuarios

  Implantar un CAU y garantizar un Nivel de Servicio[5] a las personas usuarias de las Infraestructuras y Comunicaciones del SI, utilizando herramientas para medir y gobernar dicho servicio.

- Gestión de la Ciberseguridad.

  La empresa adjudicataria del servicio realizará todas aquellas labores que sean necesarias para salvaguardar a AEU de ataques no deseados, inyectando las modificaciones necesarias en los elementos de Seguridad Perimetral para evitarlos.

3.- DEFINICIONES Y CONCEPTOS DE LOS SERVICIOS A REALIZAR

- Se entiende como **Mantenimiento Preventivo** aquellas actuaciones **que se realizan de manera anticipada con el fin de prevenir que surjan averías dentro del Sistema Informático.**
- Se entiende como **Mantenimiento Correctivo** aquellas actuaciones que corrigen los defectos observados en los equipamientos o que se hayan producido en el SI y consiste en localizar averías y/o defectos y corregirlas.
- Se entiende como **Mantenimiento Evolutivo[6]** aquellas actuaciones que modifican y/o mejoran algo que funcionaba o estaba correcto o propongan nuevas soluciones que hayan de licenciar, con el objeto de aumentar, disminuir o cambiar las funcionalidades del sistema, ya sea por las necesidades del usuario, del Sistema o por otras causas como pueden ser, por ejemplo, cambios normativos.
- Se entiende como **actualizaciones de Software**, todos los parches, nuevas releases, nuevas versiones de las cuales se posea licencia de uso activa del software ya existente o que se adquiera durante la ejecución del servicio.
- Se entiende como **software básico corporativo**, todo aquel software necesario para que la persona usuaria del sistema pueda realizar sus labores correctamente (Sistema Operativo, Office 2103, Kaspersky, Papercut[7].)
- Se entiende por **Gestión del Parque de dispositivos móviles**, la detección de incidencias, resolución si ello es posible y/o interlocución con la empresa adjudicataria al amparo del expediente 60/2019 “Servicios de Telecomunicaciones”, integración dentro de la herramienta Ibm MaaS 360.

[5] En adelante ANS.
[6] Se excluye de esta definición actualizaciones de Software.
[7] Este Software Básico Corporativo, podrá verse alterado en función

- En el concepto de **Infraestructura Informática,** se incluyen los equipos (servidores, Nas, PC's, FW, Switches, ordenadores personales y/o portátiles, tablets, impresoras, Multifunciones, scánners, webcams, lectores, grabadoras y regrabadoras, monitores, discos duros externos, cámaras digitales, memorias USB, tarjetas USB/PCI/PCMCIA, smartphones, y resto de periféricos y/o accesorios) con garantía en vigor, así como aquellos con garantía vencida.
- Se entiende por **tiempo de respuesta** el plazo transcurrido desde la comunicación de una incidencia hasta el momento en que un técnico de la empresa adjudicataria se pone en contacto con el usuario, personándose en las propias instalaciones para resolverla o por control remoto cuando pueda resolverse así la incidencia. Dado que la mayoría de las herramientas informáticas disponen de un envío de respuestas automáticas, no se considerará la apertura de incidencia como tiempo de respuesta.
- Se entiende por **tiempo de resolución** el plazo transcurrido desde el comienzo del tiempo de respuesta y la aceptación de la resolución de la misma.
- Se entiende por **Gestión de Garantías** de aquellos equipos que la tengan, que la empresa adjudicataria asumirá la gestión de las incidencias de estos equipos con el fabricante del equipo informático, desde la apertura de la incidencia, supervisión y ejecución de las posibles soluciones facilitadas por éste. La **Gestión de Garantías** supondrá hacer los traslados que fueran precisos a nuestras dependencias y realizar el seguimiento de la resolución de la incidencia. Todo ello se llevará a cabo de tal manera que se pueda controlar el nivel de servicios prestados por el emisor de la garantía y determinar, en caso de eventuales incumplimientos, la responsabilidad de cada una de las partes. Una vez caducada la garantía de fabricante la empresa adjudicataria del servicio asumirá la gestión del mismo.
- En el concepto **Gobernanza de IT** se entiende la realización de análisis de cualquier tipología IT y soluciones en los Sistemas IT, de manera que la empresa adjudicataria trace un correcto plan de implantación, proyecto y gestión que dé solución a la llegada nuevas necesidades o peticiones en el ámbito de IT. Dentro de este apartado se incluye las oportunidades de mejora, análisis de requerimientos y supervisión de la puesta en marcha del proyecto hasta su correcta finalización. En este apartado se incluye todas las labores de consultoría necesarias para la correcta ejecución del mismo.
- El mantenimiento tanto preventivo como correctivo serán ejecutados, **de modo prioritario**, por medios remotos, si esto no fuera posible se ejecutará con soporte presencial.
- Se entiende por **Incidencia Critica,** aquellas que afecten a equipos que sin su participación produzcan una grave alteración de los procedimientos de trabajo (servidores físicos y virtuales, Almacenamientos, Nas, Seguridad perimetral, Comunicaciones, Impresoras de red). También serán aquellas solicitudes extraordinarias que por su gravedad o gran impacto se consideren críticas por parte del Departamento de IT. Dentro de este a apartado, se considerará a los equipos VIP de AEU.

- Se entiende por **Incidencia Muy Urgente,** aquellas que impidan a un conjunto de trabadores no poder realizar sus funciones de manera ordinaria o que afecten de forma grave al servicio de AEU.
- Se entiende por **Incidencia Urgente,** aquellas que afecta a un departamento, edificios, etc.
- Se entiende por **Incidencia normal**, aquellas que no impidan el cumplimiento de las tareas de ningún trabajador
- Limpieza de archivos temporales y desfragmentación de DD. Cada actuación en un equipo conllevara una limpieza de archivos temporales y una desfragmentación del mismo bien con las herramientas propias del Sistema Operativo o con herramientas de terceros[8].

4.- FUNCIONES A DESEMPEÑAR

La empresa adjudicataria deberá realizar, entre otras, las siguientes funciones[9], atendiendo siempre a la política marcada por el Departamento de IT:

4.1.- DataCenter

- Gestión de personas usuarias (Altas, bajas, Gestión de permisos y accesos)
- Gestión de Ad y Gestión de Unidades Organizativas, Grupos globales, etc.
- Mantenimiento de servicios DNS, etc.
- Coordinación de intervenciones de terceros sobre el SI de AEU.
- Actualización de Sistemas Operativos y Software básico e instalación de nuevas releases y versiones.
- Detección y Resolución de problemas en los servidores tanto físicos como virtuales.
- Mantenimiento de servidores, tanto físicos como virtuales, así como instalación y configuración de tanto nuevos servidores como sean necesarios.[10]
- Activación y/o desactivación del sistema de contingencia en caso de necesidad.
- Mantenimiento de la red y su topología.[11]
- Gestión de la solución de Backup dentro de los límites tecnológicos impuestos por el Departamento de IT y las infraestructuras disponibles.
    - Revisión de Jobs de trabajo tanto de los Backup de gestión como de las políticas de retención.
    - Revisión de la correcta ejecución de los mismos.

[8] Si las herramientas necesitan licencia, éstas correrán cargo de la empresa adjudicataria del Servicio.
[9] Las empresas licitadoras deben ser conocedoras de que las actuaciones incluidas en esta descripción no resultan un listado excluyente, siendo objeto de contrato cualquier otra actuación necesaria para el buen cumplimiento del servicio.

[10] Queda fuera del alcance de este punto el suministro de licencias de Sistemas Operativos, si las hubiere.
[11] En este caso, si los equipos están en garantía se tramitará su resolución con el fabricante.

- Configuración e implementación de nuevos Jobs y/o nuevas políticas de retención en caso de necesidad.
- Restauración de copias de seguridad ante incidentes.
  - Recuperación de ficheros de datos.
  - Recuperación de réplicas.

- Gestión de la solución de Antivirus dentro de los límites tecnológicos impuestos por el Departamento de IT y las infraestructuras disponibles.
  - Actualización de versiones de Consola
  - Actualización de la versión del agente de red
  - Actualización de la aplicación de seguridad.
- Mantenimiento y Gestión de la herramienta de Office 365 y su proceso de implantación en la operativa diaria, en Pc, Smartphone, Tablet, etc.
  - Aplicación de medidas que venga derivadas de la seguridad y cumplimiento de GDPR
- Apertura y cierre de armarios de comunicaciones.[12]

4.2.- Seguridad Perimetral

- Soporte a la gestión de los sistemas y medidas de seguridad perimetral, configurando, probando, actualizando, corrigiendo y monitorizando los sistemas para detectar actividades o vulnerabilidades que puedan suponer un riesgo para la seguridad de la información, tanto en el entorno del puesto de trabajo, como en el entorno de la infraestructura, de la seguridad perimetral y del parque de dispositivos móviles, y colaborando en la gestión de respuesta ante incidentes de seguridad y elaborando informes de manera periódica sobre el estado de los sistemas.

  - Monitorización de:

    - Estados de Maquina
    - Fallos en el Cluster
    - Estado de las CPU
    - Estado de la memoria
    - Error de Paquetes
    - Sesiones
    - Estado de las interfaces

  - Modificación de

    - Reglas
    - Perfiles

[12] La apertura de armarios de comunicaciones se establecerá con una antelación de 48 horas, en caso contrario, solo corresponderá a la empresa adjudicataria la obligación del cierre de los mismos.

- Actualización de Parches
    - Detección y Corrección de Incidencias
- Creación de Nuevas Vlan
- Integración de Nuevas Sedes

- Aplicación de medidas extraordinarias contra amenazas que desde el SOC de la empresa adjudicataria se estimen como importantes, críticas y generalizadas; como por ejemplo, la definición de reglas genéricas para el bloque de ficheros infectados por Malware, etc.

4.3.- Gestión en el Parque de equipos:

- Instalación, Reinstalación, Configuración y mantenimiento de los endpoints, así como su posible reubicación[13].[14].
- Gestión del Parque de dispositivos móviles.
- Actualización de Sistemas Operativos y Software básico e instalación de nuevas releases y versiones, en coordinación con la política marcada por el Responsable de IT.
- Gestión, atención y resolución de incidencias de cualquier índole, bajo el amparo de este contrato, en el software de las personas usuarias.

4.4.- Gestión en el Parque de Equipos Multifunción

- Detección y Supervisión de problemas del Servicio de Impresión, en caso de incidencia interna así como interlocución previa, seguimiento y personación en el lugar de la incidencia si ello fuera preciso, y control de ANS con la empresa adjudicataria en los servicios de Impresión. Implementación de medidas que sean necesarias para el buen funcionamiento del sistema

4.5.- Gestión de las Comunicaciones entre edificios y/o salida de internet.

- Detección y Supervisión de problemas de comunicaciones, en caso de incidencia interna así como Interlocución previa, si ello fuera necesario, seguimiento y personación en el lugar de la incidencia si ello fuera preciso, y control de ANS con la empresa adjudicataria en los servicios de Telecomunicaciones.

---

[13] Este apartado incluye S. Operativo así como software básico corporativo de AEU.

[14] Si la reinstalación y/o instalación es consecuencia de un mantenimiento evolutivo, ésta operación será considerada fuera de éste pliego y por lo tanto facturable. En ningún caso, se considerará evolutivo la reubicación de endpoints que formen parten en la actualidad de la Infraestructura Informática o que se hayan incorporado a la ejecución de este contrato.

- Seguimiento de planes de implantación de nuevos proyectos de comunicaciones
- Análisis junto a AEU de los informes de emitidos por la empresa adjudicataria del servicio de telecomunicaciones.
- Implementación y gestión de la conexión con otras redes (BizkiaSarea, Jaso, Sara, etc)

4.6- Gestión Parque Wifi Privado y Público

AEU, dispone de dos SSID[15] para la gestión de sus Wifis (Wifi Publica interna y Programa Europeo Wifi4eu)

- Detección, Supervisión y resolución de problemas de comunicaciones en AP´s.[16]
- Seguimiento de planes de implantación de nuevos puntos AP.

4.7.- Mantenimiento preventivo

AEU dispone de un sistema de monitorización continua[17] para la Gestión de los activos más críticos del SI, que la empresa adjudicataria del servicio deberá mantener y explotar, tanto en el Front-Office como en back-office. Los elementos a monitorizar y supervisar serán, entre otros:

- Servidores
- Vm´s
- Nas
- Fw
- Electrónica de Red
- Impresoras de Red.
- Elementos Wifi (pública y Privada)
- Nodos MPLS
- Alarmas de Intrusión.

El resto de funciones dentro del Mantenimiento preventivo serán, entre otras:

- Gestión de actualizaciones y nuevas versiones de software y/o firmware. Siempre que sea recomendado por el fabricante, Ccn-Cert o por las Buenas practicas recomendadas por la empresa adjudicataria.

- Gestión y seguimiento de la realización de copias de seguridad

[15] Esto no excluye que durante la duración del contrato surgan nuevos SSID que haya que implementar y gestionar
[16] De esta resolución se excluyen las incidencias en las líneas de comunicaciones que gestionan los operadores de telecomunicaciones.
[17] Herramienta Centreon IT & Network Monitoring

- Gestión de Solución de antivirus

    - Actualización de versiones de Agente
    - Gestión y análisis de permisos de accesos.
    - Monitorización, supervisión y análisis periódico de los PCs

5.- GOBERNANZA IT. ASISTENCIA TÉCNICA A PROYECTOS Y TAREAS DE EVOLUCIÓN TECNOLÓGICA

El personal adscrito por la empresa adjudicataria participará en proyectos que los responsables del AEU estimen oportuno, siempre y cuando sean actividades relacionadas con el objeto de ese contrato, realizando aquellas tareas que le sean asignadas por el Responsable de IT desde la consultoría previa hasta la supervisión de la ejecución del proyecto. La participación puede corresponder a cualquiera de las fases de un proyecto y siempre dentro de la infraestructura objeto del presente contrato. Los tipos de proyectos en los que podrán participar son:

- Consultoría para detallar la infraestructura o el nuevo servicio.
- Identificación de nuevas líneas de mejora.
- Implantación de nuevos productos o infraestructuras. (requisitos de infraestructura, hardware, redes para que la infraestructura siga rindiendo a un nivel óptimo)
- Estudios de viabilidad y pilotos de nuevos productos o infraestructuras.
- Evolución tecnológica de infraestructuras existentes y migraciones de software.
- Modificaciones de configuración para permitir su crecimiento.
- Migraciones de versión de productos software.
- Seguridad informática tanto física como lógica.

Las empresas licitadoras deben ser conocedoras de que las actuaciones incluidas en esta descripción no resultan un listado excluyente, siendo objeto de contrato cualquier otra actuación necesaria para el buen mantenimiento ordinario de los sistemas microinformáticos similares a los dispuestos en las oficinas de AEU.

6.- CENTRO DE ATENCIO DE USUARIOS. CAU

Todas las incidencias que se generen durante el periodo del servicio se solucionarán de forma preferente de forma telemática.

Este servicio se deberá prestar de forma bilingüe, en las dos lenguas oficiales de la CAPV.

El CAU, será el responsable de centralizar el servicio de atención de AEU, para ello se la aplicarán los diferentes ANS que se detallan más adelante en este mismo pliego.

EL CAU, se responsabilizará entre otras funciones:

- Recepcionar todas las incidencias y peticiones.
- Gestionar las incidencias de forma proactiva.
- Deberá disponer de varios métodos de acceso al mismo. (mail, teléfono, aplicación telemática)
- Servicio técnico remoto y presencial.
- Escalado de incidencias a terceros o a otros servicios adscritos al CAU.
- Notificación a la persona usuaria del sistema y seguimiento de la misma hasta su completa resolución.

Para ello contará con una herramienta, que permita entre otras funcionalidades:

- Deberá poder registrar día, hora, forma de registro y usuario.
- Poder registrar su estado (abierta, en progreso, solucionada, reabierta, cerrada) registrado en momento de cambio de cada uno de los estados.
- Poder clasificar las incidencias por urgencia (Críticas, muy urgentes, urgentes, normales) priorizándose en función de las mismas.
- Poder clasificar las incidencias por tipo de incidencia (actuación mantenimiento correctivo/preventivo, mantenimiento evolutivo, reparación, nuevo suministro)… y por subsistema (comunicaciones, software, hardware, servidores, etc…).
- Poder asignar las incidencias a personas internas de AEU.
- Poder sacar informes del conjunto de las incidencias, en especial para medir los niveles de servicio
- Todas los partes de trabajo y cierres de aviso estarán digitalizados e incorporados en la aplicación de mantenimiento.

6.1.- Resolución de Incidencias.

El servicio se prestará, en todas sus fases, de forma telemática, de forma prioritaria.

Para ello, en una primera fase, la empresa adjudicataria, activará en los equipos que no lo estén el servicio Walk-on-lan. Dejando constancia por escrito de aquellos equipos en los que no sea posible aplicar este servicio.

En el caso que la resolución de la incidencia no sea posible de forma telemática, se asignará a un técnico con los recursos técnicos necesarios para la resolución de la misma de forma presencial.

La empresa adjudicataria será la responsable de la ejecución de todo tipo de pruebas, análisis, etc. que se deba realizar sobre los equipos informáticos, como consecuencia de una incidencia.[18]

[18] En los equipos con garantía y en los equipos que dependan de terceros a través de otros contratos, solo se responsabilizaran de su supervisión y de control de ANS.

La empresa adjudicataria deberá poseer las herramientas necesarias para la sustitución, cambio temporal de hardware, formateo de DD, etc. de los equipos VIP. (Maqueta operativa del sistema, cambio de pc, etc.)

6.2.- Horario de Servicio

El horario de atención, para todos los centros municipales es de Lunes a Viernes de 8:00 a 19:00.

En los centros Abaed01, Abaed02, Abaed06, Abaed08, será necesario, en caso de tener que acudir de forma presencial, establecer una ventana para garantizar el acceso a las instalaciones.

Gestión de Actualizaciones

La empresa adjudicataria del servicio, programará las actualizaciones de parches del Sistema, actualizaciones de Firmware, actualización de nuevas releases, actualización de versiones, actividades de control del sistema de Contingencia, y las demás establecidas en este pliego de forma prioritaria en horario vespertino. Si fuera necesario realizarlo en otro horario se establecerá la intervención con el tiempo necesario para poder dar cuenta de las actuaciones a realizar a las personas usuarias que puedan verse afectadas.

6.3.- Control de Infraestructuras

A la empresa adjudicataria se le facilitaran un juego de tarjetas de identidad que todas las personas que se personen en las instalaciones de AEU deberán portar de forma visible.

Se le facilitará un juego de llaves de los armarios de comunicaciones y una llave electrónica que permitirá el acceso al Datacenter.

7.- SEGUIMIENTO DEL SERVICIO.

El Responsable de Operaciones, el Responsable Comercial mantendrán, al menos, una reunión anual, que se realizará de forma preferente de forma telemática.

Todas las reuniones que sean necesarias, surgidas de este servicio, se realizaran de forma telemática, a través de herramientas corporativas bien de la empresa adjudicataria o de AEU, pudiéndose utilizar para ello las herramientas corporativas de ambas empresas[19].

[19] AEU pondrá a disposición de la empresa adjudicataria una licencia comleta del software de herramienta colaborativa que en ese momento este implementada.

A ella asistirán, de forma excepcional, aquellas personas que se consideren necesarias tanto por parte de la empresa adjudicataria como el Responsable de IT de AEU.

El objetivo de estas reuniones será realizar un seguimiento del servicio. Se realizara una convocatoria previa junto al orden del día de la misma y con posterioridad, se realizará una acta que deberá ser firmado por parte de las dos empresas.

8.- CAMBIOS EN LA COMPOSICION DEL EQUIPO

Para garantizar la solvencia técnica del equipo, la sustitución en la composición del equipo de trabajo requerirá de las siguientes condiciones:

- Solicitud escrita incluyendo mediante justificación detallada y suficiente, explicando el motivo que suscita el cambio, con un mínimo de 15 días antes de que el mismo se haga efectivo.
- Presentación de sustituto con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir, según punto 10 de este mismo pliego.
- Aceptación por escrito del sustituto por parte del Responsable de IT de AEU.
- El traspaso de conocimientos a la persona elegida correrá a cargo de la empresa, estimándose que estas jornadas, no serán facturables a AEU.

En caso de que exista una justificación probada por parte de AEU, en la cual se demuestre el servicio prestado por las personas sujetas a cambio no cumplen con las expectativas descritas en el presente pliego, la empresa adjudicataria procederá al cambio conforme a las condiciones establecidas en dicho punto.

AEU se reserva el derecho de solicitar el cambio de una persona asignada al servicio, debiendo justificar de forma adecuada su solicitud.

9.- ACUERDO DE NIVEL DE SERVICIO. ANS.

El calendario de ANS, se regirá por el calendario laboral de Abadiño.

El tiempo máximo de resolución de incidencias es:

Tipo de Incidencia	Tiempo de Respuesta	Tiempo de Solución
Critica	½ Hora	8 horas
Muy Urgente	½ Hora	12 horas
Urgentes	1 hora	16 horas
Normal	1 Hora	38 horas

Las empresas licitadoras deberán de acreditar la posibilidad de acudir in situ en el plazo máximo de una hora, en horario laboral del AEU, ante cualquier incidencia o petición critica que así lo requiera.

Esta acreditación se realizará con los medios probatorios que estime oportunos. Esta acreditación se entregará con carácter previo a la adjudicación del contrato.

Las incidencias consideradas cítricas y/o muy urgentes, deberán tratarse de forma continuada hasta el restablecimiento del servicio. AEU facilitará el acceso a edificios en horario no laboral para la resolución de las mismas.

10.- MEDIOS TÉCNICOS

Las empresas licitadoras deberán adscribir a este contrato el siguiente equipo mínimo, adscripción que deberá acreditarse en el requerimiento que se haga a la mejor propuesta para que previa a la adjudicación, y como requisito para la misma, se aporte la documentación pertinente:

- Responsable de Operaciones que acredite Certificado de en Gestión de Servicios ITIL con al menos 2 años de experiencia en funciones similares.
- Responsable Comercial.
- Técnico de Sistemas que acredite al menos Certificado en VmWare 6.0 o superior.
- Técnico de Seguridad que acredite al menos uno de ellos:
    - Master en Seguridad de la Información o ciberseguridad.
    - CISM (Certified Information Security Manager)
    - CISA (Certified Information System Auditor)
    - CEH (Certified Ethical Hacker)
    - OSCP (Offensive Security Certified Professional)
    - al menos 3 años de experiencia
- Técnico de Comunicaciones que acredite:
    - Certificación PCNSE Palo Alto Networks Certified Network Security Engineer.
    - al menos tres años de experiencia
- Técnico de campo
    - Con al menos 2 años de experiencia en labores de atención in-situ
    - Certificado Euskera PL1[20]. En caso de no poseerlo será el Servicio de Euskera de AEU quien realizará la correspondiente prueba.[21]

[20] En cumplimiento de la ordenanza municipal sobre el uso del Euskera, la empresa adjudicataria deberá cumplir su artículo 3 ***"… Del mismo modo, las empresas prestadoras de servicios municipales deberán cumplir lo establecido en las leyes generales vigentes y en esta ordenanza en todo lo referente al uso de las lenguas oficiales – y especialmente al uso del euskera – en las relaciones que como consecuencia del servicio municipal prestado surjan con la administración municipal y con la ciudadanía"***

[21] Este certificado logrado en esta prueba NO tendrá ninguna validez fuera del ámbito de esta adjudicación.

11.- FASES DE EJECUCION

11.1.- Traspaso del Conocimiento.

La empresa adjudicataria contará a la firma del contrato, con un informe[22] en formato pptx, vdsx o pdf en el cual constará toda la información referente al SI, en el que constará entre otros:

- Relación de trabajos pendientes de ejecución de la anterior empresa adjudicataria.
- Relación de usuarios
- Listado actualizado del inventario de equipos y del estado de garantías.

11.2.- Fase de Transición

La empresa adjudicataria contará con un plazo de cuatro semanas naturales para abordar una ejecución al 100% de la ejecución del contrato, adoptando todas las medidas y herramientas de índole internas necesarias para la correcta ejecución del contrato.

En un plazo de 5 días hábiles desde la firma del contrato, la empresa adjudicataria deberá hacer entrega de un plan de inicio del servicio que no se podrá alargar en el tiempo más de cuatro semanas naturales.

11.3.- Fase de explotación del Servicio.

La fase de explotación se extenderá durante 59 meses a partir de la finalización de la fase de transición.

Entrega de documentación.

- Informe mensual de incidencias con cumplimiento de ANS por incidencia y mensual acumulado. Entrega junto a punto 30 de la Caratula.
- Informe trimestral de Herramienta de Antivirus
- Informe semestral de simulación de Caída del SI y entrada en funcionamiento del sistema de Contingencia. Semestralmente. (obligatorio una vez al principio del contrato y otra al final del mismo)
- Informe semestral de resultado de Caída de estabilizadores.
- Informe semestral de ocupación de anchos de banda de electrónica de red interna. Incluirá un proyecto anual de mejoras de la red (identificación de carencias, análisis de trafico de aplicaciones, detección de cuellos de botella y propuesta de soluciones)
- Informe semestral de ocupación de anchos de FW y estado de la plataforma. Se propondrán recomendaciones de mejora; tras su elaboración, el técnico agendará una

[22] Este informe será suministrador por AEU

reunión para presentación del mismo y a su finalización, mandará un acta de la misma con las conclusiones y las acciones acordadas y su plan de acción[23].

- Informe anual de Revisión general instalación física de los equipos.
- Informe anual de inventario actualizado.
- Informe anual en aras de implementaciones necesarias para garantizar la seguridad de la información de acuerdo al ENS o normativas de referencia que surjan a lo largo del desarrollo del documento[24].
- Mantenimiento de la documentación técnica operativa en formato vsdx de los sistemas, aportando la información necesaria tanto para poder actualizar los manuales o documentos ante cualquier cambio o evolución o como para diseñar nueva documentación.
- Informe semestral de la revisión del sistema MPLS. Entrada en funcionamiento del Sistema de Contingencia y en supervisión de incidencias hasta su solución.

11.4 Fase Traspaso de conocimiento

Un mes antes de la finalización del contrato, la empresa adjudicataria deberá realizar las siguientes actuaciones:

- Deberá actualizar los sistemas incluyendo los últimos parches, tanto de sistemas como de Agentes de Antivirus, Fw., que en esos momentos estén pendientes de actualización.
- Deberá completar el conjunto de actuaciones de mantenimiento preventivo pendientes.
- Deberá acordar con AEU, el conjunto de actuaciones de mantenimiento evolutivo o similares pendientes que se podrán abordar y cuales finalmente no se podrán acometer.
- Similarmente con los suministros, en caso de existir suministros pendientes, se acordarán cuales serán entregados y cuáles no dentro del plazo de contrato.
- Se entregarán todo material de repuesto y/o complementario que tenga el adjudicatario.
- Igualmente entregará toda información en soporte físico o electrónico que disponga de los sistemas, estos últimos en formato pptx y/o vsdx
- Se entregará un listado con el inventario actualizado, incluyendo marca, modelo, números de serie, vigencia de garantías u otros soportes, versión de software, etc…
- Se entregara un plano actualizado del conjunto del SI y ahí donde sea posible las configuraciones, en formato vsdx.

[23] Este plan de acción puede contemplar acciones fuera del alcance de este pliego. Éstas deberán ser indicadas en el mismo y valoradas económicamente.
[24] Este plan de acción puede contemplar acciones fuera del alcance de este pliego. Éstas deberán ser indicadas en el mismo y valoradas económicamente.

- Desconfigurará todos los accesos externos remotos empleados para la prestación del servicio.

12.- ACCESO A LA INFORMACION NECESARIA PARA LA ELABORACION DE LA OFERTA

Por motivos de seguridad, en este pliego no se incluye referencias técnicas de equipamiento e infraestructuras.

Por tanto, las empresas licitadoras que deseen acceder a la información del SI y para evitar posibles restricciones de movilidad a las que podamos vernos afectados con motivo de la Covid-19, las empresas licitadoras que deseen acceder con más detalle a la estructura del SI, deberán solicitarlo a través de nuestra sede electrónica www.abadiño.org, en la sección de tramites Online.

A éstas empresas se les facilitará la información a través de la firma de un documento de confidencialidad.

A modo de resumen, para que las empresas licitadoras puedan hacerse un escenario:

- Sedes.
  AEU, dispone de 8 sedes a las cuales se da servicio. 4 unidas con Fibra Óptica y 4 con MPLS
- Sistemas Operativos
  - Windows 7 (20)
  - Windows 10 (37)
  - Windows Server 2008, 2012 y 2019
- infraestructura
  - 2 Servidores físicos
  - 15 Servidores virtuales
- Sistema de Copias de Seguridad
  - 1 Nas
- Smartphones
  - 42 smartphones

13.- PROPIEDAD INTELECTUAL Y CONFIDENCIALIDAD

- **Propiedad intelectual de los trabajos**. Toda la documentación, información y herramientas de soporte que se produzcan como resultado del contrato serán de propiedad única y exclusiva de AEU, siendo un secreto irreproducible y no divulgable sin la expresa autorización escrita de su propietario. También se pacta expresamente

que cualquier modificación, o creación por parte del adjudicatario que tenga como base AEU, será propiedad de éste, que podrá utilizarlo, explotarlo y cederlo sin ninguna limitación.

- **Confidencialidad de la información**. La empresa adjudicataria queda expresamente obligada a mantener absoluta confidencialidad y reserva sobre cualquier dato que se pueda conocer con ocasión del cumplimiento del contrato, especialmente las de carácter personal, que no podrá copiar o utilizar con una finalidad diferente a la que figura en este pliego, ni tampoco ceder a otros ni tan solo a efectos de conservación sin la autorización escrita de AEU. Igualmente la empresa adjudicataria se compromete a mantener absoluta confidencialidad y reserva sobre cualquier tipo de documentación e información que se pueda conocer con ocasión del cumplimiento del contrato, que no podrá copiar o utilizar con una finalidad diferente a la que figura en este pliego, ni tampoco ceder a otros ni tan solo a efectos de conservación sin la autorización escrita de AEU.
- La empresa adjudicataria quedará obligada al legislación de protección de datos, especialmente en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos.
- **Seguridad**. La empresa adjudicataria no podrá difundir ningún tipo de código de acceso o cualquier otro tipo de información que pueda facilitar la entrada a los sistemas del AEU, así como a no hacer un uso incorrecto de los permisos y privilegios que se concedan a su personal para la ejecución de este contrato. En tal sentido, el adjudicatario se hará responsable de los perjuicios que se le puedan ocasionar al Ayuntamiento de Abadiño debido al incumplimiento de cualquiera de las condiciones mencionadas.
- Durante la ejecución de los trabajos objeto del contrato el adjudicatario se compromete a facilitar en todo momento, a las personas designadas por el Ayuntamiento de Abadiño para estos efectos, la información y documentación que soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollen los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizadas para solucionarlos.

Abadiño a 28 de abril de 2021.

El Responsable de IT.

Firmado electrónicamente por GORKA ARROYUELOS GOROSTIZA - 15250164Z, el día 28/04/2021 con un certificado emitido por EAEko HAetako langileen CA - CA personal de AAPP vascas (2)