1.- OBJETO DEL CONTRATO.

El Ayuntamiento de Talavera de la Reina dispone en su instalación municipal de equipos de Fortinet encargados de la seguridad de la red.

El contrato tendrá por objeto el suministro de renovación de las licencias de soporte de fabricante y características avanzadas de seguridad necesarias para el equipamiento firewall de fortinet (Fortigate y FortiWEB) y la prestación de servicios profesionales en materia de seguridad de la red, seguridad gestionada compartida, para cualquier aspecto de configuración, instalación, mantenimiento, supervisión y monitorización de los equipos Fortigate y los aspectos relacionados con la seguridad de la red municipal.

2.- EQUIPAMIENTO DE SEGURIDAD DE LA INSTALACIÓN.

El equipamiento que actualmente forma parte de la instalación de seguridad y para el que se tendrá que realizar la renovación anual de las suscripciones con fabricante, es:

- 2 Fortigate 100 D en disposición de alta disponibilidad Activo-Activo, con la siguiente suscripción de licencias:
  - Suscripción Unified UTM de los Fortigate 100D, incluye: Unified (UTM) Protection (24x7) FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud).

- 1 FortiWeb 100D (FWB-100D-BDL)-Virtual appliance for all supported platforms. 1 x vCPU core, con la siguiente suscripción.
  - FC-10-VVM01-935-02-12. FortiWeb-VM01 Standard Bundle (8x5 FortiCare plus AV, FortiWeb Security Service, and IP Reputation)

- 15 AP Wifi Fortinet:
  - 9 FP221B
  - 3 FP221C

3.- SUSCRIPCIÓN DE LICENCIAS

3.1.- Renovación anual

El detalle de licencias a renovar es:

- Suscripción Unified UTM de los 2 Fortigate 100D, incluye: Unified (UTM) Protection (24x7) FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud).
- FC-10-VVM01-935-02-12. FortiWeb-VM01 Standard Bundle (8x5 FortiCare plus AV, FortiWeb Security Service, and IP Reputation)

Las renovaciones serán por cuenta del adjudicatario dentro del importe del contrato y durante la vigencia del mismo. No se podrán repercutir costes adicionales al importe definitivo anual de adjudicación durante el periodo de vigencia del contrato, por lo que las empresas licitadoras tendrán esta circunstancia en cuenta a la hora de elaborar sus propuestas.

4.- PRESTACIÓN DE SERVICIOS PROFESIONALES, SEGURIDAD GESTIONADA COMPARTIDA.

La empresa adjudicataria será la encargada de la correcta configuración y operación de los equipos, de la supervisión, monitorización, gestión de incidencias y peticiones de configuración formuladas por el ayuntamiento. El ayuntamiento por su parte y según un modelo compartido, también podrá acceder a los dispositivos para realizar configuraciones y monitorizar los sistemas pudiendo generar peticiones de asesoramiento si se considera necesario.

Los accesos a los dispositivos por parte de la empresa adjudicataria y por parte del personal técnico del ayuntamiento se realizarán con usuarios diferentes, auditando los accesos y los cambios que se produzcan.

Para la prestación de los servicios, la empresa adjudicataria contará con un servicio de helpdesk, que permita comunicar las incidencias y peticiones. Este servicio estará operativo como mínimo en horario de 8 a 18 horas y permitirá diferentes canales de comunicación: teléfono, correo electrónico y web.

Además del servicio de helpdesk, las empresas licitadoras tendrán que cumplir y acreditar:

- Estar acreditada por Fortinet como partner certificado.
- Disponer al menos de 2 ingenieros certificados en el máximo nivel reconocido por Fortinet.
- Disponer de un centro de control y el personal necesario que permita prestar el servicio de monitorización 24x7x365.

Dentro de los servicios profesionales se distinguen los siguiente casos:

4.1.- Actualizaciones y gestión de incidencias relacionadas con los equipos

Las actualizaciones de los equipos Fortigate y Fortiweb estarán cubiertas y tendrán que ser realizadas por la empresa adjudicataria, siendo la responsable de que los equipos se encuentren permanentemente actualizados con respecto a las recomendaciones del fabricante. En el proceso de actualización de los equipos, la empresa adjudicataria se coordinará con el Servicio de Informática Municipal para elegir el momento más adecuado para aplicar las actualizaciones.

Cualquier incidencia relacionada con las licencias, las actualizaciones de software o los equipos físicos (excluyendo las infraestructura de virtualización sobre la que se encuentra el

FortiWeb), tendrá que ser solucionada por la empresa adjudicataria, actuando de intermediaria entre el Ayuntamiento de Talavera de la Reina y el fabricante, creando los ticket o casos que fueran necesarios hasta la resolución de la incidencia.

4.2.- Consultoría inicial

Al comienzo del contrato la empresa adjudicataria realizará un estudio inicial de los sistemas que actualmente se encuentran operativos, las configuraciones, las políticas, etc, reuniéndose con el personal técnico municipal para identificar también las necesidades y escenarios respecto de la seguridad. Tras este estudio planteará una propuesta de modificación motivada, en la que se reflejen los cambios que se proponen y el propósito de los mismos, siempre con el objetivo de aumentar la seguridad y el rendimiento. Esta propuesta podrá ser negociada con el personal técnico municipal hasta llegar a un acuerdo.

Una vez aprobada la propuesta de modificación por el ayuntamiento, se elaborará una planificación para aplicar los cambios, teniendo como prioridad la menor interferencia con el trabajo habitual de los usuarios.

4.3 Peticiones de cambio y asesoramiento

El ayuntamiento de Talavera de la Reina podrá realizar cuantas peticiones sean necesarias a lo largo del contrato, estas peticiones podrán ser de:

- Asesoramiento: En las actuaciones que el personal técnico del ayuntamiento vaya a realizar determinados cambios y que requieran información o la mejor forma de realizarlos, así como en las consultas a los registros y logs de los equipos.
- Cambios: Cambios de configuración, políticas, routing, túneles o cualquier otro aspecto relacionado con las funcionalidades incluidas en los equipos fortinet objeto del contrato.
- Informes: En caso de incidentes o por necesidades del ayuntamiento, se podrán realizar peticiones de informes sobre eventos, ataques, tráfico u otro tipo de información que consten en los registros de monitorización y logs de los equipos fortinet.

4.4 Notificación de incidencias

Cualquier incidencia de seguridad, rendimiento o relacionada con los equipos fortinet detectada por el personal técnico municipal y que no haya sido previamente detectada por el servicio de monitorización, será comunicada mediante el servicio de helpdesk. Estas notificaciones ,en función de su gravedad, tendrán que ser atendidas a la mayor brevedad, solucionando la incidencia si es posible o planteando alternativas al personal técnico municipal para actuar en otros sistemas conjuntamente.

4.5 Servicio de monitorización 24x7x365

La empresa adjudicataria prestará un servicio de monitorización de la seguridad de la red municipal las 24 horas durante los 365 días del año. En la propuesta se indicará

específicamente qué aspectos de la seguridad se controlarán, la capacidad de detección y de respuesta, con indicación de posibles medidas.

Como mínimo se deberá controlar:

- Intrusiones
- Ataques DoS
- Tráfico anormal o a destinos maliciosos conocidos
- Malware (detección en firewall no en endpoint)

Las incidencias localizadas durante la monitorización que por su importancia lo requieran, se tratarán en un primer nivel desde el equipo Fortinet si es posible y se notificarán por correo electrónico, o teléfono si la urgencia lo requiere, al personal técnico municipal. Si no se pudiera tratar desde el propio firewall, en el correo de aviso se incluirán las posibles medidas que se debería adoptar por parte del personal técnico municipal.

4.6 Informes periódicos

Con una periodicidad mínima quincenal se elaborará un informe de estado. En el mismo se reflejaran tanto los aspectos básicos del estado de los Fortigate, como los principales aspectos sobre el tráfico y la seguridad. En estos informes se podrán proponer medidas correctoras en base al resultado de los mismos.

4.7.- Acuerdos de nivel de servicio

Los acuerdos de nivel de servicio solicitados son de mínimos, las propuestas podrán mejorar los acuerdos requeridos siendo tenido en cuenta en la valoración de las ofertas. Los acuerdos de nivel de servicio se indicarán por grupo en función de la casuística de servicios citadas anteriormente.

Definiciones:

- Tiempo de respuesta: Periodo desde que la incidencia es notificada hasta que se hace la evaluación de la misma y se empieza a trabajar en su resolución. Requerirá una notificación al ayuntamiento con el diagnóstico y la posible solución. En caso de requerir escalado a fabricante, el tiempo computa hasta que se genera el ticket o caso con el fabricante.
- Tiempo de resolución: Periodo desde la notificación al ayuntamiento con la evaluación o diagnóstico hasta su solución.

Actualizaciones y gestión de incidencias relacionadas con los equipos

- Actualizaciones

  Una vez liberada por el fabricante una nueva versión estable, se deberá comunicar al ayuntamiento en un plazo máximo de una semana para acordar el mejor momento para proceder a la actualización. Si la versión es debida a un agujero de seguridad crítico, el plazo de comunicación se reducirá a 2 días.

- Incidencias relacionadas con fallos o mal funcionamiento de los equipos fortigate:

  - Incidencia leve: Incidencia que no afecta a la seguridad que causa pequeños trastornos o pérdida de rendimiento leve.
    Tiempo de respuesta: 1 día
    Tiempo de resolución: 1 semana
  - Incidencia media: Incidencia que afecta levemente a la seguridad o pérdida de rendimiento apreciable
    Tiempo de respuesta: 5 horas
    Tiempo de resolución: 2 días
  - Incidencia alta: incidencia que afecta a la seguridad o pérdida de rendimiento importante.
    Tiempo de respuesta: 2 horas
    Tiempo de resolución: 5 horas
  - Incidencia crítica: No operatividad del sistema, entorno parado.
    Tiempo de respuesta: 30 minutos
    Tiempo de resolución: 2 horas

  Las incidencias críticas podrán requerir la presencia física de personal de la empresa adjudicataria en las instalaciones municipales y si es necesario sustituir temporalmente los equipos por otros de su propiedad para poder cumplir los plazos hasta que se solucione la incidencia.

Peticiones de cambio y asesoramiento

- Asesoramiento e informes:
  - Peticiones normales: Peticiones que no requieren una rápida respuesta, la respuesta se realizará en un plazo máximo de 3 días.
  - Peticiones urgentes: Cuando la consulta o informe tenga carácter de urgencia se resolverá en el mismo día de la petición o al día siguiente si se formula después de las 14:00 H.
- Cambios:
  - Cambios normales: Peticiones que no requieren una rápida respuesta, la respuesta se realizará en un plazo máximo de 2 días.
  - Cambios urgentes: Cuando la petición de cambio tenga carácter de urgencia se resolverá en el mismo día de la petición o al día siguiente antes de las 10:00 h si se formula después de las 14:00 H.

Incidencias de seguridad notificadas o procedentes de la monitorización 24x7x365

En este tipo de incidencias, la resolución podrá ser por parte de la empresa adjudicataria actuando directamente sobre los firewall o si fuera necesario actuar en otros dispositivos o servidores de la instalación, se debe comunicar al personal técnico del ayuntamiento, en este último caso se considera el tiempo de resolución el de la recepción de la comunicación al personal técnico municipal e incluirá un seguimiento posterior hasta la resolución definitiva de la incidencia.

- Incidencia leve: Incidencia con riesgo bajo de exposición.
  Tiempo de respuesta: 1 día
  Tiempo de resolución: 3 días
- Incidencia media: Incidencia con riesgo medio de exposición sin afectar a sistemas internos.
  Tiempo de respuesta: 5 horas
  Tiempo de resolución: 1 días
- Incidencia alta: Incidencia con riesgo alto de exposición, que afecta a la operatividad de los sistemas.
  Tiempo de respuesta: 2 horas
  Tiempo de resolución: 5 horas
- Incidencia crítica: Incidencia con riesgo muy alto de exposición o sistemas expuestos (como intrusiones) o que imposibilita el funcionamiento de sistemas como ataques DoS
  Tiempo de respuesta: 30 minutos
  Tiempo de resolución: 2 horas

Las incidencias críticas podrán requerir la presencia física de personal de la empresa adjudicataria en las instalaciones municipales y si fuera necesario.

Talavera de la Reina, a 04 de Noviembre de 2019
Manuel Ignacio Castro Márquez
Jefe de Servicio de Informática