INDICE

1. OBJETO DEL CONTRATO

El objeto del contrato consiste en la prestación de servicios de seguridad gestionada en modalidad mixta, renovaciones de los licenciamientos de los dispositivos de seguridad de la instalación IT y operación de un Centro de Operaciones de Seguridad (SOC) externo.

Los licitadores deberán disponer de un SOC gestionado 24x7 sobre el que integrar los eventos generados desde los dispositivos de la red del Ayuntamiento de Talavera de la Reina. El Centro de Operaciones de Ciberseguridad tendrá que formar parte de la Red Nacional de Centros de Operaciones de Ciberseguridad.

2. ALCANCE.

El Ayuntamiento de Talavera de la Reina dispone de una instalación de seguridad consolidada para la protección de los sistemas y un contrato para la gestión de dicho entorno, la monitorización de la seguridad de los sistemas y un SOC externalizado integrado en la Red Nacional de SOC. Dado que el actual contrato está próximo a finalizar, este contrato pretende dar continuidad a los servicios, manteniendo los niveles de servicio actuales y mejorando la eficiencia y niveles de seguridad dentro de las condiciones e importes del contrato.

2.1. EQUIPAMIENTO DE SEGURIDAD DE LA INSTALACIÓN

El equipamiento que actualmente forma parte de la instalación de seguridad y que se incluye en el alcance del presente contrato, para el que se tendrá que realizar labores gestión, monitorización, actualización, configuración, soporte y realizar la renovación anual de las suscripciones con fabricante para los productos que lo requieran, es:

- 2 Palo Alto PA-460 en disposición de alta disponibilidad, con la siguiente suscripción de licencias:
  - Pofessional Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Wildfire, DNS Security and SD-WAN)- PAN-PA-460-BND-PRO
  - PA-460, Partner enabled premium support - PAN-SVC-BKLN-460
- 2 Fortigate 200F en disposición de alta disponibilidad, con la siguiente suscripción de licencias:
  - FortiGate-200F Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)
- 1 FortiWeb 100D (FWB-100D-BDL)-Virtual appliance for all supported platforms. 1 x vCPU core, con la siguiente suscripción.
  - FORTIWEB Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation)

- 15 AP Wifi Fortinet, FP231G.
- Herramientas de seguridad implantadas del productos de CCN
    - Sonda SAT-INET.
    - Herramienta microclaudia instalada en los equipos de la instalación.
    - Herrramienta LUCIA.
    - Herramienta REYES.

De los productos software corresponde al adjudicatario mantenerlos actualizados a la última versión o a la recomendada por el fabricante. Las que requieran pago por suscripciones de licenciamiento de software correrá a cargo del adjudicatario, estando incluido en el precio del contrato.

2.2. ENTORNO A PROTEGER Y VOLUMETRÍAS

La infraestructura TI actual del Ayuntamiento que debe proteger el sistema y las volumetrías de eventos y otra información relevante es la siguiente:

En cuanto a las volumetrías más destacadas:

- Servidores:
    - Físicos: 7
    - Virtuales:30
- 2 cabinas de almacenamiento en configuración activo-activo.
- Entorno de backup compuesto por un servidor físico y una cabina de almacenamiento.
- Puestos de trabajo 450
- Eventos: Promedio: 1000 eps. Pico: 3.000 eps

3. CONDICIONES GENERALES

Se establecen las siguientes condiciones generales para el contrato:

- Se utilizarán tanto las guías técnicas publicadas como las recomendaciones del CCN para la gestión y monitorización de la seguridad y configuración de dispositivos.
- Con el objeto de integrar el sistema resultante en la definición del Esquema Nacional de Seguridad del Ayuntamiento, se proporcionará inventario de activos y aplicabilidad de medidas.
- La gestión de dispositivos y configuraciones de los mismos se realizarán de forma que todo el sistema funcione de forma integrada entre sí y con el CCN.

- Los servicios a prestar incluye al Ayuntamiento de Talavera de la Reina y a sus Organismos Autónomos. Los datos aportados en el pliego sobre dimensionamiento incluyen a los Organismos Autónomos.
- Si para prestar los servicios que cada licitador oferte se requiere algún dispositivo o software de seguridad adicional a los citados en este pliego como parte de la infraestructura existente, las ofertas lo indicarán expresamente, con detalle de requerimientos mínimos y deben estar incluidos en la oferta, sin costes adicionales ocultos a los importes del contrato.
- Los productos adicionales requeridos o las herramientas necesarias para prestar el servicio deben estar incluidos en la Guía de Seguridad de las TIC CCN-STIC 105.

4. REQUERIMIENTOS EN LA PRESTACIÓN DEL SERVICIO DE SOC

4.1. Requisitos mínimos para el SOC

El SOC de la adjudicataria debe formar parte de la Red Nacional de Centros de Operaciones de Ciberseguridad.

El SOC actual y siguiendo la recomendación del CCN en cuanto a SOC privados que den servicio a las Administraciones Públicas, colabora con el CCN-CERT a través de las herramientas LUCIA y REYES. En el caso de REYES, el acceso es desde el adjudicatario, no existiendo en la instalación municipal ningún equipamiento. En el nuevo contrato debe mantenerse dicha colaboración a través de las herramientas mencionadas, debiendo el adjudicatario hacerse cargo de las mismas, migrando desde la situación actual.

Las propuestas deberán incluir los detalles de la infraestructura del SOC del licitador con el que se prestará el servicio, el plan de implantación del mismo y la puesta en marcha, detallando las herramientas de seguridad necesarias en la instalación del Ayuntamiento para garantizar la comunicación y operatividad. Se podrán proponer herramientas adicionales a las requeridas, dentro del alcance y ámbito del contrato, siendo objeto de valoración adicional. Un factor importante es el nivel de integración de todas las herramientas propuestas, centralización de la gestión y facilidad de administración.

1. La adjudicataria deberá formar parte de la Red Nacional de SOC, además de formar parte de la red Csirt.es.
2. La adjudicataria deberá acreditar la certificación ENS a NIVEL ALTO, además de la ISO 27001.
3. La adjudicataria debe disponer de infraestructura de SOC en modo alta disponibilidad, para poder hacer frente a contingencias sin pérdida de servicio.
4. Los servicios de monitorización deberán prestarse a través de un SOC ubicado y operado desde España.

4.2. SIEM

El SIEM es el núcleo o instrumento fundamental del SOC, recogerá en una única plataforma todos los eventos generados por los sistemas del Ayuntamiento y de otras fuentes externas la información existente sobre amenazas potenciales. Mediante correlación u otras técnicas de análisis permitirá identificar y reaccionar ante posibles ataques y en la medida de lo posible, adelantarse a ellos para remediarlos antes de que sucedan.
El SIEM debe ser aportado por la adjudicataria desde sus instalaciones y como mínimo permitirá:

- Centralizar y custodiar eventos sobre el funcionamiento de los sistemas de información, infraestructuras tecnológicas y de comunicaciones.
- Alertar en tiempo real ante anomalías y ataques informáticos al Ayuntamiento de Talavera. de la Reina
- Investigar los sucesos ocurridos para poder responder y defenderse ante los ciberataques, con el objetivo de proteger los sistemas de información del Ayuntamiento de Talavera.
- Aportar la información necesaria para atender las peticiones de información relativa a sucesos relacionados con sistemas de información, infraestructuras tecnológicas y de comunicaciones por parte de Juzgados y Fuerzas y Cuerpos de Seguridad del Estado.
- La herramienta de SIEM con la que se preste el servicio tendrá que estar en el Guía de Seguridad de las TIC CCN-STIC 105.

Las fuentes de información para el SIEM que se consideran inicialmente serán, al menos:

- Controladores de dominio y otros servidores relevantes.
- Firewalls y WAF.
- Servidores de aplicaciones (Apache, Apache Tomcat e IIS).
- Plataforma corporativa de antivirus y EDR.
- Sonda SAT-INET y otras sondas propuestas en la solución.
- Plataforma de virtualización.
- Entorno de backup.

La propuestas podrán incluir otras fuentes de información que se consideren necesarias, formando parte de su diseño de SOC y que será tenido en cuenta en la valoración. Los licitadores propondrán los diferentes escenarios o caso de uso de los eventos recolectados en el SIEM, así como su posterior tratamiento.

El periodo de retención de los logs será como mínimo de una semana a corto plazo y al menos 1 año para medio y largo plazo, periodos superiores a los indicados se valorarán. Podrá ser en caliente para el corto plazo y en frío para el largo plazo.

Los productos de SIEM suelen desarrollarse por módulos, cada uno de ellos con funciones especificas y que aportan capacidades. Cuentan con agentes recopiladores de registros, servidores de almacenamiento con bases de datos, motores de correlación de datos para ofrecer información relevante, etc. Pueden contar con herramientas avanzadas (Machine Learning, Big Data Analytics, IA, u otras) que permitan detectar eventos relacionados con amenazas de tipo “0-day”, amenazas desconocidas, APT, movimientos laterales, compromiso del endpoint, exfiltración de información, actividad sospechosa en general, etc. También pueden incluir herramientas para la automatización de la respuesta y remediación (como aislar máquinas o Ips públicas, lanzar scripts, etc).

Las propuestas incluirán las características y capacidades del SIEM desde el que prestarán el servicio y que forme parte de su infraestructura, además se detallará, dentro del diseño propuesto, las capacidades de recolección, de correlación/análisis avanzado y medidas de remediación y respuesta (automáticas y revisión manual). Todo ello será objeto de valoración, por lo que el nivel de detalle y descripción del diseño del SOC en la propuesta es un factor importante.

Se debe disponer de una consola de acceso para el personal del Ayuntamiento, donde a modo de cuadro de mando se puedan realizar consultas, informes, seguimiento de la actividad, acceso a notificaciones y eventos, etc. Este acceso o consola para el Ayuntamiento no podrá suponer un coste adicional y debe estar incluido en los costes de la solución.

4.3. LUCIA, REYES y SAT-INET.

En la infraestructura de seguridad actual ya se cuenta con las herramientas LUCIA, REYES y SAT-INET. El adjudicatario tendrá que gestionar, mantener y actualizar, si procede, las herramientas y la coordinación con el CCN-CERT.

La herramienta **LUCIA** se encuentra bajo LUCIA NUBE. El adjudicatario debe gestionar con CCN-CERT la autorización y acceso al registro del Ayuntamiento de Talavera de la Reina. La apertura y gestión de tickets, incluidos los tickets generados en LUCIA desde la sonda SAT-INET, será responsabilidad del adjudicatario, notificando al personal técnico municipal y requiriendo de coordinación en caso necesario.

La herramienta **REYES** para disponer de acceso a ciberinteligencia, tanto a la hora de realizar búsquedas y análisis como para la consulta de listas de reputación. Actualmente es la adjudicataria la que cuenta con acceso a dicha herramienta. El modelo se mantendrá, realizando las notificaciones necesarias a CCN-CERT.

La sonda **SAT-INET**, para la ayuda a la detección temprana de posibles incidentes de seguridad, es un servicio desarrollado e implantado por el Equipo de Respuesta ante

Incidentes de Seguridad de la Información del CCN (CCN-CERT) para la detección en tiempo real de las amenazas e incidentes existentes en el tráfico que fluye entre la red interna del Organismo adscrito e Internet. Actualmente ya está implantada y operativa en la infraestructura municipal. La adjudicataria se encargará de la actualización de versiones y la gestión de problemas e incidentes relacionados con la sonda y las comunicaciones con el CCN-CERT. La versión instalada es la 3.0.0.

4.4. Prestación de servicios de seguridad desde el SOC.

Se establecerá un servicio de vigilancia proactiva 24x7x365, desde el SOC de la adjudicataria con capacidad para recibir, correlado y gestión de eventos de seguridad en tiempo real, y que actúe en caso de ser preciso tanto para soporte como en respuesta a un incidente de seguridad.

Todas las alertas generadas por el motor SIEM deberán ser revisadas por un técnico de seguridad de la adjudicataria, como paso previo a su envío al Ayuntamiento de Talavera de la Reina. Esto deberá permitir con un importante nivel de acierto la eliminación de falsos positivos en la identificación de incidentes. Toda la información recolectada junto a las posibles alertas generadas y el estado de salud global del sistema, así como el de cada uno de los elementos, deberá ser accesible mediante una consola centralizada que permita una gestión ágil.

El servicio debe incluir como mínimo:

- Servicio de soporte ofrecido 24x7x365 por teléfono, correo electrónico y sistema de tickets, en castellano.
- Service Packs y hotfixes: Acceso a las mejoras técnicas del producto durante el tiempo de activación del servicio.
- Web de soporte: Acceso a foros, blogs, información sobre últimas amenazas, enciclopedia de virus.
- Soporte técnico vía email o teléfono 24x7x365, por técnicos certificados en la solución implementada.
- Acceso ilimitado al Helpdesk: sin límite de incidencias.
- Mantenimiento y soporte de los sistemas instalados.
- Servicio de Monitorización. Vigilancia 24x7 de la seguridad de los dispositivos incluidos en el servicio, que permite reducir los riesgos de seguridad y acelerar la respuesta ante incidentes. Esta función está orientada a la prevención y mitigación de amenazas que pueden afectar a la seguridad de la organización.
- Seguridad Gestionada. Que permita externalizar la gestión de la seguridad de los elementos dentro del alcance del contrato.
- Correlación de eventos de seguridad o análisis mediante herramientas avanzada, con respuesta y análisis forense ante eventos de seguridad.

- Gestión de la configuración del sistema implantado. Mantenimiento y configuración de todos los elementos implantados en el proyecto al objeto de mantener los niveles de seguridad, adaptarse a los cambios que se puedan producir en los sistemas del Ayuntamiento preservando los niveles de integración, mantenimiento de la integración con CCN si se producen cambios y evolución de la seguridad del sistema como consecuencia de incidentes o recomendaciones.

Todo el software y hardware objeto de esta licitación estará en mantenimiento y garantía hasta el final del contrato. Todo el licenciamiento será con licencias que permitan una funcionalidad completa de los productos de acuerdo a la función para la que fueron desplegados, siempre durante el periodo de vigencia del contrato.

5. REQUERIMIENTOS EN LA PRESTACIÓN DE SERVICIOS PROFESIONALES, SEGURIDAD GESTIONADA COMPARTIDA E INCIDENTES DE SEGURIDAD

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.
- Estar acreditada por Palo Alto como partner certificado.
- Disponer al menos de 2 ingenieros certificados en el nivel NSE 6 o superior de Fortinet.
- Disponer al menos de 2 ingenieros certificados PCNSA o superior de Palo Alto.
- 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:

5.1. 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.

5.2. Actualizaciones y gestión de incidencias relacionadas con los equipos

Las actualizaciones de los equipos Palo Alto, 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 la 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 tickets o casos que fueran necesarios hasta la resolución de la incidencia.

5.3. 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 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 objeto del contrato.

5.4. Mejora continua.

Con una periodicidad semestral o anual, a la vista de la operación del SOC y los incidentes recogidos, se establecerá un sistema de mejora continua que revise las fuentes de información recabadas, el análisis realizado y los procedimientos de respuesta, para proponer posibles mejoras. Para ello se generará un informe de mejora y mediante una reunión con el equipo de seguridad del Ayuntamiento se aprobarán las medidas a establecer.

5.5. Gestión y respuesta ante incidentes de seguridad

Una vez se detecte un incidente a través del servicio de monitorización, o bien este le sea comunicado por alguno de los canales establecidos, el SOC procederá a la gestión completa del incidente realizando, al menos, las siguientes actividades:

- Registrar, clasificar, valorar, priorizar y escalar los incidentes de seguridad que sean detectados a través del servicio de monitorización, que sean comunicados por el personal TIC del Ayuntamiento de Talavera de la Reina o que sean notificados por parte los organismos nacionales, regionales o locales de respuesta a incidentes de ciberseguridad.
- Emitir las alertas oportunas ante eventos de seguridad, tanto internas como a terceros (autoridades nacionales y/u otras organizaciones).
- Realizar la notificación de los incidentes de seguridad mediante la herramienta LUCIA.
- Adoptar medidas de contención para los incidentes de seguridad, o dar indicaciones precisas para que estas sean implementadas por el personal del área TIC del Ayuntamiento de Talavera de la Reina.
- Elaboración de informe del incidente.

También se incluirán servicios post-incidente y recuperación para al menos un incidente de seguridad que pueda tener alto impacto, con independencia de si deben ser realizadas por el SOC u otros departamentos o servicios como CSIRT. Entre estos servicios se incluirán:

- Investigación del incidente de seguridad, localizando y recolectando evidencias.
- Investigación forense.
- Elaborar el informe post-incidente, con inclusión de las evidencias medidas y lecciones aprendidas y propuestas de planes de acción para prevenir incidentes futuros.
- Ratificación, si fuera necesario, ante Tribunales de justicia.

En todo caso en la gestión de incidentes de seguridad se atenderá a la guía CCN-STIC 817 Esquema Nacional de Seguridad. Gestión de ciberincidentes.

Bajo las premisas indicadas para la gestión de incidentes de seguridad, el licitador deberá detallar en su propuesta los planes de respuesta ante contingencias graves y el nivel de acciones a tomar que permitan contener y mitigar los posibles incidentes de seguridad sobre los datos en las infraestructuras digitales del Ayuntamiento de Talavera de la Reina. Durante la duración del contrato, la adjudicataria dispondrá de procedimientos de respuesta ante incidentes aprobados, que serán actualizados periódicamente como parte de la mejora continua de la seguridad.

5.6. Acuerdos de nivel de servicios

Los tiempos de respuesta ante consultas, peticiones, actualizaciones o incidentes de seguridad no podrán superar los establecidos a continuación.

- Para consultas y peticiones/solicitudes, no excederá de 24 horas.
- Para actualizaciones críticas por vulnerabilidades en los firewall, no excederá de 48 horas desde que el fabricante libere la versión o revisión que la corrige.
- Para actualizaciones no críticas en los firewall, no excederá de 1 semana desde que el fabricante libere la versión o revisión.
- Por incidente se seguridad de prioridad alta, no excederá de 1 hora desde la detección del incidente.
- Por incidente se seguridad de prioridad media, no excederá de 5 horas desde la detección del incidente.
- Por incidente de seguridad de prioridad baja, no excederá de 24 horas.

6. FASES DEL SERVICIO

Una vez adjudicado y firmado el contrato, en un plazo no superior a una semana, se realizará una reunión inicial de lanzamiento en la que se recabarán datos específicos de la instalación y otros elementos necesarios. En un plazo no superior a 7 días posteriores a la reunión, la adjudicataria presentará al Ayuntamiento un Plan de implantación/migración revisado y adaptado, sobre todo en la parte de diseño de la solución, que recoja los datos más específicos de la reunión inicial. También se incluirá la planificación definitiva, que respetará el periodo máximo de 1 mes.

En cuanto a la gestión del proyecto se atenderá al plan de implantación, al equipo de trabajo y a la formación del personal TIC una vez finalizada la implantación.

6.1. Implantación/Migración de los servicios

En caso necesario se establece un periodo de migración de los servicios desde el prestador actual al nuevo adjudicatario, el plazo máximo para realizar la migración será de 1 mes.
A la firma del contrato se realizará una reunión inicial para planificar la migración de los servicios. En la planificación se tendrá en cuenta el plazo máximo, minimizar el impacto en

la operativa diaria de trabajo y evitar la exposición de la seguridad de los sistemas a proteger. La adjudicataria presentará un plan de migración teniendo en cuenta los objetivos citados, con especificidad de tareas y planificación temporal, así como las pruebas a realizar para poder comprobar que la migración es completa y todos los servicios son accesibles y operables. Los servicios que formarán parte de la migración son:

- Conectividad segura desde la adjudicataria a los sistemas del Ayuntamiento.
- Traspaso de la gestión con el software de CCN: LUCIA, REYES, SAT-INET.
- Recolección de eventos de los sistemas por el SIEM de la adjudicataria.
- Gestiones, en caso de ser necesarias, con los fabricantes de los productos de seguridad instalados.

La planificación estará sujeta a revisión y aprobación por los técnicos municipales. El proceso de migración estará supervisado por técnicos de la adjudicataria que cuenten con la certificación necesaria en los productos que forman parte del servicio, manteniendo informado a los técnicos municipales de los avances.

6.2. Operación de los servicios y mantenimiento

La fase de operación y mantenimiento comprenderá desde la realización efectiva de la migración de los servicios, en caso de ser necesaria, hasta el final del contrato. Durante la misma la empresa asumirá todas las funciones bajo las condiciones y acuerdos de nivel de servicio incluidas en la prestación del contrato, según consta en los apartados 4 y 6 del presente pliego.

Durante toda la duración del contrato el adjudicatario designará un responsable como interlocutor con el Ayuntamiento para cualquier cuestión relacionada con la prestación de los servicios, al margen de las incidencias o consultas de carácter técnico que seguirán otra via. En caso de cambio de interlocutor, la adjudicataria tendrá que comunicarlo en un plazo no superior a 15 días.

Al comienzo de la fase de operación, una vez realizada la migración de los servicios, la adjudicataria realizará una consultoría del estado de la seguridad, evaluando el estado, configuraciones, parametrizaciones y políticas de los dispositivos de seguridad existentes. Como resultado de la misma se presentará un informe sobre el estado de la seguridad, con indicación, si las hubiera, de puntos críticos y debilidades, con propuestas de mejoras o mitigación. Evaluado el informe por los técnicos municipales, en coordinación con ellos, se elaborará una planificación de posibles cambios en los sistemas de acuerdo a las recomendaciones señaladas en el informe. Estos cambios se realizarán conjuntamente por personal técnico de la adjudicataria y técnicos municipales.

La realización de la consultoría inicial, elaboración del informe y planificación de cambios, deberá realizarla un técnico de la adjudicataria con perfil de gestor de proyectos de

ciberseguridad, arquitecto de ciberseguridad, auditor de seguridad o similar, con una experiencia mínima de 2 años.

6.2.1. Formación

Con el objetivo de permitir el máximo aprovechamiento de las soluciones desplegadas, la empresa adjudicataria deberá diseñar un plan de formación que contemple sesiones formativas para cada uno de los componentes desplegados, incluyendo las temáticas a tratar, explicación de la forma de despliegue, explotación de la solución, mantenimiento de la misma, posibles reconfiguraciones, depuración de problemas y trazabilidad de eventos. La duración no será inferior a 20 horas.

La formación ofertada deberá indicar las horas y jornadas previstas, así como el contenido de las sesiones formativas. La empresa deberá facilitar el material didáctico. Los medios para esta formación serán en acuerdo con el Servicio TIC del Ayuntamiento de Talavera de la Reina.

6.3. Devolución del servicio

A la finalización del contrato y en previsión de un cambio de empresa, el adjudicatario adquiere el compromiso de facilitar toda la información relacionada con los servicios vinculados en el contrato y colaborar con los técnicos municipales y la empresa entrante en la migración de los servicios hacia la misma, a fin de facilitar el proceso y minimizar los riesgos de seguridad que pudieran ocasionarse en el proceso de migración.

7. PROTECCIÓN DE DATOS

Los datos de carácter personal de las personas usuarias están afectados por la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y su normativa de desarrollo.
La adjudicataria deberá formar e informar a su personal en cuanto a las obligaciones que en materia de protección de datos deban cumplir en el desarrollo de sus tareas para la prestación del servicio, en especial las derivadas del deber de secreto, respondiendo la empresa adjudicataria personalmente de las infracciones legales en que por su incumplimiento se pudiera incurrir.
La adjudicataria se compromete a guardar la confidencialidad debida respecto a los datos personales y documentos de los usuarios a los que tuviere acceso, obligación que subsiste incluso después de la resolución del contrato.

Solo podrán acceder a los datos de carácter personal, información y documentación, las personas estrictamente imprescindibles para el desarrollo de las labores inherentes al contrato.

La adjudicataria será responsable del cumplimiento de estas obligaciones por parte de su personal.

La adjudicataria deberá implantar las medidas de carácter técnico y organizativo necesarias para garantizar la seguridad de los datos de carácter personal, evitándose su alteración, perdida o acceso no autorizado, en estricto cumplimiento de la normativa vigente en materia de protección de datos. Dichas medidas deberán ajustarse al Esquema Nacional de Seguridad.

La adjudicataria habrá de poner en conocimiento de la administración cualquier incidencia detectada, sospecha o constatación de fallos o errores que puedan producirse en el sistema de custodia.

Talavera de la Reina a fecha de firma electrónica

Documento firmado electrónicamente

Documento firmado por:	Cargo:	Fecha/hora:
MANUEL IGNACIO CASTRO MARQUEZ	JEFE DE SERVICIO DE INFORMATICA	22/01/2026 09:47