Ayuntamiento de Talavera de la Reina

GOBIERNO DE ESPAÑA · MINISTERIO DE POLÍTICA TERRITORIAL

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL CONTRATO DE SUMINISTRO E INSTALACIÓN DE PRODUCTOS DE CIBERSEGURIDAD CON EL DESPLIEGUE DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y POSTERIOR OPERACIÓN DEL MISMO.

INDICE

Documento firmado por:	Cargo:	Fecha/hora:
MANUEL IGNACIO CASTRO MARQUEZ	JEFE DE SERVICIO DE INFORMATICA	24/11/2022 09:40

1. OBJETO DEL CONTRATO

El objeto del contrato consiste en el suministro e instalación de productos de ciberseguridad con el despliegue de un Centro de Operaciones de Seguridad (SOC) y posterior operación del mismo.

El proyecto constará de dos fases. En cada fase se desglosan las siguientes actuaciones:

Fase I: Suministros, instalaciones y despliegue del SOC:

- Suministro, instalación y puesta en marcha de servicios de ciberseguridad
  - Instalación de la herramienta microClaudia.
  - Suministro e instalación de una doble barrera de firewall en alta disponibilidad.
- Diseño, implantación y puesta en marcha del SOC.
  - Despliegue y activación de las herramientas LUCIA, REYES y SAT-INET.
  - SIEM y elementos necesarios.

FASE II: Operación del SOC y servicios de soporte

- Servicios de operación del SOC por dos años.
- Servicios de seguridad gestionada y soporte del entorno por 2 años.

El Centro de Operaciones de Ciberseguridad que se despliegue en el ámbito del presente pliego tendrá que formar parte de la Red Nacional de Centros de Operaciones de Ciberseguridad.

Este contrato se enmarca en el Plan de Recuperación, Transformación y Resiliencia, en su Componente 11 (Subvenciones destinadas a la transformación digital y modernización de las administraciones de las entidades locales), con cargo a los fondos Next Generation de la Unión Europea para los importes del contrato correspondientes a los suministros.

2. ALCANCE Y OBJETIVOS

La Estrategia de Ciberseguridad para la Década Digital de la UE, de diciembre de 2020, señala que “las redes y los sistemas informáticos requieren de una vigilancia y un análisis constantes para detectar intrusiones y anomalías en tiempo real”. Los SOC son el medio que permite realizar esa vigilancia de la seguridad, son responsables de supervisar y proteger la tecnología, la red, servidores, aplicaciones y hardware. Los esfuerzos de monitorización de un SOC se extienden más allá de la respuesta a un incidente. Deben vigilar y analizar de forma constante las redes y los sistemas para detectar intrusiones y anomalías en tiempo real, parametrizar al atacante e implantar medidas concretas para su mitigación.

El Ayuntamiento de Talavera de la Reina dispone de productos de ciberseguridad para proteger los sistemas, entre los que destacan: Firewall (que incluye IDS/IPS, navegación segura o VPN entre otros), WAF y protección en los endpoints con EDR.

Con este contrato se pretende, por un lado, avanzar en la incorporación de nuevos productos que añadan un mayor nivel de seguridad como una doble barrera de firewall y la herramienta microClaudia, pero sobre todo, el despliegue de un SOC que permita monitorizar y analizar los eventos generados por los productos de seguridad, para detectar posibles incidentes de seguridad y en caso de producirse establecer los mecanismos de mitigación y respuesta necesarios, así como comunicar el incidente siguiendo los medios legalmente establecidos y las recomendaciones del CCN.

En este despliegue se usarán herramientas del CCN como: Lucía para comunicación de incidentes al CCN-CERT, Reyes para compartir información de ciberamenzas con el CCN y la sonda Sat-inet. Además se desplegarán todas los elementos necesarios para la operación del SOC.

Dado que el Ayuntamiento de Talavera de la Reina no dispone de la capacidad para la operación del SOC, esta labor se hará por parte de la empresa adjudicataria, para ello el SOC a implementar se encontrará en las instalaciones del adjudicatario, a excepción de los elementos que necesariamente tengan que estar en la instalación local.

Como objetivo final, el SOC que se despliegue tendrá que formar parte de la Red Nacional de Centros de Operaciones de Ciberseguridad.

Por otro lado, este proyecto complementará y reforzará el proyecto municipal de adecuación y certificación de conformidad con el ENS de los sistemas de información.

El Ayuntamiento de Talavera de la Reina es beneficiario de una ayuda en forma de subvención cuyas bases reguladoras se aprueban en la Orden TER/1204/2021, encuadrada en el Componente 11 del Plan de Recuperación, Transformación y Resiliencia, la Inversión 3 – Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública y de las Administraciones de las CCAA y las EELL. El alcance y objetivos de este contrato responden a la Memoria Técnica de Proyecto presentada a la convocatoria y a los requisitos incluidos en las bases de la Orden TER/1204/2021.

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 implementación particularizada de la seguridad y configuración de dispositivos.

Documento firmado por:	Cargo:	Fecha/hora:
MANUEL IGNACIO CASTRO MARQUEZ	JEFE DE SERVICIO DE INFORMATICA	24/11/2022 09:40

- 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.
- Todos los dispositivos suministrados y las configuraciones de los mismos se realizarán de forma que todo el sistema funcione de forma integrada entre sí y con el CCN.
- Los Servicios de Implantación y operación son para los sistemas tanto del Ayuntamiento de Talavera de la Reina como de sus Organismos Autónomos. Los datos aportados en el pliego sobre dimensionamiento incluyen a los Organismos Autónomos.
- Si en la implementación de los elementos de seguridad o para el despliegue del SOC, fueran necesarios dispositivos hardware no citados en el pliego, las ofertas lo indicarán expresamente, con detalle de requerimientos mínimos.
- Los dispositivos de seguridad, ya sean requeridos o propuestos por los licitadores, que deban instalarse en las instalaciones del Ayuntamiento de Talavera de la Reina para el cumplimiento de requisitos u operación del SOC, deben estar incluidos en la Guía de Seguridad de las TIC CCN-STIC 105, atendiendo al cumplimiento de las condiciones de la Orden TER/1204/2021.
- Para los suministros, instalaciones, despliegue y operación del SOC, se establecerán una serie de requisitos mínimos que las propuestas deben cumplir. Toda propuesta que no cumpla uno o varios de los requisitos establecidos o no quede suficientemente acreditado en su propuesta el cumplimiento de los mismos, podrá ser no valorada por incumplimiento de requisitos.

4. SUMINISTRO, INSTALACIÓN Y PUESTA EN MARCHA DE PRODUCTOS DE CIBERSEGURIDAD

4.1.- Instalación de la herramienta microClaudia.

Trabajos de instalación necesarios para el despliegue de la herramienta microClaudia del CCN-CERT, para la vacunación anti-ransomware de los puestos de usuario, sobre los equipos de la instalación municipal y servidores compatibles. Este despliegue se intentará realizar de forma automatizada con instalación silenciosa siempre que sea posible.

4.2.- Suministro e instalación de una doble barrera de firewall.

Como se ha indicado anteriormente, en el Ayuntamiento se disponen de dos Firewall Fortigate 100F en HA. Se trata de dotar de una doble barrera mediante un cluster adicional de firewall en HA con capacidades de firewall de última generación (NGFW), arquitectura centrada en la prevención contra las amenazas de seguridad modernas, como el robo de credenciales y los

ataques basados en archivos. Los firewall serán instalados, configurados y puestos en producción por la empresa adjudicataria, teniendo en cuenta los firewall ya existentes.

En este sentido, se realizará una propuesta motivada de configuración de la doble barrera, con el Firewall ya disponible y el incluido en la propuesta, en la que se indique qué Firewall formará la barrera externa y cual la interna. La propuesta deberá ser motivada en base a aspectos como:

- Nivel de protección que aporte cada dispositivo especificando: protección de navegación web, IDS/IPS, securización de VPN , etc.
- Rendimiento: Througthput de cada dispositivo por funcionalidades (IPS, NGFW, VPN,etc)
- Número de puertos y velocidades de los mismos. Los Firewalls propuestos como internos deben disponer de un mínimo de 14 puertos con al menos uno de 10 Gb. Los internos tendrán un mínimo de 8 puertos.

Como características mínimas que deben cumplir los firewall que se propongan al proyecto:

- Rendimiento del cortafuegos (HTTP/combinación de aplicaciones) 3,0/2,4 Gbps
- Rendimiento de VPN IPsec 1,6 Gbps
- Rendimiento Threat Prevention (HTTP/combinación de aplicaciones)0,9/1 Gbps
- Nuevas sesiones por segundo 39.000
- Número máximo de sesiones 200.000
- Según la función a desempeñar (interno o externo) y la propuesta de funcionalidades, suscripción de Licencias :Threat Prevention, Advanced URL Filtering, Wildfire, DNS Security and SDWAN.

Rendimientos superiores a los expresados como mínimos serán valorados.

El suministro de la doble barrera de firewall incluirá: Hardware y licenciamiento/suscripción del software necesario durante la duración del contrato, instalación y configuración del equipo con establecimiento de políticas o reglas necesarias.

Es requisito que el fabricante y modelo ofertado debe estar certificado por el Centro Criptológico Nacional mediante la inclusión en la Guía de Seguridad de las TIC CCN-STIC 105 a la fecha de finalización de la presentación de ofertas.

5.- DISEÑO, IMPLANTACIÓN Y PUESTA EN MARCHA DEL SOC.

El SOC aporta un servicio de vigilancia y análisis constante de las redes y sistemas, tiene como funciones principales la prevención, detección, respuesta y recuperación ante ciberataques. Para ello, se requiere de una infraestructura y personas con perfiles profesionales determinados. La infraestructura permitirá recabar tanto la información de eventos generados desde los sistemas y elementos de ciberseguridad de la entidad, como de otras fuentes de información, y mediante correlación u otras técnicas permitirán identificar posibles incidencias o ataques. Los perfiles profesionales del personal, capacitan a los operadores del SOC para que ante un posible incidente o ataque detectado por la infraestructura, puedan realizar un análisis manual del mismo para confirmarlo y realizar acciones de comunicación y respuesta.

Tanto por infraestructura como por perfiles profesionales, el Ayuntamiento de Talavera de la Reina no puede contar con un SOC propio, por ello, el servicio de SOC deberá ser prestado desde la infraestructura y con los medios personales de la adjudicataria. Para ello se establecerá un túnel seguro entre ambas redes de forma que toda la información viaje en condiciones de seguridad, contando con los máximos niveles de seguridad en cuanto a protocolos y normativa.

Dado que uno de los objetivos es que el SOC que se despliegue forme parte de la Red Nacional de Centros de Operaciones de Ciberseguridad, es requisito imprescindible que el SOC de la adjudicataria forme parte de la misma.

Entre los elementos a desplegar para el SOC y siguiendo la recomendación del CCN en cuanto a SOC privados que den servicio a las Administraciones Públicas, señala que estos SOC colaborarán con el CCN-CERT a través de las herramientas LUCIA y REYES.

Las propuestas deberán incluir el diseño del SOC para el Ayuntamiento de Talavera de la Reina, con 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 proyecto, 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.

En los siguientes puntos se relacionan la infraestructura a proteger, elementos de ciberseguridad, volumetrías estimadas, herramientas y requisitos a tener en cuenta para la elaboración de las propuestas.

5.1 Entorno y volumetrías

Actualmente el Ayuntamiento cuenta con dos firewall Fortinet 100F. Para la operación y mantenimiento del mismo se cuenta con un contrato de seguridad gestionada con una empresa externa. Este factor se tendrá en consideración en cuanto a que pueda afectar a las posibles propuestas de los licitadores. En todo caso el personal TIC del Ayuntamiento, actuará de intermediario en cualquier cuestión planteada en el presente contrato que pudiera entrar en conflicto con el ya existente.

En cuanto a las volumetrías más destacadas:

- Servidores:
  - Físicos: 7
  - Virtuales:30
- Puestos de trabajo 400
- Retención mínima de los datos 1 mes en caliente y sin límite en infraestructura municipal
- Eventos: Promedio: 1200 eps. Pico:3.000 eps

5.2 Despliegue y activación de las herramientas LUCIA, REYES y SAT-INET.

5.2.1 LUCIA

LUCIA es la herramienta de gestión de incidentes del CCN-CERT que operará de modo federado con el de la Plataforma Nacional. Deberá incluirse un servicio de cibervigilancia que recopile contenido de fuentes amplias de información en línea, tales como fuentes abiertas de sitios web convencionales, paste bins, repositorios de código, fuentes cerradas como sitios TOR o foros que requieren verificación antes de que se otorgue acceso: mercados dark web o foros underground y fuentes técnicas como sitios de análisis de malware o amenazas.

5.2.2 REYES y SAT-INET

Despliegue y configuración de la herramienta del CCN-CERT SAT-INET, para la ayuda a la detección temprana de posibles incidentes de seguridad, así como el alta en REYES, para disponer de acceso a ciberinteligencia, tanto a la hora de realizar búsquedas y análisis como para la consulta de listas de reputación que puedan ser integradas en las soluciones de seguridad perimetral del Ayuntamiento.

El Sistema de Alerta Temprana (SAT) de Internet 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. Para su puesta en marcha es necesaria la implantación de una sonda individual en la red del Organismo, que se encarga de recolectar la información de seguridad relevante que detecta y, después de un primer filtrado, enviar los eventos de seguridad hacia el sistema central que realiza una correlación entre los distintos elementos y entre los distintos dominios (organismos).

Los licitadores indicarán las características necesarias para el equipo que actuará de sonda. No es un requisito que se incluya el equipo en la oferta, pero sí será objeto de valoración.

5.3 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.

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.
- Sondas de red propuestas en la solución.
- Plataforma de virtualización: Vmware vCenter.
- 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.

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.

5.4.- Requisitos para el SOC.

1. La adjudicataria deberá formar parte de la Red Nacional de SOC, nivel GOLD, 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.

6. PRESTACIÓN DE SERVICIOS POSTERIORES AL DESPLIEGUE DEL SOC. SERVICIOS DE SOPORTE Y OPERACIÓN DEL SOC.

Una vez implantado y cuando se encuentre totalmente operativo el SOC el contrato entrará en la fase de Operación del SOC y servicios de soporte.

Se establecerá un servicio de vigilancia proactiva 24x7x365 de la instalación de los sistemas de información del Ayuntamiento de Talavera de la Reina, desde el SOC de la adjudicataria con capacidad para recibir, correlar y gestionar 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.

El servicio también incluirá el soporte de la infraestructura implantada en las instalaciones del Ayuntamiento de Talavera de la Reina incluida en el contrato, incluyendo consultas del personal TIC del ayuntamiento y actualizaciones/configuraciones de los elementos implantados.

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.
- 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.
- 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. 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, a fin de reducir 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.
- 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.

El equipo de trabajo propuesto deberá haber formado parte del equipo de la adjudicataria que haya desembocado en el cumplimiento de esos requisitos.

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.

6.1 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.

6.2 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.
- Investigar los incidentes de seguridad, localizando y recolectando evidencias.
- Investigación forense.
- Elaborar el informe de cierre del incidente, así como el informe post-incidente, con inclusión de lecciones aprendidas y propuestas de planes de acción para prevenir incidentes futuros.

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.

6.3 Acuerdos de nivel de servicios

Los Acuerdos de Nivel de Servicio (ANS) permiten obtener indicadores para evaluar el grado de cumplimiento del servicio. En los mismos encontramos el tiempo de respuesta y el tiempo de resolución.

El tiempo de respuesta es el transcurrido entre la comunicación del incidente al adjudicatario, por el canal acordado, hasta que el adjudicatario asume la resolución del incidente asignando los recursos necesarios para cumplir con el tiempo de resolución, respondiendo al Ayuntamiento con la posible causa del incidente y el tiempo estimado de resolución. El tiempo de resolución transcurre entre la respuesta al Ayuntamiento y la resolución, incluida la documentación, de la incidencia.

Se establecen diferentes tipos de ANS para los servicios de soporte y para los servicios de respuesta a incidentes de seguridad

Los servicios de soporte incluirán incidentes de tipología genérica para soporte de productos, soluciones, plataformas, etc. Se clasificarán en:

- Prioridad Alta: Caída del servicio. El producto o la plataforma está en peligro de caída o esta parado o sin funcionalidad, o bien su funcionalidad está afectada de forma severa.
- Prioridad Media: El incidente produce problemas operacionales de forma intermitente, o bien hay un bajo rendimiento, pero el incidente no produce ningún tipo de problema a los usuarios en el ámbito operacional, que pueden acceder y trabajar sin demasiadas complicaciones.
- Prioridad Baja y consultas: Consultas relativas la configuración, resolución de incidentes no críticos, como notificación de alertas preventivas, o asistencia general.

Los ANS son:

Nivel	Alta	Media	Baja
T. Respuesta	2 horas	4 horas	Siguiente laborable.
T. Resolución	8 horas	24 horas	48 horas
SLA Resolución	95%	90%	90%
Penalizaciones	Indicadas en el PCAP		

En el caso de los incidentes de seguridad de la información, estos se clasificarán según la guía del CCN-CERT de Gestión de ciberincidentes, CCN-STIC 817, según el nivel de peligro de los incidentes y su nivel de impacto. Los niveles son: Crítico (L5), Muy Alto (L4), Alto (L3), Medio (L2), Bajo (L1).

Para los incidentes de seguridad, se considera tiempo de respuesta el transcurrido desde que se detecta la alerta en el SOC o desde que se notifica el incidente al adjudicatario por el canal acordado, hasta que la empresa adjudicataria registra y notifica la alerta al personal técnico del ayuntamiento. El tiempo de resolución es aquel que va desde la notificación al personal del ayuntamiento hasta que se realizan las acciones relacionadas en el procedimiento de remediación y respuesta establecido, que incluirán acciones de mitigación/contención o de comunicación de tareas al personal TIC del ayuntamiento, así como la notificación del incidente, si procede, a los organismos necesarios de acuerdo a la guia CCN-STIC 817.

Los ANS son

Nivel	Crítica	Muy alta	Alta	Promedio	Baja
Respuesta	2 horas	2 horas	4 horas	8 horas	16 horas
Resolución	4 horas	4 horas	8 horas	12 horas	24 horas
SLA Resolución	95%	90%	85%	85%	85%
Penalizaciones	Indicadas en el PCAP				

Documento firmado por:	Cargo:	Fecha/hora:
MANUEL IGNACIO CASTRO MARQUEZ	JEFE DE SERVICIO DE INFORMATICA	24/11/2022 09:40

7. GESTIÓN DEL PROYECTO

La fase de Suministros, instalaciones y despliegue del SOC, tendrá que finalizar antes del 31 de Marzo de 2023, al ser la ampliación de plazo máxima concedida a este Ayuntamiento según las bases de la orden TER/1204/2021.

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 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 para la Fase I del 31 de Marzo de 2023

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

7.1 Plan de implantación

El plan de implantación recogerá las acciones necesarias para la instalación y despliegue de todos los elementos incluidos en el contrato previos a comenzar la fase de de prestación de servicios. Se indicará la asignación de personal u otros recursos necesarios en cada actuación, detalle de tareas y requisitos necesarios por parte del Ayuntamiento o su personal TIC.

En el plan de implantación se incentivará el despliegue progresivo. A medida que cada pieza tecnológica va estando disponible, se podrán desplegar los servicios que se permitan. El objetivo es no esperar a la fecha final para desplegar todas las soluciones sino ir haciéndolo a medida que la planificación lo permita.

7.2 Equipo de trabajo y comité de seguimiento

La Componente 11.I1 del Plan de Recuperación, Transformación y Resiliencia, en relación a la ciberseguridad, cita los siguientes perfiles: Gestor de proyectos de ciberseguridad; Consultor normativo y de gobernanza en ciberseguridad; Consultor de Gobernanza, Riesgos y cumplimiento; Arquitecto de ciberseguridad; Auditor de seguridad; Administrador de sistemas de ciberseguridad.

El equipo de trabajo propuesto para la fase de Suministros, instalaciones y despliegue del SOC tendrá al menos dos personas cuyo perfil profesional sea equivalente a un gestor de proyectos de

ciberseguridad y un arquitecto de ciberseguridad, ambos con dos años como mínimo de experiencia en ese perfil y habiendo trabajado al menos en tres proyectos de ciberseguridad.

Los perfiles aquí descritos con los requisitos de años en el puesto de trabajo y proyectos realizados tienen la consideración de compromiso de adscripción a la ejecución del contrato de medios personales, de acuerdo con el Pliego de Clausulas Administrativas Particulares.

El gestor de proyecto ejecerá de responsable del contrato por parte del adjudicatario y de interlocutor con el Ayuntamiento. Tendrá que asistir a las reuniones presenciales de seguimiento en las instalaciones del Ayuntamiento.

Con el personal propuesto por la adjudicataria y el personal TIC propuesto por el Ayuntamiento de Talavera de la Reina se formará un comité de seguimiento del proyecto que se reunirá periódicamente para evaluar la actividades llevadas a cabo, la evolución y las acciones de corrección necesarias para mantener el proyecto dentro de los estándares fijados.

7.3 Documentación y Formación

Como mínimo se entregará la siguiente documentación:

- Acta de la reunión inicial, que tendrá que contar con el visto bueno del Ayuntamiento.
- Plan de implantación revisado, con respecto al propuesto al procedimiento de licitación, posterior a la reunión de inicio.
- Actas de las reuniones del comité de seguimiento.
- A la finalización de los trabajos se entregará la documentación definitiva de la solución implantada, con detalle de diseño y configuraciones realizadas

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.

Documento firmado por:	Cargo:	Fecha/hora:
MANUEL IGNACIO CASTRO MARQUEZ	JEFE DE SERVICIO DE INFORMATICA	24/11/2022 09:40