RIVAS VACIAMADRID

PLIEGO DE PRESCRIPCIONES TÉCNICAS-ECONÓMICAS, PROCEDIMIENTO ABIERTO, PARA LA CONTRATACIÓN DE LOS SERVICIOS DE MANTENIMIENTO DE LOS SISTEMAS GESTIÓN DE LA SEGURIDAD DE ACCESO A LOS DATOS EN LA RED INTERNA Y DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD DEL AYUNTAMIENTO DE RIVAS VACIAMADRID. Exp.: 2474/2024

1.OBJETO DEL CONTRATO

Los ciberataques a administraciones públicas han crecido exponencialmente, lo que supone una amenaza para los sistemas de información. Esto implica un elevado riesgo para el buen funcionamiento de las áreas de trabajo pudiendo conllevar la paralización de la actividad municipal y, sobre todo, afectar de forma crítica a la debida protección y seguridad de la información reservada de nuestra ciudadanía y empresas, así como a los servicios prestados.

A estas evidencias se suma el deber de cumplimiento normativo que incide en la necesidad y deber de las administraciones públicas de protegerse ante ataques informáticos externos, de tal modo que toda acción encaminada a alcanzar el objetivo de la ciberseguridad toma una importancia crítica, tanto presente como futura.

El contrato tiene por objeto mantener los servicios de sistemas de seguridad informática, telecomunicaciones y ciberseguridad relativos a los actuales sistemas de información, acometiendo las actuaciones de prevención, detección y respuesta adecuadas a las características propias de la actual red de datos del Ayuntamiento.

Naturaleza, razones de eficiencia en la configuración, provisión e integración de elementos y servicios de mantenimiento relacionados, el objeto de este contrato debe ser prestado por un único contratista, por lo que no se realiza división por lotes en esta licitación.

Numeración del Vocabulario Común de Contratos Público (código CPV):

48500000-3 Paquetes de software de comunicación y multimedia
35120000-1 Sistemas y dispositivos de vigilancia y Seguridad
79417000-0 Servicios de consultoría en seguridad (principal)
72253000-3 Servicios de unidad de asistencia y de apoyo.
72212730-5 Servicios de desarrollo de software de seguridad

2.- PRECIO. VALOR ESTIMADO. TIPO DE LICITACIÓN.

El valor estimado del contrato es de 330.578,00 €.

El precio total del contrato es 198.346,80 € al que se incorporarán el IVA al tipo vigente del 21 %, por importe de 41.652,84 €, sumando un total de 239.999.64 €.

Concepto	Valor económico total período (€)
VALOR ESTIMADO (sin IVA):	330.578,00.-€ comprensivo de las posibles prórrogas.
PRESUPUESTO LICITACIÓN:	198.346,80.-€
I.V.A. 21 %	41.652,84.-€
PRECIO TOTAL:	239.999,64-€

3.- FORMA DE PAGO.

Se abonará previa presentación y posterior aprobación de la factura por el órgano competente de la prestación debidamente ejecutada. En el caso de mejoras, todo este material será inventariable, por lo que tendrá que efectuarse de forma presencial y también con anterioridad al abono, su correspondiente acta de recepción del suministro efectuado.

Previo a la presentación de cada factura se deberá realizar por cada periodo de pago (trimestralmente), un informe justificativo relativo al conjunto de las principales actividades realizadas durante el mismo, de modo que, estando incluidas en el servicio de mantenimiento contratado, vendrán desglosadas por cada una de los tres puntos de actuación descritos en el punto 5 de este pliego, así como los correspondientes tiempos y recursos dedicados para su realización, que serán como mínimo los siguientes:

1. *La gestión y control de acceso dentro de la actual red interna y perimetral* de horas trabajadas en el trimestre por personal técnico dedicado.

2. *La adaptación de las medidas de seguridad en todo tipo de acceso a datos a través de zonas no controladas*: número de horas trabajadas en el trimestre por el personal técnico dedicado.

3. *La renovación de los servicios del Centro de Operaciones de Ciberseguridad (SOC)*: número de horas trabajadas en el trimestre por el personal técnico dedicado.

El número de horas por trimestre, resultado de sumar las actividades de mantenimiento de todos los técnicos para el conjunto de los 3 apartados deberá ser de 210 horas cómo mínimo.

Los periodos de pago para cada factura tendrán carácter trimestral, tal como se detalla en la siguiente tabla de distribución del gasto:

Fecha Factura	Período	Base imponible	IVA (21%)	Total importe
30 junio 2024	Ab 24-Jun 24	16.528,90 €	3.471,07 €	19.999,97 €
30 septiembre 2024	Jul 24-Sep 24	16.528,90 €	3.471,07 €	19.999,97 €
31 diciembre 2024	Oct 24-Dic 24	16.528,90 €	3.471,07 €	19.999,97 €
31 marzo 2025	En 25-Mar 25	16.528,90 €	3.471,07 €	19.999,97 €
30 junio 2025	Ab 25-Jun 25	16.528,90 €	3.471,07 €	19.999,97 €
30 septiembre 2025	Jul 25-Sep 25	16.528,90 €	3.471,07 €	19.999,97 €
31 diciembre 2025	Oct 25-Dic 25	16.528,90 €	3.471,07 €	19.999,97 €
31 marzo 2026	En 26-Mar 26	16.528,90 €	3.471,07 €	19.999,97 €
30 junio 2026	Ab 26-Jun 26	16.528,90 €	3.471,07 €	19.999,97 €
30 septiembre 2026	Jul 26-Sep 26	16.528,90 €	3.471,07 €	19.999,97 €
31 diciembre 2026	Oct 26-Dic 26	16.528,90 €	3.471,07 €	19.999,97 €
31 marzo 2027	En 27-Mar 27	16.528,90 €	3.471,07 €	19.999,97 €
Total importe		198.346,80 €	41.652,84 €	239.999,64 €

La presentación de las facturas es de forma electrónica a través del Punto general de Entrada (FACE) que actúa como portal Web. Información https://face.gob.es.

Oficina contable Órgano gestor Unidad tramitadora

L01281230 Departamento de Contabilidad e Intervención
L01281230 Ayuntamiento de Rivas Vaciamadrid o Concejalía de Hacienda
L01281230 Ayuntamiento de Rivas Vaciamadrid o Concejalía de Hacienda

4.- DURACIÓN DEL CONTRATO.

La duración del contrato será de tres años desde su formalización, estimándose el inicio de la ejecución el 1 de abril de 2024. El contrato podrá prorrogarse por dos años adicionales más, hasta un máximo de cinco años en su totalidad.

5.- CARACTERÍSTICAS DE LA PRESTACIÓN.

El ámbito de las medidas necesarias de prevención, detección y respuesta que se precisan optimizar con los servicios de mantenimiento requeridos, se centra en tres puntos de actuación sobre la arquitectura de red del Ayuntamiento:

a).- La gestión y control de acceso dentro de la actual red interna y perimetral de datos mediante una adecuada arquitectura de sistemas de firewalls o cortafuegos que protejan las redes del Ayuntamiento.

b).- La adaptación de las medidas de seguridad en todo tipo de acceso a datos a través de zonas no controladas, en cumplimiento del R.D. 311/2022, de 3 de mayo, normativa que regula el Esquema Nacional de Seguridad (ENS), con el refuerzo basado en doble factor de autenticación (2FA).

c).- La renovación de los servicios del Centro de Operaciones de Ciberseguridad (SOC).

Consideraciones a tener en cuenta en caso de propuestas de mejora:

-Hardware:

Suministro y puesta en marcha de todos los dispositivos de cada punto de actuación.

Cualquier indicación contenida en este pliego relativa a marca o modelo comercial debe entenderse referida a sus características esenciales como equivalentes.

-Software:

Instalación y puesta en marcha del software necesario para la administración de toda la infraestructura en cada punto de actuación.

Cualquier indicación contenida en este pliego relativa a marca o modelo comercial debe entenderse referida a sus características esenciales como equivalentes.

-Integraciones:

Plan de integración de herramientas hardware y software tanto, dentro de cada punto de actuación, como entre los puntos de actuación. Según los requerimientos que las características determinan, para lograr una la solución conjunta y coordinada de las mejoras de medidas de seguridad que se recogen en el pliego.

-Formación de herramientas de gestión de usuario:

Plan de formación de administrador del personal del Ayuntamiento de Rivas-Vaciamadrid para el correcto uso del hardware y software ofertado en cada punto de actuación.

El número de horas mínimo es de 40 horas anuales.

-Mantenimiento y garantía total del hardware, software y licencias:

Para todos los casos, con y sin mejoras, mantenimiento mínimo 8x5 NBD de toda la infraestructura de los servicios de mantenimiento prestados para su estado óptimo de funcionamiento, en todos y cada uno de los puntos de actuación, durante toda la duración del contrato y su posible prórroga.

5.1 CARACTERÍSTICAS DE LA ARQUITECTURA DE SEGURIDAD DE LAS COMUNICACIONES EN LA RED INTERNA A MANTENER

Las características que definen y dimensionan las herramientas actuales (hardware y software) usadas para las correspondientes actuaciones de mantenimiento preventivo y de respuesta a incidentes sobre la red de datos interna y perimetral son las indicadas en el siguiente punto 5.1.1.

5.1.1 Características de la arquitectura de herramientas firewall para gestión y control de acceso a la red interna.

Actualmente el Ayuntamiento dispone de dos firewalls perimetrales/internos, para proteger la red de datos del Ayuntamiento al controlar y filtrar el tráfico de datos en capa 7 tanto de la red interna como el acceso a Internet. Estos equipos analizan tráfico hacia internet como tráfico interno entre diferentes segmentos de la red interna del Ayuntamiento.

Incluyen características adicionales, como acceso SSL VPN para 1.100 usuarios, políticas por aplicación, políticas por usuarios (sin ninguna interacción por parte del usuario, integrados a través de Active Directory) , antivirus, inspección de archivos a través de Sandbox, IPS, url filtering, e inspección de tráfico encriptado así como protección de las distintas navegaciones de usuarios por Internet y otras medidas de seguridad para fortalecer la defensa de la red contra amenazas cibernéticas. Estos dispositivos desempeñan un papel crucial en la seguridad de la red al establecer una línea de defensa contra posibles ataques y amenazas.

Estos equipos tienen un throughput de aproximado de 30 Gbit/s UDP 64 byte cada uno.

Además, las sedes principales de la red interna del Ayuntamiento (4 sedes) cuentan con protección capa 4 para que no puedan llegar a verse unas redes con otras, protegiendo de este modo los servicios que albergan cada una de ellas.

El throughput concurrente entre todas las redes internas y red perimetral del Ayuntamiento es de unos 170 Gbit/s.

5.2 DIMENSIONADO DE ZONAS NO CONTROLADAS PARA 2FA

Un sistema de autenticación de doble factor garantiza que únicamente aquellos usuarios autorizados puedan acceder a información sensible, añadiendo una capa extra de seguridad que disminuye significativamente el riesgo de pérdida de datos. La implementación de este segundo factor será extensiva, cubriendo tanto la autenticación en accesos remotos VPN, como VDI (Vmware), Wifi, Suite de Google y Microsoft Windows, entre otros, como el posible uso desde aplicaciones externas al Ayuntamiento. Además, puede integrarse en la gestión de sistemas y plataformas de seguridad, siendo esencial para aspectos críticos del funcionamiento municipal.

La plataforma solicitada debe ser compatible con diversos tipos de Token, que son códigos únicos y temporales utilizados como segunda capa de verificación, para confirmar la identidad del usuario. El proceso de autenticación de dos factores implica generalmente dos elementos distintos que el usuario debe proporcionar para acceder a una cuenta o sistema.

Tal y como se ha establecido en este mismo apartado y para la resolución de "*La adaptación de las medidas de seguridad en todo tipo de acceso a datos a través de zonas no controladas, en cumplimiento del R.D. 311/2022, de 3 de mayo, normativa que regula el Esquema Nacional de Seguridad (ENS), con el refuerzo basado en doble factor de autenticación (2FA)*.".

Por tanto, se busca una solución 2FA para 1.000 usuarios mínimo, que pueda ser ofrecida tanto en formato de aplicación para móvil (compatible con sistemas Android, iOS), y token físicos (como tarjetas de crédito/visita o llaves USB), siendo como mínimo de 300 tokens físicos mínimo y de 700 tokens virtuales (aplicación móvil) mínimo. Todas las licencias suministradas deberán ser permanentes.

Es esencial que la plataforma admita notificaciones push, permitiendo al usuario confirmar la autenticación con un simple toque (token virtual).

5.3 CARACTERÍSTICAS SERVICIO DE MANTENIMIENTO DEL SOC soporte

El SOC del Ayuntamiento de Rivas está integrado en la Red Nacional de SOC (RNS) desde abril de 2023.

Este SOC, que actualmente y con carácter privado, da soporte 8x5 al Ayuntamiento de Rivas Vaciamadrid, de gestión de incidentes de seguridad, monitorización, operación, administración y notificación de incidentes, está caracterizado por los siguientes elementos:

- 2 Sondas BoxICAque ayudan a detectar patrones de distintos tipos de ataques o amenazas.
- Sistema de Alerta Temprana (SAT) de Internet (250 activos).
- Herramienta de intercambio de ciberincidentes LUCÍA que permite el intercambio automático, implantación y configuración de la herramienta microClaudia, proporcionando protección contra código dañino de tipo ransomware.
- Sistema de Gestión de Eventos de Seguridad MONICA NGSIEM está montado en formato virtual, con licencia Standalone MONICA NGSIEM y con licenciamiento para 16 MONITORES MONICA NGSIEM para la integración de las respectivas fuentes del Ayuntamiento. El SIEM está integrado con REYES CCN y LUCIA (requisito de permanencia en la RNS). Se dispone de acceso en modo administrador.

- Esta licencia incluye las siguientes funcionalidades:

  - ❖ Recolección de logs
  - ❖ Múltiples protocolos
  - ❖ Agentes de monitorización (multitecnología y multifabricante)
  - ❖ Repositorio Centralizado de Logs
  - ❖ Integridad del repositorio de logs
  - ❖ Búsqueda cruzada eventos – logs
  - ❖ Motor centralizado de correlación
  - ❖ Correlación: eventos / anomalías / IOC / Entidades
  - ❖ Gestión de reglas de correlación
  - ❖ Analítica avanzada
  - ❖ Tendencias y evolución de comportamientos en la red
  - ❖ Gestión de incidentes
  - ❖ Análisis estadístico de eventos de seguridad
  - ❖ Análisis forense
  - ❖ Monitorización de eventos en tiempo real
  - ❖ Cuadros de mando en tiempo real
  - ❖ Tablas y gráficos personalizables
  - ❖ Geolocalización de incidentes
  - ❖ Threat Intelligence. Feeds, reputacional y APTs. IOCs externos y fuentes IOCs de CCN. Integración MISP-REYES CCN
  - ❖ 16 licencias de MONITOR MONICA NGSIEM para monitorizar en tiempo real, entre otras, estas fuentes indicadas por el Ayuntamiento de Rivas:

    - Controladores de dominio
    - Servidores Backup
    - Servidor antivirus

- Servidor de aplicaciones Linux
- Servidor control de accesos
- Servidores gestión policia
- Servidores CCTV
- Firewall Huawei USG6635e
- Huawei S12708
- Huawei S7700
- Servidor WIFI
- Sophos XG Firewall
- EDR CrowdStrike

6.- SOLVENCIA TÉCNICA Y FINANCIERA

La entidad licitadora presentará la declaración responsable conforme al modelo recogido en el pliego de condiciones administrativas. Únicamente la entidad propuesta como adjudicataria deberá acreditar el siguiente extremo que se menciona a requerimiento del Ayuntamiento:

Relación de los principales suministros o trabajos realizados de igual o similar naturaleza que los que constituyen el objeto del contrato en el curso de los tres últimos años, en la que se indique el importe, la fecha y la persona destinataria, pública o privada de los mismos, avalada por certificados de buena ejecución; estos certificados indicarán el importe, las fechas y el lugar de ejecución de los servicios y precisarán si se realizaron según las reglas por las que se rige la profesión y se llevaron normalmente a buen término, cuyo importe anual acumulado en el año de mayor ejecución sea igual o superior al 70% de la anualidad media del contrato (46.280,92 € IVA no incluido).

7.- PRESENTACIÓN DE OFERTAS

La presentación de ofertas será por medios electrónicos a través de la plataforma de contratación del sector público y del siguiente modo

Se presentará en archivos electrónicos independientes:

<u>Archivo electrónico nº 1:</u>

- Contendrá declaración responsable

<u>Archivo electrónico nº 2:</u>

- Contendrá criterios evaluables mediante valoración técnica.

Contendrá criterios evaluables mediante valoración técnica que comprenderá la memoria descriptiva de la solución ofertada con un índice explicativo de los apartados.

Los videos demostrativos, en su caso, deberán entregarse en formato electrónico y deberán estar accesibles para su visualización a través de una dirección en internet o similar.

Archivo electrónico nº 3:

- Contendrá criterios evaluables mediante la aplicación de fórmulas.

8.- CRITERIOS DE ADJUDICACIÓN

Los criterios de adjudicación se distribuirán de la siguiente manera:

8.1. Archivo Electrónico 2: Criterios evaluables por valoración técnica (hasta 45 puntos)

Memoria Descriptiva, hasta 45 puntos:

Se establece un límite máximo de 120 páginas numeradas y que comprenderá portada, índice, contraportada, anexo, planos, bibliografía o similar: (no se valorará lo que exceda del límite establecido):

Valoración global de la solución Para la valoración de la calidad de la propuesta técnica se tendrá en cuenta la contextualización de este tipo de servicios de mantenimiento, la coherencia, idoneidad y la definición de la solución técnica a aportar, valorando todo lo relacionado con la solución propuesta, y que deberá versar sobre cada de las tres actuaciones a), b) y c) indicadas en la cláusula 5 de este PPT. Se valorarán todos los aspectos generales de cada solución, el cumplimiento de los requisitos técnicos	**Hasta 25 puntos**

generales y particulares, funcionalidades y ejemplos de integración en Ayuntamientos de similar tamaño o complejidad. Dentro de este apartado se valorará una explicación nítida y realista de la planificación de la configuración de la solución propuesta, su puesta en marcha, especificando tareas detalladas, integraciones necesarias y tiempos de realización de cada fase e intervinientes . Se pretende securizar una solución que aporte al Ayuntamiento seguridad en todos sus redes tanto internas como externas a nivel de capa 7 (Analisis de trafico IPS, Protection Malware, Control de aplicaciones, Url Filtering, Anti Spam, grupo de usuarios, y analisis de trafico encriptado) a sí mismo, acceso a todos sus usuarios a través de VPN, se requiere que el fabricante de esta solución propuesta tenga que estar reconocido en el cuadrante líder del último Cuadrante Mágico de Gartner para Network Firewall, por otra parte se requiere securizar con 2FA, estos accesos VPN, el acceso VDI de VMware, red WIFI y accesos de los Pcs clientes y servidores través de Active Directory del Ayuntamiento, a través de token virtuales o físicos, las licencias deberán ser permanentes y permitir Universal ZTNA. La solución de mantenimiento propuesta en su conjunto debe tener, la capacidad de envío de tráfico al SIEM el cual estará integrado con REYES y LUCIA del CCN, así esté SIEM deberá de poder interactuar de forma bidireccional con la solución propuesta para realizar de forma autónoma configuraciones en los FWs y EDR de forma nativa a través	

de API, garantizando la configuración de políticas que eviten un incidente de Ciberseguridad. Se valorarán soluciones que permitan la securización de la solución de Google Workspace utilizada por el Ayuntamiento.	
Sencillez y facilidad de uso de los servicios Valorándose de forma especial la facilidad de uso que los servicios ofrezcan al personal y terceros para poder adaptarse a los mismos. Esta valoración subjetiva se realizará a partir de la descripción de los procedimientos de gestión para todos los puntos de actuación.	**Hasta 10 puntos**
Servicios de Soporte y Acompañamiento Valorándose de los servicios de consultoría, formación (sin indicar el número de horas adicionales ofertadas de formación, soporte y acompañamiento) previstos para garantizar el uso correcto de los servicios contratados para cumplir con todos los objetivos descritos en este PPT.	**Hasta 10 puntos**

8.1.2.- Archivo Electrónico 3: Criterios evaluables mediante aplicación de fórmulas (hasta 55 puntos).

Mejor precio ofertado (5 puntos máximo):. Se asignará 5 puntos al licitador que oferte mayor porcentaje de baja sobre el precio del contrato, IVA no incluido, y al resto de forma proporcional, siguiendo la siguiente fórmula: X puntos obtendrá = % de baja ofertada * 5 puntos /% de la mayor baja ofertada. Para la apreciación de baja temeraria se aplicarán los criterios contenidos en el Art. 85 del RD 1090/2001, Reglamento General de la Ley de Contratos de la Administración Pública.	**Hasta 5 puntos**
Aumento de Funcionalidades y Equipamiento Se asignan las siguientes puntuaciones en cada uno de los puntos de actuación, hasta un máximo de 35 puntos: **1.- Adecuación con el ENS (5 puntos máximo):** Se valorará que las soluciones ofertadas dispongan del Certificado de Conformidad con el ENS con el Esquema Nacional de Seguridad como mínimo de Nivel MEDIO. Si dispone y acredita la certificación en vigor mediante su presentación se le asignan **5 puntos**.	**Hasta 35 puntos**

2.- Gestión y control de acceso a la red perimetral (8 puntos máximo): Mejora de los dos Firewall perimetrales en configuración activo-activo con las siguientes características o superiores, Throughput 64 byte UDP de 70 Gbps cada uno, acceso VPN de cliente para 1.000 usuarios mínimo,que tenga capacidad para: análisis de tráfico IPS, protección malware, control de aplicaciones, url filtering, antispam, antivirus, políticas por usuarios/grupos, desencriptación de tráfico para su análisis, posibilidad de envío para análisis a Sandbox virtual o local, los dispositivos tendrán analisis de protección para entornos OT y permitirán Universal ZTNA. La gestión y administración de la plataforma ofertada se hará de forma centralizada. **Se asignarán 8 puntos** por la acreditación mediante la aportación del modelo del equipo ofertado y sus correspondientes licencias de uso permanente que justifique las características citadas en el párrafo anterior. Se puntuará con 0 puntos cualquier oferta que no incluya todas las características descritas en este apartado. **3.- Gestión y control de acceso a la red interna (hasta 8 puntos máximo):** Mejora de seguridad de la red interna del Ayuntamiento en cuatro de sus sedes, a través de la inclusión de firewalls con las siguientes características o superiores, Throughput 64 byte UDP de 11 Gbps, análisis de tráfico IPS, protección malware, control de aplicaciones, url filtering, antispam, antivirus, políticas por usuarios/grupos, desencriptación de tráfico para su análisis, posibilidad de envío para análisis a Sandbox virtual o local, los dispositivos tendrán analisis de protección para entornos OT y permitirán Universal ZTNA. Además, la gestión y administración de la plataforma se hará de forma centralizada.	

Se asignarán 2 puntos por cada equipo ofertado y acreditado hasta un máximo de 8 puntos, mediante la aportación del modelo del equipo ofertado en cada una de las 4 sedes correspondientes y que justifique las características citadas en el párrafo anterior. Se puntuará con 0 puntos cualquier oferta que no incluya todas las características descritas en este apartado. **4.- Alta disponibilidad de las Medidas de seguridad en zonas no controladas (2FA) (1 punto máximo)** Por el cumplimiento y de una solución de 2FA que incluya alta disponibilidad, a través de la duplicación de herramientas de autenticación, se valorará con 1 punto. Para su valoración se deberá presentar compromiso expreso firmado en el que conste el cumplimiento de la Alta disponibilidad en Medidas de seguridad en zonas no controladas (2FA) **5.- Servicio de 50 licencias de recolección de datos (2 puntos máximo):** Por la inclusión de un mínimo de 50 licencias para recolectar datos a nivel de syslog de las fuentes externas: **2 Puntos.** Para su valoración se deberá presentar compromiso expreso firmado en el que conste las licencias de recolección de datos. **6.- Servicio de análisis de red de Servidores del Ayuntamiento (servidores Windows y Linux) desplegados en un entorno virtual Vmware (4 puntos máximo):** Se valorará con **1 punto por cada paquete de 25 servidores hasta un máximo de 4 puntos.**	

Para su valoración se deberá presentar compromiso expreso firmado en el que conste cada paquete de 25 servidores ofertados que incluya las características antes citadas. **7.- Mejora en la securización de los datos residentes en la Google Workspace del Ayuntamiento (7 puntos máximo):** Por la visibilidad y protección de malware para aplicaciones SaaS para 900 usuarios de Google Workspace, incluyendo el análisis de escaneo para un mínimo de 10 TB/año, se asignarán 7 puntos. Para su valoración se deberá presentar compromiso expreso firmado en el que conste la mejora de la securización con las características antes descritas.	
Inclusión del soporte (24x7x365) sobre el SIEM (10 puntos máximo): Inclusión del soporte (24x7x365) sobre el SIEM para la notificación de incidentes detectados de seguridad al CCN y al propio Ayuntamiento, así como para su contención y remediación: 10 puntos. Se asignarán 10 puntos al compromiso expreso firmado en el que conste el soporte antes descrito.	**10 puntos**

Horas de formación adicional (5 puntos máximo): Formación adicional a las 40 horas requeridas: La formación será para un grupo de 5 a 8 personas y se realizará en el Ayto. de Rivas Vaciamadrid en las sesiones y turnos que estime oportunas según necesidades municipales. El número máximo de horas adicionales de formación que se podrán ofertar son 40 horas conforme a la siguiente fórmula: X puntos obtendrá = nº de Horas Ofertadas adicionales * 5 puntos/ 40 (máximo Número de Horas adicionales a las exigidas).	**Hasta 5 puntos**

9.- CONDICIONES DE MODIFICACIÓN DEL CONTRATO

No se contempla.

10.- INCUMPLIMIENTO. CUMPLIMENTO DEFECTUOSO. PENALIDADES. RESOLUCIÓN DE CONTRATO.

Según la LCSP.

DOCUMENTO FIRMADO ELECTRÓNICAMENTE

EL TÉCNICO MEDIO DE INNOVACIÓN

EL JEFE DE SERVICIOS DIGITALES

EL JEFE DE SERVICIO DE INNOVACIÓN Y MODERNIZACIÓN

COORDINADOR DEL ÁREA DE ECONOMÍA Y ORGANIZACIÓN