PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE TELECOMUNICACIONES

ÍNDICE

1.- OBJETO DEL CONTRATO.

El presente pliego tiene por objeto el establecimiento de las condiciones técnicas que regirán la contratación de los servicios de comunicaciones: telefonía fija (IP y Analógica), telefonía móvil y de datos en movilidad, transmisión de datos, infraestructura de red LAN-Wifi, puesto de trabajo y de seguridad, acceso a internet para el Ayuntamiento de Mérida así como los servicios de transmisión de datos que posibilitan la integración de todas las sedes del Ayuntamiento de Mérida (Intranet del Ayuntamiento de Mérida).

La Red Corporativa del Ayuntamiento se establece por tanto como elemento crítico sobre el que se deben soportar todos los servicios internos al organismo y externos hacia los ciudadanos alineándose con las tendencias del mercado:

- El valor de la nube.
- La importancia de los Datos y reutilización.
- Refuerzo de la Ciberseguridad.
- Propiciando la Multicanalidad.
- Permitiendo operaciones más flexibles y resilientes en base a estándares de mercado.
- Potenciando la automatización de procesos.

El Ayuntamiento de Mérida acomete con este proyecto la modernización, evolución , optimización y mantenimiento de las infraestructuras de los servicios de comunicaciones, lo cual le permitirá acometer nuevos proyectos orientados a:

- Disminución de costes de comunicaciones.
- Aumento de los anchos de banda de las comunicaciones.
- Aumento de la seguridad para el alojamiento de nuevos servicios. Implantación de nuevos servicios de administración digital.
- Mantenimiento de la Adecuación al Esquema Nacional de Seguridad e Interoperabilidad. Soluciones de continuidad de negocio (CPD de respaldo).
- Soluciones de movilidad y trabajo colaborativo.
- Eficiencia energética.
- Palanca de proyectos de ciudad y turismo inteligente.
- Reducción de emisiones.

A modo de resumen, los servicios y evoluciones incluidos en el objeto del contrato son los siguientes:

1. **Transmisión de Datos (Red Corporativa Multiservicio):**

   a. Aumento de anchos de banda de 1Gb a 10GB para las Sedes de Palacio y Urbanismo.

   b. Aumento a 1Gb de sedes Remotas con fibra propia de operador para el total de sedes.

   c. Mejora de los anchos de banda de navegación Internet.

   d. Seguir ampliando sedes con tecnología SDWAN.

   e. Mantenimiento la red de fibra propietaria del Ayuntamiento.

2. **Seguridad**

   a) Renovación total de los equipos actuales (firewall de primer y segundo nivel) buscando eficiencias en fabricantes de primer nivel.

   b) Servicios de administración delegada.

   c) Detección de vulnerabilidades y pentesting.

3. **Puesto de Trabajo**

   a) Renovación total de los equipos actuales buscando eficiencias en fabricantes de primer nivel.

4. **Red de Área Local**

   a) Seguridad desde la red: Buscar la eficiencia y seguridad en la gestión consolidando consolas de gestión y unificando el equipamiento de switching integrado con la seguridad.

   b) Sustitución de Switches de Core y Acceso obsoletos, con filosofía de consolidación y unificación.

5. **Voz Fija y Móvil**

   a) Adquisición de terminales móviles de gamas media y alta.

   b) Contemplar el móvil como una extensión del puesto de trabajo, con servicios de disponibilidad total.

   c) Mantenimiento de la plataforma de voz IP actual on premise ampliando el stock de los terminales.

6. **CPD y Servicios Web**

   a) Mantenimiento de la nueva infraestructura de CPD encargada de prestar servicios digitales a través de la Red.

b) Renovación de los servidores de Bases de Datos contemplando la mejora en la resiliencia y continuidad de negocio.

c) Disponer de más direcciones IP para publicación de servicios.

d) Soporte a las webs institucionales.

e) Incremento en Cuentas de correo electrónico, correos masivos y gestión de webs actuales.

f) Incremento de espacio Cloud para backup tercera copia, planes de contingencia y almacenamiento masivo.

El periodo de vigencia de este contrato queda fijado en 60 meses.

2.- CONDICIONES GENERALES.

Las ofertas presentadas por los licitadores deben cumplir las siguientes condiciones generales:

- Al objeto de realizar la valoración económica de las ofertas, los licitadores presentarán su oferta económica teniendo en cuenta las estructuras y tipo de servicios y la situación actual. Los licitadores podrán incluir cuantos descuentos, planes, etc. consideren necesarios.

- Se prevé un tiempo suficiente desde la firma del contrato para el despliegue de los equipos y servicios ofertados por el adjudicatario. No obstante, lo anterior, el adjudicatario deberá, a partir de la fecha entrada en vigor del contrato, asumir los costes asociados al funcionamiento actual del servicio de comunicaciones, hasta la migración/implantación de las nuevas soluciones ofertadas en caso de no alcanzarse la sustitución completa a fecha de inicio del nuevo contrato, los costes de migración/implantación serán asumidos por el adjudicatario.

- Durante el desarrollo del contrato, el Ayuntamiento de Mérida podrá dar de baja o incorporar nuevas sedes a su Red Corporativa según los crecimientos establecidos en dicho PPT. En el caso de las altas, el adjudicatario se encargará del suministro y mantenimiento de los enlaces y equipos que sean necesarios. En el caso de las bajas, el Ayuntamiento de Mérida no estará sujeta a ningún tipo de penalización por permanencia, aunque no se haya cumplido el plazo de duración del contrato.

- Así mismo, a los proyectos singulares que se presenten durante la vigencia del contrato de prestación de servicios de comunicaciones electrónicas, y que fueran asimilables a las condiciones de los servicios del CSPS, les serán de aplicación todas las condiciones acordadas con el adjudicatario. En otro caso, serían objeto de negociación.

- Los licitadores presentarán un plan de formación de todas las tecnologías, soluciones y equipamientos ofertados.

Además, se deberán tener en cuenta las siguientes premisas:

- Soporte IPV6: configuración e implantación de dicho protocolo dentro del direccionamiento IPv6 del Ayuntamiento de Mérida, en todo el equipamiento incluido en el contrato, donde dicha característica sea aplicable y sin coste adicional.

- Arquitectura compatible con los servicios y aplicativos corporativos, direccionamiento de red, protocolos, conectividad con servidores, VLANs y tecnologías existentes en la actualidad.

- Integración del equipamiento que lo requiera con los servicios de directorio corporativo del Ayuntamiento de Mérida y servidores de autenticación. Así mismo deberá soportar el uso de factor múltiple de autenticación aquellos equipos que sean accesibles desde fuera de las instalaciones del Ayuntamiento.

- Integración de los equipos que lo requieran con las plataformas de monitorización y seguridad (por ejemplo, SIEM, sondas del CCN, etc.).

- El equipamiento actual es susceptible de ser utilizado, si bien todos los costes de operación y mantenimiento correrán por cuenta del adjudicatario.

- Todo el equipamiento que, como consecuencia de la nueva infraestructura de comunicaciones quede sin servicio, deberá ser retirado por el adjudicatario para su reciclado o destrucción cumpliendo éste, en cuanto a su tratamiento, con toda la legislación existente sobre de reciclado y destrucción de equipamiento electrónicos en base a las características del mismo que puedan ser exigibles. El coste de dichos trabajos correrá a cargo del adjudicatario.

- Todo el equipamiento suministrado por el adjudicatario durante la vigencia del contrato pasará a ser propiedad del Ayuntamiento de Mérida, una vez finalizada la duración del mismo.

- Todos los equipamientos y trabajos auxiliares necesarios para la implantación de los servicios objeto del presente concurso, correrán por cuenta del adjudicatario.

- Todo el equipamiento suministrado deberá estar dentro del Catálogo del CCN- CERT, COMMON CRITERIA o Cuadrante Mágico de Gartner 2024.

2.1. PREPARACIÓN Y EJECUCIÓN DEL CONTRATO.

Los licitadores dispondrán en todo momento de los recursos humanos adecuados y suficientes para prestar apoyo y soporte técnico a todas las sedes incluidas en el proyecto, a fin de garantizar la correcta y óptima realización de las fases de implantación y operación. Deberán detallar en concreto:

- Situación y número de centros de Gestión de Red que estarán directamente implicados en los servicios del contrato.

- Procedimientos de detección, comunicación, tratamiento y escalado de incidencias y averías, tipificación de averías, tiempos de respuesta y tiempos de resolución.

- Servicio de asistencia técnica y mantenimiento (garantía de servicio, línea telefónica de asistencia 24 horas/7 días semana) para recogida y resolución de incidencias, averías y problemas.

El Ayuntamiento de Mérida podrá contar con una oficina técnica de apoyo a la fase de transición entre el contrato actual y el de objeto de la presente contratación.

2.2.1 ORGANIZACIÓN DEL TRABAJO.

En general, los trabajos se llevarán a cabo de modo que se interfiera lo menos posible el funcionamiento normal de las diferentes dependencias del Ayuntamiento de Mérida. En todos los casos deberá preverse una vuelta atrás a la situación anterior, en caso de que surjan problemas, en el plazo máximo de 6 horas. Será el Ayuntamiento de Mérida la que decidirá en última instancia la fecha y hora de realización de dichos trabajos.

La implantación de estos servicios en los diferentes edificios se realizará teniendo en cuenta su singularidad y su volumen de servicios y criticidad de los mismos, contando todos los usuarios con los servicios de voz y datos durante el período que dure la instalación de la nueva solución.

En todo caso, salvo que se demuestre la imposibilidad de hacerlo, existirá un periodo de funcionamiento “en paralelo” que garantizará permanentemente el servicio y la posibilidad de recuperar la configuración anterior, caso de que existan problemas.

2.2.2. IMPLANTACIÓN.

La fase de implantación comprende la dotación, instalación, configuración y puesta en marcha de las líneas, circuitos y equipamiento físico de cada una de las sedes, así como de las pruebas de aceptación requeridas.

Para el desarrollo de los trabajos de puesta en marcha, el adjudicatario deberá designar un responsable del proyecto que actuará como interlocutor único con el personal que el Ayuntamiento de Mérida designe a fin de supervisar el proceso de implantación de los servicios objeto del pliego.

La oferta deberá incluir un Plan de Implantación de las infraestructuras ofertadas, la elaboración de un programa de trabajo y su planificación temporal, para la instalación, prueba y puesta a punto del servicio en cada una de las sedes o grupos homogéneos de sedes. El contenido del plan responderá a lo solicitado en el apartado “Plan de Implantación”.

Las distintas actuaciones del Plan de Implantación necesitarán el visto bueno del Ayuntamiento de Mérida y serán comunicadas como mínimo con 48 horas antes de su ejecución. Igualmente, el emplazamiento del equipamiento, cableados, etc. se determinará de acuerdo con el Ayuntamiento de Mérida.

La fecha de inicio de la prestación de los servicios será la definida en el plan de implantación, siendo responsabilidad del adjudicatario la prestación del servicio a partir de dicha fecha. En caso de ser un servicio ya ofrecido por un anterior prestador, el adjudicatario debe asegurar el correcto funcionamiento del servicio en las condiciones definidas en el actual pliego, debiendo llegar a los acuerdos necesarios con el anterior prestador del servicio a sustituir para asegurar el correcto funcionamiento del mismo. En ningún caso, el Ayuntamiento de Mérida se hará cargo de los costes derivados de dicha transición siendo la responsabilidad total y exigible del mantenimiento del servicio actual al adjudicatario.

Los licitadores deberán especificar en sus propuestas los procedimientos de portabilidad de servicios, que tendrán que coincidir con el cambio de red, Al objeto de minimizar el tiempo de indisponibilidad, las migraciones deberán ser realizada preferentemente en horario nocturno y fines de semana.

El calendario del plan de migración tendrá que incluir la ejecución de las actividades necesarias fuera del horario de actividad habitual de cada sede.

En cuanto al cambio de infraestructura, se procederá de la misma forma, minimizando siempre el tiempo de indisponibilidad y fuera del horario de actividad del edificio.

El plan de migración incluirá un procedimiento con el detalle de las actividades a realizar, los requerimientos estimados por parte del responsable del edificio correspondiente, el equipo de trabajo que intervendrá, el tiempo previsto para la finalización de los trabajos y el tiempo previsto de indisponibilidad.

2.2.2. ALCANCE Y CONDICIONES.

En el apartado de Mantenimiento de la infraestructura se define explícitamente la provisión de los servicios, que subdividimos en 3 grupos:

1.- Entrega de infraestructuras / provisión de sedes:

- Puesta en servicio de la sede desde la recepción de la infraestructura en el adjudicatario.

2.- Modificaciones del servicio:

- Traslado de origen o destino de un edificio a otro.
- Traslado de origen o destino de circuitos y equipamiento de acceso a Internet de un edificio a otro.
- Traslado interno de circuitos y equipamiento dentro de un mismo edificio, aun cuando el mismo implicase traslado de los medios de transmisión y/o acometida física al edificio.

- Traslado interno de circuitos y equipamiento de acceso a Internet dentro de un mismo edificio, aun cuando el mismo implicase traslado de los medios de transmisión y/o acometida física al edificio.
- Actualizaciones de versiones de software de todo el equipamiento y herramientas de gestión.

3.- Cambios de configuración puntuales:

- Alta / baja/modificaciones de configuración de líneas.
- Alta / baja/modificaciones de los datos administrativos de DNS, IPs públicas, dominios, etc.

No computarán para el cálculo del tiempo de resolución los de retrasos debidos a la imposibilidad de resolución de las peticiones por motivos imputables al Ayuntamiento de Mérida (por ejemplo, la inaccesibilidad de las instalaciones).

2.2.3. PRUEBAS

El licitador deberá incluir en su oferta un Plan de Pruebas con el objeto de validar el funcionamiento de los servicios antes de su puesta en explotación. Este plan debe permitir al Ayuntamiento de Mérida revisar y garantizar que los servicios tienen la calidad y funcionalidades exigidos en el pliego y descritos en la oferta del operador.

El Plan de Pruebas será revisado por Ayuntamiento de Mérida durante la fase de implantación, pudiendo exigir su actualización con el objeto de adecuarlo a las necesidades vigentes en esa fase.

Si en algún caso es necesaria la desconexión de los servicios o sistemas actuales, ésta no se llevará a cabo hasta que el Ayuntamiento de Mérida haya validado los resultados del plan.

2.2.4. OPERACIÓN Y MANTENIMIENTO.

La fase de operación comprende el periodo posterior a la implantación y supone el comienzo de la prestación del servicio contratado, previa aceptación por parte del Ayuntamiento de Mérida. Esta fase incluye el mantenimiento, la gestión, detección y resolución de incidencias y la actualización (cuando sea preciso) de los circuitos y servicios contratados de acuerdo con los requerimientos de este pliego.

Las ofertas deberán incluir un Plan de Operación y Mantenimiento, donde se definan las actividades y responsabilidades encaminadas a asegurar el correcto y continuo funcionamiento del servicio, de acuerdo con el esquema de gestión indicado en el presente pliego. En esta fase se requiere el mantenimiento y la gestión de los servicios de telecomunicaciones, en modalidad de atención 24 horas al día, 7 días a la semana.

Para el desarrollo de estos planes el adjudicatario otorgará al Ayuntamiento de Mérida la condición de “Gran Cuenta”, facilitando el acceso a los servicios que se incluyan dentro de este estatus por parte del adjudicatario como:

- Tratamiento personalizado de incidencias.
- Tiempo de resolución de las mismas
- Tiempo elaboración de nuevos proyectos técnicos
- Asesoramiento técnico
- Etc.

Estos servicios se realizarán desde el Centro de Gestión definido con más precisión en el apartado "Centro de Gestión", como medio de contacto disponible las 24 horas al día.

Con el fin de controlar el equipamiento operativo, al inicio de la prestación del servicio el adjudicatario aportará una relación exhaustiva del equipamiento existente en cada centro, del que hará uso y del equipamiento nuevo instalado por el adjudicatario. Esta relación servirá de base para la prestación del mantenimiento y será actualizada reflejando las modificaciones realizadas a lo largo de la prestación del servicio.

2.2.5. INCIDENCIAS.

El adjudicatario presentará un Plan de Emergencia que contendrá la descripción de los planes de actuación que deberán seguirse en el caso de que se produzca un desastre o incidencia grave en los servicios ofertados.

2.2.6. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.

La naturaleza especialmente confidencial de toda la información generada en el Ayuntamiento de Mérida, y que será transportada por la red del adjudicatario, hace necesario un meticuloso plan de seguridad de la información.

El adjudicatario se asegurará de que los servicios prestados en virtud del presente Pliego, así como los sistemas de información que los sustentan, se prestan de conformidad a los requisitos de seguridad establecidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, o cualquier actualización de estas leyes a lo largo de la vigencia del contrato, así como la Política de Seguridad, los Procedimientos y las Instrucciones Técnicas existentes en Ayuntamiento de Mérida.

El Ayuntamiento de Mérida se reserva el derecho a trasladar futuros requisitos de seguridad al proveedor dentro del marco de actividades objeto del presente contrato.

El adjudicatario deberá cumplir en todo momento la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la normativa de desarrollo de la misma, y será responsable de la seguridad y confidencialidad de las comunicaciones electrónicas

contratadas. El adjudicatario suscribirá un contrato de confidencialidad con el Ayuntamiento de Mérida en el que se regulará su relación con la misma al respecto.

Los licitadores deberán presentar evidencias de certificaciones oficiales en materia de seguridad tales como ISO/IEC 27001 y 27002 o equivalente, como medida de garantía en esta materia.

Sin perjuicio de lo anterior, el licitador deberá contar con las certificaciones siguientes o equivalentes correspondientes al esquema nacional de seguridad (ENS):

- ENS Alto en comunicaciones fijas (VPN IP, MPLS, Data Internet, NGN) y móviles.
- ENS Alto comunicaciones fibra.

2.2.7. ACTUALIZACIÓN TECNOLÓGICA.

Si durante el período de vigencia del contrato la empresa adjudicataria hubiera introducido en el mercado innovaciones tecnológicas que impliquen, a juicio del Ayuntamiento de Mérida, mejoras en el servicio inicialmente contratado, éste se reserva la decisión de introducir dicha tecnología en la red ya operativa, previo acuerdo con el adjudicatario.

2.2.8. GARANTÍA Y MANTENIMIENTO DE LOS EQUIPOS.

Todos los equipos que se suministren a partir de la firma del contrato, así como aquellos que forman la planta actual de seguridad deben estar vigentes en el mercado y disponer de mantenimiento técnico oficial. Se incluirá garantía de reparación o, en su caso, sustitución en caso de avería para el período de duración del contrato. En el momento en que queden descatalogados deben sustituirse por los que les reemplacen o por otros superiores en cuanto a prestaciones y calidades, siempre de acuerdo y previa conformidad de Ayuntamiento de Mérida. El adjudicatario asumirá el mantenimiento integral de toda la infraestructura de acceso de la Red de Datos en un horario 24x7, 365 días al año para el equipamiento definido como crítico y que no superará el 15% del total.

En caso de avería, el adjudicatario siempre deberá suministrar un equipo de iguales o superiores prestaciones para garantizar la prestación de servicio. Este equipo se suministrará de acuerdo con los parámetros definidos en los ANS. Los períodos de reparación y sustitución de los equipos averiados respetarán los tiempos descritos en los ANS.

Cualquier actuación física para reparación de averías, realización de traslado de líneas, altas, bajas, sustitución de equipos, desplazamientos de personal, programación de routers, etc. estarán incluidos en el servicio ofertado por el adjudicatario, no suponiendo ningún coste adicional para Ayuntamiento de Mérida, sea cual sea el origen o motivo de las labores de mantenimiento a realizar.

Este mantenimiento incluye explícitamente el siguiente equipamiento, además del que se indica a lo largo del presente pliego:

- Doble fuente de alimentación en equipos de transmisión.
- Mantenimiento de la red troncal WAN/MAN.
- Todos los routers de backbone necesarios para la terminación de todas las interconexiones de fibra óptica o similar y de las sedes remotas.

- Conexión de todas las sedes existentes actualmente con una línea de capacidad suficiente para dar servicio adecuado a voz y datos.
- Todos los routers para la interconexión de las sedes.
- Herramientas de gestión y/o tarificación.
- Líneas para el acceso a Internet (principal y secundaria).
- Routers de acceso a Internet.

También se considerarán tareas de mantenimiento la provisión del servicio, por lo que no podrán suponer coste adicional al Ayuntamiento de Mérida:

- Alta/baja/modificaciones de configuración de líneas.
- Traslado de origen o destino de un edificio a otro.
- Traslado interno de circuitos dentro de un mismo edificio, aun cuando el mismo implicase traslado de los medios de transmisión y/o acometida física al edificio.
- Actualizaciones de versiones de software de todo el equipamiento y herramientas de gestión.
- Alta/baja/modificaciones de los datos administrativos de DNS, IPs públicas, dominios, etc.
- Traslado de origen o destino de circuitos de acceso a Internet de un edificio a otro.
- Traslado interno de circuitos de acceso a Internet dentro de un mismo edificio, aun cuando el mismo implicase traslado de los medios de transmisión y/o acometida física al edificio.
- Actualizaciones de versiones de software, firmware, updates, upgrades, etc., de todo el equipamiento y herramientas de gestión.

- Asimismo, el adjudicatario deberá mantener todo el equipamiento ofertado objeto de mantenimiento, en la última versión de software o firmware homologada.

Cada vez que los fabricantes liberen una nueva versión de software o firmware para cualquier elemento de la red de acceso de datos e Internet (routers, herramientas de gestión, equipamiento de interconexión, etc.) el adjudicatario deberá comunicárselo al Ayuntamiento de Mérida. El adjudicatario deberá proporcionar todas las actualizaciones de seguridad para el equipamiento del Ayuntamiento de Mérida lo más rápidamente posible, de modo que el tiempo de exposición a vulnerabilidades por parte del Ayuntamiento de Mérida se vea reducido al mínimo posible.

En todo caso, previa a la instalación de nuevas versiones, deberá realizar pruebas de compatibilidad de este software con las funcionalidades implantadas en la Red.

Una vez realizadas estas pruebas deberá presentar un informe de planificación, a realizar por el adjudicatario, para acometer la actualización, que incluirá tiempos estimados de corte, medidas explícitas para minimizar el impacto del corte, etc.

El adjudicatario deberá garantizar que todos los productos que suministre al Ayuntamiento de Mérida serán nuevos y en su empaquetamiento original. Ningún tipo de sustitución deberá ser provista sin el consentimiento escrito del Ayuntamiento de Mérida. El adjudicatario certificará que los productos son genuinos del fabricante, con total garantía del mismo y que cualquier tipo de software relacionado al equipo tiene una licencia original autorizada para ser utilizada por el comprador.

Al inicio del contrato y para cada suministro de material realizado a lo largo del mismo, el adjudicatario deberá presentar documento que acredite lo anterior.

2.2. CENTRO DE GESTIÓN.

El adjudicatario dispondrá, durante todo el periodo de vigencia del contrato, de un "Centro Técnico de Gestión" con soporte remoto, con personal cualificado y que conozca perfectamente todos los equipos y sistemas desplegados en la Red Corporativa Multiservicio del Ayuntamiento de Mérida para su supervisión y mantenimiento de los mismos.

La franja horaria para el soporte remoto personalizado del "Centro Técnico de Gestión" serán en la modalidad de atención 24x7 de los equipos y sistemas que se desplieguen.

Sin menoscabo de lo anterior, aquellos trabajos que, dada su naturaleza o impacto sobre los elementos y tecnologías existentes en producción, requieran una mayor atención por parte del adjudicatario serán efectuados por los integrantes del "Centro Técnico de Gestión" en cualquier franja horaria de manera remota y/o presencial según lo más aconsejable en función de las características de la actuación. Se realizarán, además, reuniones periódicas entre el Ayuntamiento de Mérida y los ingenieros de red del adjudicatario.

El "Centro Técnico de Gestión" abarcará los servicios objeto de este concurso como son de: Datos, de Telefonía IP, de LAN y Seguridad. Hará el nivel 0, será la Ventanilla única, entre el Ayuntamiento de Mérida y el adjudicatario. Sus funciones serán:

- Recoger las incidencias por parte de los técnicos del Ayuntamiento de Mérida y gestionar dichas incidencias de acuerdo con el sistema de gestión propuesto.
- Comunicar de forma proactiva las averías críticas.
- Reunirse con los responsables de sede cuando así sea solicitado para las revisiones de servicio.
- Realizar análisis y propuestas de mejora en función del estado de los servicios.
- Supervisar el estado de los elementos de su red y de todos aquellos elementos incluidos en el objeto de este contrato.
- Gestionar las alarmas ante fallos.
- Realizar el mantenimiento exigido en este PPT y cambios en la configuración.
- Administrar la seguridad de los elementos de la infraestructura.
- Realizar inventario de los elementos utilizados para la provisión de los servicios.
- Realizar los informes mensuales exigidos en este PPT, vigilando el cumplimiento de los niveles de servicio.

El Centro de Gestión tendrá, adicionalmente a las anteriores, asignadas las siguientes tareas:

- Gestionar las alarmas para prevenir fallos.
- Recoger las incidencias por parte de los técnicos del Ayuntamiento de Mérida y gestionar dichas incidencias de acuerdo con el sistema de gestión propuesto.
- Comunicar de forma proactiva las averías críticas.
- Administrar la seguridad de los elementos de la infraestructura.

3. GESTIÓN DEL SERVICIO.

3.1. PRINCIPIOS DEL MODELO DE GESTIÓN.

El correcto funcionamiento de los servicios de comunicaciones electrónicas objeto del presente contrato, sólo es posible mediante el adecuado desarrollo operativo de un modelo de gestión a la medida de las necesidades del Ayuntamiento de Mérida. Por ello es necesario que se le proporcione al Ayuntamiento de Mérida una serie de servicios como:

3.1.1. RECONOCIMIENTO DE "ESTATUS DE GRAN CUENTA".

Este reconocimiento deberá traducirse en hechos tangibles, entre los que cabe citar:

1.- Interlocución nominal: El acceso a cualquier servicio de gestión se hará a través de interlocutores nominalmente identificados, no mediante un pool de agentes, centros de atención telefónica generales o recursos compartidos con el gran público.

A lo sumo el adjudicatario definirá 3 Responsables de Proyecto, pudiendo recaer todas las funciones en una o más personas, con los siguientes perfiles:

- Responsable Comercial.
- Responsable de Ingeniería e Implantación.
- Responsable de Mantenimiento.

Los interlocutores Comercial y de Ingeniería deberán estar disponibles, de forma ordinaria, en horario laboral y, para situaciones excepcionales, en horario 24x7 cuando así lo demande el servicio.

El Responsable de Mantenimiento estará disponible en horario 24x7, como interlocutor de escalado de incidencias e informará periódicamente del estado de la avería para aquellas averías que afecten a las líneas y servicios críticos.

Además, uno de estos responsables se designará como Responsable de Cuenta, que será el responsable máximo del proyecto.

2.- Tratamiento de excepción para servicios críticos o necesidades sobrevenidas: servicio de atención presencial y telefónica 24x7 para incidencias en los servicios y líneas críticos.

3.- Interlocución presencial para los casos y temas que se solicite. Esta interlocución se realizará de forma ordinaria en reuniones quincenales. Estas reuniones se celebrarán en los locales del Ayuntamiento de Mérida en el día y hora que se determine oportuno. Puntualmente se podrá requerir la celebración de reuniones de carácter excepcional. La convocatoria de estas reuniones se realizará siempre con al menos 24 horas de antelación.

4.- Designación de interlocutores cualificados, con suficiente disponibilidad y capacidad de actuación, influencia y decisión dentro de la empresa adjudicataria.

5.- Consideración de cliente preferente, lo que implica no sufrir agravio comparativo respecto a las ofertas técnico-económicas del adjudicatario para otros grandes clientes.

En la actualidad se dispone para la gestión técnica del servicio de un servicio del adjudicatario que actúa como centro de gestión compartido para todo tipo de cuestiones técnicas y de mantenimiento y que intervienen como interlocutores de primer nivel.

3.1.2. DOTACIÓN DE RECURSOS SUPEDITADA A LAS NECESIDADES DEL SERVICIO.

El número, dedicación y cualificación de los recursos humanos directa o indirectamente implicados en la gestión del servicio al Ayuntamiento de Mérida, así como la cantidad, tipología y adecuación de los medios técnicos puestos a disposición de la misma, serán en cada momento los necesarios para la prestación del servicio con la calidad requerida.

Para cada oferta se adjuntará el organigrama técnico del Servicio, así como una descripción de cada uno de los integrantes y sus curriculum vitae.

3.1.3. GESTIÓN PERSONALIZADA.

Los procedimientos de gestión generales del proveedor se adaptarán a las necesidades del Ayuntamiento de Mérida.

En los casos en que no exista un procedimiento interno del adjudicatario que pueda servir de base para la transformación en el servicio deseado, o éste no resulte satisfactorio para el objetivo de gestión definido por el Ayuntamiento de Mérida, se diseñarán y ejecutarán procedimientos a medida, que serán validados y aceptados una vez probado su adecuado funcionamiento.

3.2. INFORMES DE SEGUIMIENTO DEL PROYECTO.

La información mínima que debe aportar el adjudicatario, por escrito y de acuerdo al formato que establezca Ayuntamiento de Mérida, es la siguiente:

3.2.1. INFORMES DE ACTIVIDAD.

Estos informes incluirán, al menos, el detalle y estadísticas de los siguientes elementos, para el periodo de interés (pudiendo incluir un histórico en los casos necesarios):

- Altas, bajas y modificaciones de servicio.
- Infraestructuras, equipamiento y terminales entregados.
- Solicitudes en curso, con grado de avance y fecha prevista de resolución.
- Solicitudes cursadas.
- Actas de reuniones mantenidas.

3.2.2. INFORMES DE INCIDENCIAS.

Incluirán la relación de incidencias del servicio acontecidas, con una clasificación según criticidad. Para las más críticas se presentará un informe detallado de los hechos, una justificación, si cabe, de las actuaciones efectuadas y medidas a aplicar para evitar la reiteración del problema o paliar su impacto en caso de reincidencia. Este informe deberá estar validado y firmado, al menos, por el Responsable de Cuenta.

3.2.3. INFORMES DE CALIDAD Y SEGUIMIENTO DEL ANS.

Incluirán una relación detallada y pormenorizada caso por caso de los elementos de servicio medible que componen cada ANS.

Los parámetros a reportar en cada ANS, los procedimientos de medida y cálculo detallados, así como formato de presentación se verán en el punto posterior.

3.2.4. INFORMES DE ANÁLISIS DE INVENTARIO, TRÁFICO Y COSTES.

Además de proporcionar la información base que permita realizar los análisis particulares que se precisen, se establecerá un formato de documentación de inventario, tráfico y costes para su entrega periódica, tanto correspondiente al período analizado como el histórico anual y del contrato completo. Se analizará asimismo la desviación del histórico respecto a las previsiones de la base de licitación o de las previsiones económicas realizadas al principio de cada año.

El modelo detallado de cada informe y el contenido concreto se decidirán durante la ejecución del proyecto, y deberá ser validado por el Ayuntamiento de Mérida.

Al inicio del periodo de contrato se definirá la periodicidad de estos informes, que podrá variar a lo largo del tiempo o en periodos de alta actividad.

Adicionalmente se elaborarán los informes extraordinarios y/o a medida que solicite el Ayuntamiento de Mérida, relacionados con cualquier aspecto del servicio objeto del presente contrato.

El adjudicatario mantendrá en todo momento ordenada y actualizada, para su presentación en un plazo máximo de 3 días laborables desde su solicitud (salvo excepciones que deberán estar justificadas), toda la documentación relevante del proyecto: planificación, informes presentados, procedimientos de operación, cuadro de tarifas, acuerdos alcanzados, mapas o tablas de cobertura de servicio (actualización de datos con antigüedad máxima de 6 meses), etc.

3.3. GESTIÓN TÉCNICA DEL SERVICIO.

El adjudicatario dispondrá durante todo el periodo de vigencia del contrato de los recursos técnicos humanos y materiales necesarios y adecuados para la prestación de los servicios de soporte y asistencia técnica, mantenimiento, gestión de incidencias y resolución de problemas (averías, etc.).

Dentro del servicio de soporte y asistencia técnica se podrán incluir estudios de viabilidad de servicios, de implantación de nuevos proyectos, ayuda a la resolución de problemas de interconexión de equipos suministrados por el adjudicatario y equipos de otros proveedores o del propio Ayuntamiento, etc.

Será responsabilidad del adjudicatario la gestión de la infraestructura necesaria para la prestación del servicio, así como la reparación de las averías que pudiesen surgir (caídas de enlaces dedicados, fallos en las redes de transporte, fallos en las estaciones base, etc.) con independencia de si implican la sustitución de equipos, desplazamiento de personal, mano de obra, etc. tanto a ubicaciones del Ayuntamiento de Mérida como del propio operador. La resolución de las averías se regirá por los ANS establecidos al efecto. Los gastos de reparación serán por cuenta del adjudicatario.

El adjudicatario habrá de informar con al menos 48 horas de antelación de todas de las paradas programadas del servicio y contar con la aprobación del Ayuntamiento de Mérida, para sustituir, actualizar y reconfigurar equipos y sistemas obsoletos, averiados o inadecuadamente configurados. Cualquier parada programada habrá de producirse en horario de mínimo impacto para el servicio (mínima demanda, mínima criticidad del tráfico cursado, etc.).

Si el adjudicatario necesitase, para la ejecución de estos u otros trabajos (instalaciones, averías, etc.) desplazar técnicos in situ a cualquier centro dependiente del Ayuntamiento de Mérida, sería necesario que comunicase previamente el nombre y DNI de estos técnicos, de cara a que se pudiese autorizar convenientemente el acceso a las instalaciones.

La capacidad de resolución de problemas será 24x7 todos los días del año.

En el caso de avería masiva, se adoptarán dos medidas inmediatas, aparte de las propias medidas de resolución de la avería:

- Se notificará al Ayuntamiento de Mérida, de acuerdo con el plan de interlocución y escalado establecido, favoreciendo el desencadenamiento inmediato de sus propios mecanismos de notificación e información interna.

- El Responsable de Mantenimiento del Adjudicatario se podrá de inmediato en contacto para informar al Ayuntamiento de Mérida de la evolución en la identificación de las causas, alcance y previsible plazo de resolución de la avería. Este interlocutor estará localizable vía móvil las 24 horas del día mientras dure la avería en cuestión.

Tras una avería masiva, se entregará en el plazo máximo de 2 días, un informe explicativo de las causas de la avería, el impacto sobre el servicio al Ayuntamiento de Mérida, el periodo preciso de caída del servicio y el resto de los aspectos relevantes sobre el asunto en cuestión.

3.3.1. SOPORTE TÉCNICO.

Para todos los equipos suministrados el adjudicatario deberá proporcionar las últimas actualizaciones de: software, firmware, updates, upgrades, etc., homologadas por su servicio técnico, así como las actualizaciones de seguridad que estén disponibles por parte del fabricante. La responsabilidad de llevar a cabo la actualización será del adjudicatario, sin perjuicio de que ciertas actualizaciones específicas puedan ser realizadas por el Ayuntamiento de Mérida con el apoyo del adjudicatario.

Para todos aquellos equipos que se oferten como parte de la solución, el adjudicatario deberá proporcionar al Ayuntamiento de Mérida el mayor acceso posible a la documentación sobre dicho equipamiento. Lo que incluye la disponible en la web del fabricante, en las mismas condiciones de las que disponga el adjudicatario o sus subcontratas.

El operador dará soporte ante todos los problemas de configuración y operatividad que puedan surgir. Esto incluirá:

- Apertura de casos en el fabricante.
- Desplazamiento “in situ” para la revisión de los equipos por parte del adjudicatario en caso de averías graves.

Para todas las instalaciones, el adjudicatario deberá desplazar y tener personal propio coordinando las mismas.

El Ayuntamiento de Mérida podrá requerir el desplazamiento de personal del adjudicatario cuando se sea necesario documentar in situ cualquier aspecto de la Red de acceso de Datos del centro o su funcionamiento, principalmente: infraestructura física de la acometida del operador, ubicación o estado de los elementos de la Red.

3.3.2. ATENCIÓN A USUARIOS.

El adjudicatario es el responsable de la detección y solución de fallos en el Servicio, por lo que dispondrá de un sistema de gestión de incidencias que recoja los mismos.

La empresa adjudicataria pondrá a disposición del Ayuntamiento de Mérida una aplicación web para la gestión y seguimiento de incidencias. En dicha aplicación, los responsables del Ayuntamiento de Mérida podrían proceder a la apertura de incidencias, así como un número de teléfono directo con el responsable del proyecto.

Independientemente de lo indicado en el párrafo anterior, la empresa adjudicataria proporcionará una herramienta de ticketing de uso interno, en español, para los trabajadores del Ayuntamiento, como forma fácil y eficiente de comunicarse con Transformación Digital, y así poder administrar, procesar y resolver cualquier tipo de incidencia y/o consulta de los trabajadores, y conseguir una mejor experiencia del usuario, así como el seguimiento claro del flujo del trabajo y solución.

El adjudicatario registrará las incidencias, así como, todas las acciones realizadas, incluido el cierre de las mismas en dicha aplicación, de modo que en todo momento el Ayuntamiento de Mérida disponga de información precisa y actualizada del estado de sus incidencias. Todo ello sin perjuicio

de que el Ayuntamiento de Mérida pueda proceder a la apertura o anticipación de incidencias también por las siguientes vías:

- Telefónica.
- Correo electrónico.

En todos los casos, la apertura de la incidencia tendrá igual validez y deberá ser tratada por el adjudicatario del mismo modo que una incidencia abierta mediante la aplicación web. El adjudicatario proporcionará en todos los casos una atención personalizada, y se accederá directamente al nivel de soporte correspondiente al perfil del Ayuntamiento de Mérida.

El procedimiento de gestión de incidencias será el siguiente:

i. El Ayuntamiento de Mérida o el técnico destinado por el adjudicatario a tal fin en el Ayuntamiento de Mérida, realizará la notificación del aviso, en la web del adjudicatario mediante alguno de los métodos anteriormente descritos, informándole de todos los datos relacionados con el equipo origen del problema o con los datos de la reconfiguración a realizar.
ii. El adjudicatario registrará en tiempo real la incidencia y la procesará en función de la prioridad asignada por el Ayuntamiento de Mérida a la misma.

iii. El adjudicatario informará al Ayuntamiento de Mérida, en el mismo momento en que este le comunica la avería, del número de incidencia, que le servirá para el seguimiento de la misma o para cualquier reclamación sobre dicha incidencia. Asimismo, se informará del técnico asignado a la avería, proporcionándole teléfono de contacto del mismo, con el fin de que en todo momento se pueda conocer la evolución del estado de la avería.
iv. Durante el periodo de reparación de la avería, existirá una fluida comunicación entre el adjudicatario y el responsable técnico del Ayuntamiento de Mérida, tendente a facilitar la reparación y minimizar el tiempo de resolución.

Una vez resuelta la avería se llevarán a cabo las siguientes acciones:

1.- El adjudicatario comunicará la solución de la incidencia al responsable técnico del Ayuntamiento de Mérida, a fin de que este compruebe la operatividad del equipo y de su aprobación.

2.- Aceptada la solución de la incidencia, el técnico procederá al cierre de la misma. Durante el transcurso de la incidencia el adjudicatario realizará en la aplicación todas las anotaciones necesarias para el correcto seguimiento de la misma.

Esta herramienta de gestión de incidencias, como mínimo contendrá los siguientes campos en cada ticket:

- Fecha apertura incidencia.
- Hora apertura.
- Centro en el que sucede la incidencia.
- Persona que abre la incidencia.
- Elemento de red afectado.
- Criticidad de la incidencia. Para la clasificación de la criticidad de una incidencia se tendrán en cuenta en general las siguientes consideraciones:

- ✓ Alta: el fallo impide el correcto funcionamiento de los servicios de acceso de la red de Datos y/o servicios de acceso de Internet en cualquiera de los centros de más de 5 usuarios (el centro está incomunicado) durante el horario de trabajo del mismo, o afecta a una de las líneas o servicios definidos como críticos.

- ✓ Media: el fallo no impide el correcto funcionamiento de los servicios y elementos de red, pero afecta a elementos operativos (ejemplo: baterías, servidores redundantes, etc.) o ha incomunicado un centro de menos de 5 usuarios.

- ✓ Baja: resto de incidencias.

- Descripción incidencia.

- Estado de la incidencia. Los estados serán los siguientes (aunque se aceptarán variaciones en los literales):

  - ✓ "Abierta": La incidencia ha sido registrada en el sistema, pero aún no se está tratando.

  - ✓ "En curso": La incidencia está siendo tratada.

  - ✓ "En observación por cliente": La incidencia está en observación por parte del Ayuntamiento de Mérida.

  - ✓ "Pendiente aceptación solución": La incidencia está pendiente de aceptación de la solución propuesta por el adjudicatario.

  - ✓ "Cerrada": El Ayuntamiento de Mérida ha aceptado la resolución de la avería

  - ✓ Fecha cierre incidencia.

  - ✓ Hora cierre incidencia.

El Ayuntamiento de Mérida tendrá visibilidad sobre las anotaciones realizadas en dichas aplicaciones y el operador adjudicatario registrará todas las operaciones llevadas a cabo.

El tiempo que la incidencia se encuentre en los estados "En observación por cliente", "Pendiente de aceptación solución" o "Cerrada", no se computará a la hora de calcular los ANS correspondientes.

El adjudicatario no podrá cerrar ninguna incidencia cuya solución no haya sido previamente aceptada por el Ayuntamiento de Mérida. Las incidencias, una vez resueltas, podrán estar en estado "pendiente de validación", "en observación" o similar. Si se pasase de nuevo a "en curso", cuando la solución no sea válida, nunca implicará la apertura de un nuevo ticket por parte del Ayuntamiento.

El adjudicatario nunca podrá pasar una incidencia a "En observación por cliente" o "pendiente de aceptación solución" sin consentimiento expreso del Ayuntamiento de Mérida.

Un fallo puede ser detectado por el Ayuntamiento de Mérida o el propio adjudicatario.

La actualización de la información sobre el tratamiento de las incidencias en la aplicación web por parte del adjudicatario será de al menos cada 20 minutos en el caso de incidencias de criticidad alta, 60 minutos en el caso de media y 120 minutos en las de criticidad baja.

El adjudicatario describirá en la oferta el sistema empleado para la gestión de incidencias atendiendo especialmente a los detalles siguientes:

- Descripción detallada del sistema de gestión de incidencias que utilizará para informar sobre incidencias.
- Descripción detallada del procedimiento de escalado que se utilizará ante la detección de una incidencia.
- Descripción detallada del sistema de gestión que usará el oferente para monitorizar los servicios de la red de telecomunicaciones.

4.- ESTRUCTURA NORMALIZADA Y CONTENIDO DE LAS OFERTAS.

Con carácter general, la información presentada debe estar estructurada de forma clara y concisa. La propuesta no debe contener referencias a documentos externos o anexos no incluidos. Se deben entender los anexos como documentos generales de consulta, no como información vital en la propuesta.

La Oferta no podrá exceder de 50 páginas, sin incluir Anexos.

La estructura de las ofertas técnicas deberá ajustarse al formato especificado para cada uno de los documentos que se describen a continuación, cuyo conjunto constituye la documentación técnica.

4.1. RESUMEN.

Consistirá en un breve resumen de la oferta que indicará de forma esquemática, los siguientes puntos:

- Breve presentación del operador u operadores si se tratase de una oferta conjunta.
- El enfoque del trabajo de la empresa licitadora, así como una descripción de sus objetivos.
- Resumen y diagramas descriptivos de la solución y de la infraestructura.
- Resumen de los servicios. Soluciones planteadas y características operativas.
- Resumen del sistema de gestión, facilidades de operación y mantenimiento ofertados.
- Resumen de los parámetros de calidad y compromisos propuestos.

En caso de discordancia de entre lo expresado en distintos apartados de la documentación aportada por el licitador, los valores consignados en estos resúmenes tendrán consideración de valor comprometido, prevaleciendo lo expresado en el resumen.

4.2. PRESENTACIÓN DE LA EMPRESA Y REFERENCIAS TÉCNICAS.

Presentación de la empresa licitadora, indicando los campos en los que trabaja, sus objetivos, ámbito presencial, etc.

4.3. ORGANIZACIÓN DEL PROYECTO Y PERSONAL TÉCNICO ADSCRITO AL CONTRATO.

Se detallará la planificación de la organización propuesta, así como el equipo de proyecto, donde deberá existir un interlocutor único, y los procedimientos de control de calidad a seguir durante todo el proyecto.

Incluirá la descripción de los equipos de trabajo que se crearán para el desarrollo del proyecto, tanto en su Fase de Implantación como de Operación, y definición del personal que estará involucrado junto con las funciones y responsabilidades que tendrá cada uno de ellos dentro de los grupos.

4.4. SOLUCIÓN TÉCNICA.

Se describirá, de forma detallada, la arquitectura propuesta para proveer el servicio ofertado, así como las tecnologías empleadas. Así mismo, se describirá con el máximo detalle, claridad y precisión posible, la solución técnica propuesta, incluyendo específicamente configuración, terminales, líneas, enlaces, etc. para cada sede, indicando claramente si se trata de infraestructuras ya existentes o de nueva implantación.

Los licitadores presentarán un proyecto técnico que deberá contener la información de los sistemas soporte del servicio y las especificaciones técnicas de todos los elementos que lo componen, de modo que cumplan las especificaciones descritas en el presente pliego.

En este proyecto se deberá incluir, al menos, una descripción detallada de:

- Topología de la red, debiéndose acompañar de esquemas gráficos con: tecnología utilizada, ubicación física de los nodos de transporte, interconexión, rutas redundantes, etc.
- Flujo de trabajo para cada proyecto y definición de las responsabilidades en cada caso.
- Propuesta de Acuerdos de Nivel de Servicio.
- Capacidad de crecimiento, mediante la ampliación del ancho de banda de los enlaces ofertados o para la incorporación de nuevas sedes.
- Descripción de los sistemas de Operación y Gestión.
- Anchos de banda ofertados, en función de las necesidades de comunicación de las diversas ubicaciones del Ayuntamiento de Mérida.
- Protocolos a utilizar, los niveles de gestión de calidad de servicio (QoS) y sus herramientas de gestión.
- Se incluirá, para los equipos ofertados, la fecha prevista de fin de venta (ESL) y fin de servicio y soporte (ESL).

4.5. PLAN DE IMPLANTACIÓN.

Se entregará un plan de implantación que garantice la operatividad permanente de los sistemas actuales del Ayuntamiento de Mérida mientras dure el tránsito desde la situación actual a la situación propuesta. Se hará indicación expresa de las necesidades y limitaciones que dicha implantación presente. Este plan de implantación debe explicitar cómo se prestará el servicio durante esta fase y si se contempla algún acuerdo compartido entre operadores.

A su vez, el licitador presentará una planificación del plan de implantación en el que al menos se incluirán:

- Las tareas más relevantes necesarias para la implantación de la solución propuesta.
- Estimación de la duración de cada una de las tareas.
- Medidas conducentes a garantizar la no afectación sobre los servicios de comunicaciones actuales.
- Tiempo total de ejecución del proyecto.

Se destacarán aquellas actividades que puedan implicar cortes del servicio.

4.6. PLAN DE GESTIÓN, OPERACIÓN Y MANTENIMIENTO.

Contemplará la gestión y control del funcionamiento del sistema soporte del servicio que garantice el mantenimiento de los objetivos de calidad y que consiga el nivel de operatividad deseado. Se deberá confirmar el cumplimiento de las funcionalidades mínimas requeridas.

El licitador deberá proponer en su oferta unos procedimientos de actuación, que serán validados tras la firma del contrato, y que incluirán, al menos los siguientes aspectos:

- Gestión de peticiones de provisión y administración: el licitador deberá proponer un procedimiento ágil y sencillo que permita la tramitación y seguimiento del estado de las solicitudes de provisión (altas, bajas, modificaciones, cambios de configuración, etc.). Dicho procedimiento incluirá la posibilidad de hacer consultas automáticas online del estado de las solicitudes.
- Gestión y mantenimiento proactivo: el licitador deberá contar con los mecanismos de supervisión y monitorización necesarios para detectar y anticiparse, con las correcciones oportunas, a las incidencias que pudieran aparecer, de modo que se pueda minimizar el impacto real sobre los usuarios.
- Gestión y mantenimiento reactivo: el licitador deberá proponer un procedimiento que permita la tramitación de incidencias. Cualquier incidencia detectada deberá dejar constancia detallada en una base de datos del adjudicatario.
- Gestión de acuerdos de nivel de servicio (SLAs): el adjudicatario deberá disponer de los mecanismos necesarios que permitan la evaluación del cumplimiento de los niveles de servicios finalmente acordados. Todos los procedimientos que se establezcan, tanto para la provisión como para la gestión de incidencias, deberán poder establecer los hitos necesarios (tiempos de parada, etc.) que permitan un control preciso del cumplimiento de los SLAs. Asimismo, se deberán implantar

los mecanismos necesarios que permitan conocer de manera precisa y en todo momento, las variables de calidad que afectan al cumplimiento de los SLAs.

- Control de la Gestión por el Ayuntamiento de Mérida: el adjudicatario deberá suministrar las herramientas necesarias que permitan al Ayuntamiento de Mérida realizar peticiones, el seguimiento del estado de cada una de las peticiones de provisión/administración, incidencias producidas, configuraciones de equipamientos y líneas, indicadores de la calidad de servicio y cumplimiento de SLAs, informes, etc.

4.7. PLAN DE EMERGENCIA.

El licitador presentará un plan de gestión de incidencias, con especial atención a las que se consideren críticas. Este plan deberá incluir los siguientes aspectos:

- Plan de mantenimiento operativo de líneas y equipamientos de emergencia, detallando los números de las líneas y extensiones de emergencia del sistema.
- Tipificación de los diferentes grupos de incidencias que puedan surgir a lo largo de la prestación del servicio.
- Metodología de actuación en caso de avería.
- Teléfonos de contacto para la tramitación, seguimiento y resolución de la incidencia.

El documento deberá especificar explícitamente los siguientes aspectos:

- Definición de las situaciones de emergencia.
- Definición de métodos y herramientas para diferenciar y aislar áreas afectadas.
- Definición de la asignación de responsabilidades primarias y alternativas del personal, tanto directivo como técnico.
- Procedimientos de escalado y centros de soporte, así como relación de medios efectivos puestos a disposición.
- Diagrama de tiempos máximos en cada escalón de soporte.

4.8. PLAN DE CALIDAD.

Se deberá confirmar el cumplimiento de las especificaciones mínimas de calidad y de nivel de servicios requeridos. Se indicará expresamente cuáles son las mejoras propuestas sobre los mínimos exigidos, indicando la viabilidad de su medición, el procedimiento y frecuencia de su medida y la capacidad de empleo de acciones correctivas.

Identificará los recursos, procedimientos y medios que el licitador pondrá a disposición del contrato para el aseguramiento de los niveles de calidad ofertados.

El oferente realizará una descripción de los recursos de los que dispondrá y de los procedimientos que implantará para garantizar el cumplimiento de los compromisos de calidad contenidos en este apartado.

4.8.1. NIVELES DE CALIDAD DEL SERVICIO.

El licitador indicará los valores de los parámetros siguientes por cada grado de criticidad de las incidencias:

- Tiempo máximo de detección y comunicación.
- Tiempo máximo de diagnóstico.
- Tiempo máximo de respuesta.
- Tiempo máximo para la resolución.

4.9. PLAN DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.

El adjudicatario elaborará un Plan de Seguridad donde se detallarán los controles orientados a garantizar confidencialidad, integridad, disponibilidad, autenticidad y

trazabilidad de la información del Ayuntamiento de Mérida que maneje el adjudicatario en virtud del presente contrato.

El Plan de Seguridad deberá describir las medidas de carácter organizativo, físico y lógico que implementará el adjudicatario para proteger la información asociada a los trabajos objeto del presente contrato.

El Plan de Seguridad deberá ser validado y aceptado por el Ayuntamiento de Mérida con objeto de verificar la inclusión de las medidas de seguridad, adicionales a las propuestas por el adjudicatario, derivadas de las Políticas de Seguridad específicas del Ayuntamiento de Mérida. Se deberá tener en cuenta, para todos los efectos, las actuaciones necesarias (dentro del objeto del concurso) para el cumplimiento del ENS y legislación de Protección de datos. Así mismo, se debe contemplar la participación del licitador en todas las actuaciones necesarias tanto en la parte de prevención o auditorias derivadas de la adecuación a las legislaciones en seguridad que estén en vigor durante el periodo de vigencia del contrato, como en la de resolución de incidencias que surjan en dicho periodo.

El adjudicatario deberá realizar semestralmente un análisis de riesgos general de sus sistemas e infraestructuras empleadas para dar servicio al Ayuntamiento de Mérida.

El adjudicatario deberá contar con un sistema de gestión de incidencias que permita al Ayuntamiento de Mérida estar al tanto de los incidentes de seguridad que afecten a las infraestructuras y servicios de su ámbito.

El adjudicatario queda expresamente obligado a mantener absoluta confidencialidad sobre la información manejada con ocasión del cumplimiento del contrato.

4.10. PLAN DE FORMACIÓN.

Los licitadores elaborarán un Plan de formación sobre las soluciones implantadas, que deberá ser aprobado por el Ayuntamiento de Mérida.

Dicho Plan de Formación deberá proporcionar los conocimientos necesarios para complementar la formación del personal del Ayuntamiento de Mérida y conocer la especificidad de los nuevos servicios y las tecnologías e infraestructuras que los soportan, debiendo estar totalmente orientado a las soluciones implementadas.

La formación recibida debe capacitar a este personal para tener un conocimiento detallado de las tecnologías base y el conocimiento de las habilidades necesarias para desarrollar su trabajo de acuerdo a las actividades y responsabilidades encomendadas.

4.11. PLAN DE FINALIZACIÓN DEL CONTRATO.

El adjudicatario definirá un Plan de Finalización que comenzará al menos tres meses antes de la finalización del contrato. El adjudicatario deberá facilitar el cambio de prestador de servicios. Con este fin, se deberá entregar un inventario del equipamiento y servicios de la plataforma objeto de este contrato así como del equipamiento que el adjudicatario haya decidido reutilizar, de manera que la información tenga un estado de actualización constante.

5. TRANSMISION DE DATOS (RED CORPORATIVA MULTISERVICIO), INFRAESTRUCTURA DE RED Y PUESTO DE TRABAJO, INFRAESTRUCTURA DE SEGURIDAD Y SERVICIO DE ACCESO A INTERNET TRANSMISIÓN DE DATOS.

5.1. TRANSMISION DE DATOS

5.1.1 SITUACIÓN ACTUAL.

El Ayuntamiento de Mérida cuenta con una infraestructura de comunicaciones que soporta diferentes servicios de voz y datos.

Por otra parte, con el fin de dar acceso a los servicios que oferten actualmente o en el futuro otras administraciones públicas, el Ayuntamiento de Mérida se encuentra comunicado con la Diputación de Mérida, Junta de Extremadura y la Administración General del Estado a través de la red SARA.

Esta infraestructura de comunicaciones está constituida por la Red Corporativa Multiservicio (Intranet Corporativa), que permite el establecimiento de comunicaciones entre las distintas sedes del ayuntamiento.

Esta red permite la comunicación entre las distintas sedes del ayuntamiento, posibilitando a los usuarios de las mismas el acceso a los distintos servicios de datos y de voz.

Se encuentran implantados los siguientes tipos de comunicaciones entre la sede central (Palacio Municipal) de la institución y el resto de las sedes:

• Accesos con fibra óptica propietaria.

• Accesos a través de operador con fibra óptica de operador y calidad de servicio y accesos VPN sobre tecnología FTTH.

El Ayuntamiento de Mérida dispone de una infraestructura propia de fibras ópticas, en modalidad de auto prestación, a través de las cuales realiza la interconexión de sus sedes para la transmisión de datos entre ellas. Esta interconexión se realiza con una parte de las sedes (sedes

troncales) a 1 GB mediante un par de fibras ópticas (multimodo), en topología de estrella, y con otra parte de las sedes (sedes principales y troncales) a 1 GB utilizando otro par de fibras ópticas (monomodo) en topología de estrella. Cada sede dispone de la electrónico adecuada y de los elementos necesarios (transceptores, latiguillos, etc.) que posibilitan estas interconexiones.

En lo referente a los diferentes tipos de acceso de operador sobre fibra óptica del operador o accesos VPN sobre FTTH se incluye en anexos donde se especifican los accesos y caudales implantados actualmente en la Red Corporativa Multiservicio (Intranet Corporativa).

En la actualidad se utiliza la fibra propia del Ayuntamiento cómo backup de la fibra del operador.

Debido a la criticidad de la información sobre dicha infraestructura, aquella información no incluida en el apartado y que los oferentes consideren necesaria para la elaboración de la propuesta, podrán solicitarla, arbitrando el Ayuntamiento de Mérida la conveniencia o no de suministrar dicha información, los documentos de confidencialidad que deberá firmar el oferente y los medios para suministrarla (escrito, reunión, etc..).

5.1.2 SERVICIOS REQUERIDOS.

El Ayuntamiento de Mérida desea seguir disponiendo de una única Red con un acceso principal de 10 Gbps ubicado en la sede "Edificio Principal" Ubicado en Plaza de España, N° 1 y un acceso de backup o de respaldo de 10 Gbps ubicado en una sede alterativa Urbanismo Ubicada en calle Concordia.

Es objeto de este concurso la evolución técnica de dicha red con la implantación, mantenimiento y ampliación de los servicios de datos con el objetivo de contar con redes de datos flexibles, fiables y con grandes capacidades de ampliación y adaptación a nuevos servicios que se puedan establecer a lo largo de la duración del contrato.

El diseño de la Red cubrirá todas las necesidades actuales, incluyendo los circuitos y las líneas necesarias para interconectar las distintas sedes con los anchos de banda exigidos, todo el equipamiento necesario para la prestación del servicio, la instalación y configuración de todas las infraestructuras y finalmente, la gestión, administración y mantenimiento de toda la Red durante la vigencia del contrato.

Para el Ayuntamiento de Mérida es importante la garantía de evolución de la arquitectura de red propuesta, así como su capacidad para soportar los nuevos servicios y aplicaciones que el Ayuntamiento de Mérida pueda implementar en un futuro. Desde este punto de vista, es fundamental la capacidad de escalado de la red y su capacidad para soportar nuevos servicios colaborativos y de voz sobre IP, el tráfico generado por las sondas y monitorización de la ciberseguridad, así como, las garantías ofrecidas por el licitador para incorporar nuevos tipos de accesos y escalabilidad de ancho de banda a su red.

Como criterios generales la solución debe cumplir las siguientes premisas:

- El servicio de Transmisión de Datos se prestará en todas las sedes del Ayuntamiento de Mérida integrantes de la Red Corporativa Multiservicio.

• Para el desarrollo de los trabajos a realizar, será necesaria la entrega de una planificación previa que incluirá todas las actuaciones a realizar y los hitos más. importantes que se vayan a producir. Dicha planificación deberá ser entregada por el adjudicatario en el plazo máximo de 30 días hábiles, a partir de la fecha de adjudicación del concurso. Es necesaria una autorización previa de dicha planificación para el inicio de los trabajos a desarrollar.

• En la medida de lo posible, se reutilizarán las acometidas existentes para dar acceso a los servicios de datos en cada una de las sedes y/o entidades locales, excepto para el cumplimiento de los criterios de redundancia de acceso en las sedes en las que se solicite. Cualquier cambio de acometida deberá ser aceptada por el Ayuntamiento de Mérida y todos los costes asociados serán asumidos por el adjudicatario.

• Estarán incluidos los costes de instalación, mantenimiento y cambio de ubicación tanto del equipamiento como de los accesos de datos que se produzcan, en cualquier sede, durante la duración del contrato.

• El equipamiento necesario para la interconexión de las redes (enrutadores) deberá permitir la realización, en caliente, de cambios en toda su configuración, posibilitando de forma automática según su programación, tras un breve espacio de tiempo (por ejemplo, no más de 5 minutos), el retorno a la última configuración guardada en caso de fallo o error en la nueva configuración, minimizando de este modo el riesgo de incomunicación de una sede.

• Se exige transparencia de la red entre nodos sin filtrado de protocolos. Es objeto de este concurso la evolución, implantación, mantenimiento y ampliación de los servicios de datos con el objetivo de contar con redes de datos flexibles, fiables y con grandes capacidades de ampliación y adaptación a nuevos servicios que a lo largo de la duración del contrato puedan establecerse.

Será condición indispensable que los enlaces de datos se realicen mediante medios físicos terrestre, de fibra, como acceso de datos para las sedes principales, sedes troncales y otras sedes normales. Las dos sedes principales del Ayuntamiento, (Palacios y Urbanismo), debido a su criticidad, deberán ser a través de medios terrestres no compartidos con otros usuarios. A través de fibra óptica del operador, garantizando la QoS.

El diseño de la Red cubrirá todas las necesidades actuales, incluyendo las líneas necesarias para interconectar las distintas sedes con los anchos de banda exigidos, todo el equipamiento necesario para la prestación del servicio, la instalación y configuración de todas las infraestructuras, y finalmente la gestión, administración y mantenimiento de toda la Red, durante la vigencia del contrato.

Teniendo en cuenta todo lo anteriormente expuesto, los licitadores deberán presentar una solución que cumpla los objetivos marcados y que se adapte a los requerimientos que a continuación se exponen y que se pueden agrupar en:

- Conexiones con fibra óptica propietaria del Ayuntamiento de Mérida en sedes de la Red Corporativa.
- Conexiones con fibra óptica propiedad del adjudicatario en sedes de la Red Corporativa Multiservicio.

CONEXIONES CON FIBRA OPTICA PROPIEDAD DEL AYUNTAMIENTO DE MERIDA

El Ayuntamiento de Mérida dispone para la conexión de sus sedes troncales una red de fibra óptica de su propiedad con topología en estrella y en modo de auto prestación. A cada sede troncal llegan 6 fibras de las cuales solo se utilizan dos hilos.

En la configuración actual, estas fibras ópticas se utilizan para realizar la conexión principal de datos entre las distintas sedes troncales del Ayuntamiento de Mérida. Esta interconexión se realiza a 1 GB mediante un par de fibras ópticas. Cada sede conectada al anillo dispone de la electrónica adecuada y de los elementos necesarios (transceptores, latiguillos, etc..) que posibilitan estas interconexiones.

Es objeto del concurso el mantenimiento de estas fibras en todo su recorrido desde el nodo central hasta cada uno de los edificios y la electrónica necesaria.

En el supuesto caso de necesitar más información que los oferentes consideren necesaria para la elaboración de la propuesta, podrán solicitarla al Jefe de Servicio de Transformación Digital, arbitrando el Ayuntamiento de Mérida la conveniencia o no de suministrar dicha información, así como los documentos de confidencialidad que deberán firmar.

CONEXIONES CON FIBRA OPTICA PROPIEDAD DEL ADJUDICATARIO EN SEDES DE LA RED CORPORATIVA MULTISERVICIO.

En todas aquellas sedes del Ayuntamiento de Mérida que no dispongan de conexión a través de la fibra óptica indicada anteriormente, el adjudicatario proporcionará el servicio de acceso a datos con independencia de la ubicación del mismo, corriendo por su cuenta los costes de implantación, equipamiento eléctrico, cableado, licencias y en general cualquier componente o actuación necesaria para su puesta en marcha, salvo lo que corresponda a obra civil que será responsabilidad del Ayuntamiento.

En aquellas sedes que dispongan de conexión a través de la fibra óptica dedicada, el adjudicatario instalará y realizará el mantenimiento de los circuitos y las líneas necesarias para que puedan dar servicio tanto de red troncal o principal como de backup o de respaldo, incorporando los componentes electrónicos necesarios que permita su configuración en modalidad activo/activo y activo/pasivo. Estos circuitos y líneas deberán contar con las características necesarias para el mantenimiento del servicio tanto de voz como de datos, garantizando la calidad y fiabilidad de los servicios que se produzcan por dichas líneas, que se dimensionarán en función del número de extensiones y números de puestos de red existentes en cada sede. En caso de caída de la conexión de una sede conectada, se producirá la conmutación automática a la conexión de backup o de respaldo implantada.

En la siguiente tabla se indican los tipos de accesos y caudales existentes actualmente en el Ayuntamiento:

TECNOLOGIA	VELOCIDAD	UDS.
FIBRA	1G	2
FIBRA	600/600	31
FIBRA	300/300	3
TOTAL		36

Se requiere que los accesos de operador que componen la solución sean de fibra óptica.

Los caudales mínimos requeridos en los accesos de operador serán de 600 Mbps simétricos. Se valorará dicho incremento como mejora.

El adjudicatario deberá garantizar la escalabilidad de los accesos y la electrónica necesaria para aumentar en los casos que se requiera el caudal mínimo exigido.

Además, en todas las sedes se definirán políticas de calidad de servicio (QoS) que garanticen los servicios de Telefonía IP. Durante la vigencia del contrato y sin repercutir el adjudicatario coste alguno, el Servicio de Transformación Digital podrá solicitar el aumento de los caudales de datos hasta alcanzar el máximo posible según el acceso implantado y en su caso la modificación del mismo para llegar al caudal necesario.

Durante la vigencia del contrato se podrán incorporar sede de nueva creación y futuras ampliaciones de las ya existentes en un porcentaje no superior al 5% del volumen total contratado. Tanto unas como otras serán por cuenta del adjudicatario y la conexión será mediante fibra óptica propiedad del adjudicatario, el enlace y caudal mínimo exigidos para este tipo de conexiones que se indica en el párrafo anterior, así como los equipamientos de voz. Todos y cada uno de los costes derivados de la puesta en marcha de la(s) nueva(s) sede(s), correrán a cargo del licitador.

CALIDAD DE SERVICIO

El objetivo de los Acuerdos de Nivel de Servicio (ANS) es definir de una manera objetiva el nivel de calidad del servicio que se presta, utilizando variables objetivas que permitan a al Ayuntamiento de Mérida verificar que el servicio que le presta el adjudicatario entra dentro del marco de contratación.

Los ANS se definirán a partir de los siguientes parámetros:

- Plazo de Entrega de Sede.
- Disponibilidad de Sede.
- Disponibilidad Global.
- Pérdida de Paquetes.
- Retardo de Tránsito en red IP.
- Jitter en red IP.
- Tiempo medio de respuesta a averías.
- Tiempo de resolución de incomunicaciones.

El cumplimiento o incumplimiento de los ANS se verificará de forma mensual, y las disminuciones en las facturas correspondientes a los incumplimientos de dichos ANS se ejecutarán sobre las cuantías que se especifiquen en cada apartado, en función del tipo de parámetro de que se trate.

5.3 RED DE ÁREA LOCAL (LAN Y WIFI).

5.3.1 SITUACIÓN ACTUAL.

Actualmente el Ayto. de Mérida dispone en cada una de sus sedes de dispositivos de electrónica de red de área local a través de los cuales se proporciona la conectividad a los distintos elementos (Servidores, PCs, Periféricos, Cabinas, etc..) que están conectados a los puntos de red instalados en cada sede y que constituyen en su conjunto la red de datos corporativa. Todos estos dispositivos router, switches o conmutadores que componen la infraestructura de red de área local son de diferentes fabricantes.

5.3.2 SERVICIOS REQUERIDOS DE RED LAN.

Los licitadores deberán adjuntar una propuesta que contemple la renovación total del equipamiento LAN, así como proveer de una plataforma de gestión del mismo. Además del mantenimiento de la infraestructura WIFI actual.

Respecto a la infraestructura WIFI existente que da cobertura a los siguientes edificios: C.C. Alcazaba, S. Sociales, Ayuntamiento (Casa Oliart y Edificio Administrativo) y Urbanismo. Se indican a continuación:

- 22 instalaciones simples (un router con WiFi en cada una de ellas)

- 87 puntos de acceso Galgus (1200Mbps 2x2 Wave 2. 2,4GHz y 5GHz. Licencia de Cloud Manager anual que se deberá de abonar por cada AP para ser gestionado (Cloud-Man_logs_AP)).

Los licitadores, en su oferta o solución técnica, deberán incluir soluciones en las que el licitador debe estar homologado y certificado por los fabricantes ofertados para proporcionar directamente con sus recursos propios los servicios de soporte técnico de primer y segundo nivel.

Se valorará la calidad, fiabilidad y el prestigio de los fabricantes ofertados, así como las características y escalabilidad de los elementos ofertados.

Esta propuesta de renovación del equipamiento incluirá el suministro, instalación, configuración (migración y optimización de configuración actual) y puesta en marcha de cada elemento nuevo (se incluirá todo lo necesario: cableado, transceptores, etc.), detallándose en la oferta o solución técnica.

Asimismo, se deberá proporcionar herramienta (software) que permita la gestión centralizada de todos los elementos, switches y puntos de acceso.

Se deberán de inventariar todos y cada uno de los elementos requeridos, a través de una herramienta de análisis de IP, control de direcciones IP y gestión de la información asociada al espacio

de direcciones de protocolo de Internet de una red y a la LAN con el objeto de garantizar que el inventario de direcciones IP asignables se mantenga actualizado y sea suficiente dicho direccionamiento; esto permitirá simplificar y automatizar la administración de muchas tareas relacionadas con la gestión del espacio IP, incluyendo la escritura de registros DNS y la configuración de los ajustes DHCP, así como funciones de red adicionales, como el control de las reservas en DHCP, otras funciones de agregación de datos y de elaboración de informes.

La solución propuesta por los conmutadores principales de agregación debe tener alta disponibilidad: debe ser robusta, tolerante al fallo de un elemento cualquiera de los que la compone sin que ello suponga una degradación del servicio ofrecido. El equipo ofertado no puede estar en la lista de End-of-Sale del fabricante.

Todo el hardware ofrecido constituirá un mismo sistema que dará servicio de conectividad a los ordenadores de la infraestructura, para maximizar las prestaciones de baja latencia, máximo rendimiento y facilitar la gestión de los mismos todo el hardware ofrecido deberá ser del mismo fabricante. Todo el material, conectores y adaptadores necesarios incluidos, debe ser nuevo y original del fabricante.

Para garantizar una total integración y homogeneidad con el equipamiento de seguridad, es necesario que todos los conmutadores ofertados sean del mismo fabricante de seguridad ofertado. Quedarán excluidas todas las soluciones de otros fabricantes, así como, soluciones alternativas que no utilicen la propia gestión webGUI del Cortafuegos, como integraciones vía API y similares.

La gestión del equipamiento de conmutadores debe ser gestionada centralizadamente desde el equipamiento de seguridad (utilizando la propia webGUI del Cortafuegos), a fin de aplicar cambios de configuración sobre los puertos de los equipos (cambio de vlan nativa, permitir VLAN y perfil de seguridad), actualizaciones y generación de topologías automáticas y gráficas de los equipos.

Será necesario que la información entre el equipo de seguridad y la del conmutador esté correlada a nivel de usuario / endpoint, para saber qué usuario de dominio (en su caso) o mac address hay en cada puerto de cada switch. Es necesario que esta información también sea a través de la propia webGui del Firewall.

Desde el equipo de seguridad debe permitir aplicar políticas NAC a cada uno de los puertos, con el fin de asignar una vlan en función de la información relativa al dispositivo (MAC address, hardware vendor, familia de dispositivo, tipo, sistema operativo y usuario), el usuario (grupo de usuarios) o tag de una integración con solución de endpoint. Esta funcionalidad de NAC debe estar incluida en la solución de seguridad / conmutador sin coste, sin licenciamiento y sin añadir ningún otro elemento a la propuesta.

Hay que tener la funcionalidad poder generar acciones automáticas hacia problemas / incidentes de seguridad en la red de conmutador, para meter en cuarentena un dispositivo catalogado como comprometido.

Se detallan en este apartado los requerimientos mínimos que deberá cumplir el adjudicatario.

SWITCHES CORE

Se solicita para los equipos de CORE sustitución del equipamiento actual, mejorando las prestaciones, con los siguientes requisitos mínimos:

TIPO 1: (2)

- 48 puertos GE / 10 GE / 25 GE SFP28.
- 2 puertos 1GE/10GE SFP+
- 8 puertos 40GbE QSFP28
- Switching capacity min: 2.0Tbps
- Packets Per Second (Duplex) 4000 MPPS
- Mac Address Storage 96 K
- Network Latency < 1 us
- VLANs Supported 4K
- Link Aggregation Group Size: mínimo de 48
- Total Link Aggregation Groups: hasta del número máximo de puertos
- Queues / Puerto 8
- Packet Buffers 32MB
- DRAM 8GB
- NAND 128Mb
- Ventilación Front to back
- Soporte de MC-LAG
- Protocolos de routing soportados: OSPFv2, RIPv2, VRRP, BGP, ISIS
- Soporte de VRF
- Soporte de SFLOW
- Doble fuente de alimentación.

TIPO 2 (2)

- 24 puertos GE / 10 GE SFP +.
- 2 puertos 2x 40GE / 100GE QSFP+
- 1 RU de altura como máximo.
- Switching Capacity (Duplex) 880 Gbps
- Packets Para Second (Duplex) 1309 MPPS
- Mac Address Storage 64 K
- Network Latency < 1us
- VLANs Supported 4K
- Link Aggregation Group Size: mínimo de 24
- Total Link Aggregation Groups: hasta del número máximo de puertos
- Queues / Puerto 8
- Packet Buffers 8MB
- DRAM 8GB
- NAND 32MB
- Ventilación Front to back
- Soporte de MC-LAG
- Protocolos de routing soportados: OSPFv2, RIPv2, VRRP, BGP, ISIS
- Soporte de VRF
- Soporte de SFLOW
- Doble fuente de alimentación

SWITCHES DE ACCESO

TIPO 1 (19)

- 48 puertos GE / RJ45.
- 4 puertos 10 GE SFP +.
- Switching Capacity (Duplex) 176 Gbps

- Packets Para Second (Duplex) 260 MPPS
- Mac Address Storage 32 K
- Network Latency <1µs
- VLANs Supported 4K
- Link Aggregation Group Size: 8
- Total Link Aggregation Groups: 16
- Packet Buffers 2MB
- Puertos PoE 802.3af/at 48
- Capacidad global PoE: 770W
- Doble fuente de alimentación

TIPO 2 (15)

- 24 puertos GE / RJ45.
- 4 puertos 10 GE SFP +.
- 1 RU de altura como máximo.
- Switching Capacity (Duplex) 128 Gbps
- Packets Para Second (Duplex) 190 MPPS
- Mac Address Storage 32 K
- Network Latency <1µs
- VLANs Supported 4K
- Link Aggregation Group Size: 8
- Total Link Aggregation Groups: 16
- Packet Buffers 2MB
- Puertos PoE 802.3af/at 24
- Capacidad global PoE: 420W
- Doble fuente de alimentación

5.3.3 SERVICIOS DE SOPORTE Y MANTENIMIENTO DEL EQUIPAMIENTO DE RED

El adjudicatario contratará, en nombre del Ayuntamiento de Mérida y para todo el periodo de vigencia del contrato, los servicios de soporte y mantenimiento de fabricante para todos los elementos o dispositivos integrantes actualmente de la infraestructura de red corporativa LAN y WIFI que se han detallado anteriormente.

El adjudicatario proporcionará los servicios de soporte y mantenimiento correctivo de primer, segundo y tercer nivel para todos los elementos que conforman la infraestructura de red corporativa LAN y WIFI. A través de estos servicios se comunicarán las incidencias relativas a averías, anomalías, dudas o consultas relativas a configuraciones, etc., relacionadas con los elementos integrantes de la infraestructura.

Los servicios de soporte y mantenimiento de primer nivel (diagnóstico y resolución de incidencias simples) serán prestados por los integrantes del Centro de Técnico de Gestión.

Los servicios de soporte y mantenimiento de segundo nivel (diagnóstico y resolución de incidencias complejas) serán prestados por un técnico cualificado y certificado por el fabricante, o empresas debidamente certificadas por el fabricante, de cada elemento hardware y/o software integrante de la infraestructura de red corporativa LAN.

Los servicios de soporte y mantenimiento de tercer nivel (apertura y seguimiento de casos específicos con fabricante) serán prestados directamente por el fabricante, o empresas debidamente certificadas por el fabricante, accediéndose a los mismos, como norma o procedimiento habitual, desde los servicios de soporte de segundo nivel. No obstante, lo anterior y para aquellas incidencias que se consideren críticas desde el Servicio de Informática y Comunicaciones del Ayuntamiento de Mérida, se podrá acceder a estos servicios de soporte y mantenimiento de tercer nivel directamente desde los servicios de soporte y mantenimiento de primer nivel o desde el personal técnico del área TIC.

Como norma general los servicios de soporte y mantenimiento de primero, segundo y tercer nivel serán prestados de forma remota. Sin menoscabo de lo anterior, si una incidencia en alguno de los elementos integrantes de la infraestructura de red corporativa LAN precisara para su resolución de la intervención de un técnico de manera presencial, se realizará sin limitación alguna en cuanto a cómputo de horas y sin repercutir coste alguno para el Ayuntamiento de Mérida.

El adjudicatario especificará en su oferta y designará un responsable o jefe de proyecto de red que será el interlocutor válido del adjudicatario con la Dirección del Servicio de Transformación Digital del Ayuntamiento de Mérida para todas aquellas cuestiones técnicas relativas o relacionadas con los elementos integrantes de la infraestructura de red corporativa LAN y WIFI durante toda la vigencia del contrato.

El adjudicatario proporcionará los servicios de soporte y mantenimiento correctivo de primer, segundo y tercer nivel para todos los elementos que conforman la infraestructura de Red Corporativa LAN-WIFI. A través de estos servicios se comunicarán las incidencias relativas a avería, anomalías, dudas o consultas relativas a configuraciones, etc.

Los servicios de soporte y mantenimiento de primer nivel (diagnósticos y resolución de incidencias simples) serán prestados por los integrantes del Centro de Gestión Técnico.

Calidad de Servicio.

El objetivo de los Acuerdos de Nivel de Servicio (ANS) es definir de una manera objetiva el nivel de calidad del servicio que se presta, utilizando variables objetivas que permitan al Ayuntamiento de Mérida verificar que el servicio que le presta el adjudicatario entra dentro del marco de contratación. Cualquier medida de calidad de servicio se llevará a cabo sobre períodos mensuales.

El adjudicatario indicará al menos los siguientes parámetros y sus valores máximos:

- Tiempos máximos de respuesta (entendiendo como tal el tiempo transcurrido desde la comunicación de una incidencia y obtención de respuesta para realizar cualquier intervención, bien sea de mantenimiento como de administración, por parte del técnico que tenga asignada la incidencia) para los distintos niveles de los servicios de soporte y mantenimiento:

• Para los servicios de soporte y mantenimiento de primer nivel: 1 hora

• Para los servicios de soporte y mantenimiento de segundo nivel: 3 horas

• Para los servicios de soporte y mantenimiento de tercer nivel: 6 horas

- Tiempo máximo de reemplazo de equipamiento. En el supuesto caso de que fuera preciso reemplazar algún elemento integrante de la infraestructura de red por avería del mismo, se establece un compromiso máximo de 48 horas para el reemplazo del elemento averiado.

Estos valores relativos a los tiempos máximos de respuesta y de reemplazo, podrán ser mejorados por el licitador en su oferta, lo cual será tenido en cuenta en el estudio de la misma.

En el caso de no cumplir con los valores de ANS indicados anteriormente o los presentados en su oferta por el adjudicatario, se aplicará una penalización del 2% del coste mensual imputado al servicio de infraestructura de red en la factura correspondiente al mes siguiente de producirse el incumplimiento.

5.4 PUESTO DE TRABAJO.

5.4.1 SITUACIÓN ACTUAL.

El Ayuntamiento cuenta en la actualidad con un parque de equipos, procedentes de la actual relación contractual, que el nuevo adjudicatario deberá de mantener en los mismos términos durante la vigencia del nuevo contrato; a su vez se deberá incluir en su oferta, el suministro, instalación, gestión y mantenimiento in-situ durante toda la vigencia del contrato, los siguientes puestos de trabajo:

- Equipos de sobremesa:
    - 193 uds ordenadores de sobremesa.
    - 193 uds pantallas TFT DE 22”
- Equipos portátiles:
    - 5 uds portátiles de 15”

Se detallan las características mínimas (tanto equipos de sobremesa como portátiles):

- Inter Core i5 arquitectura 64bits
- 8G Ram DDR4
- 500Gb SSD
- Wifi
- Tarjeta de red Ethernet LAN 10/100/1000 Mbits/s
- USB 3.X
- HDMI
- Teclado y ratón
- Pantalla con resolución 1920x1080
- Windows 11 Pro instalado

Además, disponemos de 2 portátiles MAC Book Pro de 16 pulgadas Intel Core i9 de ocho núcleos a 2,3GHz de novena generación con Radeon Pro 5500M con 4GB de memoria GDDR6, 16GB de memoria DDR4 y 1Tb de almacenamiento SSD y ratón inalámbrico los cuales se incorporan al mantenimiento y garantía de cualquiera de los componentes.

El licitador deberá incluir en su oferta:

- Portal de usuario para apertura de incidencias
- Gestión de escritorio, incluyendo el despliegue de parches de seguridad y de paquetes de aplicaciones, además de la toma de control remoto de los equipos para resolución de incidencias.
- Horarios de atención de incidencias 24x7
- Horarios de resolución de incidencias: 12x5 con un compromiso de resolución NBD (Next Business Day)
- Cuadro de mando para 1 interlocutor del Ayuntamiento de Mérida

Los equipos pasarán a ser propiedad del Ayuntamiento de Mérida a la finalización del contrato.

La migración de datos de los actuales equipos de usuario a los nuevos será realizada por el Servicio de Transformación Digital del Ayuntamiento de Mérida. No obstante, el adjudicatario prestará soporte a la migración de los datos.

Los equipos se ubicarán en las sedes que indique el Ayuntamiento.

Además, el licitador deberá incluir en su oferta:

- Mantenimiento de la solución Fortimail existente para 500 cuentas de correo
- Mantenimiento de licenciamiento EDR Crowdstrike existente para 500 puestos de trabajo (dispositivos y servidores) compatible para MAC, Windows y Linux, antiramsonware y desplegable a través de active directory.
- Mantenimiento de 25 licencias O365 tipo E1 o E3 Enterprise con vigencia durante todo el contrato.
- Mantenimiento de 25 licencias Office Personal 365. El mantenimiento de estas licencias empezará a partir del 01 de marzo de 2026 hasta la finalización del contrato.

5.5 SERVICIOS SDWAN.

Se requiere que el licitador ofrezca un servicio SDWAN en 5 sedes principales del Ayuntamiento de Mérida (Palacio, Urbanismo, Servicios Sociales, Policía y Deportes) con las siguientes características:

1. Interoperabilidad 100% garantizada con las sedes tradicionales.
2. Solución nativa de red de operador, con visión extremo a extremo de toda la solución de acceso de datos.
3. Servicio escalable independientemente del número de sedes iniciales.
4. Convivencia con el resto de los servicios actuales.
5. Alta disponibilidad: redundancia geográfica de la plataforma de servicio.
6. Encriptación de datos.
7. Visibilidad de red con informe en tiempo real.
8. Parametrización de la red en un único punto.
9. Capacidad de creación y gestión de políticas de seguridad en la red.
10. Capacidad para realizar priorización de tráfico por aplicación. Optimización del tráfico
11. Posibilidad de crear sedes hibridas con diferentes tipos de acceso. Break out local en sedes híbridas.
12. Balanceo de tráfico según calidad de red (AAR)
13. Portfolio de soluciones virtualizadas de funciones de red (Firewall)
14. Capacidad de realizar microsegmentación.
15. Gestión del servicio extremo a extremo.

Se valorará el crecimiento en el número de sedes ofertadas en el Pliego.

5.6 SERVICIOS ADICIONALES.

5.6.1 TERCERA COPIA.

Se requiere disponer de una tercera copia fuera del CPD principal del Ayuntamiento que cumpla con los siguientes requisitos:

• Solución de backup a disco basadas en appliance específicos de backup, no se aceptarán soluciones tipo NAS ni de servidores.

• Solución que permita una eficiencia de datos elevada, gracias a la duplicación que se realice de forma online y por bloque variable.

• Debe servir almacenamiento a través de los protocolos NFS, SMB y OST

• Debe ofrecer la posibilidad de dotar a la solución de protección de datos de mecanismos de movimiento de datos (larga retención y/o DR) hacia soluciones de cinta y/o de cloud (Privada/Hibrida o pública), mediante protocolos eficientes como S3.

• Debe ofrecer el suficiente espacio para albergar el entorno actual (bases de datos, servidores, etc.) del Ayuntamiento.

5.6.2 SERVIDORES.

Se requieren 2 Equipos con las siguientes características:

• 1 x Xeon Gold 6534 (8 cores – 3,9GHz) o similar, pero no pueden superar el número de cores por temas de licenciamiento.

• 512 GB RAM

• RAID 940-8i 4 GB Flash

• 2 x 1,92TB NVMe

• 2 x 25GbE QSFP28

• 2 x 1GbE base T

• Dos cables DAC de 20 metros QSFP28

• Doble Fuente 1100W Titanium

• Instalación física

• Configuración

• Migración del sistema actual de Oracle a esta nueva infraestructura.

5.6.4 ALOJAMIENTO WEB Y CORREO.

El Ayuntamiento de Mérida dispone de Hosting Web y Correo con las siguientes características:

• Servidor para alojamiento Web

• Correo electrónico para un mínimo de 500 cuentas de correo.

Las páginas web actualmente operativas en el Ayuntamiento de Mérida, son las siguientes:

1. merida.es
2. turismomerida.org
3. emerita-lvdica.es
4. archivohistorico.merida.es
5. huertoseducativos.merida.es
6. transparencia.merida.es
7. intranet.merida.es
8. edusi.merida.es

Deberán de ser migradas y actualizadas, en todo su ámbito, es decir; todos los componentes a la última versión, plugins, el gestor de contenidos, etc., incluyendo el código necesario para ello. El coste será asumido en su totalidad por el adjudicatario. Se explica a continuación con más detalle.

En la actualidad el portal web merida.es tiene un diseño con gestor de contenidos, temas y plugins actualizados, pero es muy pesada y carga muy lenta. Es necesario hacer un nuevo diseño, migración, mantenimiento y actualizaciones tanto a nivel de contenidos como de plugins, temas, CMS, etc., y/o herramientas necesarias para el nuevo diseño. Deberá de realizarse desde cero actualizada con las últimas versiones que respeten la estructura actual de contenidos o que, en su caso, la mejoren. Es importante que todos los contenidos, históricos (noticias, eventos, etc.) y actuales, de las diferentes secciones de la actual web se migren a la web con el nuevo diseño.

La web turismomerida.org tiene versiones obsoletas de Wordpress, temas y plugins, por sus características no es posible actualizarlos. No obstante, la delegación de Turismo está trabajando en la creación de un nuevo portal web. Hasta entonces habrá que dar soporte a la web actual, aunque no pueda actualizarse.

Una vez que la delegación de Turismo apruebe la nueva web, ésta sustituirá a la actual. El mantenimiento de la misma con las sucesivas actualizaciones y mejoras corresponderá a la empresa que la diseñe durante un periodo determinado de tiempo. Cuando concluya este periodo, el adjudicatario de este contrato tendrá que asumir dicho mantenimiento, migración, mejora de la misma, etc.

La web emerita-lvdica.es, en este caso, actualmente, el soporte y mantenimiento lo tiene una empresa externa por un determinado tiempo. En cuanto finalice, el adjudicatario de este contrato tendrá que asumir dicho mantenimiento, mejora de la misma, etc.

Ocurre lo mismo con la web archivohistorico.merida.es, actualmente el soporte y mantenimiento lo tiene una empresa externa. En cuanto finalice, el adjudicatario de este contrato tendrá que asumir dicho mantenimiento, mejora de la misma, etc.

El objetivo final es que el ayuntamiento disponga de unos portales web que estén completamente actualizados para impedir su mal funcionamiento o caída que los pueda dejar inoperativos; que se disponga de soporte para que, en cualquier momento, y ante cualquier necesidad, se solvente la incidencia y/o se ofrezca ayuda al personal TIC del Ayuntamiento, de cara a que dichos portales estén siempre ofreciendo el mejor servicio posible y se adapte a nuevas funcionalidades futuras.

Es necesario dar un servicio que de soporte y mantenimiento para garantizar la correcta operación de los portales web descritos mediante la prestación de un servicio completo e integral de mantenimiento preventivo, correctivo y evolutivo de:

• Software que se utilice en los portales web (gestor de contenidos CMS (Wordpress, Joomla, Drupal, etc.), temas, plugins, etc.) realizándose todas las actualizaciones necesarias y el adecuado control de versiones de dicho software utilizado para el correcto funcionamiento del sistema y adecuación del mismo a nuevos requisitos.

• Los portales web, que garantice la incorporación de nuevas funcionalidades que den respuesta a nuevas necesidades de los mismos.

• Soporte, ante cualquier duda y/o incidencia, a los usuarios administradores de los portales web.

• Garantía del funcionamiento ininterrumpido de los portales y restablecimiento del servicio en caso de indisponibilidad. La empresa adjudicataria deberá de hacerse cargo de los Backups necesarios y planes de contingencia, al objeto de que las webs indicadas estén disponibles 24x7x365.

• Acciones preventivas oportunas para evitar incidencias que puedan afectar a la operación de los portales, y la realización de las actividades necesarias para minimizar el impacto de incidencias sobre la operativa normal de dichos portales.

• Servicio de hosting o alojamiento de los portales web y correo electrónico.

Los portales web deben permitir la navegación y correcta visualización de contenidos de manera sencilla tanto en ordenadores como en dispositivos móviles, redimensionando y colocando los elementos de manera que se adapten al ancho de cada dispositivo y optimizando la velocidad de carga de las webs. Los portales deben tener la mayor facilidad de navegación y usabilidad y ser compatible con los navegadores más utilizados.

El portal deberá cumplir con el nivel de accesibilidad establecido por la normativa vigente y realizar todas las acciones necesarias para que tenga el mayor nivel de seguridad posible, hoy en día https, o la evolución de éste.

Se debe optimizar el SEO que permita aplicar buenas prácticas para el posicionamiento óptimo en buscadores, integración de canales de Social Media y de analítica web para medición de accesos y uso enfocadas al comportamiento del ciudadano. Correcta configuración de Google Analytics.

Por último, las páginas web deben incluir una solución para la accesibilidad que actúe sin modificar la url original del dominio web, que inserte las modificaciones en los formatos y los recursos, enlaces, textos, archivos de voz, balizas de navegación y demás elementos necesarios para incorporar las herramientas de usabilidad y accesibilidad necesarias alineadas con la WCAG 2.1. La solución deberá de disponer al menos de los siguientes perfiles /interfaces de accesibilidad: Personas con Discapacidad Visual, Personas mayores no competentes digitalmente o con discapacidad por la edad, Personas con Discapacidad física u orgánica, Personas con Discapacidad cognitiva o intelectual y Personas con baja visión. Dicha solución tiene que ser responsive para adaptarse a los dispositivos móviles.

Es muy importante destacar que la funcionalidad tiene que estar integrada en interfaces/perfiles de discapacidad que permitan la navegación autónoma según el perfil de discapacidad, no serán válidas widgets y funcionalidades de accesibilidad que no permitan la navegación autónoma con el interfaz aportado, para ser validos deberán aportar un marcado semántico en la página que permita la navegación con interfaces distintos al ratón.

La solución presentada tendrá que estar integrada con los CMS usados en las webs municipales, para todos los niveles, especialmente el etiquetado de contenido para simplificar la navegación con los interfaces accesibles, siendo demostrable como se puede navegar de manera autónoma por toda la web con el interfaz seleccionado sin necesidad de utilizar el ratón. Para acreditar esta integración se aportarán en la memoria técnica enlaces de otros clientes del ámbito público con la solución funcionando en el CMS.

Hay que cumplir con el Real Decreto 1112/2018, el cual exige la accesibilidad a los sitios web y apps móviles de la administración pública.

CORREO ELECTRÓNICO.

Actualmente se disponen de 500 cuentas de correo electrónico, para ello el licitador deberá de ofertar un mínimo de 500, la ampliación del número de cuentas será objeto de valoración. Las cuentas de correo deben usar certificado de seguridad.

La empresa adjudicataria deberá de migrar todos los buzones existentes (entrada, salida, enviados, etc.) en las actuales cuentas del correo que posee el Ayuntamiento.

El Ayuntamiento de Mérida tiene la necesidad puntual, en algún servicio, o diaria en otros, de emitir correos masivos sin restricción de volumen de enviados en un período de tiempo, a saber; restricciones de correos emitidos por hora o por mes, por lo que se precisan que al menos a 10 cuentas de correo -inicialmente para: cultura, comercio, turismo, comunicación- deberán de permitir la emisión de correos masivos diarios sin limitación alguna.

No deberá de existir restricción alguna para la emisión de correos del dominio de merida.es en ninguna de las cuentas que cree el Ayuntamiento.

Todos los servicios deberán de estar disponibles 24x7x365; la empresa adjudicataria deberá velar por el buen funcionamiento de la plataforma de correo y servicio ftp del Ayuntamiento, así como aplicar toda la normativa de seguridad que indica el ENS nivel alto.

Para el alojamiento web, correos electrónicos, servicios de ftp, etc., se deberá de contar como mínimo con un espacio disponible de 5Tb ampliable bajo demanda hasta un máximo de 10Tb.

Para estos requerimientos, el alojamiento deberá de contar con una política de Seguridad de la Información que se garantice en el servicio prestado, considerando los aspectos de confidencialidad,

integridad y disponibilidad de los datos en las diferentes áreas involucradas en la prestación de los servicios: seguridad física, seguridad lógica y seguridad político-corporativa.

Todas las licencias, migraciones, etc., así como cualquier coste adicional necesario para la puesta en marcha del 100% de lo requerido correrán a cargo del adjudicatario.

5.7 INFRAESTRUCTURA DE SEGURIDAD.

5.7.1 SITUACION ACTUAL.

Actualmente la Red Corporativa del Ayuntamiento de Mérida dispone de un conjunto de elementos hardware y software que constituyen la infraestructura de seguridad perimetral de la misma y que está integrado por:

- Un primer nivel de protección perimetral compuesto por un clúster Checkpoint 6200 en alta disponibilidad, teniendo activos los servicios de soporte y mantenimiento de fabricante y con licenciamiento NGTX (Sandblast).

- Un segundo nivel de protección perimetral formado por un clúster FortiGate 400E en alta disponibilidad, teniendo activos los servicios de soporte y mantenimiento de fabricante y con licenciamiento UTP.

- Un FortiAnalyzer virtualizado para recolección y análisis de logs de los equipos Fortinet.

- Una consola cloud para la gestión y recolección de logs de los equipos de Checkpoint.

Esta infraestructura está mantenida en su totalidad por la actual empresa adjudicataria. Todos los equipos y software correspondiente están conveniente y suficientemente licenciados hasta la finalización del contrato. Además, se incluyen los servicios de Administración delegada (primer y segundo nivel) y de Soporte de Fabricante (tercer nivel) correspondiente.

Debido a la criticidad de la información sobre dicha infraestructura, aquella información no incluida en el apartado y que los oferentes consideren necesaria para la elaboración de la propuesta, podrán solicitarla, arbitrando el Ayuntamiento de Mérida la conveniencia o no de suministrar dicha información, los documentos de confidencialidad que deberá firmar el oferente y los medios para suministrarla (escrito, reunión, etc..).

El licitador deberá asumir el coste de renovación de licencias, soporte, mantenimiento y administración delegada de la solución global.

5.7.2 SERVICIOS REQUERIDOS.

Es objeto de este contrato la sustitución del equipamiento, mantenimiento y mejora de las prestaciones ofrecidas por los diferentes elementos integrantes de actual infraestructura de seguridad de la red de datos implantada en el Ayuntamiento de Mérida debiendo el adjudicatario proporcionar los servicios solicitados cumpliendo con los requerimientos indicados a continuación.

Se pretende disponer de una arquitectura de seguridad conformada por dispositivos que permitan proteger todos los flujos de información. Toda aquella información y/o comunicación que entre o salga de la infraestructura TIC, debe ser analizada por los servicios de protección perimetral para aceptar, bloquear

o retener su paso según corresponda en función de la naturaleza de la información y las reglas de la configuración establecida. A tal efecto los licitadores deberán incluir en sus propuestas el licenciamiento software necesario para ello y que como mínimo deberá ser equivalente o superior en funcionalidades y prestaciones a los actualmente en producción.

Los dispositivos que propongan los licitadores estarán formados por sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y se encuentren recogidos en el "Catálogo de Productos de Seguridad TIC" CCN- CERT, COMMON CRITERIA o Cuadrante Mágico de Gartner 2024.

La solución del doble clúster de seguridad, de primer nivel y de segundo nivel, deberá de cumplir con las recomendaciones que se recogen en el Esquema Nacional de Seguridad en esta materia, vigente en el momento de publicación de este pliego.

A su vez, y será objeto de valoración, el licitador deberá de presentar una planificación de análisis periódico, según marque el ENS, de pruebas de penetración y detección de vulnerabilidades informáticas (externas e internas), asociadas a los sistemas de información que dan soporte a los servicios del Ayuntamiento, a través de un conjunto de ataques simulados y dirigidos a la infraestructura con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas (pentesting), incluyendo en el pentesting, un análisis de vulnerabilidades.

Finalmente, el adjudicatario elaborará un informe acorde a las directivas indicadas por el ENS, donde se indicará si los ataques tendrían éxito, y en caso afirmativo porqué y qué información o acceso obtendrían, es decir, se simulan ataques tal y como los llevaría a cabo un ciberdelincuente que quisiera hacerse con el control del sistema o con la información en él contenida. De esta forma, se puede determinar:

• Si el sistema informático es vulnerable o no.

• Evaluar si las defensas con las que cuenta son suficientes y eficaces.

• Valorar la repercusión de los fallos de seguridad que se detecten.

El adjudicatario incluirá en su propuesta el reemplazo de los elementos integrantes del sistema de cortafuegos de primer y segundo nivel realizando el suministro e instalación de los appliances que se correspondan con la evolución de los elementos actualmente implantados, pero disponiendo de características y prestaciones superiores, entre las que podemos destacar las siguientes relativas a funcionalidades, rendimiento y conectividad (número de interfaces o puertos):

Cortafuegos de primer nivel:

- Posibilidad de integración en entornos de alta disponibilidad mediante configuración de clúster tanto en modo activo/activo como activo/pasivo.
- Inspección profunda de contenido.
- Capacidades de enrutamiento estático, enrutamiento basado en políticas y enrutamiento dinámico soportando BGP, OSPF, RIPv2.

- Gestión de VLANs en integración de 802.1Q.
- Autenticación basada en grupos de usuarios con integración con servicios de directorio (Microsoft AD y LDAP).
- Posibilidad de creación de reglas de protección basadas en perfiles aplicables a usuarios individuales y/o grupos.
- Capacidad de gestión de accesos VPN licenciada para soportar al menos 50 usuarios remotos conectados de forma simultánea.
- Rendimiento mínimo del servicio firewall con APP-ID: 9.5 Gbps.
- Rendimiento mínimo del servicio VPN (IPSec): 2,7 Gbps.
- Rendimiento mínimo Threat Prevention: 5,5Gbps.
- Capacidad mínima de gestión de conexiones: 1.400.000 sesiones concurrentes.
- Número de interfaces GE (1000Base-T): 8.
- Número de interfaces 10 GE: 4
- Módulos SFP+: 2 SR + 2 LR (por cada equipo)
- Almacenamiento interno mínimo: 240 GB SSD
- Posibilidad de disponer de un puerto específico o dedicado de gestión en el appliance para su uso con tecnologías Ethernet con el objetivo de garantizar que no consuma interfaces de servicio para esta tarea.
- Posibilidad de contratar un sistema cloud para la recolección de logs y eventos de forma nativa, que permita la generación de informes y disponga de capacidad de almacenamiento para al menos 3 meses.

Cortafuegos de segundo nivel:

- Posibilidad de integración en entornos de alta disponibilidad mediante configuración de clúster tanto en modo activo/activo como activo/pasivo.
- Inspección profunda de contenido.
- Múltiples modos de despliegue (modos mirror, transparente y NAT/PAT).
- Capacidades de enrutamiento estático, enrutamiento basado en políticas y enrutamiento dinámico soportando BGP, OSPF, RIPv2 y Multicast tanto para IPv4 como IPv6.
- Gestión de VLANs en integración de 802.1Q.
- Autenticación basada en grupos de usuarios con integración con servicios de directorio (Microsoft AD y LDAP).

- Posibilidad de creación de reglas de protección basadas en perfiles aplicables a usuarios individuales y/o grupos.
- Rendimiento mínimo del servicio firewall IPv4/IPv6 (con paquetes de 1518 bytes UDP): 79 Gbps.
- Rendimiento mínimo del servicio VPN (IPSec): 55 Gbps.
- Rendimiento mínimo NGFW (IPS + control de aplicaciones): 10 Gbps.
- Rendimiento mínimo Threat Protection (IPS más control de aplicaciones más Antimalware): 9 Gbps.
- Capacidad mínima de gestión de conexiones: 7.800.000 sesiones concurrentes, permitiendo como mínimo 500.000 nuevas sesiones por segundo.
- Número mínimo de interfaces 10 GE SFP+: 4.
- Número mínimo de interfaces ULL 10 GE SFP+: 4 ultrabaja latencia <2,5ms
- Número mínimo de interfaces 1 GE SFP: 8.
- Número mínimo de interfaces GE (1000Base-T): 16.
- Módulos SFP+: 2 SR + 2 LR (por cada equipo)
- Posibilidad de disponer de un puerto específico o dedicado de gestión en el appliance para su uso con tecnologías Ethernet con el objetivo de garantizar que no consuma interfaces de servicio para esta tarea.
- Prevención de fuga de datos (DLP), incluyendo firmas y patrones distribuidas desde el servicio de ciberseguridad en cloud del fabricante.
- Servicio de Seguridad de la Superficie de Ataque:
    - Detección de dispositivos de IoT
    - Correlación de vulnerabilidades ce dispositivos IoT
    - Servicio de Security Rating, que permite evaluar el estado de seguridad y cumplimiento normativo de la infraestructura y de los dispositivos conectados a ella.
    - Chequeo de avisos de amenazas de día cero (ourbreak)
- Sistema cloud para la recolección de logs y eventos de forma nativa, que permita la generación de informes y disponga de capacidad de almacenamiento para al menos 3 meses. Esta consola deberá recibir también de forma nativa los logs de la solución de protección de correo y protección de aplicaciones Web, que se solicita más adelante.

El adjudicatario deberá de proveer de un sistema de volcado del histórico de logs de ambos firewalls (clúster de primer y segundo nivel), sobre el sistema de almacenamiento que indique el Ayuntamiento.

Los sistemas de cortafuegos de primer y segundo nivel estarán conformados cada uno de ellos por dos appliances hardware NGFW (acrónimo de "Next Generation Firewall", en castellano "Firewall de próxima generación") configurados en alta disponibilidad mediante un clúster Activo-Pasivo e instalados en el CPD. Tendrán activos los servicios de soporte y mantenimiento de fabricante y dispondrán de las licencias para las funcionalidades que poseen los actualmente implantados (prevención de ataques conocidos) más las licencias necesarias para la prevención de ataques "Zero-Day".

Estos sistemas de cortafuegos tienen, para el Ayuntamiento de Mérida, la consideración de infraestructura crítica, por ello:

- En ningún caso el fallo de uno de los elementos que lo integran debe ser motivo de indisponibilidad de los servicios que protegen.
- Los elementos deben mantener el rendimiento exigido en caso de caída de uno de los miembros del clúster.
- El equipamiento ofrecerá un diseño sin puntos singulares de fallo y un elevado nivel de redundancia en todos los elementos que lo componen: fuentes de alimentación y ventiladores redundantes e intercambiables en caliente.
- El adjudicatario deberá realizar el suministro de todos aquellos elementos de conectividad que resulten necesarios para la implantación y puesta en marcha e integración de estos elementos en la red de datos corporativa según un diseño de óptima configuración (a nivel de rendimiento, prestaciones y conectividad) que deberá ser aprobado por el Ayuntamiento de Mérida.

Todas las características indicadas con anterioridad relativas a estos elementos tienen la consideración de mínimas.

El reemplazo (suministro e instalación) de los elementos integrantes del sistema de cortafuegos de primer y segundo nivel será efectuado por parte del adjudicatario en los tres (3) primeros meses de vigencia del contrato.

Las tareas de instalación implican las de migración de la configuración implantada en los elementos actualmente instalados que incluirá la realización de un estudio o análisis previo que recogerá tanto las prestaciones ofrecidas como la configuración establecida en los elementos que serán reemplazados. Ese análisis de la situación de partida deberá detectar los posibles fallos, errores o deficiencias de configuración que pudiera haber en cada uno de los niveles de cortafuegos y propondrá las correcciones y mejoras necesarias. Con las conclusiones de este estudio o análisis previo el adjudicatario realizará la propuesta de implantación de los nuevos elementos que integrarán el sistema de cortafuegos de primer y segundo nivel de manera que se establezca una óptima configuración para obtener una mejora en las prestaciones.

Así mismo el adjudicatario deberá como parte del proceso de implantación de los nuevos equipos cortafuegos tanto de primer como de segundo nivel, realizar su correcta integración con el sistema de gestión de eventos de seguridad (SIEM) disponible en el Ayuntamiento de Mérida y basado en la solución MONICA homologada por el CCN, detallado en un apartado más adelante.

5.7.3 SISTEMA DE SECURIZACIÓN DEL CORREO ELECTRÓNICO

Actualmente el Ayto. Mérida dispone de:

- Dos 2 equipos Fortimail 200F en clúster activo-pasivo con licencias activas Bundle FortiGuard Enterprise ATP Bundle Contractus y antispam y soporte del fabricante en modalidad 24x7 con disponibilidad de soporte L3 ante incidencias software o de seguridad.

El adjudicatario incluirá en su propuesta el reemplazo de los elementos integrantes del sistema de securización del correo electrónico realizando el suministro e instalación de los appliances que se correspondan con la evolución de los elementos actualmente implantados, pero disponiendo de características y prestaciones superiores, entre las que podemos destacar las siguientes relativas a funcionalidades, rendimiento y conectividad (número de puertos):

• Posibilidad de integración en entornos de alta disponibilidad mediante configuración de clúster tanto en modo activo/activo como activo/pasivo.

• El sistema propuesto deberá ser un MTA (acrónimo de “Mail Transfer Agent”, en castellano “Agente de transferencia de correo”) con capacidad de enrutamiento de correos y protección frente a virus, spam, anti-malware, control de enlaces a URLs embebidos, filtrado a partir de listas negras e identificación y neutralización de amenazas específicas, como los ataques avanzados de phising.

• Soporte de múltiples protocolos seguros (HTTPS, SMTPS, SSH, IMAPS, POP3S, S/MIME, etc.).

• Soporte de múltiples dominios con posibilidad de configuraciones independientes para los dominios, tanto de políticas como de cifrado a nivel de canal para cada dominio, etc.

• El sistema permitirá aplicar políticas de filtrado por reputación de origen, contenido de tipo spam, contenido malicioso (virus), enlaces maliciosos, etc., en base a IPs, dominios de correo o incluso un grupo de direcciones de correo electrónico.

• El sistema deberá contar con protección de la reputación para impedir el envío al exterior de virus o correos no deseados. Asimismo, contará con elementos de prevención de fugas y pérdidas de datos, ya sean intencionales o accidentales, realizando la detección y protección de datos confidenciales por correo electrónico mediante el uso de diccionarios predefinidos y personalizables que admitan el uso de expresiones regulares.

• El sistema dispondrá de capacidad para establecer políticas de cuotas por usuario, establecer límites en el número de correos a enviar según dominio de origen, etc.

• La protección antispam deberá soportar el estándar de autenticación de correo electrónico DMARC y DKIM para poder validar la legitimidad de los correos electrónicos.

• El sistema dispondrá de posibilidad de integración con Sandbox para la detección y bloqueo de nuevas amenazas avanzadas y de zero-day, siendo esta integración nativa y protegiendo de forma real al usuario; es decir, el correo electrónico debe esperar al veredicto del Sandbox para decidir la acción a tomar.

• Deberá permitir el archivado de los mensajes de correo electrónicos entrantes y salientes, conforme a los requisitos legales relativos a la protección de datos y a la realización de auditorías.

• Mínimo número de dominios: 70.

• Rendimiento de mensajes/hora (medida basada en mensajes sin encolar de 100KB de tamaño):

◦ Enrutamiento de correos: 250.000.

◦ Con las funcionalidades Antispam y Antivirus activas: 200.000.

• Número mínimo de interfaces GE (1000Base-T): 4.

• Almacenamiento interno mínimo: 2 x 1TB.

• La gestión se ha de poder realizar mediante un GUI sobre HTTPS, vía CLI usando SSH, o una conexión de consola. Se ha de disponer de una API (acrónimo de "Application Programming Interface", en castellano, "Interfaz de programación de aplicaciones") para monitorización, automatización y orquestación.

• El sistema permitirá aplicar políticas de filtrado por reputación de origen, contenido de tipo spam, contenido malicioso (virus), enlaces maliciosos, etc., en base a IPs, dominios de correo o incluso un grupo de direcciones de correo electrónico.

• El sistema deberá contar con protección de la reputación para impedir el envío al exterior de virus o correos no deseados. Asimismo, contará con elementos de prevención de fugas y pérdidas de datos, ya sean intencionales o accidentales, realizando la detección y protección de datos confidenciales por correo electrónico mediante el uso de diccionarios predefinidos y personalizables que admitan el uso de expresiones regulares.

• La protección antispam deberá soportar el estándar de autenticación de correo electrónico DMARC y DKIM para poder validar la legitimidad de los correos electrónicos.

• Análisis de suplantación de identidad para la detección de ataques del tipo "impersonation" o Business Email Compromise.

Con el fin de aprovechar y consolidar la experiencia y conocimientos ya adquiridos por los técnicos correspondientes del Ayuntamiento, esta solución deberá ser del mismo fabricante de la actualmente implantada y con objeto de unificar la información de seguridad, se deberá integrar de forma nativa con la consola de gestión de logs y eventos de seguridad incluida para el sistema cortafuegos de segundo nivel.

El adjudicatario deberá de proveer de un sistema de volcado del histórico de logs de ambos equipos de protección del correo electrónico sobre el sistema de almacenamiento que indique el Ayuntamiento.

Las tareas de instalación y puesta en marcha implican las de migración de la configuración implantada en los elementos actualmente instalados que integran el sistema de securización del correo. Esta migración requerirá de un estudio o análisis previo que recogerá tanto las prestaciones ofrecidas como la configuración establecida en los elementos que serán reemplazados. Ese análisis de la situación de partida deberá detectar los posibles fallos, errores o deficiencias de configuración que pudiera haber y propondrá las correcciones y mejoras necesarias para subsanarlos.

Así mismo el adjudicatario deberá como parte del proceso de implantación del nuevo sistema de protección del correo electrónico, realizar su correcta integración con el sistema de gestión de eventos de seguridad (SIEM) disponible en el Ayuntamiento de Mérida y basado en la solución MONICA homologada por el CCN.

5.7.4 SECURIZACIÓN APLICAC IONES WEBS. WAF

Con el fin de proteger los diferentes servicios web y de administración electrónica contra las amenazas habituales en este tipo de entornos (cross-sitescripting, ataques mediante inyección SQL o inyección de comandos, buffer overflows, etc.) y obtener un el mejor rendimiento y prestaciones en dicha protección, se requiere la implantación de un sistema WAF físico, conformado por dos appliances hardware configurados en alta disponibilidad mediante un clúster Activo-Pasivo e instalados en los CPDs del Ayuntamiento (uno en cada CPD). Desde el momento de su implantación y hasta la fecha de finalización del contrato tendrán activos los servicios de soporte y mantenimiento de fabricante y dispondrán de las licencias necesarias para esta funcionalidad (licencias necesarias para las actualizaciones de seguridad de los equipos, incluyendo antivirus y reputación de IPs, etc.).

El sistema ofertado debe ser lo suficientemente flexible como para adaptarse a la evolución y cambio de las infraestructuras de las tecnologías de la comunicación e información y al panorama de amenazas, debiendo cubrir asimismo las necesidades del Ayuntamiento de Mérida planteadas en este pliego.

El sistema debe ser capaz de detectar bots, rastreadores y spammers, aunque usen técnicas para disfrazar el tráfico malicioso. Debe detectar la huella de los dispositivos, identificar listas negras y bloquear los ataques independientemente de la dirección IP que se esconda detrás, incluso si el bot cambia dinámicamente su dirección IP de origen.

El sistema debe estar basado en modelos de seguridad negativos y positivos que detecten automáticamente dominios de aplicación, analicen vulnerabilidades potenciales y asignen políticas de protección óptimas que son fundamentales. El fabricante o proveedor de la solución debe asumir la responsabilidad de actualizar las políticas de seguridad, así como supervisar activamente, detectar, alertar y mitigar los ataques en tiempo real.

Debe ser una solución unificada que garantice la disponibilidad y protección sin brechas de seguridad, cumpliendo con las siguientes características:

- Posibilidad de configuración con distintos tipos de despliegues: transparente, proxy inverso, sniffer, para ajustarse a la arquitectura de despliegue que se considere más conveniente. Asimismo, permitirá la integración de equipos de red de terceros mediante el protocolo WCCP.
- Prevención frente a los ataques más habituales a aplicaciones Web (OWASP Top 10, acrónimo de “Open Web Application Security Project”), incluyendo, como mínimo:
- Cross Site Scripting.
- SQL Injection.
- Cross Site Request Forgery.
- Session Hijacking.

- Protección frente a los ataques de fuerza bruta permitiendo validación de protocolos y de parámetros de las aplicaciones, así como prevención contra fugas de información y cambios en la estética de las aplicaciones (Web defacement).

- Dispondrá de un escáner de vulnerabilidades Web de aplicaciones o permitirá integraciones con escáneres de vulnerabilidades web reconocidos (tipo Acunetix, Qualys, AppScan, WhiteHat, Faast, HP Webinspect, etc.).

- Proporcionará funcionalidad de escaneo de virus para ficheros que se suban a las aplicaciones, con posibilidad de que esos ficheros sean enviados a una plataforma de sandboxing para la detección de malware zero-day y APTs.

- Para mejorar la entrega de las aplicaciones dispondrá de capacidades de: balanceo de tráfico HTTP y HTTPS, reescritura de URLs, compresión, enrutado de contenido y caching.

- Dispondrá de capacidades específicas de cifrado/descifrado de HTTPS y SSL, incluyendo la posibilidad de crear certificados digitales al vuelo para la autenticación de certificado en aplicaciones que en principio no sean compatibles.

- Dispondrá de interface web de configuración y administración que ofrezca herramientas gráficas de análisis del tráfico y de las amenazas, permitiendo la geolocalización desde donde se produce el ataque, disponiendo de mapas mundiales donde se muestren el origen de los ataques, y haciendo el seguimiento de usuarios y dispositivos.

- Deberá soportar el uso de CAPTCHA antes de poder acceder a la web para garantizar que no se está intentando el acceso desde un bot (aféresis de robot).

- Dispondrá de capacidades específicas de gestión de logs e informes.

- Deberá disponer de un motor nativo de antivirus embebido del mismo fabricante sin delegar su motor de antivirus a terceros. Asimismo, dispondrá de una solución de sandboxing en nube nativa del propio fabricante para detonar ficheros y detectar amenazas avanzadas. Se incluirán todas las licencias necesarias para las actualizaciones de seguridad de los equipos, así como de los elementos de protección (antivirus y reputación de IPs).

- Capacidad para, al menos, 64 dominios administrativos.

- Rendimiento de 2,5 Gbps como mínimo.

- Número mínimo de interfaces 10 GE SFP+: 2.

- Número mínimo de interfaces 1 GE SFP: 4.

- Número mínimo de interfaces GE (1000Base-T): 8 (al menos 2 de ellos deben permitir bypass).

- Módulos SFP+: 2 SR + 1 LR (por cada equipo)

- Almacenamiento interno mínimo: 2 x 480GB SSD.

- La solución propuesta se deberá integrar de forma nativa con la consola de gestión de logs y eventos de seguridad incluida para el sistema cortafuegos de segundo nivel. El adjudicatario deberá de proveer de un sistema de volcado del histórico de logs de ambos firewalls sobre el sistema de almacenamiento que indique el Ayuntamiento.

Este sistema de protección WAF tiene, para el Ayuntamiento de Mérida, la consideración de infraestructura crítica, por ello:

- En ningún caso el fallo de uno de los elementos que lo integran debe ser motivo de indisponibilidad de los servicios que protege.
- Los elementos deben mantener el rendimiento exigido en caso de caída de uno de los miembros del clúster.
- El equipamiento deberá incluir fuentes de alimentación redundantes e intercambiables en caliente.
- Las tareas de instalación incluirán todas las actividades necesarias para la puesta en marcha de los equipos, así como las de análisis de los sistemas y aplicaciones que deberán proteger para evaluar las políticas y configuraciones adecuadas a desplegar sobre los equipos para una óptima protección.
- Así mismo el adjudicatario deberá como parte del proceso de implantación de los nuevos equipos WAF, realizar su correcta integración con el sistema de gestión de eventos de seguridad (SIEM) disponible en el Ayuntamiento de Mérida y basado en la solución MONICA homologada por el CCN, detallado en un apartado más adelante.

5.7.5 SERVICIOS DE SOPORTE Y MANTENIMIENTO

El adjudicatario proporcionará los servicios de soporte y mantenimiento de todos los elementos tanto hardware como software, integrantes de la infraestructura de seguridad de la red de datos, conforme a las condiciones y prestaciones que más adelante se indican, debiendo contar para ello con un SOC (Security Operation Center) que deberá contar con todos los medios técnicos y recursos adecuados para la correcta prestación de los mismos. Los requisitos que debe cumplir el Centro de Operaciones deben ser al menos los siguientes:

- Deberá estar ubicado dentro del territorio nacional y deberá ser atendido en castellano.
- Operará de forma continuada en modalidad 24x7
- Dispondrá de una metodología alineada y armonizada con marcos y estándares de referencia como ITIL, ISO 27001, CERT, entre otras.
- Estará dotado de una estructura funcional con diferentes áreas operativas y niveles de especialización.

- Dispondrá de los medios adecuados para la conexión a los sistemas objeto del contrato, para realizar las acciones de soporte correspondiente de forma remota y totalmente segura.
- Dispondrá de medidas de tolerancia a fallos en los elementos que sustentan su funcionamiento, tanto en los sistemas de información como en los elementos auxiliares (electricidad, refrigeración, comunicaciones, etc.), requiriéndose al menos TIER III.
- Dispondrá de medios de control de acceso físico al centro.
- Dispondrá de un Plan de Continuidad.
- Dispondrá de áreas físicamente separadas para realizar sesiones de análisis de problemas sin afectar a la operación del centro.
- Contará con un proceso de formación continua del personal involucrado en la gestión de la seguridad.

Mantenimiento

Durante el plazo de vigencia del contrato, el adjudicatario será el único responsable del correcto funcionamiento de los equipos, software y servicios suministrados bajo una modalidad de soporte 24x7, participando del:

- Proceso de gestión de incidencias, con objeto de restaurar los servicios de seguridad lo más rápidamente posible ante la aparición de cualquier incidente y/o malfuncionamiento y resolver aquellas solicitudes que necesiten de una capacidad o conocimiento experto para su resolución cuando el grado de complejidad así lo requiera.
- Proceso de gestión de problemas, con objeto de gestionar las causas subyacentes de las incidencias que impacten sobre los sistemas de seguridad del Ayuntamiento de Mérida y la infraestructura técnica que los soporta.
- Proceso de gestión de peticiones, con objeto de dar respuesta ágil y ordenada de todas las peticiones derivadas por el Ayuntamiento de Mérida y relacionadas con el equipamiento suministrado.

En ese sentido, la empresa adjudicataria pondrá a disposición del Ayuntamiento de Mérida, un servicio de soporte técnico, en modalidad 24x7 con los recursos necesarios que permitan dar respuesta, dentro de los niveles de servicio que más adelante se indican, a todas aquellas incidencias y problemas que provoquen un malfuncionamiento de los equipos y/o servicios cloud adquiridos o afecten a su rendimiento. Este servicio incluirá al menos lo siguiente:

- Resolver las tareas asociadas al reemplazado por avería de un equipo incluyendo:
- Desenracado del equipo dañado en las dependencias del Ayuntamiento de Mérida.
- Recepción del equipo enviado por el fabricante
- Restauración de la configuración en base al último backup disponible.

- Envío y posterior enracado del equipo nuevo en las instalaciones del Ayuntamiento de Mérida.
- Devolución del equipo dañado al fabricante.
- Registro y control de las peticiones del servicio. Se deberá proporcionar una herramienta de ticketing para el registro y seguimiento de las incidencias o solicitudes realizadas.

Los servicios asociados al mantenimiento se prestarán preferentemente de forma remota. No obstante, dada la naturaleza de los mismos, habrá trabajos que requerirán la presencia in-situ de equipos de trabajo en las oficinas centrales del Ayuntamiento de Mérida, sin que ello deba afectar a las condiciones de la oferta.

El adjudicatario deberá contar con el correspondiente contrato de soporte con los fabricantes, que le garantice tanto su soporte técnico, servicio de inteligencia de amenazas, reposición de equipos por avería (RMA) así como las actualizaciones de software que se pudieran liberar y las actualizaciones de firmas para los diferentes servicios de seguridad requeridos, durante toda la vigencia del contrato.

Administración y monitorización

De forma complementaria al servicio de mantenimiento indicado anteriormente, el adjudicatario deberá ofrecer un servicio de administración completa de las infraestructuras de seguridad provisionadas, que deberá de incluir todas las actividades de control, revisión y perfección de los equipos, de su software, su configuración y sus políticas de seguridad. En este sentido el adjudicatario asumirá la responsabilidad de la completa gestión y administración de los equipos y servicios cloud provisionados, así como de su óptimo funcionamiento y adaptación a las nuevas necesidades del Ayuntamiento de Mérida y a las nuevas condiciones y amenazas que puedan existir.

El servicio de administración tendrá una cobertura completa en modalidad 24x7 y estará complementado con un servicio de soporte técnico especializado, que servirá de apoyo a los administradores de seguridad del Ayuntamiento de Mérida para las siguientes tareas:

- Resolver consultas o incidencias relacionadas con la operación y gestión de los dispositivos de seguridad suministrados.
- Resolver las consultas que el personal técnico del Ayuntamiento de Mérida pueda tener sobre las funcionalidades disponibles en el equipamiento objeto del presente contrato.
- Participación en incidentes de seguridad, colaborando en el descubrimiento de los orígenes y mitigación dentro del alcance de la visión que le proporcionen los equipos administrados de los incidentes de seguridad.
- Planificación y ejecución de cambios, contemplando el estudio y realización de los cambios sobre los elementos administrados que solicite el Ayuntamiento de Mérida o que puedan ser recomendados por el propio adjudicatario, en base a las mejores prácticas o normativas de administración estándares o como solución ante una incidencia o incidente de seguridad.
- Actualización del software/firmware, updates, upgrades, etc., de los dispositivos.

- Implantación de nuevas políticas de seguridad que puedan ser requeridas por parte del Ayuntamiento de Mérida y/o asesoramiento para su definición en base a las necesidades a cubrir.

- El adjudicatario deberá proporcionar también un servicio de Supervisión de Salud que monitorizará de forma permanente en cobertura 24x7 las variables de funcionamiento de los equipos firewall, fortimail y WAF.

- Este servicio deberá contar al menos con las siguientes características principales:

  - Monitorización de las variables de salud más idóneas para cada dispositivo de seguridad, como mínimo: uso de CPU, consumo de memoria, espacio de filesystems, tabla de conexiones (FW).

  - Plataforma de monitorización aportada por el adjudicatario (puede residir en su centro de gestión) que permita desplegar una arquitectura de monitorización con healthchecks a través SNMP polling.

  - Entrega mensual de un informe con volumetrías de tráfico y de actividad sobre los equipos monitorizados, entre las que como mínimo deben incluirse las siguientes:

    - Porcentaje de disponibilidad de los activos supervisados agrupados por tecnología.

    - Número de alertas detectadas en los activos supervisados agrupados por tecnología y severidad

    - Nº de notificaciones al cliente debido a alertas detectadas agrupadas por tecnología monitorizada.

Actualmente la Red Corporativa del Ayuntamiento de Mérida dispone de un conjunto de elementos hardware y software que constituyen la infraestructura de seguridad perimetral de la misma y que está integrado por:

CALIDAD DEL SERVICIO

Como medio para garantizar la calidad de la garantía, se establecerán unos ANS y el compromiso por parte de la persona adjudicataria de cumplirlos. Estos ANS podrán evolucionar a lo largo de la ejecución del contrato con el fin de conseguir una mejora continua en la calidad del servicio efectivamente proporcionado. Los recursos, tanto humanos como de otra índole, disponibles para el servicio de administración y mantenimiento, deberán ser dimensionados de forma cualitativa y cuantitativa como mínimo para garantizar los ANS vigentes en cada momento.

Los ANS se basarán en la definición de unos indicadores de calidad que reflejen de forma objetiva la calidad del servicio real proporcionado, con especial atención a los aspectos más críticos del mismo, y en el establecimiento de un umbral o valor mínimo de calidad para cada uno de ellos.

Definiciones previas

a. **Incidencia**: Fallo, degradación o comportamiento no esperado del equipamiento o servicio cloud.

b. **Peticiones**: Solicitud de ejecución de alguna tarea de configuración o consulta técnica sobre los equipos o servicios cloud.

c. **Consulta:** Solicitud de información sobre el estado o configuración de los equipos o servicios cloud, bien de forma genérica o en concreto para algún dispositivo sobre el que se esté prestando el servicio.

Se establece como criterio básico para catalogar las posibles incidencias el nivel de severidad de las mismas que como norma general vendrá determinada, además de por la severidad del propio equipo afectado, de la correspondiente al nivel de afectación del servicio prestado a otras áreas de la organización del Ayuntamiento de Mérida. En base a esto se establecen tres niveles de severidad:

CRÍTICO: Aquellas incidencias en que la hay corte de servicio.

ALTO: Aquellas incidencias en que la hay degradación de servicio.

MEDIO-BAJO: Incidencias con impacto en el servicio.

ANS

El horario sobre el que se mediarán los tiempos establecidos para determinar el cumplimiento tendrá en cuenta el horario de atención indicado para cada caso.

Los valores de compromiso que se indican no incluyen el tiempo de reposición de equipos, en caso de avería hardware, que será siempre de 24 horas NBD.

ANS de Tiempo de Respuesta para atención de Incidencias y Peticiones

Niveles de Severidad	Valor de Compromiso
CRÍTICO	30 minutos
ALTO	45 minutos
MEDIO-BAJO	60 minutos

ANS de Tiempo de Resolución de Incidencias y Peticiones

Niveles de Severidad	Valor de Compromiso
CRÍTICO	4 horas
ALTO	8 horas
MEDIO-BAJO	72 horas

5.7.2 SERVICIO DE CIBERSOC PARA LA MONITORIZACIÓN DE LA SEGURIDAD

Para la prestación del servicio, el adjudicatario deberá hacer uso de la plataforma de monitorización desplegada actualmente en el Ayuntamiento y que está basada en la herramienta CCN MONICA NGSIEM, por lo que el adjudicatario deberá estar obligatoriamente certificado en dicha herramienta.

El servicio para la gestión de la monitorización de eventos de seguridad se dispensará de forma remota desde el centro de operaciones del adjudicatario que deberá operar en modalidad 24x7 y será atendido por técnicos especialistas cualificados para tareas de monitorización, administración, soporte y operación certificados en la herramienta MONICA NGSIEM.

Los Servicios de monitorización, incluirán las siguientes funciones:

A. **Servicio de operación, monitorización, detección y notificación a través de la plataforma MONICA NGSIEM.**

El adjudicatario monitorizará mediante la plataforma MONICA NGSIEM todas las incidencias de seguridad detectadas en la red del Ayuntamiento y efectuará un análisis de la información recogida de dichos eventos, asociándoles diferentes grados de severidad a fin de obtener conclusiones y facilitar recomendaciones de actuación, ya sea esta preventiva o reactiva.

Por tanto, la función principal del servicio es monitorizar, prevenir, detectar, investigar, organizar y orquestar una respuesta a las amenazas de ciberseguridad las 24 horas del día, siendo sus actividades las siguientes:

1.- **Prevención y detección:** El servicio tendrá como objetivo detectar actividades maliciosas y prevenirlas antes de que puedan causar algún daño, reuniendo toda la información posible para una investigación más profunda, ante la detección de alguna actividad sospechosa.

El servicio se deberá encargar del mantenimiento de los casos de uso, así como de identificar necesidades de mejora en la calidad de la información de las fuentes, o nuevas fuentes a incorporar para completar el mapa de monitorización, con el objeto de asegurar la detección y envío de alertas y aumentar la eficacia en la detección.

Adicionalmente se deberá realizar una revisión periódica y proactiva por parte de los analistas del adjudicatario de los sucesos más destacables registrados con objeto de detectar incidentes que tras técnicas más diferenciadas, silenciosas o novedosas puedan haberse enmascarado entre las acciones legítimas.

2.- **Investigación**: será responsabilidad del adjudicatario analizar la actividad sospechosa reportada tanto automáticamente como proactivamente, para determinar la naturaleza de la amenaza y la medida en que ha podido penetrar en la infraestructura, bajo la perspectiva de un atacante, buscando indicadores clave y áreas de exposición antes de que sean explotadas.

Se identificará y realizará un triaje de los diversos tipos de incidentes de seguridad al comprender cómo se desarrollan los ataques y cómo responder de manera efectiva antes de que se produzca impacto, combinando

información sobre la red del Ayuntamiento con inteligencia de amenazas globales, incluyendo detalles sobre las tendencias en tácticas, técnicas y procedimientos (TTPs) de los actores de amenazas.

En este sentido el adjudicatario deberá contemplar el uso de al menos las siguientes técnicas y herramientas:

- Open Source Intelligence (OSINT): para la recopilación y análisis de información de fuentes abiertas y públicas, como redes sociales, foros en línea, sitios web públicos y bases de datos gubernamentales.
- Fuentes de Inteligencia de amenazas (Threat Intelligence): para la recopilación y análisis de información sobre posibles amenazas cibernéticas, como malware, ataques de phishing y vulnerabilidades de software.
- Análisis de malware: para el análisis de programas maliciosos para identificar su comportamiento, características y origen. Esta técnica puede ayudar a comprender cómo opera un malware específico y cómo protegerse de él.
- Análisis de vulnerabilidades: para la identificación y evaluación de vulnerabilidades en sistemas y aplicaciones, con el objetivo de proporcionar información para la mitigación de riesgos y la toma de decisiones informadas.
- Análisis de tráfico de red: para el análisis de patrones de tráfico de red para identificar posibles amenazas, anomalías y comportamientos maliciosos.
- Dark Web: para la recopilación y análisis de información en la Dark Web, que es una parte de la Internet que no se puede indexar en los motores de búsqueda convencionales y que a menudo se utiliza para actividades ilegales.

3.- **Respuesta**: el adjudicatario deberá coordinar la respuesta para remediar el problema actuando como primer respondedor, definiendo Playbooks técnicos, configurando respuestas automatizadas, realizando otras acciones como aislar puntos finales, terminar procesos dañinos, evitar que se ejecuten, eliminen archivos y más, interaccionando automática o manualmente con elementos de seguridad de la red como FW, WAF, EDR, etc.

4.- **Comunicación y colaboración**: el adjudicatario deberá participar en los procesos de comunicación a través de los canales de comunicación directa y colaboración entre equipos SOC adheridos a la Red Nacional de SOC (RNS) y Foros CSIRT/CERT nacionales e internacionales, de ciberinteligencia y organizaciones gubernamentales como CCN, siempre bajo la coordinación del Ayuntamiento.

5.- **Funciones de asesoría, administrativas y de soporte de la plataforma MONICA NGSIEM**. El adjudicatario deberá realizar las siguientes actividades relacionadas con el mantenimiento y soporte de la plataforma:

- Soporte técnico en modalidad 8x5, que ofrecerá asistencia técnica al personal técnico del Ayuntamiento para resolver problemas relacionados con la plataforma, ya sea a través de soporte telefónico, chat en línea o correo electrónico.

- Recepción y registro de solicitudes de soporte.
- Diagnóstico de problemas.
- Resolución de problemas mediante la aplicación de soluciones conocidas o escalando el problema a niveles superiores de soporte si es necesario.
- Comunicación proactiva con los usuarios para mantenerlos informados sobre el progreso de la resolución del problema.
- Administración y Operación de la plataforma.
- Vigilancia de salud de la plataforma 24x7.
- Vigilancia de la cadencia y revisión de la calidad de la información de fuentes.
- Mantenimiento y Optimización de UCs básicos.
- Actualización continua y adecuación de UCs avanzados.
- Asesoramiento en la priorización de la información e integraciones.
- Revisión de capacidades de la plataforma y necesidades de ampliación / escalado.
- Implementación de UCs ad-hoc.
- Implementación de procesos de automatización en la respuesta ante incidentes.
- Identificación continua de necesidades de mejora en:
- Integración de fuentes.
- Procesamiento de la información.
- Casos de uso (UCs).
- Informes.
- Procedimiento y documentación.

6.- Documentación e Informes de servicio, operación y ciberseguridad: El adjudicatario deberá realizar al menos los siguientes informes a petición del Ayuntamiento o cuando los mismos obedezcan a cambios o situaciones de incidente.

- Mantenimiento de la calidad de informes activos.
- Generación de informes ad-hoc.
- Documentación para la gestión de incidentes de ciberseguridad.
- Playbooks: Aportación, adaptación y creación de playbooks ad-hoc.

Equipo de trabajo

Para poder operar con una calidad suficiente es requisito mínimo e indispensable disponer del número de técnicos detallado a continuación y que dispongan de las certificaciones en la herramienta MONICA NGSIEM:

- 3 Técnicos con Certificación de usuario.
- 2 Técnicos con Certificación de usuario avanzado.
- 1 Técnico con Certificación en diseño e implementación de correlación de eventos.
- 1 Técnico con Certificación de administrador de la plataforma.

B. Gestión de eventos e incidentes de seguridad y acompañamiento en la contención y remediación de incidentes:

Los licitadores deberán incluir en sus ofertas una propuesta sobre como realizarán la gestión de eventos, considerando las actividades requeridas en este pliego, así como las que de forma adicional o complementaria puedan incluir.

La gestión de eventos propuesta deberá como mínimo contemplar el ciclo de vida completo del incidente incluyendo las siguientes etapas:

- Prevención y preparación.
- Detección e identificación.
- Notificación.
- Acompañamiento en la contención y remediación de incidentes
- Análisis e investigación.
- Solución y recuperación.
- Reflexión y mejora.

5.7.6 PLATAFORMA AVANZADA DE GESTIÓN DE LOGS

Actualmente el Ayto. Mérida dispone de un FortiAnalyzer virtualizado para recolección y análisis de logs, que permanecerá como plataforma de backup, se solicita una nueva plataforma en modo appliance con objeto de centralizar y mantener los logs a largo plazo de toda la solución de seguridad.

Todos los logs generados por el resto de los componentes suministrados deben ser procesados y almacenados en la nueva plataforma avanzada de gestión de logs.

Se requiere de una plataforma de gestión y procesamiento especializada con las siguientes características:

- Plataforma en formato appliance, con una capacidad de ingesta de al menos 200GB/día y 4000 logs/segundos sostenidos a nivel de analítica.
- 180 dispositivos/vdoms
- 50 días de analítica.
- 16 TB de almacenamiento, con 8TB usables en raid 10.
- Interfaces de red: 4x RJ-45, 2x GE SFP
- Fuente de alimentación redundante.
- Módulo de TPM (Trusted Platform Module)
- Servicio de indicadores de compromiso que permita la detección de brechas de seguridad, con posibilidad de automatizar acciones de respuesta en los cortafuegos ofertados a partir de estos.
- Cuadro de mando personalizable por usuario que accede al sistema con al menos la siguiente información: Logs relativos a las amenazas más observadas, logs de filtrados URL o recursos del sistema.
- Cuadro de mando de aplicaciones generado a partir de los logs, personalizable por usuario que permita disponer de información como las direcciones IPs que más paquetes generan por la red, ancho de banda utilizado por cada sede del PRP, aplicaciones utilizadas por las sedes, páginas webs más visitadas, consumo de ancho de banda por VPN, además de paquetes enviados y recibidos.
- Capacidad de uso de motor integrado de correlación de logs dentro de la propia plataforma de forma que a partir de los logs recibidos se pueda obtener información de alto nivel como un listado de equipos comprometidos en la red interna y las evidencias que han dado lugar a dicho listado con indicación de tiempos, usuarios, direcciones IP y vulnerabilidades o amenazas detectadas.
- Posibilidad de filtrar cada una de las vistas o cuadros de mando de forma que la información esté restringida a ciertos criterios para poder realizar análisis más exhaustivos.
- Permitir realizar un análisis detallado del uso de red de los usuarios (tráfico enviado y recibido, sesiones, aplicaciones, amenazas, sitios web por los que han navegado, políticas aplicadas, interfaces, etc).
- Opcional y valorado como mejora: Arquitectura escalable que permite al dispositivo funcionar en modo colector o analizador, para optimizar el procesamiento de eventos

- Ejecución de diferentes utilidades de diagnóstico, tales como: ping, traceroute y visor de eventos.
- Múltiples usuarios de administración con diferentes perfiles de gestión administrativa basada en roles.
- Permitir el uso de informes predefinidos y la parametrización de informes a medida, en distintos idiomas y con gráficos configurables para ayudar a monitorizar y mantener identificados patrones de ataques, políticas de uso aceptable y a demostrar el cumplimiento de políticas.
- Los logs a registrar y almacenar deben de contener como mínimo la siguiente información: la fecha y hora, dirección IP origen y destino, puerto TCP/UDP y protocolo, nombre de la aplicación y servicio, paquetes enviados y recibidos, bytes enviados y recibidos, política de cortafuegos y acción (permitir o bloquear).

5.7.7 SERVICIO AVANZADO DE AUTENTICACIÓN

Actualmente el Ayuntamiento no dispone de un servicio avanzado de autenticación, recomendado por el ENS, y por tanto se requiere un control de identidades con el que auditar, controlar y limitar el acceso de sus usuarios a los recursos digitales, ya sean internos o externos, bajo el concepto de "el recurso adecuado para el usuario adecuado".

Estos recursos van desde documentos o aplicaciones internas al servicio de Internet, extendiéndose para alcanzar un objetivo de arquitectura ZTNA (Zero Trust Network Access), que incluya también el acceso a la red corporativa propiamente dicho.

Para ello, requiere dotarse de una plataforma de Gestión de Identidades que se encargue de centralizar y simplificar la gestión y almacenamiento de la información de los usuarios presentes en cualquier red corporativa. Esta plataforma estará licenciada inicialmente para 500 usuarios, pero deberá de ser escalable, hasta el crecimiento que tenga el Ayuntamiento en materia de personal durante la duración del contrato; será desplegada en servidores virtuales del Ayuntamiento de Mérida, por lo que debe ser compatible con (ESXi / HyperV / KVM / XEN).

Esta herramienta debe ofrecer como mínimo las siguientes capacidades:

- Autenticación centralizada de usuarios y máquinas.
- Integración con autenticación de doble factor.
- Integración con autenticación de doble factor como servicio.
- Arquitecturas de Single Sign-on.
- Gestión de Invitados.
- Gestión de onboarding de dispositivos en red corporativa.

Para ello, debe ser capaz de recabar información de usuarios empleando una gran variedad de métodos:

- Interaccionando con los controladores de Directorio Activo o LDAP para recabar los grupos a los que pertenezca un usuario.
- Usando un agente propio de single-sign on (SSO), que instalado en los dispositivos detecte el login/logout de usuarios y la ip asociada.
- Autenticación basada en portales, capaz de integrarse con el resto de fuentes de identificación o incluso con redes sociales.
- RADIUS externos, monitorizando los paquetes de accounting que contienen información del usuario.

Para facilitar la operatividad e intentar impactar lo menos posible en la productividad de la infraestructura, es necesario disponer de mecanismos que permitan a la arquitectura de seguridad reutilizar las credenciales que el usuario ha usado en un sistema otros, evitando que deba introducir reiteradamente la misma información conforme vaya accediendo a diferentes recursos.

El sistema de gestión de identidades solicitado debe facilitar el despliegue de arquitecturas de single sign-on (SSO) multiservicio, añadiendo un rango mayor de métodos de autenticación e incrementando la escalabilidad.

Esta plataforma será, en definitiva, empleada como garante del acceso seguro a la red, identificando a los usuarios, preguntando a otros sistemas qué permisos tienen y comunicando esa información a otros sistemas, como pueden ser firewalls para empleen esta información en políticas de seguridad basadas en identidad.

Se describen a continuación con mayor detalle algunas de las capacidades requeridas para la plataforma de gestión de identidades:

*** Servicios de autenticación**

· Debe poder ejercer los roles tanto de servidor de autenticación, como de cliente de otros repositorios o fuentes de identidad.

· Debe poder operar como un servidor de RADIUS y TACACS+ autónomo, ofreciendo autenticación tanto basada certificados como no basada en los mismos, como EAP-TLS, EAP-TTLS, PEAP, EAP-GTC, y también autenticación MAC para entornos con MAB (MacAuthentication-Bypass). Debe permitir securizar las conexiones RADIUS mediante el uso de RADSec (RADIUS sobre TLS).

· Debe poder conectarse a un servicio LDAP (Microsoft Active Directory, OpenLDAP/Gsuite o novel eDirectory) para recabar validar usuarios, por ejemplo, cuando recibe una petición RADIUS.

· Debe poder integrarse con el AD de Windows, al menos para permitir verificar que una máquina intentando acceder a la red haya sido registrada y contenga credenciales válidas, realizando una autenticación de máquina anterior a la autenticación basada en usuario.

· Debe permitir desplegar portales de autenticación explícita para una autenticación manual, por ejemplo, para casos de uso como la gestión de invitados (en los que el usuario ni siquiera pertenece a la organización).

· Debe ser compatible con OAUTH para integrar la autenticación con redes sociales (al menos, Facebook, Google, Linkedin, Twiter), Azure Directory y G-Suite.

*** Single sign on (SSO)**

· Debe disponer de la capacidad de integrarse con otros servicios de autenticación disponibles en la red corporativa, con el fin de asegurar cada usuario sólo tenga que autenticarse una vez, y esa autenticación se reutilice en el resto de los sistemas.

· Para ello, debe poder detectar qué usuarios han hecho login en el Directorio Activo, así como permitir integraciones vía syslog, NTLM, y SAML (tanto en rol de Service Provider [SP] como en Identity Provider [IdP]).

*** Doble factor de autenticación**

· Una solución de doble factor de autenticación asegura que sólo los usuarios autorizados tengan acceso a la información sensible, aportando una capa adicional de seguridad que reduce drásticamente la posibilidad de que se produzca una pérdida de información.

· El uso de este segundo factor será muy amplio, abarcando tanto la autenticación de los accesos remotos vía VPN, como la autenticación en aplicaciones y portales, pudiendo incorporarse también a la administración de sistemas y plataformas de seguridad y críticos del Ayuntamiento.

· La plataforma solicitada debe soportar diferentes tipos de Token, tanto físicos como software, además de doble factor basado en email o SMS.

· Para facilitar la gestión de usuarios, debe incluir portales de auto-registro, auto aprovisionamiento de tokens y recuperación de password.

*** Token**

· Se requiere la provisión de una solución de OTP (One Time Password), o Token, para 500 usuarios.

· Debe proporcionarse en formato de aplicación para móvil (compatible con los sistemas Android, iOS y Windows Mobile), aunque se valorará positivamente la posibilidad de disponer de tokens físicos (en formato tarjeta de crédito/visita o llave USB) para algunos casos particulares.

· Debe soportar notificaciones push, esto es, que el usuario únicamente tenga que pulsar para aceptar la autenticación y que el token sea enviado automáticamente la plataforma de gestión de identidades, simplificando la interacción entre el sistema de autenticación y el usuario, sin necesidad de que sea el usuario el que introduzca los dígitos uno a uno.

· Esta solución no debe requerir ningún soporte recurrente, sino estar licencia de manera perpetua.

*** Gestión de certificados**

· Por último, la plataforma debe permitir gestionar el ciclo de vida de los certificados corporativos, actuando como Autoridad de Certificación para crear y firmar certificados X.509, tanto para servidores como clientes, incluyendo servicios propios de PKI's tradicionales como SCEP, CRL's y OCSP.

· El uso de estos certificados estará orientado principalmente a la autenticación de usuarios y servidores, para accesos remotos por VPN, o a servidores y servicios web.

5.7.8 ACCESO REMOTO SEGURO – ZTNA (ZERO TRUST NETWORK ACCESS)

Se requiere una solución de acceso remoto seguro y monitorización continua del estado de seguridad del endpoint, de forma que se pueda evolucionar un mecanismo tradicional como la VPN, que permite el acceso a los recursos corporativos de los usuarios remotos, a procesos que proporcionen tanto un análisis en tiempo real del riesgo como una experiencia de uso sencilla, tanto para accesos remotos como desde el propio interior de la red corporativa, en línea con los paradigmas de diseño de Zero Trust – Confianza Cero.

La solución suministrada debe contemplar 500 licencias entre puestos de usuario y servidores, pero deberá de ser escalable, hasta el crecimiento que tenga el Ayuntamiento durante la duración del contrato.

El sistema debe cumplir con las siguientes características mínimas:

Visibilidad del estado de la infraestructura y políticas de protección

- Proporcionar una vista unificada de los endpoints para facilitar su seguimiento, aplicación de políticas corporativas de seguridad, presentación de informes.
- Permitir de un modo sencillo la gestión corporativa tanto de los tradicionales túneles de red privada virtual (incluyendo implementaciones como túnel dividido, VPN siempre conectada, y VPN antes del logon) como su evolución a conexiones ZTNA, túneles automáticos y cifrados para acceso controlado,

validado por sesión y de forma granular a las aplicaciones corporativas, con independencia de que el usuario sea local o remoto.

- La herramienta debe ser capaz de establecer diferentes políticas para diferentes usuarios/grupos/equipos, integrándose con fuentes externas de identidad (al menos, con Microsoft Active Directory). Debe asimismo permitir el uso de autenticación multifactor para proporcionar una capa adicional de seguridad.

- Gestión simplificada y aplicación de políticas con desde una consola centralizada, on-premise o en la cloud del fabricante.

- La solución debe ser capaz de definir condiciones para la aplicación de reglas a los equipos protegidos, como por ejemplo versiones de ficheros ejecutables y entradas del registro. Se valorará especialmente la integración de la telemetría del endpoint y el resultado de sus evaluaciones de seguridad con el sistema de protección perimetral, de forma que dicha información pueda utilizarse tanto para complementar la visión que de los endpoints se tiene desde el perímetro como para permitir o denegar el tráfico de los mismos.

- Adicionalmente, la solución debe poder aplicar una marca de criticidad -deseablemente personalizable- en los activos, para permitir al equipo de seguridad TI identificar fácilmente dicha criticidad a la hora de realizar una correcta priorización en la gestión de eventos de seguridad de la plataforma.

- Debe permitir definir políticas de filtrado web en local, brindando seguridad web y filtrado de contenido, así control de aplicaciones basadas en web y software como servicio (SaaS).

- También debe permitir diferenciar cuándo un dispositivo está dentro de la red corporativa de cuándo no, posibilitando aplicar políticas de protección diferenciadas para cada uno de esos escenarios, inhibiendo por ejemplo el filtrado web local cuando el equipo está dentro de la red corporativa.

- Integración con el sistema de gestión de logs e informes, tanto para disponer de acceso a estos registros en la misma plataforma que otros servicios de seguridad (como los cortafuegos perimetrales o la protección avanzada del endpoint), como también para posibilidad la correlación de eventos entre todos estos elementos. Dicha integración debe permitir también la aplicar la capacidad de identificar indicadores de compromiso, de forma que se profundice en el análisis de las amenazas, o incluso que puedan llegar a identificarse antes de que lo haga ningún elemento individual de seguridad.

- Gestión de vulnerabilidades en base al inventario de aplicaciones instaladas, mediante el análisis de los niveles de riesgo de las vulnerabilidades que puedan afectar a las versiones instaladas.

- Los eventos producidos por la solución deben ser exportables a sistemas SIEM externos vía syslog.

Compatibilidad del agente con los siguientes sistemas operativos y entornos:

- La solución de protección de puesto debe estar soportada en Windows 7, 8, 8.1, 10 y 11 así como Windows Server 2012 o posterior. Se valorará especialmente la compatibilidad con otros sistemas operativos, como Linux (Ubuntu 16.04 o posterior, Red Hat 7.4 o posterior, CentOS 7.4 o posterior), macOS (10.14 o posterior), Chromebook, iOS (9.0 o posterior) y Android (5.0 o posterior).

- La solución debe soportar su despliegue en entornos VDI.

- El modelo de licenciamiento debe ser por equipos protegidos y no por otros parámetros como p.e. número de usuarios, CPUs, etc.

Despliegue, mantenimiento y requisitos del agente:

- La plataforma permitirá instalar el agente tanto de forma automática desde la consola (opción preferente) como manualmente ante equipos (principalmente portátiles) que potencialmente no estén en el dominio corporativo.
- Las actualizaciones del software agente de los equipos protegidos deben poder realizarse directamente desde la consola de gestión.

Consola de gestión de la plataforma:

- Un único servidor del sistema de gestión centralizada debe ser capaz de soportar hasta 5000 equipos protegidos. Además, la solución deberá poder escalar en caso de requerirse un despliegue superior a esta cifra, mediante la incorporación de recursos adicionales a dicho servidor, o el reparto de las funcionalidades y la carga entre más equipos.
- Toda la gestión de las configuraciones de seguridad de la solución desde el punto centralizado debe poder hacerse en su totalidad con un navegador web, sin requerirse en ningún caso la instalación de software adicional.
- Debe proporcionar cuadros de mando que muestren tanto el estado de seguridad y amenazas, como la "salud" de los diferentes elementos de la plataforma.
- Configuración granular de perfiles de acceso con diferentes privilegios, así como la asignación de usuarios a estos perfiles.
- La plataforma debe soportar por diseño el login y la operación en formato multi-tenancy (RBAC/Role-Based Access Control).
- Soporte RestFull API para desarrollar las integraciones adicionales que se requieran.

Servicios del fabricante:

- Se valorará positivamente el soporte directo del fabricante, al menos durante el primer año, en formato de consultoría sobre el despliegue y mejores prácticas en la explotación de la herramienta, a modo de guía en el proceso de aprendizaje de los técnicos de Ayuntamiento de Mérida sobre las capacidades de la solución ofertada.

5.7.9 NETWORK ACCESS CONTROL (NAC)

Actualmente el Ayuntamiento no dispone de un servicio avanzado de control de acceso a la red (NAC por sus siglas en inglés), y por tanto se requiere una solución NAC que ofrezca visibilidad de qué hay conectado en cada punto de la red, ya sea una conexión inalámbrica, cableada o a través de una VPN, obteniendo información del dispositivo y de los usuarios asociados, si los hubiere, y desplegando políticas de control de acceso en función de esta información, garantizando a la vez el acceso de los dispositivos reconocidos, y otorgándoles la conectividad mínima e imprescindible en función del rol que desempeñan, mientras se asegura el aislamiento de cualquier dispositivo no permitido, tan pronto como se conecte.

Al mismo tiempo, debe permitir responder de manera ágil ante alertas enviadas por sistemas externos al NAC, modificando la configuración de acceso a red, para el dispositivo implicado.
De esta manera, a la vez que se garantiza la seguridad de red, se automatiza la segmentación y la contención de amenazas.

El NAC debe realizar una integración total con los dispositivos de red de acceso y seguridad actual de Ayuntamiento de Mérida. Los modelos de equipamiento de red son los siguientes:

- Conmutadores de acceso y agregación
- Puntos de Acceso
- Controladores Wireless
- Firewall

El NAC debe permitir diferentes métodos y protocolos para la integración de la infraestructura de red actual y futura. Con tal de evitar al máximo posible las limitaciones que puedan dar los diferentes modelos de switch y versiones de firmware se requiere que el NAC tenga los siguientes métodos de gestión, monitorización y descubrimiento:

- SNMP v2/v3
- RADIUS
- CLI SSH – Telnet
- API
- Syslog
- CDP/LLDP

1. La solución NAC debe incluir los siguientes bloques funcionales:
    a. **Visibilidad** completa de red y perfilado de dispositivos conectados.
    b. **Control** de acceso a red basado en roles.
    c. **Respuesta** en la capa de acceso a red, respondiendo a determinados eventos.
    d. **OnBoarding** de nuevos dispositivos sencillo, versátil y potente.
    e. **Automatización** del proceso de provisión de acceso a red en función del tipo de dispositivo que se esté conectando.
    f. **Endpoint Compliance**: Permitiendo a la organización desplegar políticas asociadas a diferentes grupos de usuarios, verificando su cumplimiento y notificando las desviaciones, permitiendo

configurar diferentes políticas de remediación, desde acciones de aislamiento inmediatas a simples notificaciones, pasando por acciones diferidas.

g. **Identificación de amenazas,** a través de la integración con otros elementos de seguridad, y ejecución de acciones de remediación en función del evento.

h. **Gestión de invitados y usuarios externos:** Fácil y rápido, sin necesidad de involucrar al personal de IT en el alta de nuevos usuarios externos.

2. La solución NAC debe ser **agnóstica respecto a los fabricantes del equipamiento de acceso,** tanto cableado como inalámbrico y por tanto válida en redes heterogéneas.
3. La solución NAC debe estar integrada con los dispositivos de red y seguridad existentes, y los que se incluyan en la nueva arquitectura.
4. Debe ser capaz de trabajar tanto con agentes instalados en los endpoints como sin agentes.
5. La solución NAC **no puede ser** dependiente de soluciones **802.1x y RADIUS**, pero debe de ser compatible.
6. La solución de NAC debe disponer de un asistente de configuración que guíe al usuario por las tareas iniciales de configuración típicas del sistema NAC, pudiendo marcar como completadas aquellas que se desee.
7. El sistema soportará diferentes modos de despliegue:
    a. Virtual sobre nube privada: soportando al menos los hipervisores VMWARE, Hyper-V y KVM.
    b. Virtual sobre nube pública: al menos en AWS y AZURE.
    c. Físico: appliance hardware proporcionados por el fabricante.
8. El Sistema contará con mecanismos que **eliminen el punto de fallo único**, soportando arquitecturas de tipo activo-pasivo, en las que la configuración y base de datos se sincronice periódicamente
    d. Estas deben estar disponible tanto para nodos conectados directamente en capa dos como para aquellos que están conectados por medio de una red de capa tres.
9. El sistema soportará despliegues **centralizados o distribuidos**:
    e. Centralizados: un único clúster de appliance NAC controla todos los dispositivos de red
    f. Distribuidos: un elemento central de control gestiona varios clústeres de appliance NAC situados en ubicaciones diferenciadas, que a su vez gestionan los dispositivos de red de su zona de influencia.
10. El elemento de control de las arquitecturas distribuidas estará disponible en diferentes modos de despliegue:
    g. Virtual sobre nube privada: soportando al menos los hipervisores VMWARE, Hyper-V y KVM.
    h. Virtual sobre nube pública: al menos en AWS y AZURE.
    i. Físico: appliance hardware proporcionados por el fabricante.
11. Los despliegues en modo virtual en AWS, ESX, Hyper-V y KVM deben soportar opciones de inicialización previa a levantar la imagen (*cloud-init*), que permitan al menos pasar la configuración de la IP y gateway por defecto de la interfaz utilizada para gestión.

12. La arquitectura distribuida debe permitir combinar clústeres de diferentes formatos de despliegue.
13. Debe de ser una **solución fuera de banda**, y **no deberá estar basada en replicación de tráfico**.
14. El licenciamiento debe de tener en cuenta sólo los dispositivos registrados en la red y online, no contando aquellos que no están registrados (por ejemplo, accediendo a través de wifis abiertas sobre las que no se ejerce control) o que no están online, aunque se mantenga la información en la BBDD's.
    j. En caso de solución distribuida, el licenciamiento de dispositivos debe poder ser **compartido** entre todos los clústeres de NAC distribuidos por el entorno.
15. La solución NAC debe ser totalmente escalable, permitiendo ampliar el despliegue inicial, bien apilando más licencias de dispositivos o añadiendo más clústeres, que puedan cubrir áreas específicas de la red, o zonas geográficas concretas.
16. La solución NAC debe permitir tanto modelos de licenciamiento basado en **licencias perpetuas como en subscripciones.**
17. Debe disponer de alguna opción que permita consumir una licencia por dispositivo, independientemente del número de tarjetas de red que tenga o del número de usuarios que se hayan logado a lo largo del tiempo.
18. El modelo de licenciamiento debe permitir incrementar la funcionalidad inicial sin tener que adquirir las licencias desde cero.
19. La solución NAC debe tener capacidad para inventariar todos los dispositivos de la red, incluyendo equipamiento que no sea PC, como impresoras, Smartphones (IPhone, Android y Windows Phone), teléfonos IP, cámaras y otros dispositivos IoT que pudieran existir.
20. Debe poder **utilizar al menos 21 métodos diferentes** para identificar el tipo de dispositivo. Algunos de estos métodos serán activos y otros pasivos:
    a. NMAP scan
    b. DHCP fingerprinting
    c. Interacción HTTP/HTTPS
    d. Rangos de IP
    e. Grupo de dispositivos de red en el que se ha detectado el nuevo endpoint bajo perfilado
    f. Passive TCP/IP stack fingerprinting con herramienta *p0f*
    g. Información obtenida a través de agentes.
    h. Peticiones RADIUS recibidas. Comprobación pares atributo-valor, soportando regex y wildcards.
    i. Consulta SNMP desde el NAC
    j. Conexión e interacción SSH
    k. Puerto o rango de puertos TCP abiertos
    l. Conexión e interacción Telnet
    m. Puerto o rango de puertos UDP abiertos
    n. Vendor OUI
    o. Petición WinRM

p. Perfil WMI

q. Trafico de red en firewall Fortigate o de otro equipamiento recibido mediante Netflow.

r. Tipo de dispositivo o sistema operativo detectado por firewall Fortigate

s. Perfil ONVIF

t. Búsqueda de MAC de dispositivos IoT en base de datos online mantenida por el fabricante, para identificar el tipo y familia del dispositivo

u. Interacción mediante scripts diseñados a medida lanzados desde el NAC.

21. Debe soportar el perfilado de dispositivos Windows pertenecientes al domino mediante WMI o WINRM, utilizando canales seguros y validados mediante certificado.
22. El usuario debe poder combinar todos los métodos de perfilado que desee para crear reglas de perfilado customizadas. Las reglas se analizarán de manera secuencial.
23. El administrador podrá asociar a cada dispositivo, en función del resultado del proceso al menos tres atributos o identificativos con los que luego poder hacer filtrados y para desplegar políticas de control de acceso.
24. Las reglas de perfilado permitirán registrar los dispositivos como válidos y autorizados de manera automática o dejarlo para una intervención manual posterior de un administrador o espónsor autorizado. Se debe poder enviar una notificar a los espónsores responsables ante cada dispositivo que cumple la regla de perfilado.
25. Una vez se ha perfilado un dispositivo, el sistema debe de ser capaz de comprobar, tanto en la conexión como periódicamente, que dicho dispositivo sigue cumpliendo con todos los requisitos definidos por el administrador, notificando e incluso aislando aquellos dispositivos que hayan cambiado.
26. Las reglas de perfilado permitirán seleccionar el intervalo del día y días de la semana en las que el dispositivo que cumple la regla de perfilado es registrado y autorizado para el acceso a la red.
27. Las reglas de perfilado deben poder ser ejecutadas de manera manual por un administrador para analizar todos los rogue devices que existan en un determinado momento bajo demanda.
28. Los dispositivos perfilados deben aparecer listados en una vista, sobre la que se puedan consultar los datos disponibles del dispositivo, realizar filtrados o añadir notas por parte de los administradores. La lista debe ser exportable en CSV, XLS, PDF o RTF.
29. Con tal de poder adaptarse lo máximo posible a las necesidades y diferentes casuísticas del Ayuntamiento de Mérida es necesario que se provean, sin necesidad de añadir módulos o licencias adicionales las siguientes opciones de registro:

    - **Registro automático por perfilado:** Una vez hecho el perfilado e identificado el tipo de dispositivos realizar un registro automático y asignación de un rol o perfil sobre el que se aplicarán posteriormente los diferentes métodos de control de acceso.
    - **Registro asistido por perfilado:** Una vez hecho el perfilado e identificado el tipo de dispositivos se envía una alerta a una cuenta de correo conforme se ha realizado un perfilado de un dispositivo nuevo. El sponsor podrá acceder a la web de gestión de dispositivos para confirmar el perfilado y realizar el registro.
    - **Registro mediante importación de fichero CSV:** será posible el pre-registro de dispositivos mediante la importación de un fichero CSV con los datos de dispositivos, usuario asociado (si lo

tuviese) y características de perfil o role. Se podrán importar también usuarios mediante este método.

- **Auto-registro mediante portal:** Los usuarios podrán disponer de la capacidad de registrar dispositivos a su nombre de forma autónoma introduciendo, la MAC y el tipo de dispositivos según desplegable. Este se registrará de forma automática y podrá ser usado por el usuario posteriormente. Para la validación del dispositivo registrado, se requerirá que este esté conectado a la red previamente. En dicho portal se deberán incluir las instrucciones y condiciones de uso. Una vez registrado el usuario podrá realizar gestión de sus dispositivos.
- **Auto-registro mediante API:** El NAC dispondrá de una API REST para poder realizar el registro desde otra aplicación o servicio web externo donde se permitan todas las capacidades y opciones de registro disponibles en los métodos anteriores
- **Auto-registro mediante la autenticación 802.1x:** Para los dispositivos validados por 802.1x se debe permitir el registro automático de dispositivos y asociación al usuario validado por 802.1x ya sea con el NAC como servidor RADIUS o haciendo de Proxy RADIUS.
- **Registro mediante agente persistente:** Los dispositivos con agente persistente registraran los nuevos dispositivos conectados de forma automática enviando toda la información relativa a SO, inventario de aplicaciones y usuario asociado. El agente detectará la movilidad del dispositivo notificando al NAC cada cambio de IP que se produzca.
- **Registro pasivo:** En el momento de login de LDAP el agente pasivo registrará el dispositivo la primera vez que se conecte a la red de forma totalmente transparente al usuario.
- **Registro manual:** se podrá seleccionar cualquier dispositivo desde la vista global de dispositivos y realizar un registro manual de dicho dispositivo, de manera que quede autorizado en el sistema con el rol correspondiente.

30. La solución debe permitir conectarse a la red corporativa solo a dispositivos autenticados/registrados, desplegando políticas de seguridad que bloqueen y aíslen dispositivos que no cumplan los criterios corporativos, enviándolos a un área de cuarentena sin necesidad de intervención por parte de los administradores de red.
31. Debe ser capaz de autorizar los accesos mediante asignación dinámica de VLAN's, aplicando ACLs o configuración CLI al puerto de acceso o pasando un grupo de acceso VPN al concentrador correspondiente.
32. Debe ser capaz de controlar escenarios en los que hay más de un equipo conectado a un puerto, asociando a cada equipo la VLAN adecuada, siempre que el equipo de acceso lo permita.
33. Debe ser capaz de integrarse con los firewalls para asociar los dispositivos a reglas de seguridad concretas de manera dinámica, en función del tipo de dispositivo.
34. Debe permitir extender las políticas de seguridad al acceso VPN, ya sea SSL en modo túnel o IPSEC a través de una política de seguridad consistente.
35. Debe soportar autenticación de máquina y usuarios, pudiendo autenticar un dispositivo final sin utilizar agentes.
36. Debe soportar opciones de autenticación flexibles, incluyendo 802.1X, autenticación web y autenticación MAC.
37. Debe soportar integración LDAP y Microsoft Active Directory, sin necesitar ningún componente adicional, para desplegar políticas en función de su pertenencia a ciertos grupos. Debe soportar la sincronización periódica de usuarios con el directorio.

Las reglas de acceso permitirán configurar lógicas AND y OR basadas en los siguientes campos:

a. Atributos disponibles sobre el host reconocido
b. Atributos RADIUS
c. Grupo al que pertenece el dispositivo que se conecta
d. Dispositivo de red, puerto, grupo de puertos o SSID al que se está intentando conectar el dispositivo
e. Intervalo de tiempo en el que sucede el intento de conexión

38. Se podrá controlar los puertos sobre los que queremos que se ejecuten las reglas de control de acceso, asignándolos a diferentes grupos de control.

5.7.10 RADIUS

El sistema propuesto contará con servicio RADIUS que pueda actuar como servidor local, como proxy hacia otros servidores RADIUS de la red o como ambas funciones al mismo tiempo.

El sistema podrá utilizar autenticación RADIUS para:

1. Autenticación de usuarios o dispositivos conectando a equipamiento compatible 802.1X
2. Autenticación de usuarios de VPN
3. Autenticación de usuarios en el portal cautivo disponible en el NAC
4. Autenticación de administradores del propio sistema NAC

5.7.11 PORTALES

La solución permitirá configurar uno o más portales cautivos a mostrar en cada una de las redes especiales de control: registro, remediación, autenticación, cuarentena, etc.

1. Permitirá crear políticas que permitan redirigir al dispositivo a una configuración de portal u otra en función del perfil de dispositivo.
2. Contará con un editor de contenido que permita modificar todas las secciones y contenido escrito de la página HTML (cabecera, pie, fondo, cuerpo, etc.) y de la hoja de estilo CSS. Se podrá visualizar una página de muestra mientras se edita el estilo CSS.
3. El sistema permitirá cargar imágenes al usuario, para ser utilizadas en las diferentes secciones del portal.
4. El código de las páginas creadas para cada uno de los portales podrá ser exportadas fuera del NAC.
5. El portal podrá facilitar la descarga de alguno de los agentes de endpoint disponibles.
6. El portal podrá validar usuarios contra la base de datos local, RADIUS y LDAP
7. Debe permitir el registro de usuarios integrado con redes sociales. Como mínimo con Facebook, LinkedIn, Google, Outlook, Twitter, Yahoo.
8. La solución podrá autenticar usuarios en el portal cautivo contra Azure AD utilizando OAuth.
9. La solución permitirá mostrar a los usuarios información útil como instrucciones a seguir, escaneos de agente fallidos, dispositivos registrados en el sistema a su nombre o política de uso aceptable.
10. Se podrá configurar un portal de acceso de tipo anónimo en el que sólo se requerirá al usuario que acepte una página de condiciones de uso de la red, antes de darle acceso sin necesidad de autenticarse.

Mediante las reglas de cumplimiento, el NAC realizará una serie de análisis automáticos en el endpoint, antes de dar acceso a la red:

1. La solución debe soportar inspección de los dispositivos mediante agente, disponibles al menos para Windows, Linux, MacOS y Android. Estos agentes podrán ser de cuatro tipos:
    a. Disoluble: se requiere al usuario la instalación de un agente que realiza un análisis completo del endpoint y que tras un resultado satisfactorio se elimina del sistema automáticamente.
    b. Pasivo: al menos en sistemas windows y no requerirá de la instalación de ningún ejecutable para realizar un análisis en segundo plano.
    c. Persistente: instalable por el usuario o distribuido mediante software de distribución, permanecerá en todo momento en el endpoint del usuario, comunicándose de manera regular con el NAC.
    d. Agente móvil: estará disponible al menos para Android en el marketplace de Google. Permitirá inspeccionar las aplicaciones instaladas en el endpoint y si el equipo ha sido rooteado.
2. El agente persistente permitirá al administrador del NAC enviar mensajes a los endpoints que lo tengan instalados, así como mostrará globos de información en la barra de tareas ante determinados eventos.
3. El agente persistente permitirá detectar dispositivos con múltiples interfaces de red, facilitando que el NAC las pueda agrupar bajo el mismo endpoint, conservando de esta manera licenciamiento de endpoint y detectando situaciones con multi-homing.
4. Los agentes podrán ser distribuidos por métodos empresariales de gestión de software o directamente desde un portal cautivo de registro.
5. La solución NAC debe ser capaz de realizar, al menos, las siguientes comprobaciones, que podrán ser dependientes del sistema operativo: service packs, nivel de parcheo, que haya instalado las actualizaciones críticas, antivirus y antiSpyware, servicios y procesos, procesos prohibidos, certificados, dominio, existencia de archivos, scripting o entradas y fechas del registro de Windows.
6. La solución debe proporcionar un rol de cuarenta que se pueda utilizar para interactuar con el endpoint que incumple y sistemas de parcheo. De esta manera, los dispositivos corporativos que no cumplan los requisitos serán enviados a un portal cautivo de “auto-remediación”, donde o bien se le proporcionan instrucciones para la remediación o se ejecuta la remediación automática a través de sistemas como BigFix y Parchlink.
7. En el portal de remediación se mostrará el motivo por el que el dispositivo ha cambiado a dicho estado y se darán instrucciones y acceso a los servicios de remediación necesarios (actualización de antivirus, actualización de Windows, etc.…)

La solución NAC debe poder comprobar el estado de actualización para los AV y AntiSpyware (tanto archivos .dat como el propio motor), al menos para los siguientes Antivirus: Avast, AVG, Avira, Blink, Bitdefender, Bullguard, CA, Carbon Black, Check Point End. Sec., Cisco-AMP, Comodo Antivirus, CrowdStrike Falcon, Cylance PROTECT, Deep Instinct, Emsisoft Anti-Malware, ESET, F-Secure, Faronics, FortiClient, GData, GFI, K7, Kaspersky, LANDesk, Lightspeed, MalwareBytes, McAfee, MS Security Essentials, MS Windows Defender, MicroWorld, N-able, Norton, Palo Alto Cortex/Traps, Panda, Quick-Heal, Windows Security-Center, SentinelOne, Softwin, Sophos, Symantec, Total-Defense, TotalAV, Trend-Micro, TrustPort, Vipre, Webroot, ZoneAlarm.

8. En caso de incumplimiento se podrá:
    a. Dar acceso a red, a la vez que se genera una alerta para los administradores responsables.
    b. Dar acceso a red marcando el equipo como “en riesgo”, a la vez que se notifica al usuario mediante una advertencia.
    c. Mover el dispositivo a una VLAN de aislamiento o de remediación.
9. En caso de remediación, esta podrá ser en diferido, marcando el dispositivo como “en riesgo” y permitiendo unos días de margen para solucionar la validación que ha fallado.
10. Los agentes instalados, permitirán al NAC forzar una renovación de IP de una interfaz o informarán al NAC de manera ágil ante un cambio de IP del dispositivo.
11. Los agentes de endpoint facilitarán la detección y/o compartición de adaptadores de red extraíbles entre diferentes hosts, impidiendo su utilización en hosts no registrados.
12. El agente de endpoint permitirá detectar la conexión de dispositivos de almacenamiento USB al endpoint, pudiendo generar un evento que desencadene una alarmar y con ello una acción del NAC.
13. El sistema contará con una vista de logs dedicada en la que se mostrarán los resultados de los escáneres efectuados por los agentes disponibles.
14. El agente de endpoint podrá enviar un listado de las aplicaciones instaladas en el endpoint, permitiendo de esta manera al NAC tener información de dispositivo, usuario, aplicaciones e incluso flujos de comunicaciones.

5.7.12 GESTIÓN DE INVITADOS

El Sistema de control de acceso debe proporcionar una plataforma flexible y eficiente de gestión de usuarios no corporativos, que permita manejar el acceso de aquellos usuarios con un acceso transitorio (típicamente invitados) o con un acceso más estable (contratistas externos).

1. Debe permitir definir perfiles limitados que solo tengan acceso a la gestión de cuentas de invitados ejerciendo como espónsor de estos.
    a. El usuario espónsor contará con una vista en el GUI desde la que podrá autorizar las peticiones pendientes.
2. Debe permitir altas masivas (p.e. para conferencias), auto-registros, registros esponsorizados o dados de alta por un administrador.
3. Las cuentas de usuario para conferencias podrán ser con usuario-contraseña individuales, usuarios independientes y contraseña compartida o usuarios y contraseña compartidos.
4. Se podrán importar en bloque cuentas de usuario invitados desde un fichero CSV, pudiendo importar también la contraseña.
5. Debe ser flexible y permitir la definición de diferentes perfiles, como invitados de corta /larga estancia, asistentes a conferencias o auto-registrados.
6. Se debe poder definir los campos de registro que se solicitarán a cada usuario auto-registrado, seleccionando aquellos campos que serán obligatorios.
7. De estar integrada con las políticas de acceso, otorgando niveles de acceso en función de los perfiles o roles asignados al invitado.

8. La gestión de invitados debe soportar notificación por SMS y correo electrónico, por ejemplo, para las credenciales de acceso.
9. Se deben de poder definir diferentes portales de registro, y presentar uno u otro en función de políticas definidas por el administrador. Por ejemplo, dependiendo de la hora del día, del lugar desde el que el usuario se conecte.
10. La gestión de invitados se integrará con el módulo de cumplimiento. De esta manera, un usuario externo será sometido a las políticas de cumplimiento mediante el uso de agentes disolubles, que no necesitarán permisos de administrador de la máquina para ejecutarse y dar un veredicto.
    b. En función del veredicto se podrá mover al usuario invitado a una VLAN de remediación con indicaciones sobre las verificaciones que ha fallado.
11. Se deben incluir diferentes métodos de validación y autenticación de usuarios invitados, contratistas o auto-registro: Local, LDAP o RADIUS.
12. Debe permitir la implementación de modo Kiosco para el auto registro de usuarios y la creación de cuentas, con validación de email o SMS
13. Los portales deben ser totalmente personalizables y adaptados a las necesidades del cliente, así como también todos los mensajes o SMS usados para el registro de usuarios.
14. Se debe poder mostrar una política de uso aceptable durante el registro del usuario.
15. El sistema debe permitir a un espónsor o administrador imprimir unas etiquetas con las credenciales asignadas a cada usuario.

5.8 SERVICIO DE ACCESO A INTERNET.

5.8.1 SITUACIÓN ACTUAL.

En la actualidad la Red Corporativa del Ayuntamiento de Mérida dispone de 2 accesos Macrolan de 1GB con un caudal principal garantizado de acceso a Internet de 300Mbps bidireccional- simétrico- proporcionado a través del acceso de fibra óptica instalado en el edificio de Palacio Municipal, y un caudal de backup garantizado de acceso a Internet de 300 Mbps bidireccional-simétrico- proporcionado a través del acceso de fibra óptica instalado en la sede de Urbanismo. Asociado a estos accesos se dispone de un rango de 16 IPs públicas (en dos rangos de 8 IPs) que permiten la publicación de diferentes contenidos y/o servicios en Internet. Dicho rango de IPs públicas es propiedad del operador que resultó adjudicatario del contrato vigente del Servicio de Telecomunicaciones.

Además, se disponen de accesos FTTH 600 Mbps y 4G instalados en diversas sedes, con el propósito de poder proporcionar acceso a Internet no corporativo cuando se celebran en dichas sedes determinados eventos (circunstanciales) o de forma permanente en el caso de sedes que no están integradas en la Red Corporativa.

En total son 47 accesos.

Aquella información no incluida en este apartado y que los oferentes consideren necesaria para la elaboración de la propuesta, podrán solicitarla, arbitrando el Ayuntamiento de Mérida la conveniencia o no de suministrar dicha información, los documentos de confidencialidad que deberá firmar el oferente y los medios para suministrarla (escrito, reunión, etc.).

5.8.1 SERVICIOS REQUERIDOS.

Se pretende mantener y mejorar la infraestructura y arquitectura del servicio de acceso a Internet implantado actualmente en todas las sedes de la Red Corporativa tanto para la navegación de los usuarios como para la presencia en Internet de los distintos servicios que este Ayuntamiento presta a sus usuarios y a la ciudadanía en general, debiendo proporcionar el adjudicatario los servicios que se detallan a continuación.

El adjudicatario proporcionará al Ayuntamiento de Mérida una gestión integral de estos servicios de acceso y presencia en Internet, debiendo asumir la gestión, operación y mantenimiento de toda la infraestructura necesaria para proveer los diferentes servicios e incluyendo todos los procesos y herramientas de gestión necesarias para realizar la administración completa de los mismos. Quedan incluidas todas las labores relacionadas con el suministro de equipamiento, configuración, puesta en marcha, mantenimiento y gestión del mismo y la prestación de ciertos servicios específicos de seguridad.

El adjudicatario o proveedor del servicio de acceso a Internet dispondrá de presencia en los principales puntos neutros nacionales e internacionales. La oferta presentada por cada oferente detallará:

- Los puntos neutros en los que el ofertante esté presente
- La capacidad de los enlaces de Backbone
- Los mecanismos de seguridad y redundancia propios del oferente
- La propiedad de la fibra por la que se presta el servicio que se oferta

Toda esta información será tenida en cuenta en el análisis de las ofertas.

ACCESO A INTERNET CORPORATIVO

El adjudicatario proporcionará como acceso principal a Internet para la Red Corporativa un caudal mínimo garantizado de 500Mbps bidireccional (simétrico) a través de un acceso de fibra óptica que se instalará en la Sede Palacio Edificio Principal y de 500Mbps de backup instalado en la sede Urbanismo. El licitador podrá mejorar este caudal en su oferta, lo cual será objeto de valoración adicional.

Tanto el acceso principal como el secundario estarán balanceados y en caso de caída de uno de ellos el otro permanecerá activo sin corte alguno en la comunicación.

ACCESO A INTERNET ALTERNATIVO

El adjudicatario proporcionará al menos un acceso FTTH de las sedes para poder disponer de accesos a internet no corporativos en las mismas cuando se celebren determinados eventos o ser utilizados en determinadas circunstancias desde el Servicio de Transformación Digital, valorándose como mejora el incremento sobre dicha cifra, de manera proporcional, hasta alcanzar el 100%. En el supuesto caso de imposibilidad de acceso FTTH en una sede, se instalará un acceso 4G o 5G. En ambos casos se instalarán con el caudal máximo proporcionado por la tecnología del acceso y en función de la ubicación de la sede.

DIRECCIONAMIENTO IP PUBLICO

El adjudicatario pondrá a disposición del Ayuntamiento de Mérida un rango de IPs públicas suficiente con la finalidad de posibilitar a este Ayuntamiento la publicación de diferentes contenidos y/o servicios en Internet. Cuando sea necesario, por incremento de servicios a los ciudadanos, y a criterio del Ayuntamiento, el licitador deberá de dotar las IPs adicionales a requerimiento del Ayuntamiento, para publicación de dichos servicios sin límite de IPs públicas y sin coste alguno. En la medida que ello fuera posible, este Ayuntamiento desearía mantener el direccionamiento IPs público que está siendo actualmente utilizado para tal fin.

CALIDAD DEL SERVICIO

El objetivo de los Acuerdos de Nivel de Servicio (ANS) es definir de una manera objetiva el nivel de calidad del servicio que se presta, utilizando variables objetivas que permitan al Ayuntamiento de verificar que el servicio que le presta el adjudicatario entra dentro del marco de contratación. Cualquier medida de calidad de servicio se llevará a cabo sobre períodos mensuales.

El oferente indicará, al menos, los siguientes parámetros y sus valores máximos:

- Tiempo de respuesta, entendiendo como tal el tiempo transcurrido desde la comunicación de la avería al adjudicatario y la respuesta por parte del técnico que tenga asignada la incidencia. El tiempo de respuesta será como máximo de 2 horas.

- Tiempo máximo de resolución de incomunicaciones, entendiendo como tal el intervalo de tiempo transcurrido desde la comunicación al adjudicatario de la falta de conexión con Internet hasta la resolución del problema. El percentil 90 de los tiempos de resolución de averías debe ser menor a 24 horas.

- Disponibilidad del servicio, es decir, el porcentaje de minutos mensuales que se encuentra operativo el caudal Internet contratado. No podrá ser inferior al 99,3 % mensual.

Estos valores mínimos pueden ser mejorados en la oferta, lo cual será tenido en cuenta en el estudio de la misma.

La valoración de la disponibilidad mensual se tendrá en cuenta desde el día 1 natural de cada mes hasta el último día de ese mes.

A efectos de cómputo de tiempo no serán tenidas en cuenta aquellas averías que no sean responsabilidad del adjudicatario. Tampoco las indisponibilidades que sean fruto de pruebas o paradas técnicas, siempre y cuando hayan sido advertidas con la suficiente antelación y autorizadas por el Ayuntamiento de Mérida si, según los casos, corresponde o es pertinente tal autorización.

En el caso de no cumplir los valores de ANS indicados anteriormente o los presentados en su oferta por el adjudicatario, se aplicará una penalización del 2% del coste mensual imputado al servicio de acceso a internet en la factura correspondiente al mes siguiente de producirse el incumplimiento.

5.9. CERTIFICADOS SSL WILDCARD

Suministro de certificado SSL WildCard para el dominio merida.es y sus subdominios.

Actualmente el Ayuntamiento tiene vigente los certificados correspondientes y finalizarán en noviembre de 2026, el adjudicatario deberá de suministrar lo siguiente a partir de noviembre de 2026.

Suministrar un certificado de tipo SSL WildCard para el dominio merida.es que nos permita instalarlos en los múltiples subdominios.

Se requiere:

• La emisión de un certificado SSL de tipo Wildcard con Organization Validation para el dominio indicado sin límites en subdominios.

• El certificado deberá tener un periodo de validez de un (1) año a partir de su fecha de emisión inicial.

• El certificado debe tener activa la extensión x509 “Certificate Transparency”.

• El certificado debe permitir la firma digital de 2048 bits y un cifrado de 256 bits.

- Con el propósito de garantizar el funcionamiento de todos los certificados sin necesidad de intervención alguna por parte de los empleados del Ayuntamiento de Mérida y de sus colaboradores, se exige que el certificado raíz de la entidad certificadora emisora del certificado esté presente por defecto en el almacén de certificados de los siguientes productos:
  - Sistema operativo Microsoft Windows Server 2012R2, 2016 y 2019.
  - Sistema operativo Microsoft Windows 7, 8.1, 10 y 11.
  - Sistema operativo MacOS
  - Navegadores Edge, Mozilla Firefox y Chrome para Windows.
  - Sistemas de iPhone y iPad
  - Sistema Android.
  - Distribuciones Linux Debian, Ubuntu y RedHat.

• No será admitido como válido ningún certificado que haya sido emitido por una entidad certificadora cuyo certificado raíz tenga que ser introducido de forma manual en alguno o varios de los almacenes de certificados mencionados.

Teniendo en cuenta que el Ayuntamiento de Mérida necesita flexibilidad, que la normativa de certificados electrónicos es cambiante, y las imposiciones del propio mercado de navegadores encabezado

por compañías multinacionales, durante el periodo de funcionamiento del contrato el adjudicatario se compromete a emitir de nuevo el certificado cuantas veces sea necesario para adaptarse a las necesidades cambiantes, ya sea en materia de validez del certificado y CN, u en otra materia. En todo caso, los certificados nunca serán válidos una vez superados al año desde su emisión inicial.

El adjudicatario deberá de disponer de canales de comunicación entre el Servicio de Transformación Digital del Ayuntamiento de Mérida y la autoridad de certificación emisora del certificado con el fin de hacer consultas, resolver incidencias, y solicitar una nueva emisión del certificado en caso de ser necesario. Los canales habilitados serán al menos vía web y vía correo electrónico. La autoridad de certificación emisora del certificado deberá disponer de una página web donde el Servicio de Transformación Digital del Ayuntamiento de Mérida podrá consultar en todo momento el estado de los certificados y su fecha de expiración. Los canales deberán estar disponibles durante todo el periodo de funcionamiento del contrato.

6. TELEFONÍA FIJA Y MÓVIL Y DE DATOS EN MOVILIDAD

Se integran en este apartado la contratación de los servicios de comunicaciones de voz y mensajería y de transmisión de datos en movilidad.

Siguiendo las tendencias actuales de mercado, se solicita a los licitadores que adecuen la facturación prevista al concepto de tarifa plana (voz, datos, roaming para móviles). Esta tarifa podrá ser diferente para las extensiones de la red fija y de la red móvil, en tanto que estas últimas podrán ser diferentes para las extensiones de la red fija y de la red móvil, en tanto que estas últimas incorporarán la posibilidad de acceso al servicio de transmisión de datos en movilidad.

6.1 TELEFONÍA FIJA.

6.1.1 SITUACIÓN ACTUAL

El Ayuntamiento de Mérida en la actualidad dispone de una solución on premise de Telefonía IP Mi Voice MX-One con terminales del mismo fabricante:

- 20 terminales de operadora.
- 100 terminales de gama alta.
- 357 terminales de gama media.

La arquitectura MX-One está desplegada en la sede de Ayuntamiento de Mérida, basada en servidores físicos.

El equipamiento es el siguiente:

- Servidor Mx-One: 3 tarjetas ASU-II.
- Servidor de red: 1 tarjeta ASU Lite.
- Media Gateway: MGU2 en chasis Lite de 3U.
- Extensiones analógicas: 1 tarjetas ELU34 para dar servicio a extensiones analógicas de emergencia.
- Líneas de emergencia: 1 tarjeta FTU2 para dar servicio a 8 líneas analógicas de emergencia.
- Líneas analógicas: 1 tarjeta TLU83 para dar servicio a través de centralita a 8 líneas analógicas de emergencia.
- Servidor MiCollab: 1 tarjeta ASU-II.
- Terminales SIP: 380 terminales Mitel 6865i y 100 terminales Mitel 6940.

Aquella información no incluida en este apartado y que los oferentes consideren necesaria para la elaboración de la propuesta, podrán solicitarla por escrito al Ayuntamiento de Mérida, arbitrando los documentos de confidencialidad a firmar por el oferente y la información y medios a suministrarla.

6.1.2 SERVICIOS REQUERIDOS

El Ayuntamiento de Mérida desea mantener la Plataforma de Telefonía IP existente para las 480 extensiones que le permita configurar los diversos servicios, además de los que ya dispone, y que supongan un valor añadido a lo actual.

La solución propuesta por el licitador deberá cubrir todas las necesidades de comunicaciones de voz corporativa y de red del Ayuntamiento de Mérida.

Se requiere una ampliación del 10% del alcance inicial (mejora del límite en el consumo de voz, líneas RTB, FTTH, extensiones, terminales etc..), proporcionándose esta ampliación en incremento de facturación asumida por el adjudicatario. Se valorará adicionalmente la mejora sobre dicha ampliación de consumo.

CONEXIÓN A RED PÚBLICA

Se ha de disponer de una capacidad mínima de 90 canales bidireccionales simultáneos que serán proporcionados mediante tecnología NGN. Partiendo de dicho mínimo se dotarán los canales necesarios para el correcto funcionamiento del servicio, evitando pérdida del mismo o de llamadas individuales.

Los canales han de poder hacer enrutamiento automático de llamadas, balanceo automático de carga, señalización del número llamante y acceso a números de emergencia.

Además, se debe seguir disponiendo de las líneas y servicios:

- RTB (Policía Local y 092).
- 90X.
- EMERGENCIAS.
- Numeraciones de Extensiones.
- Faxes.
- Ascensores.
- Seguridad.
- Etc.

SERVICIOS DE LLAMADAS A RED PÚBLICA

El servicio deberá permitir cursar los siguientes tipos de llamadas desde cualquiera de las dependencias del Ayuntamiento de Mérida:

- Tráfico metropolitano.
- Tráfico provincial.
- Tráfico interprovincial o nacional.
- Tráfico internacional según destinos.
- Tráfico a móvil.
- Servicios de inteligencia de red.
- Llamadas en grupo cerrado de usuarios.
- Otras llamadas.

El adjudicatario deberá asumir dentro del contrato todos los servicios contratados actualmente sobre las líneas objeto del contrato (servicios contestador, desvíos de llamadas, llamada en espera, etc.) y deberá hacer las gestiones necesarias para dar de baja dichos servicios ante el operador que actualmente los ofrece, todo ello sin modificaciones en los servicios ni costes añadidos.

SERVICIO BÁSICO DE TELEFONÍA

El servicio deberá disponer, de forma general, de las máximas funcionalidades permitidas por la tecnología actual, debiéndose incluir en este apartado las siguientes modalidades de línea:

- Líneas analógicas para voz, faxes, ascensores, sistemas de seguridad (alarmas), etc.
- Fax IP para toda la telefonía VoIP.
- Líneas 90X con sus funcionalidades.
- Servicios de valor añadido disponibles para tipo de línea.
- Servicios que posibiliten analizar la información de consumo, tráfico y destino, por extensión, en formato papel y electrónico, para poder realizar estudios e informes de la evolución del tráfico.
- Todas las líneas contarán con un sistema de gestión y tarificación que tendrá la posibilidad de tratar y analizar la información de consumo, de tráfico y destino, por extensión, en formato papel y electrónico, para poder realizar estudios e informes de la evolución del tráfico cursado.

PLAN DE NUMERACIÓN PÚBLICO

Se requiere como mínimo el mantenimiento del plan de numeración público existente y se garantizará la conservación de la numeración actualmente asignada, llevándose a cabo, sin coste adicional y a cargo del adjudicatario, la adecuada portabilidad numérica, en caso necesario.

El Ayuntamiento de Mérida dispone de 130 números de marcación directa entrante/saliente (DDIs).

La solución planteada deberá asegurar que en el caso de desvíos de llamadas el número entrante original progrese y sea identificado correctamente en el destino.

El adjudicatario deberá pertenecer a la entidad de referencia de portabilidad y garantizará que la numeración propuesta para este apartado sea portable a la finalización del presente contrato.

PROVISIÓN DE SERVICIOS

El Ayuntamiento de Mérida considera crítico el servicio de telefonía IP fija de la que dispone la propia entidad municipal y a la ciudadanía en general. Por esta razón, el operador debe garantizar los mínimos plazos de provisión para cada uno de los servicios ofertados. Estos plazos de provisión afectan a nuevas necesidades que se contemplen durante el periodo de vigencia del contrato, así como a modificaciones en la prestación de cualquiera de los servicios iniciales. El operador adjudicatario deberá realizar todas las tareas necesarias para cumplir con los plazos exigidos.

Se considera tiempo de provisión el periodo que transcurre desde que el Ayuntamiento de Mérida solicita un nuevo servicio o un cambio sobre uno existente y el momento en que el servicio está operativo en las condiciones solicitadas.

El tiempo de provisión se medirá en días hábiles, no computándose como tal las fiestas nacionales, fiestas de ámbito regional en la Comunidad Autónoma de Extremadura, y fiestas locales.

RESPUESTA Y RESOLUCIÓN DE AVERÍAS

Como indicábamos en el punto anterior, el Ayuntamiento de Mérida considera crítico el servicio de telefonía IP fija ofrecido tanto al propio ayuntamiento y a la ciudadanía en general. Por esta razón en caso de averías en los servicios de telefonía fija, el adjudicatario del servicio deberá garantizar los mínimos plazos posibles de respuesta y resolución de las mismas, debiéndose comprometer a mantener los siguientes niveles de calidad en la respuesta y resolución de averías:

- Tiempo máximo de respuesta: 1 hora.
- Tiempo máximo de resolución de averías, en función de la severidad de las mismas: 4 horas.
- Tiempo máximo de envío de mensaje de resolución de avería: 2 días laborables.

Las penalizaciones a aplicar por el incumplimiento de las condiciones señaladas anteriormente serán las siguientes:

- Cuando a lo largo de un mes natural se produzca un incumplimiento de los tiempos comprometidos (tiempo máximo de respuesta ante averías y/o tiempo máximo de resolución de averías) en los trámites del protocolo de notificación/resolución de averías en un 10% de los casos, se penalizará con el 1% de la facturación mensual.
- A partir de dicho 10% la penalización se incrementará en otro 1% por cada 1% adicional de incremento sobre el 10% inicial.
- Se establece como límite máximo de penalización, por este concepto, el 50% de la facturación mensual.
- El retraso en la entrega de los informes de resolución de avería conllevará la aplicación de una penalización del 1% de la facturación mensual del servicio afectado, que se incrementará en un 1% más por cada día de retraso adicional hasta un máximo de un 10%.

OTROS NIVELES DE CALIDAD

Para los servicios de telefonía fija, el adjudicatario del servicio se deberá comprometer a mantener los siguientes niveles de calidad, como mínimo:

- Porcentaje de llamadas fallidas: inferiores al 1%.
- Tiempo de establecimiento de llamadas:
- A fijos: inferior a 2 segundos.
- A móviles: inferior a 6 segundos.
- Tasa global de llamadas con tarificación incorrecta menor o igual al 0,001%.
- Cualquier otro parámetro incluido en la normativa nacional e internacional que sea de aplicación deberá ser incluido siempre que el Ayuntamiento de Mérida, como organismo contratante, esté de acuerdo y los resultados de su aplicación sean en beneficio del referido organismo contratante.

MIGRACIÓN

En los servicios de telefonía fija, actualmente implantados y cuando exista cambio de operador, los licitadores deberán especificar en sus propuestas el procedimiento de portabilidad numérica, que tendrá que coincidir con el cambio de red al objeto de minimizar el tiempo de indisponibilidad. Dicho tiempo de indisponibilidad no superará en ningún caso las 24 horas y la portabilidad deberá ser realizada en horario nocturno y fin de semana.

El calendario del plan de migración tendrá que incluir la ejecución de las actividades necesarias fuera del horario de actividad habitual de cada sede.

En cuanto al cambio de infraestructura se procederá de la misma forma, minimizando siempre al máximo el tiempo de indisponibilidad y fuera del horario de actividad habitual de la sede.

El plan de migración incluirá un procedimiento con el detalle de las actividades a realizar, los requerimientos estimados, el equipo de trabajo que intervendrá, el tiempo previsto para la finalización de los trabajos y el tiempo máximo previsto de indisponibilidad.

En caso de alta de nuevas líneas por la red, el operador adjudicatario asumirá el coste de la publicitación de los nuevos números de teléfono en todos aquellos medios de fácil acceso para los usuarios.

En cuanto a las líneas existentes, tal y como se indicaba con anterioridad en el apartado.

"Plan de numeración público", se requiere la conservación de la numeración pública actualmente asignada, de tal modo que los licitadores deberán proporcionar la facilidad de portabilidad numérica en caso de cambio de operador.

6.2 TELEFONÍA MÓVIL Y DE DATOS EN MOVILIDAD.

Se incluye en este apartado la prestación de los servicios de telefonía móvil y transmisión de datos móviles. El objetivo de estos servicios es dotar los usuarios designados por el Ayuntamiento de Mérida de un "Servicio de Telefonía Móvil" que constituya una extensión móvil de la Red Corporativa Multiservicio, dotando a aquellos usuarios que lo necesiten de servicios de transmisión de datos en movilidad.

Dentro de este Pliego se incluye el tráfico con origen fijo y destino móvil desde cualquiera de los puntos de red del Ayuntamiento de Mérida y que el adjudicatario deberá considerar como tráfico con origen y destino móviles, debiendo dotar para ello del equipamiento necesario a la red de voz fija del Ayuntamiento de Mérida.

Se requiere una ampliación del 10% del alcance inicial (mejora del límite en el consumo de voz, datos, etc.), proporcionándose esta ampliación en incremento de facturación asumida por el adjudicatario. Se valorará el incremento sobre dicha ampliación. Se valorará el incremento sobre dicho alcance.

6.2.1 SITUACIÓN ACTUAL

El "Servicio de Telefonía Móvil" en el Ayuntamiento de Mérida se presta actualmente mediante un "Acceso Único IP" (AUIP) como conexión a NGN (siglas de "Next Generation Networking", en castellano "Redes de Próxima Generación") que simula la capacidad de comunicación de "Accesos de Voz Pública Móvil" a través de la tecnología IP con 50 canales.

El operador actualmente adjudicatario del servicio proporciona compromiso de cobertura de conexión a su red móvil dentro del interior de todos los edificios y/o sedes del Ayuntamiento de Mérida.

Se dispone asimismo de accesos primarios y básicos conectados a la red fija tradicional como solución de backup en caso de no estar operativa la conexión a NGN.

El parque actual consta de 203 líneas móviles con acceso a los servicios de voz y datos, 123 líneas tienen asociados terminales móviles, y 80 líneas sin terminal y con acceso a solo datos para dispositivos especiales o sensores.

En función de la tarifa asociada a cada una de las líneas móviles, se realiza el control del consumo y restricciones del tráfico generado desde cada línea móvil.

En lo referente al parque actual de dispositivos o terminales, está constituido por los siguientes tipos:

- 10 tablets sistema Android

- 48 terminales de gama vip/alta.
- 65 terminales de gama media-baja.

PLAN DE NUMERACIÓN PRIVADO

El plan de numeración privado del Ayuntamiento de Mérida para las extensiones móviles corporativas está compuesto por extensiones con numeración de 4 dígitos comenzando con el 5,6 o 7 (5xxx, 6xxx, 7xxx). A efectos de facturación se considera indiferente la marcación a una línea móvil corporativa de forma abreviada (extensión privada) o usando el número asignado en la red pública móvil.

VOLUMETRIA

Se detallan en Anexo.

6.2.2 SERVICIOS Y EQUIPAMIENTO REQUERIDOS

El Ayuntamiento de Mérida desea seguir disponiendo de un servicio de telefonía móvil de calidad y convergente con el servicio de telefonía fija. Los servicios de comunicaciones móviles deberán estar soportados por estaciones bases con tecnología digital de última generación que satisfagan las recomendaciones y normativas internacionales, siendo el proveedor responsable del diseño de la arquitectura de red que soportará el servicio. El adjudicatario del servicio proporcionará compromiso de cobertura de conexión a su red móvil dentro del interior de todos los edificios y/o sedes del Ayuntamiento de Mérida.

Los servicios de comunicaciones móviles ofertados deberán cumplir las características siguientes:

- Partiendo del mínimo actual de 50 canales se dotarán de los canales necesarios para el correcto funcionamiento del servicio, evitando la pérdida de llamadas y la indisponibilidad completa del servicio.
- Garantizarán como mínimo las volumetrías de llamadas y servicios de datos descritos con anterioridad, permitiendo compensaciones en la facturación anual entre los distintos tipos de tráfico.

- Sobre la volumetría que se recoge en este PPT se requiere una ampliación anual de, al menos, un 20% del alcance actual en cuanto al tráfico de datos. Esa ampliación debe ser tomada en cuenta a la hora del cálculo del importe de la tarifa plana ofrecida por los licitadores.
- Se desea disponer de, al menos, 10 MIFI y 150 líneas móviles, todas ellas con acceso a servicios de voz y datos UE, con tarifa plana y que podrá tener un crecimiento sostenido anual de un 10% sobre el total de líneas. Los licitadores podrán mejorar este número mínimo de líneas móviles en su oferta, lo cual será tenido en cuenta en el estudio de la misma.
- El licitador incluirá en su oferta, como mínimo, dos tarifas de datos:
    - 40% con 25 GB de datos.
    - 60% con 5 GB de datos.
- Los licitadores podrán mejorar el umbral de tráfico de datos máximo sin coste adicional asociado a cada tipo de tarifa incluida en su oferta, lo cual será tenido en cuenta en el estudio de la misma.
- El servicio de telefonía móvil ofertado permitirá la tarificación detallada por cada dispositivo o terminal, siendo capaz de proporcionar informes y estadísticas agregadas según los criterios que se pudieran definir.
- El servicio de telefonía móvil estará dotado de un sistema de gestión que permita obtener toda la información necesaria para la administración de las restricciones, el tráfico generado mensualmente, la posibilidad de tarificación mediante agrupaciones, y la monitorización del "Servicio de Telefonía Móvil Corporativo".
- El proveedor del servicio deberá proporcionar, instalar, operar y mantener todo el equipamiento necesario, así como todos los elementos accesorios y obra civil requerida hasta las dependencias del Ayuntamiento de Mérida para la prestación del servicio aquí definido.

PROVISIÓN DE TERMINALES

El adjudicatario deberá suministrar los dispositivos o terminales móviles cumpliendo las siguientes condiciones:

- Se renovará un 50% de los dispositivos o terminales móviles al inicio del contrato.
- Se renovará un 25% de los dispositivos o terminales móviles al final de cada año de vigencia del contrato.
- Las renovaciones anuales si no se hacen al principio o final de año podrán hacerse a lo largo del mismo.
- Los terminales no renovados, según los porcentajes en cada año, se podrán acumular a los años siguientes.

- El parque de dispositivos o terminales móviles integrantes del "Servicio de Telefonía Móvil Corporativo" del Ayuntamiento de Mérida estará constituido por tres tipos de terminales con la siguiente proporción:

  - 20% dispositivos o terminales de gama alta.
  - 80% dispositivos o terminales de gama media.

- Los dispositivos o terminales móviles de gama alta tendrán asociada la tarifa más alta de datos. Los dispositivos o terminales móviles de gama media tendrán asociada la tarifa inferior de datos.
- Tendrán la consideración de dispositivos o terminales móviles los smartphones y tabletas digitales de gama alta con acceso a datos. Los licitadores, en su oferta, podrán incluir dentro de este apartado ordenadores portátiles, lo cual será tenido en cuenta en el estudio de su oferta.
- Se incluirá un stock del 5% de dispositivos o terminales adicionales de cada gama.
- Como mínimo, todos los dispositivos o terminales móviles de gama alta suministrados permitirán la utilización de múltiple SIM.

Asimismo, en las ofertas presentadas por los licitadores se deberá especificar:

- Las características generales de los dispositivos o terminales móviles distribuidos por gamas (alta y media) detallando como mínimo: marca y modelo, especificaciones, dimensiones del terminal, peso, fotografía del terminal, batería (autonomía en llamadas, autonomía en modo espera o stand-by, tiempo de recarga), etc.
- Tipo de tecnología: WIFI, GSM, GPRS, UMTS, HSDPA, 4G, 5G, etc

REPARACIÓN DE TERMINALES

El adjudicatario deberá facilitar un sistema para dispositivos y/o terminales móviles que sufran averías, sin coste adicional para el Ayuntamiento de Mérida, de retirada, reparación y reposición, para los no obsoletos, o cambio para los obsoletos.

El plazo máximo de reparación o renovación de un dispositivo o terminal móvil no deberá superar los 15 días.

PROVISIÓN DE TARJETAS SIM SIN TERMINAL

El adjudicatario deberá facilitar tarjetas SIM M2M para ser utilizadas por dispositivos que requieran únicamente conexión a internet, ya sea en movilidad (por ejemplo, equipos de control de flotas, paradas para bicicletas públicas, control de alumbrado) o en instalaciones fijas (por ejemplo, equipos de telemedida), etc.

Además de mantener las tarjetas ya existentes, el adjudicatario deberá aprovisionar un número inicial de 100 unidades adicionales y que tendrán un crecimiento sostenido anual del 20% sobre el total de tarjetas durante el periodo de vigencia del contrato, para dar respuesta a nuevos proyectos del Ayuntamiento de Mérida.

Dichas líneas deberán estar adscritas al servicio de datos IoT con conectividad gestionada M2M (acrónimo de “Machine to Machine”, en castellano “Máquina a máquina”), estimándose un volumen global de tráfico mensual entre 100 Mb a 10Gb.

Se requiere un control y gestión inteligente de estas líneas (activación, desactivación y asignación de condiciones específicas a las líneas), sobre el tipo de tráfico, funcionamiento, localización y gasto (por medio de alertas) desde cualquier lugar y en tiempo real.

La gestión y control administrativo de estas líneas permitirá:

- Visualización global o selectiva de las líneas.
- Monitorización del tipo y volumen del tráfico y el consumo en tiempo real.
- Agrupación de líneas según distintos parámetros.
- Asignación de líneas a determinados grupos de facturación.
- Selección de condiciones de funcionamiento (zona geográfica, redes de comunicaciones).

La supervisión técnica de estas líneas posibilitará:

- Disponer de mapa de los dispositivos conectados en cada momento.
- Información sobre el estado de las líneas, con la posibilidad de realizar la conexión o desconexión en remoto.
- Diagnóstico avanzado de la operatividad y tráfico.
- Notificaciones de fallos en la conectividad.

Se deberán proporcionar los siguientes servicios asociados a las SIM:

- Gestión de Inventario.
- Gestión del ciclo de vida de las SIM.
- Consumo y facturación.
- Perfiles de usuarios.
- Alarmas.
- Informes.
- APIs.
- Atención y soporte comercial.

El suministro de este tipo de tarjeta SIM no representará coste alguno ni contará con cuota mensual, y el tráfico generado será añadido a la volumetría prevista.

COBERTURA

El operador deberá ofrecer los mapas actualizados de cobertura con tecnologías GSM, GPRS, UMTS, 4G, etc., en el territorio nacional español con especial detalle en las provincias de Cáceres y Mérida. El operador debe garantizar la cobertura completa para todos sus servicios en todos los centros, edificios y sedes del Ayuntamiento de Mérida.

Asimismo, el operador deberá detallar los acuerdos de roaming establecido con otros operadores en el ámbito internacional y aplicarlos a la baja en cuanto se produzca alguna modificación en este sentido.

SERVICIOS CORPORATIVOS DE VOZ. INTEGRACIÓN RED CORPORATIVA

VOZ MÓVIL.

Los servicios de voz fija y móvil deberán constituir una única "Red Corporativa de Voz" siendo responsabilidad del adjudicatario proveer el número de enlaces de voz necesarios para el "Servicio de Telefonía Móvil Corporativo" en el tiempo estipulado.

Se requiere mantener el "Servicio de Telefonía Móvil Corporativo" que actualmente se está prestando al Ayuntamiento de Mérida, de manera que las líneas móviles sigan siendo extensiones móviles de la red de voz. El adjudicatario de este servicio deberá mantener integradas las extensiones fijas correspondientes al "Servicio de Telefonía Fija" con las líneas móviles mediante la dotación de los canales necesarios.

PLAN DE NUMERACIÓN

Se requiere mantener el plan de numeración privado del Ayuntamiento de Mérida actualmente implantado para las extensiones móviles corporativas que está compuesto por extensiones con numeración de 4 dígitos comenzando con el 5,6 o 7 (5xxx, 6xxx,7xxx). A efectos de facturación se considera indiferente la marcación a una línea móvil corporativa de forma abreviada (extensión privada) o usando el número asignado en la red pública móvil. El adjudicatario deberá mantener la numeración de todas las líneas móviles existentes en el Ayuntamiento de Mérida y la de sus respectivas extensiones móviles.

FUNCIONALIDADES DEL SERVICIO

El Servicio de Telefonía Móvil Corporativo deberá ofrecer una serie de facilidades adicionales que se detallan a continuación:

Marcación y presentación de número.

La marcación a números externos a la "Red Corporativa de Voz" se realizará tal y como se hace desde cualquier línea fija o móvil no integrada en dicha red. Las extensiones fijas o móviles internas podrán ser marcadas usando el número asignado en la red pública o mediante marcación abreviada. En ambos casos, a efectos de tarificación, la llamada se considerará de la misma forma. La presentación del número llamante será diferente en función del origen y destino de la llamada. Si el llamante es una extensión fija o móvil y el destino también es una extensión fija o móvil, se presentará a éste último el número abreviado. La llamada a este número debe permitir el establecimiento de comunicación entre ambos. Si el llamante es una extensión fija o móvil y el destino es una línea externa, se presentará a este último el número asignado en la red pública. La llamada a este número debe permitir el establecimiento de comunicación entre ambos.

Restricciones por línea

Deberá ofrecer la posibilidad de restricción en cada una de las líneas en función de diferentes facilidades:

- Destino de llamada: Al menos debe proporcionar niveles de restricción entre llamadas corporativas, nacionales o internacionales, servicios de tarificación adicional, etc.

- Roaming: Se debe ofrecer la capacidad de activación o desactivación del servicio de telefonía móvil fuera del territorio nacional español.
- Listas Negras: Se debe ofrecer la capacidad de restricción de llamadas en exclusiva a una lista de números prefijados o agrupación de números en función de su numeración.
- Listas Blancas: Se debe ofrecer la capacidad de permiso de llamadas en exclusiva a una lista de números prefijados o agrupación de números en función de su numeración.
- Restricción de ser llamado en el extranjero sólo por los miembros de un grupo.
- Horario: Se debe posibilitar la activación o restricción del servicio en función de un horario determinado.

Se considera necesario que estas restricciones puedan ser gestionadas directamente por el Ayuntamiento de Mérida a través de una aplicación web y un "Servicio de Atención Telefónica" dedicado.

Control de consumo

Al objeto de racionalizar los recursos se debe permitir el establecimiento de controles de consumo por línea o grupo de líneas. Ofrecerá la posibilidad de establecer diferentes grados de restricciones sobre el uso del terminal móvil, incluyendo:

- Llamadas nacionales, internacionales, servicios de tarificación adicional, etc.
- Roaming.
- Consumo de datos.
- Restricción de llamadas a una serie de números predefinidos.
- Restricción de llamadas según horario.
- Buzón de voz.
- Servicio de llamadas perdidas.
- Marcación abreviada, posibilitando a los usuarios marcar un número menor de dígitos para aquellos números externos a la RPV más usados.
- Facilidades generales de activación / desactivación de opciones de llamadas: Identificación de la línea llamante, ocultación de la identidad de la línea, llamada en espera, desvíos de llamada, etc.
- Control de consumo por extensión y facturación detallada.
- Definición de límites de consumo por tiempo y por importe.

Otras funcionalidades

- Definición y creación de grupos de usuarios. Se permitirá crear agrupaciones de usuarios con una determinada configuración del servicio (restricciones, límites de consumo, etc.).
- Multillamadas.
- Facilidad de integración de dos líneas diferentes, con números telefónicos diferentes integrados en una única tarjeta SIM para posibilitar el uso del móvil en los ámbitos laboral y personal, pudiéndose obtener la facturación separada por ambos números.
- Facilidad de provisión de una segunda tarjeta SIM con la misma numeración que la línea principal, con el fin de poder realizar y recibir llamadas en un segundo terminal.
- Facilidad de agregación de un segundo teléfono fijo o móvil, perteneciente al Ayuntamiento de Mérida, a la línea de telefonía móvil, de forma que las llamadas dirigidas a la línea puedan recibirse en ambos destinos.

Facilidades asociadas a las extensiones

El "Servicio de Telefonía Móvil Corporativo" deberá incluir, como mínimo, las siguientes facilidades asociadas a las extensiones fijas y móviles:

- Transferencia de llamadas activas entre extensiones corporativas.
- Aviso de disponibilidad cuando una extensión corporativa deja de estar ocupada.
- Grupo de salto entre extensiones corporativas: Esta facilidad deberá poder ser gestionada en línea por el Ayuntamiento de Mérida.

Facilidades asociadas a las tarjetas SIM

Se considera necesario disponer de, como mínimo, las siguientes facilidades asociadas a tarjetas SIM especiales:

- Tarjetas con capacidad de incluir un número personal además del número corporativo asignado por el Ayuntamiento de Mérida (tarjeta DUAL).

- Tarjetas con capacidad de compartir una misma línea móvil, con la posibilidad de aviso de llamada entrante simultánea a las diferentes tarjetas SIM (tarjeta MultiSIM).

Facilidades asociadas al buzón de voz

Se considera necesario que todas las líneas móviles corporativas tengan la posibilidad de utilizar un servicio de Buzón de Voz asociado sin coste adicional. Se valorará la inclusión de, al menos, las siguientes facilidades:

- Notificación mediante SMS de la existencia de un nuevo mensaje indicando el número origen del mismo.
- Configuración en línea de las características del buzón de voz.
- Activación y desactivación mediante código de marcación.

Neutralidad

La red del operador adjudicatario se comportará de manera transparente, no pudiendo limitar o bloquear tipos de tráfico en función de su tipo. En el caso de que se detecten comportamientos anormales o ilegales, esta situación deberá ser puesta en conocimiento del Ayuntamiento de Mérida.

SERVICIO DE MENSAJERÍA

El "Servicio de Telefonía Móvil Corporativo" deberá ofrecer las funcionalidades que se indican a continuación, relacionadas con la mensajería.

Mensajes de texto SMS

Se requiere, al menos, mantener este servicio tal y como está actualmente implantado en el "Servicio de Telefonía Móvil Corporativo" del Ayuntamiento de Mérida, de manera que las líneas móviles dispongan de capacidad de envío de mensajes de texto SMS, junto a la posibilidad de envío desde aplicaciones accesibles desde la red de comunicaciones del Ayuntamiento de Mérida. El operador adjudicatario de este servicio debe proporcionar los mecanismos adecuados para las funciones que se describen a continuación, posibilitando que el Ayuntamiento de Mérida establezca las políticas de control adecuadas para cada función:

- Múltiples destinatarios. Se debe permitir el envío de mensajes cuyo destino sea una lista de números, tanto pertenecientes a la red pública como a la numeración privada.
- Envío mediante aplicación web. El operador deberá proveer los mecanismos necesarios para permitir el envío de SMS al menos a las líneas móviles corporativas usando una aplicación accesible vía web.

Mensajes multimedia MMS.

Se requiere, al menos, mantener este servicio tal y como está implantado en el actual "Servicio de Telefonía Móvil Corporativo" del Ayuntamiento de Mérida, de manera que en las líneas móviles que el Ayuntamiento de Mérida considere adecuado dotar de dispositivos o terminales móviles con esta facilidad, dispongan de la capacidad de envío de mensajes multimedia MMS, junto a la posibilidad de envío desde aplicaciones accesibles desde la red de comunicaciones del Ayuntamiento de Mérida.

6.3 CALIDAD DE SERVICIO.

Los licitadores deberán incluir en sus ofertas, como mínimo, lo que se indica en los siguientes apartados.

PLAZOS DE PROVISIÓN EN TELEFONÍA FIJA.

El adjudicatario debe garantizar los mínimos plazos de provisión para cada uno de los servicios ofertados relacionados con la telefonía fija. Estos plazos de provisión afectan a nuevas necesidades que se contemplen durante el periodo de vigencia del contrato, así como a modificaciones en la prestación de cualquiera de los servicios iniciales. El operador adjudicatario deberá realizar todas las tareas necesarias para cumplir con los plazos exigidos.

Se considera tiempo de provisión el periodo que transcurre desde que el Ayuntamiento de Mérida solicita un nuevo servicio o un cambio sobre uno existente y el momento en que el servicio está operativo en las condiciones solicitadas.

El tiempo de provisión se medirá en días hábiles, no computándose como tal las fiestas nacionales, fiestas de ámbito regional en la Comunidad Autónoma de Extremadura, y fiestas locales de la localidad.

Concepto	Plazo de provisión (máximo)
Nueva sede	25 días
Cambio de configuración que conlleve cambios en el equipamiento	10 días
Cambios de configuración de enlaces o asignación de numeración	2 días
Cambio de dimensionamiento de enlaces	2 días
RTB nueva línea	5 días
RTB cambio características línea existente	4 días
Informes estadisticos	4 días

En el caso de no cumplir los plazos de provisión indicados, se aplicará una penalización del 2% del coste del servicio en la factura correspondiente al mes siguiente de producirse el incumplimiento.

PLAZOS DE PROVISIÓN EN TELEFONÍA MÓVIL.

El adjudicatario deberá comprometerse a cumplir los tiempos de provisión especificados en la tabla siguiente. En el caso de producirse retraso en la provisión de los servicios solicitados, se aplicará una penalización del 2% del coste del servicio en la factura correspondiente al mes siguiente de producirse el incumplimiento.

Concepto de provisión	Acuse de recibo	Tiempo de respuesta
Altas y Bajas de Tarjetas	2 horas	24 horas
Segunda tarjeta de la misma línea	2 horas	12 horas
Envío de nuevos dispositivos o terminales	2 horas	48 horas

RESPUESTA Y RESOLUCIÓN DE AVERÍAS EN TELEFONÍA MOVIL

El adjudicatario del servicio deberá garantizar, ante averías producidas en los servicios de telefonía fija, los mínimos plazos posibles de respuesta y resolución de las mismas, debiéndose comprometer a mantener los siguientes niveles de calidad en la respuesta y resolución de averías:

- Tiempo máximo de respuesta: 1 hora.
- Tiempo máximo de resolución de averías, en función de la severidad de las mismas: 4 horas.
- Tiempo máximo de envío de mensaje de resolución de avería: 2 días laborables.
- Las penalizaciones a aplicar por el incumplimiento de las condiciones señaladas anteriormente serán las siguientes:
- Cuando a lo largo de un mes natural se produzca un incumplimiento de los tiempos comprometidos (tiempo máximo de respuesta ante averías y/o tiempo máximo de resolución de averías) en los trámites del protocolo de notificación/resolución de averías en un 10% de los casos, se penalizará con el 1% de la facturación mensual.
- A partir de dicho 10% la penalización se incrementará en otro 1% por cada 1% adicional de incremento sobre el 10% inicial.
- Se establece como límite máximo de penalización, por este concepto, el 50% de la facturación mensual.
- El retraso en la entrega de los informes de resolución de avería conllevará la aplicación de una penalización del 1% de la facturación mensual del servicio afectado, que se incrementará en un 1% más por cada día de retraso adicional hasta un máximo de un 10%.

RESPUESTA Y RESOLUCIÓN DE AVERÍAS EN TELEFONÍA MÓVIL.

Para los servicios de telefonía móvil, el adjudicatario del servicio deberá garantizar, en el caso de producirse averías, los siguientes niveles de calidad en la respuesta y resolución de averías:

- Tiempo máximo de respuesta: 1 hora.
- Tiempo máximo de resolución de averías, en función de la severidad de las mismas: 4 horas.
- Tiempo máximo de envío de mensaje de resolución de avería: 2 días laborables.
- Tiempo máximo de resolución de averías con envío de terminal: 48 horas.

Las penalizaciones a aplicar por el incumplimiento de las condiciones señaladas anteriormente serán las siguientes:

- Cuando a lo largo de un mes natural se produzca un incumplimiento de los tiempos comprometidos (tiempo máximo de respuesta ante averías y/o tiempo máximo de resolución de

averías) en los trámites del protocolo de notificación/resolución de averías en un 10% de los casos, se penalizará con el 1% de la facturación mensual.

- A partir de dicho 10% la penalización se incrementará en otro 1% por cada 1% adicional de incremento sobre el 10% inicial.
- Se establece como límite máximo de penalización, por este concepto, el 30% de la facturación mensual.
- El retraso en la entrega de los informes de resolución de avería conllevará la aplicación de una penalización del 1% de la facturación mensual del servicio afectado, que se incrementará en un 1% más por cada día de retraso adicional hasta un máximo de un 10%.

DISPONIBILIDAD DEL SERVICIO DE VOZ CORPORATIVA (FIJA Y MÓVIL).

Se revisará mensualmente el nivel de disponibilidad en la prestación del servicio. La fórmula a utilizar para el cálculo será la siguiente:

% Disponibilidad mensual = (Ttotal -Tnodisponibilidad)/ Ttotal * 100

Donde:

• Ttotal = tiempo total considerado expresado en minutos/mes, considerando número de 30 días/mes, 24 horas/día y 60 minutos/hora.

• Tnodisponibilidad = tiempo de no disponibilidad del servicio dentro del intervalo Ttotal considerado (minutos). El tiempo de no disponibilidad se contabilizará como la suma de todos los tiempos de no disponibilidad durante en el periodo considerado.

Se establece como objetivo de ANS para la disponibilidad mensual de los servicios de voz corporativa (fija y móvil) un 99,8 %.

El incumplimiento de este nivel supondrá la aplicación, sobre el importe de la facturación mensual del servicio, de las penalizaciones que se indican a continuación:

% ANS mensual obtenido	% Penalización
99,97 <= % ANS mensual < 99,98	1
99,96 <= % ANS mensual < 99,97	2
99,95 <= % ANS mensual < 99,96	3
99,94 <= % ANS mensual < 99,95	4
99,93 <= % ANS mensual < 99,94	5

OTROS NIVELES DE CALIDAD.

Para los servicios de voz corporativa (fija y móvil), el adjudicatario se deberá comprometer a mantener los siguientes niveles de calidad, como mínimo:

- Porcentaje de llamadas fallidas: inferiores al 1%.
- Tiempo de establecimiento de llamadas:
- A fijos: inferior a 2 segundos.
- A móviles: inferior a 6 segundos.
- Tasa global de llamadas con tarificación incorrecta menor o igual al 0,001%.
- Cualquier otro parámetro incluido en la normativa nacional e internacional que sea de aplicación deberá ser incluido siempre que el Ayuntamiento de Mérida, como organismo contratante, esté de acuerdo y los resultados de su aplicación sean en beneficio del referido organismo contratante.

En el caso de incumplimiento de los niveles de calidad anteriormente indicados, se aplicará una penalización del 2% del coste del servicio en la factura correspondiente al mes siguiente de producirse el incumplimiento.

7. CONFIDENCIALIDAD Y SEGURIDAD DE LOS DATOS

La prestación de los servicios que constituyen el presente Pliego se ajustará a la legalidad vigente en materia de Telecomunicaciones quedando el Ayuntamiento de Mérida exento de cualquier responsabilidad derivada de la no observación de dicha legalidad por parte de los operadores adjudicatarios.

Así mismo, los operadores asumirán cualquier tipo de coste (o coste extraordinario sobre las tarifas propuestas) derivado de su incumplimiento de las leyes vigentes.

Por último, los licitadores deberán describir las medidas de seguridad a aplicar con el objetivo de garantizar:

1. La confidencialidad e integridad de los datos correspondientes al Ayuntamiento de Mérida.

2. Los requerimientos en materia de Seguridad y Protección de Datos conforme a la Ley Orgánica 15/1999 del 13 de Diciembre, de Protección de Datos de Carácter Personal y al Real Decreto 1720/2007 del 21 de Diciembre, por el que se aprueba el Reglamento que la desarrolla.

8. IMPORTE DE LICITACIÓN, SENDA FINANCIERA, CPV, FACTURACIÓN

CPV: CPV08_64.200000-8 Servicio de Telecomunicaciones.

Para la facturación de los servicios se procederá a una facturación mensual de la anualidad correspondiente.

El importe estimativo seria de 3.474.941,72 euros iva incluido y su plazo de ejecución cinco años sin prórroga.

Base Imponible…: 2.871.852,67

Iva…….: 603.089,05

Total proyecto…..: 3.474.941,72

El contrato actual en vigor finaliza el próximo 12-agosto-2025.

SENDA FINANCIERA

AÑO	IMPORTE	IVA	TOTAL
2025(Agosto-diciembre)	224.308,26	47.104,74	271.413,00
2026(Enero-Diciembre)	573.872,64	120.513,25	694.385,89
2027(Enero-Diciembre)	573.872,64	120.513,25	694.385,89
2028(Enero-Diciembre)	573.872,64	120.513,25	694.385,89
2029(Enero-Diciembre)	573.872,64	120.513,25	694.385,89
2030(Enero-Agosto)	352.053,85	73.931,31	425.985,16
TOTAL	2.871.852,67	603.089,05	3.474.941,72

9. DOCUMENTACIÓN ANEXA

Por motivos de política de Seguridad de Datos hay cierta información que no se ha publicado en el PPT. Los licitadores interesados deberán solicitarla de forma motivada la documentación necesaria para valorar su propuesta según lo indicado en este PPT.

Volumetría Fija.

DESCRIPCION	LLAMADAS	SEGUNDOS
Llamadas a móviles	115	62312
Llamadas a Numeraciones 800/900	539	125425
Llamadas a Numeraciones 901	82	20935
Llamadas a Numeraciones 902	67	12968
Llamadas a Sº de Información y Emergencia	984	97728
Llamadas Internacionales	2	152
Llamadas Interprovinciales	2129	555542
Llamadas Metropolitanas	13804	2100041

Volumetría móvil.

TIPO DE TRÁFICO	LLAMADAS	UNIDAD MEDIDA	CANTIDAD MEDIDA
DATOS EN ROAMING	360	MEGABYTES	7.568
DATOS INTERNET	39.748	MEGABYTES	21.141.953
DATOS INTERNET EN UE	71	MEGABYTES	78.184
EN ROAMING	19	SEGUNDOS	1.755
INTERNACIONAL	76	SEGUNDOS	26.462
INTERNO BUZON	23	SEGUNDOS	1.398
INTERNO BUZON EN UE	3	SEGUNDOS	180
INTERNO CORPORATIVO	4.861	SEGUNDOS	560.612
INTERNO MÓVILES	10.625	SEGUNDOS	1.437.677
LLAMADAS A 800/900	216	SEGUNDOS	67.942
LLAMADAS A 800/900 EN UE	1	SEGUNDOS	607
LLAMADAS A 901	5	SEGUNDOS	1.586
LLAMADAS A 902	20	SEGUNDOS	3.000
LLAMADAS A INFORMACIÓN Y EMERGENCIAS	62	SEGUNDOS	5.114
LLAMADAS DUO	89.777	SEGUNDOS	12.117.964
LLAMADAS DUO EN UE	182	SEGUNDOS	25.967
MENSAJES MULTIMEDIA	5	MEGABYTES	1
RECIBIDAS EN ROAMING	10	SEGUNDOS	659
RESTO DE TRÁFICO NACIONAL	40	SEGUNDOS	16.178
SERVICIOS EMOCION	1.294	SEGUNDOS	-
SMS	686	SEGUNDOS	-
TRÁFICO NAC.OTROS OPER.MÓVILES	37.340	SEGUNDOS	5.681.984
TRÁFICO NACIONAL A FIJOS	2	SEGUNDOS	120

ACCESOS VPN SOBRE FTTH

SERVICIO	CALLE	NÚMERO
MACROLAN	Concordia	9
MACROLAN	España	1
VPN-IP	Antonio Rodríguez-Moñino	3
VPN-IP	Zaragoza	2
VPN-IP	Villafranca de los Barros	2
VPN-IP	Felipe VI	2
VPN-IP	Antonio Rodríguez-Moñino	5
VPN-IP	Trébol	4
VPN-IP	Cabo Verde	4
VPN-IP	Eugenio Hermoso	15
VPN-IP	Santa Eulalia	64
VPN-IP	Nuestra Señora del Perpetuo Socorro	7
VPN-IP	Marquesa de Pinares	38
VPN-IP	Zaragoza	2
VPN-IP	Ronda de los Eméritos	30
VPN-IP	Zaragoza	2
VPN-IP	D José Álvarez Sáenz de Buruaga	3
VPN-IP	España	1
VPN-IP	Tomas Romero de Castilla	22
VPN-IP	Pio Baroja	7
VPN-IP	John Lennon	5
VPN-IP	Vía de la Plata	40
VPN-IP	Marco Agripa	4
VPN-IP	Lusitania	10
VPN-IP	Juan Francisco Babiano Giner	5
VPN-IP	Nerja	1
VPN-IP	Dulce Chacón	2
VPN-IP	Antonio Montero Arzobispo	4
VPN-IP	Felipe VI	2
VPN-IP	Zaragoza	2
VPN-IP	John Lennon	5
VPN-IP	José de Echegaray	2
VPN-IP	Villarta de los Montes	22
VPN-IP	Manuel Núñez	1
VPN-IP	John Lennon	5
VPN-IP	Luis Álvarez Lencero	5

Mérida a fecha de firma electrónica

SEUDÓNIMO - JEFE SECCIÓN DE TRANSFORMACIÓN DIGITAL - AYUNTAMIENTO DE MERIDA

Firmado digitalmente por SEUDÓNIMO - JEFE SECCIÓN DE TRANSFORMACIÓN DIGITAL - AYUNTAMIENTO DE MERIDA
Fecha: 2025.02.27 11:44:59 +01'00'