

Este documento se ha obtenido directamente del original que contenía todas las firmas auténticas y se han ocultado los datos personales protegidos y los códigos que permitirían acceder al original

# PLIEGO DE PRESCRIPCIONES TÉCNICAS

***“MANTENIMIENTO, SERVICIOS DE SEGURIDAD  
AVANZADOS Y ADQUISICIÓN DE SOLUCIONES  
ANTIMALWARE CYTOMIC EPDR IMPLANTADAS EN LA  
COMUNIDAD DE MADRID”***



**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EL CONTRATO DE  
SERVICIOS DENOMINADO “MANTENIMIENTO, SERVICIOS DE SEGURIDAD AVANZADOS Y  
ADQUISICIÓN DE SOLUCIONES ANTIMALWARE CYTOMIC EPDR IMPLANTADAS EN LA  
COMUNIDAD DE MADRID” A ADJUDICAR MEDIANTE PROCEDIMIENTO NEGOCIADO SIN  
PUBLICIDAD**

**ÍNDICE**

CLÁUSULA 1. INTRODUCCIÓN.....	3
CLÁUSULA 2. OBJETO DEL CONTRATO .....	4
CLÁUSULA 3. ÁMBITO DE ACTUACIÓN.....	4
CLÁUSULA 4. ALCANCE REQUERIDO .....	5
4.1 MANTENIMIENTO Y ACTUALIZACIÓN DE LICENCIAS DE CYTOMIC EPDR (ENDPOINT PROTECCIÓN, DETECCIÓN Y RESPUESTA).....	6
4.2 MANTENIMIENTO Y ACTUALIZACIÓN DE LICENCIAS ENDPOINT PROTECTION PLUS PARA MÓVILES (ANDROID E IOS).....	8
4.3 SERVICIOS DE SEGURIDAD AVANZADOS .....	8
4.4 ADQUISICIÓN DE NUEVAS LICENCIAS CYTOMIC EPDR.....	14
4.5 ADQUISICIÓN DE NUEVAS LICENCIAS ENDPOINT PROTECTION PLUS PARA MÓVILES (ANDROID E IOS) .....	15
4.6 ADQUISICIÓN DE LICENCIAS DE LA CONSOLA ORION .....	16
CLÁUSULA 5. MODELO OPERATIVO Y DE ORGANIZACIÓN .....	17
5.1 EQUIPO DE TRABAJO.....	17
5.2 HORARIO Y LUGAR DE PRESTACIÓN DE LOS SERVICIOS .....	19
5.3 ACUERDOS DE NIVEL DE SERVICIO – ANS.....	20
CLÁUSULA 6. MODELO DE GESTION .....	24
6.1 SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO.....	24
6.2 CONDICIONES GENERALES APLICABLES AL EQUIPO DE TRABAJO.....	27
6.3 DOCUMENTACIÓN DE LOS SERVICIOS .....	29
6.4 DISPONIBILIDAD DE MEDIOS .....	29
CLÁUSULA 7. INFORMACIÓN RELEVANTE PARA LOS LICITADORES .....	30
7.1 ENTORNO TECNOLÓGICO .....	30
7.2 REQUISITOS PARA ACCESO REMOTO DE PROVEEDORES .....	31
7.3 MODELO DE CURRÍCULUM VITAE DEL EQUIPO PRESTADOR DEL SERVICIO .....	34
CLÁUSULA 8. CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS .....	34

## **CLÁUSULA 1. INTRODUCCIÓN**

De acuerdo con lo establecido en el *Artículo 10 de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas* (B.O.C.M. núm. 311, de 30 de diciembre de 2005); modificada parcialmente por la *Ley 9/2015, de 28 de diciembre, de Medidas Fiscales y Administrativas* (B.O.C.M. núm. 311, de 31 de diciembre de 2015); por el *Artículo 26 de la Ley 11/2022, de 21 de diciembre, de Medidas Urgentes para el Impulso de la Actividad Económica y la Modernización de la Administración de la Comunidad de Madrid* (B.O.C.M. núm. 304, de 22 de diciembre de 2022); y por el *Artículo 7 de la Ley 8/2024, de 26 de diciembre, de medidas para la mejora de la gestión pública en el ámbito local y autonómico de la Comunidad de Madrid* (BOCM número 308, de 27 de diciembre de 2024), la **Agencia para la Administración Digital de la Comunidad de Madrid** (en adelante la **Agencia**), se configura como ente público de los previstos en el *Artículo 6 de la Ley 9/1990, de 8 de noviembre, Reguladora de la Hacienda de la Comunidad de Madrid*, con personalidad jurídica propia, plena capacidad jurídica y de obrar para el cumplimiento de sus fines y con plena autonomía orgánica y funcional, que tiene por objeto, de acuerdo con las directrices establecidas por la consejería competente en materia de Digitalización, la planificación y ejecución de proyectos y servicios relacionados con tecnologías de la información, comunicaciones electrónicas y ciberseguridad, garantizando la interoperabilidad, escalabilidad, compatibilidad, suministro e intercambio de información, en el ámbito de actuación definido en el apartado dos de este artículo 10.

Entre las **competencias** que, conforme al *Artículo 10 – Tres, de la Ley 7/2005*, se atribuyen a la Agencia, bajo la dirección y coordinación de la Consejería competente en materia de Digitalización, para el cumplimiento de sus objetivos, se recogen, en concreto, las siguientes:

- a) La planificación, desarrollo y ejecución de planes y proyectos de tecnología, de comunicación electrónica y de seguridad de la información de la administración General e Institucional de la Comunidad de Madrid, garantizando la interoperabilidad, escalabilidad, compatibilidad, suministro e intercambio de información.*
- d) La adquisición, el diseño, desarrollo, implantación, mantenimiento, gestión y evolución de la infraestructura tecnológica, sistemas de información y de comunicaciones electrónicas y seguridad de la información de titularidad de la Agencia, así como la ejecución de las actuaciones para su consolidación y racionalización, incluyéndose en particular el puesto de trabajo, las infraestructuras de almacenamiento, los centros de procesos de datos, incluido el uso de nubes públicas y privadas de la Comunidad de Madrid y el archivo electrónico único de los expedientes y documentos electrónicos.*
- j) La elaboración y aprobación de las políticas de seguridad de los sistemas de información y comunicación electrónicas de titularidad de la Agencia y la gestión de los recursos comunes para la prevención, detección y respuesta a los incidentes y amenazas de ciberseguridad en el ámbito de sus funciones, sin perjuicio de las competencias de la Agencia de Ciberseguridad de la Comunidad de Madrid.*

El desarrollo de estas competencias de seguridad de la información y ciberseguridad es uno de los cinco objetivos del Plan Estratégico 2022-26 de Madrid Digital, cuyo propósito es: *Hacer de la Comunidad de Madrid una Administración más segura, confiable y resiliente*. Este objetivo se desarrolla en dicho plan a través de cuatro líneas de actuación: dos de ellas dedicadas a la



prevención, cibervigilancia y detección de amenazas y vulnerabilidades de forma proactiva y temprana, con el fin de eliminarlas, neutralizarlas, minimizando las consecuencias de materialización de incidente de seguridad, y otra de respuesta y recuperación ante incidentes de seguridad que permitan gestionar el riesgo, minimizando el impacto del incidente e identificando sus causas.

En este sentido, hay que tener en cuenta que, según va avanzando y aumentando la digitalización de la Comunidad de Madrid y, por tanto, el número y diversidad de servicios digitales y sistemas de información que utilizan los ciudadanos y los empleados públicos, mayor es la necesidad de ciberseguridad que garantice de forma transversal e integradora que la información y los datos personales están protegidos. Y más aún si consideramos que cualquier Administración se relaciona de forma continua con el ciudadano, con otras Administraciones y con las empresas por Internet, red abierta a todo el mundo, en la que se detecta una tendencia al alza sobre todo tipo de ciberdelitos (sobre todo el ransomware, el phishing y las estafas por Internet) como la propia INTERPOL informó en su último informe global de tendencias de criminalidad de octubre de 2022.

Por tanto, en un panorama de amenazas cibernéticas en constante evolución, donde los ataques se vuelven cada vez más sofisticados y dirigidos, contar con un sistema **EPDR** (Endpoint Protection, Detection and Response) es fundamental para garantizar la seguridad de nuestra organización. Los cibercriminales utilizan tácticas cada vez más evasivas para eludir las soluciones de seguridad tradicionales. Una solución **EPDR**, al monitorear continuamente los dispositivos y detectar comportamientos anómalos, permite identificar y responder a estas amenazas de manera proactiva, antes de que causen daños significativos.

Es por todo ello que, en la actualidad, Madrid Digital ha desplegado una solución de EPDR del fabricante PANDA S.L.U., denominada en **Cytomic EPDR** (anteriormente Panda Endpoint Protection) que está protegiendo, ante cualquier intento de ataque, a los Endpoint gestionados por ella y que dan servicio a la Comunidad de Madrid.

## **CLÁUSULA 2. OBJETO DEL CONTRATO**

El objeto del contrato es la prestación de los servicios de **mantenimiento y actualización de la solución Endpoint Protection, Detection & Response (Cytomic EPDR)** instalada en los puestos, servidores y dispositivos móviles (Endpoint Protección Plus para Móviles-Android e IOS), así como el **soporte técnico avanzado y especializado, y el servicio de “Threat Hunting”** (caza de amenazas). Además, es objeto del contrato la **adquisición de nuevas licencias bajo demanda** de los productos Cytomic EPDR, Endpoint Protección Plus para Móviles (Android e IOS) y Cytomic ORION (Plataforma para detección, búsqueda, investigación y respuesta ante incidentes,) para cubrir las nuevas necesidades que puedan surgir durante la totalidad de la vigencia del contrato.

Todo ello, dentro del ámbito de competencia de la Agencia, de conformidad con lo establecido en el presente Pliego de Prescripciones técnicas.

## **CLÁUSULA 3. ÁMBITO DE ACTUACIÓN**

El ámbito de actuación de los servicios descritos en este documento se circunscribe a los puestos, servidores y dispositivos móviles (Android e IOS) que sustentan los servicios digitales de la

Comunidad de Madrid, así como los puestos del Servicio Madrileño de Salud (SERMAS) de la Consejería de Sanidad, competencia de Madrid Digital.

Asimismo, indicar que, el contrato actualmente en vigor gestiona un total de **104.676 licencias del Cytomic EPDR** (anteriormente Panda Endpoint Protection Plus y Adaptive Defense) que deberán mantenerse y actualizarse, así como **457 licencias de Endpoint Protección Plus para Móviles (Android e IOS)** que también deberán mantenerse durante el plazo de ejecución de contrato cuyas prescripciones técnicas se definen en el presente documento.

Finalmente, de manera aproximada, se estima que los puestos y servidores sobre los que se aplicarán los servicios demandados serán unos 3.500 Servidores Windows y Linux y más de 100.000 puestos de usuarios Windows y MacOs, de los cuales unos 30.000 serán equipos portátiles, distribuidos en más de 5.000 sedes. Adicionalmente, cabría la posibilidad de adquirir licencias de protección para unos 5.000 dispositivos móviles.

#### **CLÁUSULA 4. ALCANCE REQUERIDO**

Tal y como se ha mencionado con anterioridad, debido al actual panorama, cada vez más sofisticado y complejo, de ciberataques es necesario **mantener un servicio de protección, detección y respuesta** ante estos, por ello, es necesario garantizar la continuidad del actual servicio de EPDR junto con el soporte técnico especializado y dedicado que incluya, además, un servicio de “Caza de Amenazas” que esté revisando y gestionando cualquier posible incidente que pudiera surgir durante la ejecución del contrato.

Alineado con todo ello, las prestaciones objeto del contrato serán las siguientes:

**4.1 MANTENIMIENTO Y ACTUALIZACIÓN DE LICENCIAS DE CYTOMIC EPDR (ENDPOINT PROTECCIÓN, DETECCIÓN Y RESPUESTA)** para protección de puestos de usuario (PC's de sobremesa y portátiles), servidores con sistema operativo Windows y Linux. Este servicio incluirá el mantenimiento, soporte y actualización de las distintas versiones de software del antimalware Cytomic EPDR disponibles en la Comunidad de Madrid.

**4.2 MANTENIMIENTO Y ACTUALIZACIÓN DE LICENCIAS DE ENDPOINT PROTECTION PLUS PARA MÓVILES (ANDROID E IOS)**. Este servicio incluirá el mantenimiento, soporte y actualización de las distintas versiones de este software.

**4.3 SERVICIOS DE SEGURIDAD AVANZADOS**, que incluirá el conjunto de tareas y servicios que se describen más adelante, y que se resume en tres prestaciones o líneas de servicio diferenciadas:

- A) Soporte técnico especializado y dedicado**, necesario para la implantación, mantenimiento y puesta en producción de los servicios de seguridad, así como la monitorización, la gestión de incidentes de seguridad en la base instalada y su resolución mediante la mecanización y automatización de tareas. Este soporte a prestar por un equipo de técnicos especialistas dispondrá de las herramientas de detección y desinfección de malware necesarias para el servicio e incluirá la prestación de un **soporte Premium**, que permitirá realizar consultas sobre los productos Cytomic EPDR objeto de mantenimiento y contar con tiempos de respuesta máximos para resolver las infecciones de malware de la forma más rápida y eficiente posible.



**B) Servicio de soporte 24x7x365**, cuya descripción de detalla más adelante.

**C) Servicio Threat Hunting (“caza de amenazas”) 24x7x365**, servicios de búsqueda proactiva de nuevas amenazas avanzadas y las TTPs (tácticas, técnicas y procedimientos) que usan los atacantes en sus reconocimientos y ataques, a través del análisis de la información generada por los puestos de trabajo, equipos portátiles y servidores.

**4.4 ADQUISICIÓN DE NUEVAS LICENCIAS CYTOMIC EPDR**, debido al crecimiento de los puestos y servidores por necesidades del servicio, habrá que comprar nuevas licencias para cubrir todos los equipos gestionados por Madrid Digital, tal y como se indica en el último párrafo de la cláusula anterior.

**4.5 ADQUISICIÓN DE NUEVAS LICENCIAS ENDPOINT PROTECTION PLUS PARA MÓVILES (ANDROID E IOS)**, debido al incremento previsto de dispositivos de la Comunidad, tal y como se indica en el último párrafo de la cláusula anterior.

**4.6 ADQUISICIÓN DE LICENCIAS DE LA CONSOLA ORION**, como **Plataforma de detección, búsqueda e investigación**, para acceso a la información almacenada en ella y recogida de las máquinas protegidas por Cytomic EPDR, con una antigüedad mínima de 365 días, para detectar, investigar y responder a incidentes de seguridad. Las licencias a suministrar deberán llevar incluido el producto accesorio Cytomic SiemConnect.

**Con carácter general, las infraestructuras en nube que presten servicios deberán estar alojadas en datacenters de la Unión Europea.**

#### **4.1 MANTENIMIENTO Y ACTUALIZACIÓN DE LICENCIAS DE CYTOMIC EPDR (ENDPOINT PROTECCIÓN, DETECCIÓN Y RESPUESTA)**

Con el actual panorama de ciberataques es necesario mantener y actualizar la herramienta que actualmente está instalada y que protege a los dispositivos y datos de las ciberamenazas existentes. En concreto, el número de licencias a mantener será de **104.676 unidades**.

A tal efecto, dicha herramienta debe estar basada en el paradigma **Zero Trust**, “confianza cero”, esto es: *no se confía en nada desconocido hasta analizarlo y comprobar que no es malicioso*; así como debe ser capaz de automatizar la prevención, detección, contención y respuesta ante cualquier amenaza avanzada. Por ello, es necesario **mantener y actualizar** la herramienta que Madrid Digital ya tiene desplegada en su infraestructura: **Cytomic EPDR**, para seguir protegiéndola ante posibles amenazas y, en consecuencia, es preciso que esta herramienta mantenga, en todo momento, las funcionalidades que se describen a continuación:

- Esta solución ofrecerá una **protección multicapa contra amenazas avanzadas**, combinando tecnologías preventivas (firewall, control de aplicaciones, antimalware) con capacidades de detección y respuesta (EDR) basadas en la nube, incluyendo **servicios de Zero-Trust** para clasificar automáticamente archivos y **Threat Hunting** para descubrir amenazas ocultas, permitiendo una respuesta rápida y automatizada a incidentes, minimizando el tiempo de respuesta y la fatiga por alertas.

- Esta tecnología, basada en cloud, combinará la tecnología de protección de endpoints (EPP) con capacidades automatizadas de detección y respuesta (EDR) en un solo producto, el cual cumplirá con los siguientes requerimientos técnicos:
  - Agente único, que incluya ambas tecnologías, EPP y EDR.
  - Inteligencia colectiva y heurística previa a la ejecución de los programas.
  - Antimalware permanente multivectorial y análisis a demanda.
  - Filtrado de URL, navegación web y protección contra suplantación de identidad.
  - Evaluación de vulnerabilidad de Sistemas operativos y aplicaciones.
  - Bloqueo de dispositivos USB.
  - Firewall personal o administrado.
  - Supervisión continua de endpoints con EDR.
  - Servicio de Zero Trust: Aprendizaje basado en la nube que clasifica el 100% de los procesos (APT, ransomware, rootkits, etc.).
  - Sandboxing en entornos reales.
  - Protección antiexploit.
  - Protección contra ataques de red para evitar que los ataques exploten vulnerabilidades en servicios expuestos en Internet.
  - Detección y prevención de ataques de RDP.
  - Capacidades de contención y corrección, como el aislamiento de computadoras, y el bloqueo de programas por hash o nombre del programa.
  - Análisis de comportamiento.
  - Motor de búsquedas por IoC's y reglas YARA.
  - Se podrá generar listas negras de aplicaciones, por nombre o hash.
  - Se podrá generar excepciones de software.
  - Se protegerá la desinstalación de la protección mediante contraseña y establecer protecciones para que no pueda ser detenida.
  - Protección contra ransomware.
  - Escalabilidad: La solución debe poder adaptarse a entornos de diferentes tamaños y complejidad.
  - Fácil implementación, debe ser fácil de implementar y configurar.
- **Consola de administración:** El servicio se gestionará desde una única consola, en español, y de manera centralizada, a la cual se accederá mediante cualquier navegador web y con doble factor de autenticación. Además, permitirá definir permisos basados en perfiles que se asignarán a los usuarios, e indicar el ámbito de acción de los usuarios restringiendo el acceso a determinados grupos de equipos.

Todas las acciones realizadas por los administradores serán auditadas, recogiendo acción, IP de la conexión y usuario.

- **Certificación:** La solución estará incluida en el “Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación. (CPSTIC), publicado por el CCN (Centro Criptográfico Nacional), dentro de la familia de protección del Puesto de Trabajo como CUALIFICADO **ENS** al menos con cualificación **MEDIA** y recomendable con cualificación **ALTA**, tanto en la categoría de EPP (Endpoint Protection Platform) como en la de EDR (Endpoint Detection and Response).

#### **4.2 MANTENIMIENTO Y ACTUALIZACIÓN DE LICENCIAS ENDPOINT PROTECTION PLUS PARA MÓVILES (ANDROID E IOS)**

En el amplio y variado panorama de las amenazas móviles, es necesario disponer de soluciones de seguridad para dispositivos móviles corporativos. Esto se agrava debido a que el nuevo lugar de trabajo híbrido, con opciones remotas y de trabajo desde casa, convierte a estos dispositivos móviles en un componente más común y crítico dentro en la infraestructura de TI de una organización.

De esta manera, cada vez es más importante para las organizaciones proteger a los dispositivos móviles y sus datos, a fin de evitar sufrir vulneraciones de datos y acceso no autorizado a información confidencial como consecuencia de un mayor acceso a los datos corporativos a través de dispositivos móviles que están fuera del perímetro corporativo, ya que los usuarios de los mismos desempeñan sus tareas de manera remota. Por tanto, es necesario mantener y actualizar las **457 licencias de Endpoint Protección Plus para Móviles (Android e IOS)** ya instaladas con la doble finalidad de proteger los dispositivos móviles y garantizar que los empleados puedan trabajar de manera productiva, en consecuencia, es preciso que esta herramienta mantenga, en todo momento, las funcionalidades que se describen a continuación.

- Esta solución deberá permitir administrar de manera centralizada, en la misma consola que se gestiona el EPDR, la seguridad y confidencialidad de los datos almacenados en sus teléfonos inteligentes y tabletas iOS y Android. Además, deberá ofrecer la opción de proteger los dispositivos móviles contra malware, extravío y robo. También deberá proteger contra otras potenciales amenazas contra los dispositivos móviles, tales como:
  - Amenazas físicas contra los dispositivos móviles relacionadas con el extravío o robo de un dispositivo, lo que permite a los hackers tener acceso directo al hardware en el que se almacenan los datos privados.
  - Amenazas basadas en aplicaciones: los usuarios descargan aplicaciones que parecen legítimas, pero que en realidad sustraen datos de sus dispositivos.
  - Amenazas basadas en la web: los usuarios visitan sitios afectados que parecen no tener problemas en el front-end, pero que, de hecho, descargan de manera automática contenido malicioso en los dispositivos. Los intentos de suplantación de identidad en los dispositivos móviles siguen creciendo año tras año.

#### **4.3 SERVICIOS DE SEGURIDAD AVANZADOS**

El adjudicatario del contrato deberá prestar los servicios de seguridad avanzados que se detallan a continuación y que incluyen la realización de las siguientes tres prestaciones o líneas de servicio:



- A. SOPORTE TÉCNICO ESPECIALIZADO Y DEDICADO:** Su finalidad será facilitar las labores de mantenimiento y evolución de la herramienta, así como de coordinación y resolución eficiente de problemas e incidentes. A tal efecto, se necesitará un equipo de especialistas dedicado cuyo perfil está recogido en el apartado **5.1 equipo de trabajo**.

En concreto, el trabajo de estos especialistas en seguridad consistirá en la realización de todas las actividades asociadas al mantenimiento preventivo, correctivo y evolutivo de la solución, además de la monitorización continua y respuesta ante incidentes:

- **Mantenimiento preventivo:** Revisión de los sistemas para determinar la salud y el estado de la infraestructura. Se plantearán planes de acción y acciones correctoras, así como guías de buenas prácticas para operar y mantener la infraestructura y el servicio de forma eficiente.
- **Mantenimiento correctivo:** Tratamiento especializado ante incidencias y problemas, así como de puesta en práctica de soluciones en el menor tiempo posible.
- **Mantenimiento evolutivo:** Adecuación de las infraestructuras de seguridad para atender las nuevas sedes, traslados, etc. Así como la actualización de nuevas versiones de producto y su implantación en los equipos de la Comunidad de Madrid.
- **Monitorización:** Deberán realizar una monitorización continua de las máquinas para evitar incidentes.
- **Respuesta ante incidentes:** Una vez se tenga constancia de un posible incidente deberán realizar las actividades necesarias para evitarlo.

A continuación, se describen algunas de las actividades más significativas:

- **Mantenimiento de la infraestructura del servicio EPDR y Endpoint Protection Plus para Móviles:** Para garantizar la disponibilidad y acceso de los distintos equipos de la Comunidad de Madrid a las distintas consolas de Cytomic EPDR que disponen de las actualizaciones tanto del motor, como de los ficheros de firmas, de manera que se optimicen los recursos de la red y se mantengan actualizados todos los puestos diariamente de manera rápida y fiable. Para ello, será necesario realizar las siguientes tareas:
  - **Certificación de nuevas versiones:** Certificación de las nuevas versiones de producto conforme a los procedimientos establecidos, realizando las pruebas en entornos restringidos de laboratorio, validando el plan de pruebas en las distintas plataformas hardware y software de puestos homologados.
  - **Elaboración de paquetes de nuevas versiones:** Elaboración de los paquetes de software para distribuirlos a través de Microsoft System Center, plan de pruebas para validar su distribución en las distintas plataformas de hardware y de las versiones de software de los puestos de la Comunidad de Madrid, y colaboración en la distribución en las fases de despliegue del piloto y su puesta en producción.
  - **Definición de procedimientos manuales:** Elaboración de los procedimientos manuales de instalación y configuración para aquellos equipos que no se pueda automatizar su instalación.

- **Elaboración de los Informes y documentación:** Elaboración de informes y la documentación relativa a los procedimientos operativos para la gestión del software de antimalware, así como del seguimiento de las incidencias en el servicio, etc.
- **Extensión del servicio de mantenimiento y soporte técnico a nuevas dotaciones de puestos y servidores:** Se incluirá en el servicio de mantenimiento y soporte las nuevas dotaciones de puestos y servidores que se desplieguen en centros existentes o nuevos de la Comunidad de Madrid ofreciéndoles la solución corporativa que mejor se adapte a sus necesidades. Para ello, será el adjudicatario el que deberá realizar las siguientes tareas:
  - **Instalación del antimalware en los servidores:** Instalación y configuración de los servicios de Cytomic EPDR en los servidores de los nuevos centros, conforme a los procedimientos establecidos.
  - **Adecuación de los puestos e instalación del cliente:** Instalación y configuración del cliente de antimalware Cytomic EPDR en los puestos de los nuevos centros, conforme a los procedimientos establecidos y de Endpoint Protection Plus en los dispositivos móviles.
  - **Implantación de procedimientos operativos:** Colaboración en la elaboración de la documentación de implantación, revisión y mantenimiento de los procedimientos para prestar los servicios de seguridad de antimalware de puestos y las actividades formativas necesarias para la difusión de los procedimientos operativos.
- **Mantenimiento de la base instalada:** Realización de las labores de administración del entorno de seguridad ofimático descrito con anterioridad, dichas tareas serán asignadas y planificadas por el jefe de proyecto, entre ellas podemos destacar:
  - Tareas asociadas al mantenimiento correctivo y evolutivo de los sistemas de antimalware Cytomic EPDR y Endpoint Protection Plus.
  - Seguimiento y atención a las incidencias de seguridad.
  - Colaboración en la solución de incidencias, su documentación, y publicación conforme a los procedimientos establecidos.
  - Colaboración en el despliegue y seguimiento en la distribución del software de antimalware Cytomic EPDR en los puestos de la Comunidad de Madrid.
  - Generación de procedimientos, documentación, pruebas, e implantación en el entorno de producción.
  - Elaboración de paquetes y distribución de parches críticos de seguridad, cambios de configuración, y utilidades de desinfección en los equipos de la Comunidad de Madrid.
  - Seguimiento y control de la base instalada.
  - Elaboración y generación de informes de la base instalada.
- **Mecanización y automatización de tareas:** Elaboración, prueba, e implantación de la automatización de tareas y la mecanización de procedimientos que permitan su implementación a través de directivas de Directorio Activo de Microsoft, así como de

paquetes de Microsoft SMS que permitan la configuración y adaptación de los puestos conforme a los procedimientos establecidos.

- **Incidentes de Ciberseguridad:** El equipo del adjudicatario colaborará de forma activa en la respuesta a ciberamenazas e Incidentes de seguridad dentro del proceso de Respuesta a Incidentes de la Agencia, entre ellas podemos destacar:
  - Monitorización del cumplimiento de las políticas de seguridad establecidas por la Agencia e informar de las deficiencias identificadas.
  - Notificación y elaboración de informes de comportamientos anómalos detectados.
  - Gestión de los Indicadores de Ataques (IoA) notificados por el servicio de Threat Hunting y canalizarlos a los equipos internos de la Agencia para su investigación y resolución de los mismos.
  - Realización de informes donde se recoja la información obtenida del incidente y los pasos dados para su resolución.
  - Establecimiento de métricas para poder medir la mejora de la seguridad dentro de los informes a presentar a la Agencia en las reuniones de seguimiento.
  - Mantenimiento del historial de incidentes de seguridad y de las incidencias de los distintos productos contratados.
  - Reducir el tiempo de respuesta cuando se identifique un incidente de seguridad, desde su fase inicial, reportando la forma de contenerlo/remediarlo.
  - Mejora del tiempo de recuperación objetivo (RTO) cuando se identifique un incidente cibernético confirmado.
  - Búsqueda proactiva de amenazas dentro del ámbito de puestos y servidores de la Agencia, mejorando los tiempos de detección actuales y buscando la anticipación proactiva de caza de amenazas.
  - Mejora de los protocolos de escalado de incidentes de seguridad dentro de Agencia y su evaluación en términos de eficacia, con objetivo final de la mejora de dicho proceso.
  - Análisis de los Indicadores de Compromiso, en adelante IOCs, y búsqueda de esos IOCs dentro de los equipos bajo el ámbito de responsabilidad de la Agencia y la monitorización de los mismos. Verificación de la detección por parte de las herramientas de WatchGuard de dichos IOCs.

### **Gestión de Incidencias**

Antes de que el adjudicatario proporcione soporte en un incidente, la Agencia y los técnicos especialistas de soporte asignados por el adjudicatario acordarán cual es el problema a resolver, así como los parámetros para una resolución adecuada. Un incidente podrá requerir la realización de múltiples llamadas telefónicas, así como trabajo de investigación fuera de línea para alcanzar la solución final, incluyendo la necesidad de disponer del soporte Premium que se describe a final de este apartado. En todo caso, la Gestión de Incidencias se ejecutará bajo las siguientes premisas:



- **Diagnóstico Remoto.** A petición de la Agencia, el adjudicatario podrá acceder a los sistemas de ésta remotamente para analizar problemas. Este acceso se efectuará, exclusivamente, con el consentimiento de la Agencia, y el personal del adjudicatario accederá, exclusivamente, a los sistemas autorizados por ésta. El adjudicatario deberá proporcionar a la Agencia software para asistirle en el diagnóstico y/o resolución del problema.
- **Coordinación entre diversos fabricantes.** El adjudicatario trabajará con otros proveedores clave en la resolución de problemas en entornos heterogéneos. Cuando los problemas notificados sobre los productos de seguridad que impliquen interacciones con productos de terceros, y la Agencia tenga acuerdos de soporte con dichos terceros, el adjudicatario compartirá información de diagnóstico y colaborará con ellos para proporcionar una solución.

La Agencia pondrá a disposición del adjudicatario los medios y recursos necesarios para facilitar su labor, facilitándole la información que precise para ello, así como el acceso al lugar donde se encuentren instalados los productos objeto del presente contrato, al personal destinado por el contratista a la ejecución de los trabajos.

Tal y como se ha mencionado con anterioridad, para la prestación del servicio descrito anteriormente, se dispondrá de un **servicio de soporte Premium** con la finalidad de mejorar la disponibilidad y acceso de los distintos equipos de la Comunidad de Madrid a los servicios que disponen de las actualizaciones tanto del motor, como de los ficheros de firmas, de manera que se optimicen los recursos de la red y se mantengan actualizados todos los puestos diariamente de manera rápida y fiable. A continuación, se describe las condiciones que definen este soporte adicional:

- **Servicio de soporte técnico personal 24 horas al día 365 días al año.** Servicio de atención al cliente, atendido por expertos del producto a través de teléfono, para la resolución de cualquier consulta o incidencia relacionada con la detección de malware o con la configuración del producto, 24 horas al día los 365 días al año.
- **Soporte técnico preferente.** Vía de comunicación exclusiva para contactar con el departamento de soporte Premium. Para atender estas consultas de forma preferente, se registrarán las personas de la Agencia para la Administración Digital de la Comunidad de Madrid, que serán las autorizadas para utilizar estas vías de comunicación exclusivas.
- **Servicio de soporte telefónico VIP.** Consultor técnico en línea identificado como responsable de la resolución de las incidencias, y con preferencia en el soporte frente a otros clientes. En todo caso, la resolución de las incidencias será responsabilidad del técnico especialista asignado durante todo el “ciclo de vida de la incidencia”, según el procedimiento descrito en el presente documento.
- **Actualización del fichero de firmas (Intelligent Updates).** Acceso a las actualizaciones del fichero de firmas de virus a través de internet. A tal efecto, el adjudicatario se comprometerá a actualizar TODOS LOS DÍAS el fichero con las nuevas detecciones de virus, así como las rutinas de desinfección que se incorporan al fichero de firmas de forma incremental.

- **Acceso a las mejoras de producto (Intelligent Upgrades).** Acceso a las mejoras del software antimalware a través de internet, incluyendo el uso de las herramientas del adjudicatario para permitir el despliegue de nuevas versiones del motor de antimalware en la red corporativa con un mínimo uso de los recursos de comunicaciones.
- **Generación de herramientas de desinfección especiales.** Específicas para todo el malware detectado, que permitan eliminar la amenaza y restaurar los equipos para dejarlos operativos, minimizando el coste de despliegue y de reparación ante una infección.

**B. SERVICIO DE SOPORTE 24x7x365:** Como prestación adicional al soporte dedicado descrito en el apartado anterior, el adjudicatario, también deberá prestar un servicio soporte 24x7x365 ante cualquier incidencia o incidente que pudiera ocurrir con los técnicos especialistas incluidos en el contrato. Para este servicio el adjudicatario pondrá a disposición de Madrid Digital un número de teléfono de soporte técnico operativo durante 24 horas al día / 7 días a la semana los 365 días del año.

**C. SERVICIO THREAT HUNTING (“CAZA DE AMENAZAS”) 24x7x365:** El servicio Threat Hunting Service es una práctica proactiva de ciberseguridad que irá más allá de la simple detección de amenazas, se centrará en la búsqueda proactiva de nuevas amenazas avanzadas y de nuevas tácticas, técnicas y procedimientos, en adelante TTPs, que usan los atacantes en sus reconocimientos y ataques.

Este servicio permitirá reducir los tiempos medios de detección y respuesta ante incidentes. También permitirá identificar las vulnerabilidades y puntos débiles que pueda haber en la seguridad para tomar, cuanto antes, medidas mitigadoras.

Por tanto, el servicio de Threat Hunting es algo esencial para proteger los activos digitales de manera proactiva, ya que combina herramientas avanzadas con inteligencia artificial y con la experiencia de los analistas de seguridad del proveedor; es por ello, que esta Agencia ha considerado necesario ampliar la prestación de este servicio en relación con el contrato actualmente en vigor, cuya prestación se establecía en 8x5.

Durante el plazo de ejecución del contrato, los **servicios de Threat Hunting Service**, descritos en este pliego, deberán prestarse por el fabricante de la solución EDPR en la franja horaria de 00:00 h. a 24:00 h., todos los días de la semana, incluidos los días festivos. Es decir, el servicio se prestará en 24x7x365.

En concreto, la prestación de este servicio comprenderá la realización de las siguientes tareas:

- Supervisión continua de actividad en las máquinas durante las 24 horas.
- Búsqueda proactiva las 24 horas, detección de comportamiento e investigación.
- Notificación por email ante potenciales amenazas, o por teléfono en caso de ser un ciberincidente grave o crítico.
- Seguimiento Post-incidente para asegurarnos la resolución de incidentes críticos.
- Reporte mensual de la actividad ocurrida, durante el mes, en las máquinas gestionadas por el EPDR.



- Informes detallados de ataques ocurridos.
- Almacenamiento de la telemetría durante un año. La telemetría almacenada debe permitir a los equipos de ciberseguridad investigar ataques de manera retroactiva.

En definitiva, el servicio de Threat Hunting proactivo permitirá:

- **Detectar “ataques” en fase temprana.** Son ataques que aún están en sus fases iniciales que, en caso de no controlarse, podrían acabar comprometiendo a parte o a toda la organización.
- **Detectar equipos comprometidos:** Se trata de equipos comprometidos por ataques que se han saltado las diferentes protecciones establecidas por la organización. En algunos casos se trata de equipos comprometidos hace días, semanas o incluso meses que no son detectados por utilizar técnicas “fileless”, ataques de malware sin fichero. Estos equipos comprometidos no actúan de forma inmediata y permanecen a la espera para conseguir la información que necesitan para alcanzar el objetivo de su ataque.
- **Detectar malas prácticas.** Las malas prácticas detectadas deberán ser comunicadas a Madrid Digital para confirmar que, en efecto, son una mala práctica y no un principio de ataque. La Agencia establecerá los medios adecuados para eliminar estas malas prácticas y reducir la superficie de ataque para hackers o personal interno, denominado “insiders”.
- **Detectar comportamientos anómalos de usuarios y equipos.** Estos comportamientos anómalos deberán ser comunicados a la Agencia para confirmar si se trata o no de un principio de ataque, o de un ataque en curso.

Este servicio avisará a los técnicos especialistas dedicados ante cualquier detección de posible incidente para que ellos valoren, junto con Madrid Digital, las acciones a realizar para mitigarlo.

#### **4.4 ADQUISICIÓN DE NUEVAS LICENCIAS CYTOMIC EPDR**

Durante la ejecución del contrato, la Agencia podrá **adquirir nuevas licencias del producto Cytomic EPDR** para los equipos de la Comunidad de Madrid, a fin de hacer frente a posibles crecimientos de la planta instalada. La adquisición de nuevas licencias incluirá la garantía a prestar por el fabricante de las mismas, todo ello con la finalidad de mantener y actualizar estas licencias durante el tiempo restante de duración del contrato, en el momento de la compra.

En concreto, sobre la base de los datos recogidos en el último párrafo de la cláusula tercera del presente Pliego, y a efectos del cálculo del presupuesto base de licitación, se ha estimado la posibilidad de adquirir un número de unidades a lo largo de la ejecución del contrato, con el desglose que se detalla en la siguiente tabla. El número de unidades que finalmente se adquieran dependerán de las necesidades reales del servicio.

Las solicitudes de adquisición de licencias se realizarán a demanda del Responsable del Contrato designado por la Agencia, según necesidades del servicio, mediante peticiones concretas del número de licencias y del tipo. Cada petición requerirá una propuesta por parte del proveedor indicando número de licencias solicitado, tiempo de garantía de dichas licencias e importe, que deberá ser aprobada por Madrid Digital. Estas se facturarán, como cuota variable con el siguiente



desglose de precios unitarios, al que se le aplicará la baja obtenida, en su caso, como resultado de la adjudicación:

TABLA ESTIMATIVA SUMINISTRO BAJO DEMANDA	
Descripción de licencias	Unidades estimadas
Panda Cytomic EPDR con 35 meses de garantía del fabricante	15.324
Panda Cytomic EPDR con 30 meses de garantía del fabricante	0
Panda Cytomic EPDR con 24 meses de garantía del fabricante	8.000
Panda Cytomic EPDR con 18 meses de garantía del fabricante	5.000
Panda Cytomic EPDR con 12 meses de garantía del fabricante	3.000
Panda Cytomic EPDR con 6 meses de garantía del fabricante	20.000

Finalmente indicar que, si las licencias adquiridas dejan de estar en uso, podrán ser convertibles en licencias de Endpoint Protection Plus para móviles, según equivalencia en el precio de adjudicación o según indique el proveedor, lo que sea más beneficioso para Madrid Digital.

#### **4.5 ADQUISICIÓN DE NUEVAS LICENCIAS ENDPOINT PROTECTION PLUS PARA MÓVILES (ANDROID E IOS)**

Durante la ejecución del contrato la Agencia podrá **adquirir nuevas licencias del producto Endpoint Protección Plus para Móviles (Android e IOS)** para los dispositivos de la Comunidad de Madrid, a fin de hacer frente a posibles necesidades de proteger los dispositivos móviles desplegados en la Comunidad de Madrid. La adquisición de nuevas licencias incluirá la garantía a prestar por el fabricante de las mismas, todo ello con la finalidad de mantener y actualizar estas licencias durante el tiempo restante de duración del contrato, en el momento de la compra.

En concreto, sobre la base de los datos recogidos en el último párrafo de la cláusula tercera del presente Pliego, y a efectos del cálculo del presupuesto base de licitación, se ha estimado la posibilidad de adquirir un número de unidades a lo largo de la ejecución del contrato, con el desglose que se detalla en la siguiente tabla. El número de unidades que finalmente se adquieran dependerán de las necesidades reales del servicio.

Las solicitudes de adquisición de licencias se realizarán a demanda del Responsable del Contrato designado por la Agencia, según necesidades del servicio, mediante peticiones concretas del número de licencias y del tipo. Cada petición requerirá una propuesta por parte del proveedor indicando número de licencias solicitado, tiempo de garantía de dichas licencias e importe, que deberá ser aprobada por Madrid Digital. Estas se facturarán, como cuota variable con el siguiente desglose de precios unitarios, al que se le aplicará la baja obtenida, en su caso, como resultado de la adjudicación:

TABLA ESTIMATIVA SUMINISTRO BAJO DEMANDA	
Descripción de licencias	Unidades estimadas
Endpoint Protection Plus para móviles (Android e IOS) con 35 meses de garantía fabricante	850
Endpoint Protection Plus para móviles (Android e IOS) con 30 meses de garantía fabricante	850
Endpoint Protection Plus para móviles (Android e IOS) con 24 meses de garantía fabricante	850
Endpoint Protection Plus para móviles (Android e IOS) con 18 meses de garantía fabricante	850
Endpoint Protection Plus para móviles (Android e IOS) con 12 meses de garantía fabricante	850
Endpoint Protection Plus para móviles (Android e IOS) con 6 meses de garantía fabricante	850

Finalmente indicar que, si las licencias adquiridas dejan de estar en uso, podrán ser convertibles en licencias de Cytomic EPDR, según equivalencia en el precio de adjudicación o según indique el proveedor, lo que sea más beneficioso para Madrid Digital.

#### **4.6 ADQUISICIÓN DE LICENCIAS DE LA CONSOLA ORION**

Junto con la adquisición de nuevas licencias de los dos productos ya implantados por Madrid Digital, será necesario **adquirir licencias de acceso a la plataforma Cytomic ORION** para detectar, investigar y responder a incidentes de seguridad de manera eficiente y minimizar las brechas de seguridad. Esta solución, en nube, recogerá y almacenará toda la actividad realizada por las distintas máquinas que tengan instalada la protección EPDR, permitiendo una administración del ciclo de vida de amenazas continua y eficaz, desde la prevención hasta la detección, investigación y contención de amenazas que pudieran haber evadido los controles de seguridad existentes.

En concreto, las funcionalidades de esta herramienta serán, al menos, las que se describen a continuación:

- Incluirá **inteligencia artificial y aprendizaje automático** para descubrir y brindar respuestas a amenazas desconocidas y sofisticadas de manera proactiva y eficiente. Y tendrá acceso a la inteligencia global de amenazas para estrategias informadas de detección y respuesta.
- Además de las reglas predeterminadas que incluya la solución, para realizar análisis de seguridad avanzados, también permitirá configurar casos de uso personalizados para Madrid Digital, incluyendo el análisis de comportamiento, donde se detectará acciones inusuales del sistema, aplicaciones, etc.
- Tendrá supervisión de actividades en tiempo real de las máquinas y los programas ejecutados en ellas, clasificando al 100% los procesos ejecutados manteniendo la política de “Zero Trust” y empleando la inteligencia artificial para impulsar la clasificación automática de los procesos desconocidos.
- La información recogida se guardará, al menos, durante 365 días y será accesible por Madrid Digital y por los técnicos asignados al proyecto a través de una consola en nube. Esta consola permitirá acceder a los datos a través integraciones con otras herramientas, como un SIEM, a través de API's y/o conectores.

En concreto, sobre la base de los datos recogidos en el último párrafo de la cláusula tercera del presente Pliego, y a efectos del cálculo del presupuesto base de licitación, se ha estimado la posibilidad de adquirir un número de unidades a lo largo de la ejecución del contrato, con el desglose que se detalla en la siguiente tabla. El número de unidades que finalmente se adquieran dependerán de las necesidades reales del servicio.

La adquisición de estas licencias incluirá la garantía a prestar por el fabricante de las mismas, todo ello con la finalidad de mantener y actualizar estas licencias durante el tiempo restante de duración del contrato, en el momento de la compra.

Las solicitudes de adquisición de licencias se realizarán a demanda del Responsable del Contrato designado por la Agencia, según necesidades del servicio, mediante peticiones concretas del número de licencias y del tipo. Cada petición requerirá una propuesta por parte del proveedor indicando número de licencias solicitado, tiempo de garantía de dichas licencias e importe, que deberá ser aprobada por Madrid Digital. Estas se facturarán, como cuota variable con el siguiente desglose de precios unitarios, al que se le aplicará la baja obtenida, en su caso, como resultado de la adjudicación:

DESCRIPCIÓN DE LICENCIAS (*)	UNIDADES ESTIMADAS
Cytomic ORION con 35 meses de garantía del fabricante	120.000
Cytomic ORION con 30 meses de garantía del fabricante	0
Cytomic ORION con 24 meses de garantía del fabricante	8.000
Cytomic ORION con 18 meses de garantía del fabricante	5.000
Cytomic ORION con 12 meses de garantía del fabricante	3.000
Cytomic ORION con 6 meses de garantía del fabricante	20.000

(\*) Las licencias a suministrar deberán llevar incluido el producto accesorio Cytomic SiemConnect.

## **CLÁUSULA 5. MODELO OPERATIVO Y DE ORGANIZACIÓN**

### **5.1 EQUIPO DE TRABAJO**

El adjudicatario estará obligado a observar las condiciones generales del equipo de trabajo que pondrá a disposición del contrato, recogidas en el apartado **6.2 CONDICIONES GENERALES APLICABLES AL EQUIPO DE TRABAJO**.

En la siguiente tabla se recoge la dimensión del equipo de trabajo mínimo requerido por Madrid Digital para la ejecución del servicio de soporte dedicado con técnicos especialistas:



PERFIL – FUNCIÓN	% DEDICACIÓN	HORAS DE SERVICIO ESTIMADA EN EL CONTRATO
Jefe de Proyecto/Responsable del Servicio	100	5.760 horas
Ingeniero Senior de Seguridad/Técnico de Seguridad Senior	100	5.760 horas
Ingeniero de Seguridad/Técnico de Seguridad	100	5.760 horas

Para el cálculo de horas de servicio estimadas se ha considerado una dedicación al 100% del equipo al proyecto con un esfuerzo de 160 horas mensuales durante la totalidad del plazo de ejecución del contrato (3 años).

Todos los perfiles identificados con un 100% de dedicación están asociados a servicios continuos facturables en modalidad de cuota fija.

A continuación, se recogen el perfil profesional, funciones y requisitos de titulación, formación y experiencia, del equipo de trabajo que prestará los servicios exigidos.

Todo el equipo, jefe de proyecto y técnicos especialistas, deberán disponer de formación especializada en seguridad de productos del fabricante, y amplios conocimientos del entorno Microsoft, Linux y MacOS, así como de Hacking Ético.

<b>JEFE DE PROYECTO</b> Dedicación al proyecto:	<b>1 Persona</b> <b>100%</b>
<b>TITULACIÓN Y FORMACIÓN:</b> <ul style="list-style-type: none"> <li>Ingeniería Técnica en Informática, Formación Profesional Grado Superior en informática o equivalente.</li> <li>Formación en diseño y administración de Microsoft Windows al menos en las siguientes versiones Windows 8.1, 10 y 11, Windows Server 2022, 2019, 2016, 2012, al menos 40 horas.</li> <li>Formación en diseño y administración de Microsoft Directorio Activo, al menos 40 horas.</li> <li>Formación en diseño y administración de sistemas Linux, al menos 40 horas.</li> </ul> <b>EXPERIENCIA PROFESIONAL:</b> <ul style="list-style-type: none"> <li>Al menos <b>48 meses</b> realizando labores de administración, implantación, mantenimiento y soporte de los sistemas de seguridad basados en los sistemas Windows siguientes: Windows 8.1 o superior, Windows Server 2022, 2019, 2016, 2012.</li> <li>Al menos <b>48 meses</b> de experiencia en redes de más de 1.000 PC's distribuidos en varias sedes.</li> <li>Al menos <b>48 meses</b> de experiencia en la organización y gestión de equipos técnicos especialistas en la detección y remediación de incidencias de seguridad.</li> </ul>	

<ul style="list-style-type: none"> <li>Al menos <b>48 meses</b> de experiencia en proyectos de despliegue de soluciones de seguridad de WatchGuard.</li> </ul>	
<b>TECNICO DE SEGURIDAD SENIOR</b> Dedicación al proyecto:	<b>1 Persona</b> 100%
<b>TITULACIÓN Y FORMACIÓN:</b> <ul style="list-style-type: none"> <li>Ingeniería Técnica en Informática, Formación Profesional Grado Superior en informática o equivalente.</li> <li>Formación en diseño y administración de Microsoft Windows al menos en las siguientes versiones Windows 8.1, 10 y 11, Windows Server 2022, 2019, 2016, 2012, al menos 40 horas.</li> <li>Formación en diseño y administración de Microsoft Directorio Activo, al menos 40 horas.</li> <li>Formación en diseño y administración de sistemas Linux, al menos 40 horas.</li> </ul> <b>EXPERIENCIA PROFESIONAL:</b> <ul style="list-style-type: none"> <li>Al menos <b>36 meses</b> realizando labores de administración, implantación, mantenimiento y soporte de los sistemas de seguridad basados en los sistemas Windows siguientes: Windows 8.1 y superior, Windows Server 2022, 2019, 2016, y 2012.</li> <li>Al menos <b>36 meses</b> de experiencia en redes de más de 1.000 PC's distribuidos en varias sedes.</li> </ul>	
<b>TECNICO DE SEGURIDAD</b> Dedicación al proyecto:	<b>1 persona</b> 100%
<b>TITULACIÓN Y FORMACIÓN:</b> <ul style="list-style-type: none"> <li>Ingeniería Técnica en Informática, Formación Profesional Grado Superior en informática o equivalente.</li> <li>Formación en diseño y administración de Microsoft Windows al menos en las siguientes versiones Windows 8.1, 10 y 11, Windows Server 2022, 2019, 2016, 2012, al menos 40 horas.</li> <li>Formación en diseño y administración de Microsoft Directorio Activo, al menos 40 horas.</li> <li>Formación en diseño y administración de sistemas Linux, al menos 40 horas.</li> </ul> <b>EXPERIENCIA PROFESIONAL:</b> <ul style="list-style-type: none"> <li>Al menos <b>24 meses</b> realizando labores de administración, implantación, mantenimiento y soporte de los sistemas de seguridad basados en los sistemas Windows siguientes: Windows 8.1 y superior, Windows Server 2022, 2019, 2016, y 2012.</li> <li>Al menos <b>24 meses</b> de experiencia en redes de más de 1.000 PC's distribuidos en varias sedes.</li> </ul>	

## 5.2 HORARIO Y LUGAR DE PRESTACIÓN DE LOS SERVICIOS

El servicio de soporte dedicado de técnicos especialista seguirá el calendario laborable de Madrid Digital. El horario de este servicio será el comprendido dentro de la franja horaria de **lunes a viernes de 08:00 h - 9:00 h a 17:00 h - 18:00 h, los días laborables.**

La Agencia establecerá los turnos necesarios dentro de la franja horaria a la que se hace referencia para la prestación del servicio, sin que ello suponga coste adicional alguno.

No obstante, a petición del *Responsable del Contrato* designado por la Agencia, hasta el 4 % de las horas de servicio referidas podrán exigirse fuera de la franja horaria anteriormente citada.

Será excepción a este criterio **el servicio de soporte que será 24x7x365**, ya descrito

**Madrid Digital requiere el desempeño de estos servicios de forma prioritaria desde las instalaciones del proveedor o en modalidad teletrabajo.** En todo caso, en función de diferentes factores, como, por ejemplo, atención a reuniones que requieran trato directo, de cualquiera de los comités indicados en este contrato o bien, de cualquier otra reunión específica con personal de la Agencia, el lugar de la prestación de los servicios podría fijarse a criterio de Madrid Digital en las instalaciones de Madrid Digital y/o alguna de las dependencias de la Comunidad de Madrid. Este cambio del lugar de la prestación de los servicios deberá notificarse al menos con 24 horas de antelación.

El personal del servicio tendrá disponibilidad para desplazarse puntualmente a los distintos centros dependientes de la Comunidad de Madrid para la ejecución de actividades relacionadas con los servicios objeto del contrato.

Las tareas, planificadas o no, relacionadas con el servicio prestado que requieran realizar trabajos por parte del personal adjudicatario fuera del horario habitual, en sábados o festivos, o en régimen de nocturnidad, no serán objeto de ningún coste o compensación adicional por parte de Madrid Digital.

Todos los gastos ocasionados por los desplazamientos y estancia del personal del contratista durante el cumplimiento del contrato están incluidos en el importe del mismo. Madrid Digital no aceptará costes adicionales por tales causas, que deberán ser asumidos siempre por el contratista.

### **5.3 ACUERDOS DE NIVEL DE SERVICIO – ANS**

El adjudicatario se comprometerá a cumplir unos niveles de calidad mínimos sobre los servicios prestados. Para ello, se establecen los niveles de servicio recogidos a continuación, así como la política de penalizaciones ante incumplimientos de estos ANS, que el adjudicatario estará obligado a aceptar.

Para la definición de los ANS asociados se aplicarán los siguientes conceptos:

**Incidencia:** cualquier evento que comprometa la integridad, confidencialidad o disponibilidad de la información o los sistemas informáticos. Se clasificarán en:

Las incidencias se tipifican según su **impacto** en el servicio en:

- **Impacto Alto:** Indisponibilidad de los endpoint. Es el caso de mayor criticidad que puede tener una incidencia.

Síntomas: Servicio afectado para más del 15% de usuarios.

- **Impacto Medio:** Problema con alguna funcionalidad de los endpoint que no suponga la inoperatividad de los mismos.

Síntomas: Servicio afectado entre un 2% y el 15% de usuarios.



- **Impacto Bajo:** Problemas con alguna funcionalidad de los endpoint sin impacto en los mismos.
- Para cualquier incidencia que no se encuentre dentro de las especificadas anteriormente se describe este síntoma: Servicio afectado para menos del 2% de usuarios.

Asimismo, las incidencias se clasifican según la **urgencia** en:

- **Urgencia Alta:**
  - Departamentos, centros y servicios considerados como críticos dentro de la Comunidad de Madrid (Por ejemplo, los servicios de Emergencias, Urgencias, 112, etc.).
  - Todos los Hospitales de la Comunidad de Madrid, bajo el ámbito de gestión de la Agencia.
  - Algunos proyectos requieren de la disponibilidad del servicio durante alguna de sus fases, y la incidencia en el mismo determina que las incidencias sean calificadas como críticas.
  - Cuando las incidencias afecten al grupo de altos cargos y personal relacionado con los mismos.
- **Urgencia Media:**
  - Todos los servidores, a excepción de los descritos en los sistemas del apartado anterior.
- **Urgencia Baja:**
  - Los puestos de trabajo de los usuarios de la Comunidad de Madrid, a excepción de los mencionados en los apartados anteriores.

**Tabla de Prioridades:** Será responsabilidad de la Agencia calificar la incidencia que se produzca de acuerdo con la siguiente tipología, notificándolo al adjudicatario para que proceda al efecto.

La prioridad de una incidencia se establecerá combinando el Impacto y la Urgencia y se aplicarán los criterios establecidos en la siguiente tabla:

PRIORIDAD		IMPACTO		
		Alto	Medio	Bajo
URGENCIA	Alta	CRÍTICA	ALTA	MEDIA
	Media	ALTA	MEDIA	BAJA
	Baja	MEDIA	BAJA	BAJA

**Tiempos de respuesta de incidencias:** El tiempo de respuesta se define como el tiempo transcurrido entre el momento en que se notifica la incidencia y el momento en que un técnico de la empresa adjudicataria realiza la primera comunicación, según los canales establecidos, informando sobre el análisis de las causas de la incidencia y las acciones correctivas a realizar, con los plazos en los que se llevarán a cabo.

Los tiempos de respuesta se detallan en la tabla siguiente:

PRIORIDAD	TIEMPO MÁXIMO DE RESPUESTA
CRÍTICA	2 horas
ALTA	4 horas
MEDIA	5 horas
BAJA	6 horas

**Nota importante:** Para el cómputo de los tiempos máximos de respuesta se tendrá en cuenta todos los días naturales.

### 5.3.1 Soporte presencial

La determinación del tipo de soporte necesario en cada incidencia se llevará a cabo en función de la prioridad, teniendo la Agencia la posibilidad de exigir soporte presencial al adjudicatario en las incidencias tipificadas como críticas, altas o medias.

El adjudicatario deberá garantizar el soporte presencial de un Ingeniero de Soporte en las instalaciones de la Comunidad de Madrid, si se produce una incidencia tipificada como crítica, alta o media. El horario de atención de este tipo de incidencias será de 24 horas, 7 días a la semana los 365 días del año.

El **tiempo máximo de soporte presencial**, en el que el Ingeniero se presentará en las instalaciones de la Comunidad de Madrid, dependiendo del horario en el que se notifique la incidencia, será el siguiente:

- **De lunes a viernes desde las 8:00 h. hasta las 22:00 h.:** 1 hora para las incidencias críticas y altas, y 2 horas para las incidencias de prioridad media.
- **De lunes a viernes desde las 22:00 h. hasta las 8:00 h. del día siguiente, fines de semana y festivos:** 2 horas para incidencias críticas, 3 horas para alta y 4 para media, según se describe en la tabla adjunta.

En función del servicio descrito y tipificado por nivel de prioridad, el adjudicatario deberá disponer de los medios técnicos y humanos necesarios para garantizar el soporte, tanto presencial como telefónico, a fin de cumplir con los niveles de servicio exigidos.

En el precio del contrato quedan incluidos, en todo caso, los gastos ocasionados para solucionar las incidencias, tales como mano de obra, gastos de desplazamiento y transporte, impuestos, etc.

	TIEMPO DE SOPORTE PRESENCIAL	
	Lunes a viernes de 8:00 h. a 22:00 h.	Lunes a viernes de 22:00 h. a 8:00 h., fin de semana y festivos
CRÍTICA	1 hora	2 horas
ALTA	1 hora	3 horas
MEDIA	2 horas	4 horas
BAJA	N/A	N/A

### 5.3.2 Seguimiento y resolución de incidencias

El adjudicatario informará del orden de las actuaciones a seguir para asegurar la resolución de las incidencias, según los niveles de servicio establecidos en el presente Pliego de Prescripciones Técnicas.

Los técnicos de la Agencia estarán permanentemente informados del estado de la incidencia. Una vez resuelta la incidencia, se documentará e informará con el objeto de verificar la calidad de la solución.

Periódicamente, el responsable técnico designado por el adjudicatario, generará un informe de incidencias producidas con:

- Descripción detallada de la solución aplicada.
- Tiempo de respuesta desde el registro del incidente.
- Tiempo de resolución empleado hasta el cierre del incidente.
- Identificación del personal técnico involucrado por ambas partes.
- Número de horas empleadas en la resolución de incidentes.

Se emplearán los sistemas y procesos establecidos en la Agencia para el registro, seguimiento, gestión y resolución de las incidencias.

SERVICIOS DE SOPORTE TÉCNICO		
TIPO DE SERVICIO	NIVEL DE SERVICIO EXIGIDO	
Incidencias Crítica	Tiempo máximo de respuesta	2 horas
	Tiempo máximo Soporte presencial (lunes a viernes de 8:00 a 22:00 horas, excepto festivos)	1 hora
	Tiempo máximo Soporte presencial (lunes a viernes de 22:00 a 8:00 horas, sábados, domingos y festivos)	2 horas
Incidencias Alta	Tiempo máximo de respuesta	4 horas
	Tiempo máximo Soporte presencial (lunes a viernes de 8:00 a 22:00 horas, excepto festivos)	1 hora



SERVICIOS DE SOPORTE TÉCNICO		
TIPO DE SERVICIO	NIVEL DE SERVICIO EXIGIDO	
	Tiempo máximo Soporte presencial (lunes a viernes de 22:00 a 8:00 horas, sábados, domingos y festivos)	3 horas
Incidentes      Prioridad Media	Tiempo máximo de respuesta	5 horas
	Tiempo máximo Soporte presencial (lunes a viernes de 8:00 a 22:00 horas, excepto festivos)	2 horas
	Tiempo máximo Soporte presencial (lunes a viernes de 22:00 a 8:00 horas, sábados, domingos y festivos)	4 horas
Incidentes      Prioridad Baja	Tiempo máximo de respuesta	6 horas
Rotación equipo de trabajo (No planificada)	El número máximo de sustituciones permitidas será 1 cambio anual.	

## CLÁUSULA 6. MODELO DE GESTION

### 6.1 SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO

La prestación de los servicios solicitados en el presente pliego precisa de un estrecho seguimiento en su desarrollo por parte de Madrid Digital, con objeto de garantizar la correcta ejecución de los mismos, y el cumplimiento de los objetivos del proyecto.

Por ello el adjudicatario deberá nombrar un *Responsable del Servicio* y por parte de Madrid Digital el *Responsable del contrato* designará un *Responsable del Servicio* que se relacionará con el *Responsable del servicio* y el *equipo* del contratista.

La Agencia podrá revisar y ajustar el Modelo de Seguimiento en cualquier momento durante la vida del contrato, siempre con el objetivo de obtener alguna mejora en su ejecución. El contratista podrá proponer a la Agencia modificaciones al modelo (procedimientos, plantillas, herramientas, etc.) con el objetivo de mejorar la eficiencia y la calidad del servicio. Cualquier cambio en los procedimientos vigentes necesitará la aprobación por parte de Madrid Digital.

La Agencia distingue los siguientes niveles en el modelo de seguimiento:

- **Nivel Estratégico, de Dirección:** en el que se realiza el seguimiento y control de los aspectos contractuales, del cumplimiento y consecución de hitos del proyecto y de la gestión de sus riesgos.

- **Nivel Táctico y Operativo:** en el que se realiza el seguimiento, el control y la coordinación de las actividades a realizar al amparo del objeto del contrato, en su día a día.

Asociados a estos niveles de seguimiento, se configuran los siguientes Comités:

- **Nivel Estratégico – Comité de Dirección del Contrato.**
- **Nivel Táctico y Operativo – Comité de Operación del Contrato**

La composición y funciones de cada comité se indican a continuación.

#### **6.1.1 Comité de Dirección del Contrato**

El Comité de Dirección del Contrato estará compuesto por el Responsable del Contrato y el Responsable del Servicio objeto del contrato de Madrid Digital, y las figuras que estos definan al respecto, y por parte del adjudicatario, el Responsable del Servicio y quien él determine, siempre que sea parte del equipo de trabajo.

Las funciones de este Comité serán, entre otras, las siguientes:

- Monitorizar el avance global de los servicios.
- Aprobar los cambios propuestos en el seno del Comité Táctico y Operativo que afecten de forma horizontal a diferentes ámbitos de servicio, procesos de gestión o que, por su impacto o importancia estratégica, requieran la aprobación del Comité.
- Impulsar y promover el proyecto en cada una de las áreas implicadas.
- Controlar y garantizar que todos los trabajos se ejecutan y ajustan a los niveles de calidad requeridos por la Agencia.
- Asegurar que la ejecución del proyecto se ajusta al marco contractual.
- Hacer un seguimiento periódico del grado de avance del proyecto, haciendo especial hincapié en los hitos establecidos.
- Tomar las decisiones que sean necesarias para facilitar la consecución de los objetivos del proyecto (contenido y plazos).
- Determinar la medición del nivel de servicio conforme a los ANS establecidos, de los que derivarán las correspondientes penalidades en los casos de incumplimiento.
- Acordar la adopción de propuestas de mejora y medidas correctoras o preventivas que deba desarrollar e implantar el adjudicatario, previa autorización de Madrid Digital, en caso de incumplimiento de los ANS o derivadas de planes de mejora.
- Revisar y resolver cualquier incidencia o problema relacionado con la facturación de los servicios.
- Cualquier otro asunto que el propio Comité considere de interés.

El Comité de Dirección del Contrato se celebrará con la periodicidad que él mismo determine o, en ausencia de otras indicaciones al respecto, a propuesta del Responsable del Contrato de Madrid Digital.

Los acuerdos adoptados en el seno de este comité deberán ser de mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones. El adjudicatario será responsable de la elaboración de las actas y su traslado a revisión por los asistentes en las 48 horas siguientes a la finalización del Comité; la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y la presentación del acta definitiva para la firma de los asistentes.

### **6.1.2 Comité de Operación**

El Comité de Operación estará formado por el Responsable del Servicio de Madrid Digital, y las figuras que éste defina al respecto, y por parte del adjudicatario, asistirá el Responsable del Servicio designado y las personas del equipo de trabajo que él decida.

Las funciones de este Comité serán, entre otras, las siguientes:

- Seguimiento y evaluación del progreso de los trabajos objeto del contrato, tareas y actividades del proyecto y evaluación de sus riesgos.
- Garantizar que el personal asignado por el contratista para la ejecución de los servicios está disponible y cuenta con los medios, formación y soporte necesarios para la correcta ejecución de sus tareas.
- Verificar el cumplimiento de los requisitos establecidos para la prestación del servicio y revisar el cumplimiento de los acuerdos de nivel de servicio (ANS).
- Analizar y validar, si procede, las propuestas de mejora del servicio efectuadas por el adjudicatario. En caso de que las propuestas afecten de forma horizontal a varias fases del proyecto, o tengan impacto o importancia estratégica, serán elevadas al Comité de Dirección del Contrato.
- Cualquier otro asunto que el propio Comité considere de interés.

Los acuerdos adoptados en el seno del Comité deberán serlo por mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones. El adjudicatario será responsable de la elaboración de las actas y su traslado a revisión por los asistentes en las 48 horas siguientes a la finalización del Comité; la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y la presentación del acta definitiva para la firma de los asistentes.

### **6.1.3 Responsable del Servicio**

Además del equipo adscrito a la ejecución del servicio, el contratista designará un *Responsable del Servicio* ante Madrid Digital.

El primer día de ejecución del contrato, el adjudicatario designará un Responsable de Servicio ante Madrid Digital.

Este responsable se encontrará en permanente contacto con el personal que la Dirección de Madrid Digital designe, a los efectos que se señalan en la cláusula correspondiente del Pliego de Cláusulas Administrativas.

El adjudicatario, a través del *Responsable del Servicio*, y con la periodicidad que en cada fase del mismo Madrid Digital determine, informará sobre la planificación de trabajos, el estado de ejecución del contrato y, en su caso, sobre las incidencias producidas.



En particular, este responsable realizará, entre otras, las siguientes tareas:

- Coordinar el apoyo técnico y la formación necesaria que el adjudicatario suministrará al equipo humano que realice los servicios objeto del contrato, en todas aquellas materias que sean necesarias para el perfecto desempeño de dichos trabajos.
- Impartir, con exclusividad, instrucciones específicas sobre el trabajo a realizar al personal que el adjudicatario adscriba a la ejecución del contrato, siempre teniendo en cuenta la base de las instrucciones genéricas que se desprendan de lo establecido en el presente Pliego y encaminadas al buen término del servicio.
- Supervisar y controlar el trabajo y las actividades realizadas, e informar a Madrid Digital de las posibles incidencias y seguimiento o desviaciones de plazos.
- Ejercer el mando y el poder organizativo sobre el equipo humano del adjudicatario destinado a atender los servicios objeto del presente contrato, que estará siempre bajo la disciplina laboral y el poder de dirección del adjudicatario, con independencia de que, para el mejor cumplimiento del servicio, en determinados momentos, pueda el adjudicatario destacar personal del equipo prestador del servicio en cualquier centro de trabajo, oficinas o ubicaciones de la Comunidad de Madrid.
- Informar a Madrid Digital, con la periodicidad que ésta defina, sobre el estado de ejecución del contrato y, en su caso, sobre las incidencias producidas.
- Mantener con el *Responsable del Contrato* designado por Madrid Digital reuniones periódicas de seguimiento del contrato y de los trabajos realizados.

## **6.2 CONDICIONES GENERALES APLICABLES AL EQUIPO DE TRABAJO**

El adjudicatario asumirá la organización de los trabajos contratados, dentro del marco fijado por la Agencia, y, por tanto, ejercerán el poder organizativo y de dirección de los recursos humanos que constituyan el equipo prestador del servicio, para el cumplimiento de los fines que se le encomiendan. Para tal fin, los adjudicatarios designarán un Responsable del Servicio ante Madrid Digital, que tendrá una visión completa del servicio y se responsabilizará de su gestión y coordinación.

El equipo de trabajo ofertado deberá estar formado por personal técnico con capacitación suficiente para el desarrollo de los trabajos descritos en el presente pliego. Asimismo, contarán con la formación, categoría profesional y nivel de especialización adecuados.

El primer día de ejecución del contrato, el adjudicatario, aportará **Currículum Vitae** de las personas propuestas para la ejecución del contrato, siguiendo el modelo definido en el apartado **7.33 MODELO DE CURRÍCULUM VITAE DEL EQUIPO PRESTADOR DEL SERVICIO**, que detalle sus datos profesionales (Categoría profesional, titulación, formación y experiencia), así como toda aquella documentación que Madrid Digital estime necesaria para la acreditación de los datos contenidos en dichos Currículos.

Una vez iniciada la ejecución del contrato y por motivos debidamente justificados, Madrid Digital podrá solicitar la sustitución, sin coste adicional, de los recursos asignados a la ejecución del contrato, debiendo realizarse en el plazo de un mes desde su solicitud.

Además, el adjudicatario deberá garantizar que dispone de los mecanismos adecuados para minimizar la rotación no planificada de los recursos puestos a disposición para el contrato, y así evitar la pérdida no controlada de conocimiento, el impacto en los niveles de servicio y la dedicación adicional de personal de Madrid Digital que estas situaciones suelen llevar asociadas. Se establece un número máximo de sustituciones no planificadas de **1 recurso al año** durante la ejecución del contrato. A los efectos de su cómputo, no se tendrán en cuenta las modificaciones en el equipo que sean consecuencia de incapacidad temporal o permanente del recurso sustituido.

Se denomina **rotación planificada** a aquella que se comunica antes de que se produzca y resuelve dentro de un plazo máximo de tiempo de **dos meses**, y se acompaña de un **solapamiento** del recurso saliente con el entrante para la adecuada transferencia de conocimiento durante **un periodo de un mes natural**. Si Madrid Digital lo estimara conveniente, dicho plazo podrá reducirse. Esta transferencia de conocimiento será responsabilidad del Adjudicatario y sin coste alguno para Madrid Digital.

El Adjudicatario debe garantizar durante toda la vida del contrato que dispone de los mecanismos adecuados para minimizar la **rotación no planificada** del personal que compone el **Equipo**, para evitar la pérdida no controlada de conocimiento y el impacto en los niveles de servicio, imagen, dedicación adicional de Madrid Digital, etc. que esta situación suele llevar asociada.

El **procedimiento para gestionar una rotación planificada** es el siguiente:

#### **A. Solicitud del Cambio**

Madrid Digital podrá solicitar el cambio de uno de los recursos, si existen razones justificadas que lo aconsejen.

Si es el Adjudicatario el que propone el cambio de uno de los recursos, deberá solicitarlo por escrito, aportando una justificación detallada y suficiente, explicando el motivo que lo ocasiona.

En este mismo momento el Adjudicatario podrá ya presentar a Madrid Digital posibles sustitutos que cubran los requisitos mínimos establecidos para el perfil que corresponda con el objeto de sustituir al componente del **Equipo**.

En cualquier caso, la presentación del componente alternativo deberá realizarse en menos de **una semana desde la solicitud de cambio**.

#### **B. Aprobación del Cambio**

Madrid Digital comprobará que la alternativa propuesta cumple los requisitos establecidos y procederá a aprobar la rotación, o rechazarla si no cumpliera dichos requisitos.

En el **plazo máximo de 1 semana**, a contar desde la fecha de la presentación, debe haberse aprobado por parte de Madrid Digital o solicitar nuevas opciones. En este caso, se estaría en el paso anterior.

#### **C. Incorporación**

Tras la aprobación, se dispone de un periodo de dos semanas naturales para su incorporación.

#### **D. Periodo de Solapamiento**

Durante el periodo de solapamiento, de duración no inferior a un mes, se debe realizar la adecuada transferencia de conocimiento hasta asegurar una correcta adquisición del mismo que asegure una buena prestación del servicio.

#### **E. Validación y Aceptación**

Finalizado el periodo de solapamiento, Madrid Digital debe validar y formalizar explícitamente la aceptación/denegación definitiva del recurso al **Equipo**. El proceso contemplará la revisión de las condiciones en las que se ha ejecutado la rotación para determinar el nivel de cumplimiento de los indicadores definidos al respecto.

Asimismo, durante todo el plazo de ejecución del contrato, el adjudicatario deberá mantener los niveles de calidad del servicio objeto del mismo, por lo que deberá instrumentar los servicios de suplencia que estime oportunos, que serán cubiertos siempre con el mismo personal suplente, a los efectos de ocasionar el mínimo impacto en la prestación del servicio.

### **6.3 DOCUMENTACIÓN DE LOS SERVICIOS**

El adjudicatario deberá entregar, como parte de los trabajos objeto del contrato, toda la documentación generada durante la ejecución del contrato. Esta documentación será propiedad exclusiva de Madrid Digital sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de Madrid Digital.

Toda la documentación se entregará en castellano en el soporte electrónico que se acuerde para facilitar el tratamiento y reproducción de los mismos.

El adjudicatario deberá suministrar a Madrid Digital las nuevas versiones de la documentación que se vayan produciendo. También se entregarán, en su caso, documentos de trabajo previos, informes de referencia, etc. en idéntico soporte a los anteriores.

Madrid Digital supervisará la calidad de todos los trabajos entregados.

Toda la documentación generada deberá ser remitida al equipo designado de Madrid Digital para su validación antes de que se considere como finalizada. El adjudicatario completará las carencias detectadas y corregirá los defectos que le sean notificados por Madrid Digital como condición previa a la aprobación de cada entregable.

El modelo de documentación, si no se indica uno expreso, se acordará con el equipo designado de Madrid Digital. Los entregables deberán ajustarse, en formato y contenido mínimo, a lo indicado por Madrid Digital, y deberán ser aportados en formato electrónico.

Se contará con una carpeta digital de documentación, adecuadamente estructurada, en la que se recopilará toda la información relativa a la realización de los trabajos. La carpeta contará con un índice estructurado temáticamente que permita localizar fácilmente la documentación disponible de forma integral.

### **6.4 DISPONIBILIDAD DE MEDIOS**

En relación a los medios que el equipo de trabajo del proveedor requiera para desarrollar los trabajos objeto del contrato, todos ellos serán provisionados y gestionados por el proveedor, incluido el pc



puesto de trabajo, con todas las licencias requeridas de software ofimático, servicios de correo, entornos de colaboración, conexión a Internet, acceso vpn, etc.

Para las reuniones que se realicen de manera virtual, Madrid Digital emplea la herramienta colaborativa de Microsoft TEAMS, herramienta que también se usa para trabajo colaborativo. Debido a ello, es necesario que el adjudicatario cuente con las licencias pertinentes para su utilización.

Por cuestiones de ciberseguridad de las redes y sistemas de Madrid Digital, el adjudicatario deberá responsabilizarse que los puestos de su equipo de trabajo, contemplen las siguientes medidas de seguridad de manera obligatoria:

- Sistema operativo con versión de parcheado de seguridad permanentemente actualizado.
- Software de protección antimalware actualizado y supervisado 24x7, con capacidades de prevención, detección y respuesta ante amenazas e incidentes de seguridad, todo ello garantizado por la empresa adjudicataria y sus servicios de ciberseguridad.

La información, documentación, que se genere durante la ejecución de los servicios objeto de este pliego técnico será en formato Microsoft365. Las licencias que a tal efecto requiera el adjudicatario para sus empleados, serán provisionadas por su parte y, en consecuencia, sin coste para Madrid Digital.

En todo lo relativo a conectividad de los equipos de trabajo del proveedor y necesidades de acceso remoto a la sede de Madrid Digital y/o a los CPDs incluidos dentro del alcance de este pliego técnico, se seguirá lo indicado en el apartado **7.2 REQUISITOS PARA ACCESO REMOTO DE PROVEEDORES**.

## **CLÁUSULA 7. INFORMACIÓN RELEVANTE PARA LOS LICITADORES**

### **7.1 ENTORNO TECNOLÓGICO**

El entorno tecnológico sobre el que se prestarán los servicios definidos en el pliego es el siguiente:

SISTEMAS OPERATIVOS	
Servidor	Red Hat, SUSE, CentOS, Ubuntu, Oracle Linux, Debian, Windows
Puesto ofimático	Windows, MacOS
Dispositivos móviles	Android, IOS

Todos los puestos de usuario están homologados y estandarizados mediante imágenes denominadas **POBs**, puesto ofimático básico, que contiene los programas de software y la configuración definida como estándar para los usuarios de la Comunidad de Madrid. La mayoría de los equipos disponen de Microsoft Windows 10 y Windows 11 como sistema operativo, quedando algunos equipos con versiones Windows 8.1.

La gestión centralizada de estos equipos se realiza mediante Microsoft System Center y políticas de Directorio Activo, así como las consolas de administración propias de Cytomic EPDR.

Madrid Digital notificará puntualmente cualquier evolución tecnológica en sus sistemas que pueda afectar a los servicios objeto del contrato.

## **7.2 REQUISITOS PARA ACCESO REMOTO DE PROVEEDORES**

El servicio de conectividad entre la empresa adjudicataria y la Comunidad de Madrid se considerará incluido dentro del servicio prestado por el adjudicatario y seguirá las siguientes premisas:

- El adjudicatario será responsable de dar adecuada conectividad a sus trabajadores para poder ejecutar el contrato, esto incluye las necesidades de conexión a internet, acceso a correo electrónico, aplicaciones corporativas, accesos VPN, etc.
- El adjudicatario realizará los controles necesarios para asegurar que los accesos a través de su línea de comunicaciones a los CPDs de la Comunidad de Madrid son realizados por los usuarios y máquinas debidamente autorizados.
- En consecuencia, el adjudicatario deberá proporcionar un acceso seguro a su propia red (VPN, extensión de VLAN etc.), de manera que, a los efectos de acceso a los recursos situados en los CPD de la Comunidad de Madrid, cualquier tipo de empleado que se conecte, por cualquier medio y desde cualquier ubicación, aparezca como un usuario del equipo de trabajo y con un direccionamiento IP compatible con el rango reservado por Madrid Digital al contrato del adjudicatario.
- Los trabajadores del adjudicatario que presten sus servicios en edificios de la Comunidad de Madrid no estarán directamente conectados a la red corporativa, sino que, de forma lógica, se encontrarán en un segmento de red que se considera una extensión de la red de su empresa.
- Independientemente de la ubicación de los empleados del adjudicatario, para el acceso lógico a los distintos entornos de la Comunidad objeto del contrato usarán el servicio de conectividad descrito en este apartado.
- Los usuarios que trabajen en las instalaciones de la Comunidad de Madrid dispondrán de un direccionamiento IP en una red diferenciada, asignado por Madrid Digital.
- El adjudicatario debe ofrecer directamente a sus empleados desplazados en sedes de la Comunidad de Madrid los siguientes servicios mínimos, para los que Madrid Digital asignará otro rango IP diferenciado:
  - Servicio de nombres (DNS), en el caso de que los trabajadores en las instalaciones de Madrid Digital deban acceder a servicios locales a su empresa. Este servicio de nombres servirá para acceder a los recursos ubicados en los CPD de la Madrid Digital o a los servicios digitales ofrecidos por su empresa. Para ello, la empresa deberá proporcionar servidores de nombres (DNS), bien haciendo *forwarding DNS* para los dominios que Madrid Digital determine (si el direccionamiento es compatible con el de la red de la empresa), bien publicando dichos nombres en la red interna mediante técnicas de NAT. En el caso de que no sea preciso acceder por nombre a servicios de su empresa, los puestos de trabajo del adjudicatario podrán utilizar los servidores DNS proporcionados por Madrid Digital.
  - Proxy de navegación a internet, con el fin de que puedan acceder a internet a través de la conectividad entre el CPD de Madrid Digital y las instalaciones del adjudicatario.

- Servicio de correo electrónico, vía webmail u otras direcciones IP del rango reservado
- El adjudicatario pondrá en marcha una conexión dedicada desde su empresa a CPDs de la Comunidad de Madrid, contratada y sufragada por la empresa adjudicataria. La comunicación podrá realizarse mediante línea punto a punto o RPV-IP sobre red de operador, siempre que garantice que los datos que transiten por dicha conexión no son accesibles por terceros. En consecuencia, en los CPDs de la Comunidad de Madrid se instalarán dos equipos ajenos a Madrid Digital, que entregarán el tráfico a/desde la empresa adjudicataria en interfaces Ethernet en los conmutadores de red de Madrid Digital.
- La compatibilidad de direccionamiento (mediante NAT), si fuera necesaria, se realizará en los equipos del adjudicatario que empiezan y terminan la línea dedicada.
- Para la conexión de personal externo desde sedes de la Comunidad de Madrid a sistemas de información de la Comunidad o a su propia empresa, el adjudicatario deberá instalar, a su cargo, una conexión dedicada en configuración de alta disponibilidad (doble línea, doble equipo) desde la empresa prestadora a cada una de las sedes de la Comunidad de Madrid. Al igual que en el caso de la conexión con el CPD, la comunicación puede realizarse mediante línea punto a punto o RPV-IP sobre red de operador siempre que garantice que los datos que transiten por dicha conexión no son accesibles por terceros. En consecuencia, en las sedes de la Comunidad de Madrid se instalarán dos equipos ajenos a Madrid Digital, que entregarán el tráfico a/desde la empresa adjudicataria en interfaces Ethernet en los conmutadores de red de Madrid Digital.
- Caudales de la conexión con la empresa: el necesario en cada sentido para la prestación de los servicios objetos del contrato.
- Respecto a los trabajadores del adjudicatario que presten sus servicios en edificios de la Comunidad de Madrid descritos anteriormente, el adjudicatario será responsable de proporcionar por sus propios medios la conectividad entre su segmento de red, los servicios y herramientas de su empresa necesarias para su trabajo, y la conexión dedicada con el CPD citada anteriormente.
- En consecuencia, los trabajadores de la empresa prestataria, ya estén ubicados en instalaciones de la misma o en instalaciones de la Comunidad de Madrid, se conectarán siempre a través de un punto de entrega en un CPD de la Comunidad de Madrid, desde donde podrá acceder a los sistemas de información necesarios para realizar su trabajo.
- La responsabilidad de Madrid Digital con este equipo es:
  - Ofrecer la conectividad física de los equipos a los conmutadores LAN de la sede de la Comunidad de Madrid objeto del contrato para poder alcanzar al router de salida del adjudicatario que conecta con la sede de su empresa (ya sea mediante una línea dedicada o mediante un servicio RPV-IP contratado por dicha empresa).
  - Servicio de DHCP para asignar a cada puesto de trabajo del Adjudicatario en la sede de la Comunidad de Madrid objeto del contrato una dirección IP dentro del rango reservado al Adjudicatario. En su caso, la empresa adjudicataria deberá informar de los servidores DNS que desea que se entreguen a estos puestos.



### **7.2.1 Equipo de trabajo en instalaciones de la empresa adjudicataria**

Este equipo de trabajo se encontrará físicamente en las instalaciones y en la red de la empresa adjudicataria del contrato.

Dicha empresa deberá tener una línea punto a punto dedicada, del caudal y simetrías necesarios que termine en el CPD de Madrid Digital.

Todos los usuarios que estén en este emplazamiento usarán los servicios que la empresa adjudicataria estime oportuno para la ejecución de su trabajo en la propia red de la empresa (acceso Internet, DNS, correo, ERP, etc.).

### **7.2.2 Equipo de trabajo en las instalaciones de Madrid Digital**

En el caso de que Madrid Digital determine que el equipo, o parte del equipo, deben estar físicamente en las instalaciones de Madrid Digital, lógicamente se encontrarán en una extensión de la red de su empresa, en un segmento de red completamente aislado al del resto de trabajadores de la Comunidad de Madrid y al de otras empresas adjudicatarias.

El adjudicatario necesitará una conexión dedicada con cada una de las sedes de Madrid Digital donde estén ubicados los equipos de trabajo del caudal y características requeridos. Madrid Digital indicará el equipo de dicha ubicación en el que terminará la conexión dedicada.

La responsabilidad de Madrid Digital con este equipo es:

- Ofrecer la conectividad física de los equipos a los conmutadores LAN de la sede de Madrid Digital para poder alcanzar al router de salida del adjudicatario que conecta con la sede de su empresa (ya sea mediante una línea dedicada o mediante un servicio RPV-IP contratado por dicha empresa).
- Servicio de DHCP para asignar a cada puesto de trabajo del adjudicatario en la sede de Madrid Digital una dirección IP dentro del rango reservado al adjudicatario.

### **7.2.3 Equipo de trabajo remoto**

Este equipo de trabajo se encontrará físicamente en cualquier punto distinto de los anteriormente mencionados y en una red externa a la del adjudicatario del contrato o de Madrid Digital.

El adjudicatario deberá proporcionar un acceso seguro a su propia red (VPN, extensión de VLAN etc.), de manera que a los efectos de acceso a los recursos situados en los CPD de la Agencia aparezcan como un usuario más del equipo de trabajo en las instalaciones de la empresa. La compatibilidad de direccionamiento (mediante NAT) se realizará en los equipos que empiezan y terminan la línea dedicada si fuera necesario.

### **7.2.4 Informes de monitorización de las líneas de comunicaciones**

El adjudicatario deberá realizar informes de monitorización de línea. Dicho informe debe contener como mínimo para cada una de las líneas, información relativa a tráfico, latencia y pérdida de paquetes.

Igualmente, el adjudicatario realizará los controles necesarios para asegurar que los accesos a través de su línea de comunicaciones al CPD de Madrid Digital son realizados por los usuarios y máquinas debidamente autorizados.

Los informes se generarán con una periodicidad determinada al inicio del contrato y deberán estar a disposición de Madrid Digital para cuando le sea necesario. Adicionalmente, se generarán puntualmente cuando se requiera para asegurar la continuidad del servicio.

### **7.3 MODELO DE CURRÍCULUM VITAE DEL EQUIPO PRESTADOR DEL SERVICIO**

(A aportar para cada miembro del equipo propuesto)

<b>APELLIDOS:</b>	
<b>NOMBRE:</b>	
<b>CATEGORÍA PROFESIONAL:</b>	
<b>TTITULACIÓN / UNIVERSIDAD o CENTRO / HOMOLOGACIÓN (en caso de haberse obtenido la titulación fuera de España):</b>	
<b>FORMACIÓN:</b>	
<b>EXPERIENCIA – ACTIVIDAD PROFESIONAL (Especificando como mínimo: Empresa, duración del proyecto, descripción del mismo y actividades desarrolladas y cliente para el que se ejecuta):</b>	

El adjudicatario deberá aportar este documento, debidamente cumplimentado y firmado por la persona que ostente la representación de la empresa, para cada uno de los miembros del Equipo propuesto, indicando el perfil al que se adscribe, así como toda aquella documentación que Madrid Digital estime necesaria para la acreditación de los datos contenidos en dichos Currículos.

### **CLÁUSULA 8. CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS**

Durante el periodo de presentación de la oferta y, ante cualquier duda o necesidad de aclaración referida a las especificaciones del Pliego de Prescripciones Técnicas, el licitador podrá dirigirse a:

Agencia para la Administración Digital de la Comunidad de Madrid

Subdirección General de Ciberseguridad, Protección de Datos y Privacidad

E-mail: [md\\_seguridad\\_sistemas@madrid.org](mailto:md_seguridad_sistemas@madrid.org)

***La Subdirectora de la Subdirección General de Ciberseguridad,  
Protección de Datos y Privacidad***

Firmado digitalmente por: MUÑOZ FUENTES ESTHER  
Fecha: 2025.07.18 11:37

***Fdo.: Esther Muñoz Fuentes***