

Este documento es una traducción al castellano de la Memòria Justificativa que regirá la contratación de la renovación de las suscripciones de la herramienta de monitorización Dynatrace para la Diputación de Tarragona. En caso de discrepancias entre la versión en catalán y la versión traducida, prevalecerà la versión original en catalán.

RENOVACIÓN DE LAS SUSCRIPCIONES DE LA HERRAMIENTA DE MONITORIZACIÓN DYNATRACE PARA LA DIPUTACIÓN DE TARRAGONA

Pliego de Prescripciones Técnicas

ÍNDICE DE CONTENIDOS

<u>1.</u>	<u>OBJECTO DEL CONTRATO</u>	3
<u>2.</u>	<u>ESPECIFICACIONES</u>	3
<u>3.</u>	<u>SERVICIO DE SOPORTE</u>	6

1. OBJETO DEL CONTRATO

En el año 2019 se empezó a monitorizar el rendimiento de las aplicaciones de plataforma Actio con el fin de garantizar la disponibilidad y la adecuación de los tiempos de respuesta proporcionados mediante la implantación de la herramienta Dynatrace.

Esta herramienta proporciona las funcionalidades necesarias para poder garantizar la monitorización de los tiempos de respuesta de las aplicaciones informáticas, extracción de indicadores de errores y excepciones y gestión proactiva de posibles incidencias con las aplicaciones y servicios monitorizados.

Actualmente, la Diputación de Tarragona dispone de una suscripción de 40 *host unidos* para monitorizar diferentes servidores (cada *host unit* cubre 16 GB de RAM de servidores). Con el aumento de la carga de usuarios y aplicaciones que soportan estas máquinas, se hace necesario adquirir más *host unidos* para poder continuar monitorizando los servicios actuales, así como nuevos servicios que desde la dirección del área de IT se quieren monitorizar de forma continuada, aparte de la plataforma Actio. Además, también se quiere renovar las licencias de tipo *application security units* que permiten monitorizar las vulnerabilidades de seguridad detectadas en los diferentes servidores de aplicaciones monitorizados.

Así pues, el objeto de este contrato es el de renovar las suscripciones de las 40 *host unidos* de que disponemos, de adquirir 5 más hasta un total de 45 *host unidos*, renovar las 29 licencias de tipo *application security unidos* de que disponemos; y finalmente renovar 300.000 *Digital Experience Monitoring (DEM) unidos*.

2. ESPECIFICACIONES

El precio del licenciamiento deberá tener en cuenta los siguientes requerimientos:

- Suscripción para 45 *host unidos*, donde cada *host unido* cubre 16 GB de RAM de servidores.
- 1. Suscripción según A 29 *unidades de seguridad de aplicaciones*.
- 1. Suscripción para 300.000 *Digital Experience Monitoring unidos*.
- Instalación e instrumentación automatizada
 - o Deberá permitir el despliegue automatizado que autodescubra automáticamente los procesos y servicios que se ejecutan en el servidor donde el agente esté desplegado, así como las conexiones y dependencias entre ellos. El sistema operativo soportado deberá ser Red Hat Enterprise Linux.
 - o Los agentes deben reconocer e instrumentar los procesos correspondientes a servidores web (Apache, IIS, NGINX) y a tecnologías Java, PHP, Node.js, .NET., así como otros no instrumentables que se ejecuten en el servidor y que consuman recursos y puedan interferir en el rendimiento de la aplicación.
 - o Instrumentación de la capa cliente: agentes en el navegador, así como aplicaciones nativas móviles (Android y iOS), que capturen las sesiones de usuario y sus acciones en la aplicación.

- o Los agentes deben monitorizar la infraestructura de forma automática, monitorizando la CPU, memoria, red y los discos de cada servidor.
- o El agente detectará automáticamente contenedores e instrumentar los procesos y servicios contenidos en.
- o El agente debe poder desplegarse de forma automática en entornos Cloud (Azure y Amazon Web Services) teniendo en cuenta los componentes específicos de cada proveedor del servicio en la nube en el rendimiento.
- o Análisis de logs: el agente debe monitorizar los logs del sistema y aplicaciones, detectando errores y patrones de problemas. Estos patrones deben ser configurables y personalizables para agregar casuísticas en base a expresiones regulares.
- Monitorización profunda del rendimiento de aplicaciones
 - o Visibilidad completa y operacional a través de todas las capas tecnológicas. La solución debe ser capaz de entender y visualizar la información de monitorización independientemente de las tecnologías utilizadas
 - o Visualización detallada de la topología. Los procesos que se ejecutan en cada servidor, los servicios que utilizan los procesos y las aplicaciones que utilizan los servicios descubiertos, así como las interrelaciones entre ellos y sus dependencias. Se debe poder navegar gráficamente por la topología de los componentes citados y ver sus conexiones y dependencias.
 - o Análisis de infraestructura. La solución debe poder monitorizar con precisión las siguientes métricas de infraestructura:
 - CPU: se debe conocer en todo momento el estado de la CPU del servidor y la relación de procesos que están consumiendo CPU y en qué cantidad
 - Memoria: se debe conocer en todo momento el empleo de memoria del servidor y los procesos que están consumiendo la memoria y en qué cantidad. También se mostrarán las páginas fallidas de memoria del servidor
 - Ocupación de la red: se debe conocer en todo momento el uso de las diferentes interfaces de red de que disponga el servidor donde se desplieguen los agentes. Se debe conocer por proceso e interfaz:
 - El nivel de conectividad: si hay errores de red o no, siendo el 100% el nivel óptimo de conectividad
 - Cantidad del tráfico: volumen de tráfico consumido en las unidades correspondientes (Kbit/s, bit/s, ...)
 - Retransmisiones: porcentaje de retransmisiones
 - Además, a nivel de interfaz hay que conocer:
 - o Los paquetes perdidos
 - o Los paquetes enviados / recibos
 - o El ancho de banda nominal de cada interfaz
 - Discos: debe conocerse en todo momento el uso de los discos con las siguientes métricas:
 - *Throughput*
 - IOPS
 - Latencia
 - Espacio utilizado
- 1. Análisis de procesos. Los procesos en ejecución de cada servidor deben ser detectados y aquellos que puedan ser instrumentados por ser de una tecnología soportada mostrando las métricas relevantes de cada tecnología (Worker Process, Métricas de JVM o CLR, etc.)

- o Análisis de servicios. Los servicios deben ser autodetectados, así como su relación con los procesos que los sustentan. Se debe conocer en todo momento el número de invocaciones de cada servicio, si es invocado o invocador desde otros servicios, la topología de cada servicio, así como los principales contribuidores al tiempo de respuesta del servicio.
- o Análisis de Aplicaciones. Hay que conocer en todo momento el estado de la aplicación tanto a nivel topológico (qué servicios, procesos la forman, etc), así como a nivel de métricas. Conociendo, como mínimo:
 - Número de peticiones
 - Tiempo medio de respuesta
 - Porcentaje de usuarios Reales / Robots
 - Navegador más utilizado
 - Acciones más utilizadas
 - Análisis por localización geográfica
 - Acciones más utilizadas por los usuarios
- Análisis de problemas
 - o Detección automatizada de problemas y anomalías. La solución debe ser capaz de detectar problemas de diferente tipo de forma automática:
 - Problemas de disponibilidad: indisponibilidad de aplicaciones, servicios, etc.
 - Errores: errores en aplicaciones, servicios, procesos o infraestructura
 - Lentitud: problemas derivados del tiempo de respuesta en aplicaciones y servicios
 - Problemas de recursos
 - o Los problemas deben ser detectados de forma automática, sin establecer patrones ni umbrales, en base a *baselinas* multidimensionales y patrones de comportamiento. La detección de problemas debe incluir de forma automática:
 - Duración del problema
 - Usuarios afectados (si procede)
 - Invocaciones a servicios afectados
 - Aplicaciones afectadas
 - Descripción del problema
 - o Detección automática de la causa raíz. La solución debe ser capaz de detectar de forma automatizada la causa a raíz de los problemas (en los casos en que aplique) en base a las interdependencias entre componentes detectados por los agentes de forma automática y basándose en árboles de resolución para automáticamente indicar cuál es la causa raíz y los componentes afectados.
 - o Evitar recibir *spam* de alertas. El informe de problemas debe ser inteligente y evitar que las múltiples alertas que están relacionadas con un único problema aparezcan de forma individualizada y sin correlación. La solución debe ser lo suficientemente inteligente para agrupar las alertas relacionadas con una anomalía con un único problema, evitando así el llamado *Alert Spam*.
- Las suscripciones activas caducan el **19/07/2026**, por lo tanto habrá que tener en cuenta que éstas deberán renovarse por un periodo de **1 año** a partir de esa fecha o la fecha de formalización del contrato, si ésta es posterior al 20/07/2026. En cuanto a las nuevas suscripciones de *host unidos*, éstas deberán activarse en las mismas fechas. El cuadro resumen de tipos de licencias a renovar es el siguiente:

Producto	Licencias
Perpetual Host Units (Renovación)	5
Concurrent Host Units (Renovación)	35
Concurrent Host Units (Subscripción Nova)	5
DEM Units (Renovación)	300.000
APPSec Units (Renovación)	29

3.

SERVICIO DE APOYO

Las condiciones que deberá cumplir el servicio de soporte técnico incluido en la suscripción son las siguientes:

- Activación de la solución al servicio de soporte técnico del fabricante, facilitando a la Diputación de Tarragona el procedimiento a seguir para la apertura y seguimiento de incidencias y consultas hasta su cierre.
- Servicio de apoyo técnico y mantenimiento durante, como mínimo doce (12) meses con disponibilidad y acceso al personal de apoyo durante 24 horas al día, 7 días a la semana, 365 días al año, prioridad en las llamadas y gestión de casos. Acceso a técnicos cualificados para ayudar a la resolución de:
 - o Problemas de producto: dudas de funcionamiento, actualizaciones de versiones, información de errores conocidos, etc.
 - o Problemas de sistema: asesoramiento en parametrización, comprobación de logs, sugerencias de administración, etc.
- Acceso al portal de clientes con la información más reciente sobre productos, documentación, parches y preguntas más frecuentes.
- Suministro y operativa de las actualizaciones de software a versiones posteriores que surjan durante el periodo de vigencia del servicio de mantenimiento.
- Escalado al fabricante: gestión de las incidencias y escalado de aquellas que lo requieran al fabricante responsable del mantenimiento.
- Todas las actualizaciones que se realicen amparadas bajo el contrato de apoyo y mantenimiento por parte del adjudicatario serán realizadas por técnicos debidamente calificados por el fabricante de la solución.