

**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA RENOVACIÓN DEL SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO Y LA AMPLIACIÓN DE LA HERRAMIENTA DE PROTECCIÓN DE CORREO, DE SERVIDORES Y DE CLIENTES ACTUALMENTE EN SERVICIO EN EL GRUPO TRAGSA, A ADJUDICAR POR PROCEDIMIENTO ABIERTO SUJETO A REGULACIÓN ARMONIZADA.**

**REF: TSA000074479**

Los requisitos a continuación enumerados deben entenderse como **mínimos** pudiendo los licitadores ampliarlos y mejorarlos en sus ofertas. Las propuestas que ofrezcan características inferiores no serán tomadas en consideración en el presente procedimiento.

**Situación actual:**

Actualmente en la red del Grupo Tragsa se tienen desplegadas las soluciones de detección y respuesta ante ataques y amenazas avanzadas de seguridad (EDR / AV) del fabricante Trend Micro en:

- Servidores.
- Equipos de sobremesa.
- Equipos portátiles.
- Servicio de Correo.
- Cabinas de almacenamiento.

En concreto están en funcionamiento los siguientes productos:

Descripción / producto	Uds / usuarios
Deep Security - Malware Prevention –per Server (VM) DX3TMMMAXLIELR	550
Deep Security - Network Security – per Server (VM) DX3CMMMAXLIELR	159
Email Reputation Services STTLMMZ10LIUSR	5.500
Server Protect for Storage v6.x SPZZSSM6XLIULR	4.001
Trend Micro Smart Protection Complete CTMMMMM1XLIULR	5.500
Premium Support PSSGZZZZZY9USR	1

Para dar cobertura al incremento de usuarios del Grupo y para hacer frente a las nuevas amenazas, se requiere elevar el nivel de seguridad de la infraestructura implantada, mejorar las capacidades de detección y de respuesta frente a ataques; para ello se requiere la ampliación de funcionalidades de la actual infraestructura de seguridad de Trend Micro desplegada en la red corporativa del Grupo Tragsa, en concreto:

- Incorporar tecnología de sonda de red (DDI - Deep Discovery Inspector) para el análisis de protocolos de red, y la detección y respuesta ante anomalías o desviaciones en el comportamiento del tráfico de datos dentro de la red corporativa.
- Incorporar una solución de XDR (Detección y Respuesta Extendida) que proporcione la recopilación de información y correlación automática desde las múltiples capas de seguridad: equipos de sobremesa, portátiles, servidores, sonda de red, correo electrónico, recursos en nube.

De esta forma, toda la información obtenida por las funcionalidades anteriormente mencionadas se recogerá y se correlacionará automáticamente en la consola centralizada de VisionOne para obtener una visión completa de los indicadores de compromiso (IoC's), y de las amenazas de seguridad, y su evolución, para poder aplicar la acción de bloqueo o mitigación que corresponda en función de su criticidad.

**Situación objetivo:**

Por lo tanto, es objeto del presente pliego la renovación y activación, con el fabricante de los productos (Trend Micro) de los siguientes productos:

Descripción / producto	Uds / usuarios
Deep Discovery Inspector HW-Appliance (Software + HW 4 Gbps)	2
Service One Complete Endpoint & Workloads (includes Messaging)	8.300
Service One Complete Network - 4 Gbps	2
Trend Micro Cloud One - Workload Security with XDR	850
ServerProtect for Storage v6.x SPZZSSM6XLIULR	6.001
Trend Micro Vision One Credits, Government. 350000 users	1
Trend Micro Smart Protection Complete, incl. CAS XDR CT00921518	7.500

**Será obligación del adjudicatario la activación del servicio de soporte con el fabricante Trend Micro.** Los servicios incluidos y niveles mínimos que se muestran a continuación, serán de aplicación a todas las licencias y funcionalidades:

- El servicio de soporte será en 24 x 7

- Asignación por parte del Grupo Tragsa de la prioridad de los casos.
- Tiempo de respuesta dependiendo de la criticidad de los casos:
  - Crítica: no superior a 1 horas hábiles.
  - Alta: no superior a 2 horas hábiles.
  - Media y baja: no superior a 4 horas hábiles.
- Monitorización 24x7 de alertas críticas
- Acceso en español a un gestor técnico del fabricante, vía consola, móvil, correo y teléfono fijo para seguimiento y priorización de casos; acompañamiento durante el incidente; revisiones a medida; soporte en las actualizaciones; consultas técnicas y alerta temprana de incidentes de seguridad.
- El gestor técnico asignado deberá estar en territorio español y pertenecer a la plantilla del fabricante.
- Acceso garantizado al equipo de Respuesta ante incidentes y a expertos en ciberseguridad y CISO.
- Detección de ataques dirigidos: previsión proactiva de amenazas con supervisión ininterrumpida los 365 días del año de cualquier ataque dirigido y acceso a un experto en amenazas e informes mensuales.
- XDR monitorizado y operado por TM: previsión proactiva de amenazas con supervisión ininterrumpida los 365 días del año de alertas de XDR, investigación y respuesta con alcance proactivo que incluya barrido de IOC, búsqueda de IoA, análisis de causas, impacto y acceso a analistas de amenazas de Managed XDR.
- Soporte en la planificación de migración de versiones, instalación de productos y parches y consultas de configuración
- Posibilidad de intervenciones remotas previa aceptación por el Grupo Tragsa.
- Prioridad en la resolución de casos y desarrollo de parches cuando éstos son escalados a desarrollo. La atención para incidencias críticas de máxima prioridad será de 24x7.
- Acceso a la base de conocimientos técnica de casos de otros clientes del fabricante.
- Avisos de malware y ataques sucedidos en otros clientes, para evitar que ocurran dentro del Grupo Tragsa.
- Servicio de alerta temprana, corrección y soporte Premium.
- Un mínimo de 12 visitas anuales por parte del técnico especializado asignado, con una periodicidad mínima mensual, en las que se revisara el estado de las herramientas de protección, actuando en caso de ser necesaria cualquier intervención o mejora sobre el sistema
- Acceso a formación, base de conocimientos, buenas prácticas recomendadas, guías de administración y operación.
- El cierre de una incidencia vendrá determinado por la conformidad expresa del Grupo Tragsa.

**No se admite la presentación de variantes.**

Madrid a 28 de noviembre de 2022