S-05843-2021

Ampliación de licencias antivirus corporativo Trend Micro

MEMORIA JUSTIFICATIVA

JUSTIFICACIÓN DE LA NECESIDAD:

Es necesaria la incorporación de licencias adicionales y servicios de suscripción de sistema de protección antivirus desplegado en servidores y puestos de trabajo conectados en la Red Corporativa, para completar la protección de los mismos.

La Dirección de Sistemas de CRTVE dispone de licencias de protección antivirus del fabricante Trend Micro para equipos conectados a la Red Corporativa.

Actualmente, para mejorar la seguridad de la red, es necesario incorporar las siguientes licencias:

- Licencias antivirus para servidores.
- Suscripción anual del agente **XDR Endpoint and Server** para PCs y Servidores asociado al antivirus.

El motivo de incorporar licencias antivirus para servidores, es la necesidad de proteger estos equipos que actualmente no disponen de la citada protección.

El motivo de necesitar la suscripción para PCs y servidores del agente *XDR Endpoint and Server* se detalla a continuación.

Actualmente los equipos están expuestos nuevas formas de ciberataques de gran sofisticación, como el "ramsonware" (encriptación de la información) que no pueden ser detectados directamente por el antivirus, requiriendo un análisis detallado del comportamiento del atacante.

Este tipo de ataque se ha **incrementado de forma exponencial** en los últimos años, tal como ha sucedido recientemente en multitud de empresas y organismos públicos.

La situación actual de extensión del **teletrabajo,** hace aún más vulnerables a los equipos.

Por ello, se requiere incluir en los equipos el agente XDR, ligado al antivirus. Se trata de lo que técnicamente se denomina "agente de punto final (Endpoint Detection and Response - EDR)" que permite:

- **Detectar los ciberataques avanzados** como código malicioso complejo y comportamientos sospechosos en los equipos como el movimiento lateral en los puestos de trabajo y servidores, a partir de la información de eventos detectados por el antivirus.
- **Correlacionar la información** de lo que ocurre en los distintos equipos simultáneamente, permitiendo detectar las acciones combinadas del atacante y frenar la propagación del ataque.
- **Guardar las evidencias** para su posterior investigación, sobre cómo se originó, como se propagó, a que equipos afectó, etc, permitiendo así restaurar más rápidamente la normalidad.

Toda esta información, será monitorizada 24h al día por el Centro de Operaciones de Ciberseguridad que se está desplegando actualmente por la Dirección de Sistemas, permitiendo así reaccionar de forma rápida ante un ataque, en el momento en que se produzca.

De no contratarse este servicio de suscripción anual, **no se detectarían estos ciberataques**, lo que podría tener graves consecuencias, incluida la **completa paralización de todos los puestos de trabajo y servidores de la red corporativa de** RTVE.

Esta necesidad, viene avalada la **recomendación del Centro Criptográfico Nacional**, en la que se hace referencia al **Plan de Choque de Ciberseguridad aprobado por el Consejo de Ministros el 25/05/21,** donde se definen las medidas de protección a implantar en las entidades públicas.

La contratación necesaria, consiste en las siguientes licencias y suscripciones adicionales:

Producto	Unidades
Suscripción TrendMicro XDR Enpoint and Server	5.423
Licencia TrendMicro DeepSecurity-Network Security - per server (VM)	272
Licencia TrendMicro DeepSecurity-Malware Prevention - per server (VM)	272
Premium Support	1

INFORME DE INSUFICIENCIA DE MEDIOS

La Dirección de Sistemas no dispone de medios propios para la realización de este servicio, pues son suministros y servicios que solo puede realizar un suministrador que disponga de este tipo de solución y sus correspondientes laboratorios de soporte.

LOTES DE LA CONTRATACIÓN

El expediente se ha planteado en un único lote. El objeto del contrato no resulta divisible en lotes pue se trata de un servicio único de licencias y suscripciones de herramientas de protección avanzada y soporte asociado del mismo fabricante.

JUSTIFICACIÓN DEL PROCEDIMIENTO

Se propone el trámite de este expediente por un procedimiento ABIERTO ya que no se dan los requisitos que establece la LCSP, para tramitar esta contratación por otro procedimiento distinto a este.

Cualquier procedimiento abierto es garantía de transparencia e igualdad de trato entre los licitadores, y además garantiza mayor concurrencia

EXISTENCIA DE PRESUPUESTO

El presupuesto del CECO está aprobado y contempla esta contratación:

CECO	CC01SS2330
Cuenta de Gasto	6222002 Mantenimiento Software informático
Material	8200556 Mantenimiento Software informático
Orden inversión	I501110A1102 Hardware y Sw Ofimatico < 60.000

El valor estimado del contrato es el siguiente:

Descripción	Importe Total
Licencias Trend Micro	112.491,67

Desglose:

Producto	Unidades	Importe Unitario Anual	Importe Total
TrendMicro XDR Enpoint and Server	5.423	11,70	63.449,10
TrendMicro DeepSecurity-Network Security - per server (VM)	272	103,29	28.094,88
TrendMicro DeepSecurity-Malware Prevention - per server (VM)	272	44,27	12.041,44
Premium Support	1	8.906,25	8.906,25
	Total		**112.491,67**

Inversión (Licencias Deep Security)	40.136,32
Gasto (Suscripción XDR y soporte)	72.355,35

Al tratarse de un suministro y suscripción de componentes nuevos, no es posible comparativa con el coste actual.