Pliego de Prescripciones Técnicas

Procedimiento: Concurso

Suministro de Software de antivirus para los equipos informáticos distribuidos a los Centros Educativos

Referencia:	CRI_15_ppt_Suministro SW Antivirus (NSP) (1.0).doc
Creación:	05 de Febrero de 2014
Consejería:	Economía y Hacienda
CRI:	Centro Regional de Informática
Área:	Informática del Sector Educativo
Servicio:	Servicio de Gestión Informática (Educación, Universidades Y Empleo)

1. Introducción

El Servicio de Gestión Informática de la Consejería de Educación, Universidades y Empleo tiene entre sus funciones, la de garantizar la seguridad de ataques de virus informáticos, de troyanos, de malwares, de spywares, ..., incluida la seguridad en la navegación por internet, de todo el equipamiento informático adquirido y distribuido en los centros educativos de titularidad pública.

Para ello, desde la puesta en marcha del Proyecto Plumier en el año 2001, se han ido realizando diversas contrataciones de suministro de software antivirus, y cada una de ellas con unas prestaciones adaptadas a las nuevas tecnologías.

Para finales del año 2013, de la totalidad de equipamiento informático distribuidos en los centros educativos quedarán **10.450** (***ordenadores personales y ordenadores portátiles***) sin protección ante virus, gusanos, troyanos, spyware, rootkist y otros tipos de software malicioso.

Por ello, se plantea a la Consejería de Educación, Universidades y Empleo la necesidad de contratar el suministro de un software antivirus, con el objeto de garantizar la seguridad de ataques de virus informáticos, troyanos, malwares, spywares, ..., incluida la seguridad en la navegación por internet para los 10.450 equipamiento informático. Adquiriendo a finales del 2013 4.740 licencias (*Trend Micro Mobile Security Suite Edition - OfficeScan Client-Server Suite Advanced Plug-in - OfficeScan Superkey (AV+SW+DC+FW) ver 10.x - ServerProtect Linux / NT/NW - TMCM v6 Advanced Edition – English*), quedando pendientes 5.710 para el ejercicio actual.

2. Objeto

El objeto del presente pliego es establecer las condiciones técnicas que han de regir la contratación del **SUMINISTRO** de un software antivirus, con el fin, de garantizar la seguridad de ataques de virus informáticos, de troyanos, de malwares, de spywares, ..., incluida la seguridad en la navegación por internet, para todos aquellos equipos informáticos que no dispondrán del citado, y que han sido distribuidos desde la Consejería de Educación a los centros educativos de titularidad pública.

3. Relación de bienes a los que repercute el objeto.

A continuación se relacionan el tipo y cantidad de equipamiento informático que forma parte del objeto del contrato.

UNID.	DESCRIPCIÓN
5.710	SW antivirus

4.4. Gasto elegible

El importe del gasto elegible es **0 €, cero euros.**

5. Descripción técnica del suministro

A continuación se establecen los detalles del suministro objeto de la contratación:

5.1. Condiciones generales

De forma general, el adjudicatario deberá de suministrar 5.710 licencias de SW antivirus que garanticen la seguridad de ataques de virus informáticos, de troyanos, de malwares, de spywares, ..., incluida la seguridad en la navegación por internet.

5.2. Entorno funcional. Especificación de requisitos

En este apartado se detallan las **especificaciones técnicas mínimas obligatorias** que han de cumplir el suministro objeto de la presente licitación. Al presentar la oferta el licitador debe ajustarse a la terminología utilizada en este apartado.

Se relacionan a continuación las **especificaciones técnicas mínimas obligatorias** del software para garantizar la seguridad de al menos de:

- Virus
- Gusanos
- Troyanos
- Spyware
- Rootkist
- Y otros tipos de software malicioso
- Seguridad en la navegación por internet.

Las especificaciones mínimas detalladas anteriormente no pretenden ser una relación exhaustiva, sino las más relevantes para el cumplimiento del objeto del contrato.

5.2.1. Distribución e instalación.

Todo el suministro habrá de quedar entregado en la sede de la Consejería de Educación, Universidades y Empleo. La distribución e instalación del mismo se realizará por medios propios.

ANEXO

- Las conexiones entre los usuarios (Internet e intranet) y el sistema frontal (web, portal, https,...) está supervisado por un cortafuegos: en nuestro caso por los sistemas Cisco PIX.
- Las conexiones entre el sistema frontal y las aplicaciones (Tomcat,...) están supervisadas por otro cortafuegos: los Nokia+Checkpoint.
- Las conexiones entre las aplicaciones y las bases de datos (Sql*Net,...) están supervisadas por cortafuegos: los Nokia+Checkpoint.

Reducción del número de redes y VLANes

Basándonos en los planteamientos de simplicidad para conseguir que la propuesta fuera razonablemente operativa y segura, se realizaron diversas reuniones llegando a la siguiente conclusión de necesidad de redes.

Zona DMZ, zona de los portales

- zona de los portales. Comprende todos los portales que prestan servicio a los usuarios finales. Son las aplicaciones de estos sistemas las únicas que están en contacto con los usuarios finales.

  Su funcionamiento es como sigue:

  - estas aplicaciones reciben las peticiones de los usuarios de Internet y de intranet. Deberían ser aplicaciones frontales, del tipo servidor web, portal web, portal web seguro,...
  - Si estos portales ya tienen la información que han de dar al usuario final, la responden directamente.
  - pero si la información, la tienen que pedir a otros sistemas de información de la CARM, realizan una solicitud a las aplicaciones que están en la zona de la MZ, a través de un conector contra la aplicación, y que será distinto de la redirección de la solicitud web originaria. Por ejemplo, un servidor apache, enlazaría con el módulo mod_jk para llamar al servidor de aplicaciones Tomcat que estará en la MZ.

Red	comentario
red_dmz_publica	Red DMZ pública (equipos accesibles desde Internet)
red_dmz_privada	DMZ Privada (correspondiente a red_dmz_publica)

- interconexión intranet CARM. Esta red de interconexión del ASA con la intranet CARM permitirá que los usuarios de la CARM accedan a los frontales de los sistemas de información de la CARM, que están situados en la DMZ. Todos los accesos a las aplicaciones de la CARM se realizará a través de esta interconexión contra los frontales.

- Los sistemas involucrados en estos desarrollos no deberían tener acceso a Internet.

red_desarrollo	Red de desarrollo

- interconexión intranet CARM.
  - Esta interconexión permite que los programadores puedan realizar su trabajo contra la red de desarrollo.
  - También permite que los administradores o gestores de ASA puedan acceder a la red de gestión de toda la infraestructura.
  - No permite ningún acceso contra los servicios de las aplicaciones.
  - No permite ningún acceso contra los servicios de las bases de datos.

red_intranet_mz	Red Interconexión 6509 - Nokia