



**UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS
CONVOCATORIA PUBLICA 013 DE 2018**

**CONSOLIDADO DE RESPUESTAS A OBSERVACIONES EXTEMPORANEAS AL PLIEGO DE
CONDICIONES**

OBJETO: "CONTRATAR LA ADQUISICIÓN, INSTALACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DE EQUIPOS, LICENCIAS Y COMPONENTES, QUE PERMITAN LA ACTUALIZACIÓN Y EL REFORZAMIENTO, DE LA INFRAESTRUCTURA DE TELECOMUNICACIONES Y DE LA SEGURIDAD PERIMETRAL DE LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS, MEDIANTE DOS COMPONENTES: SISTEMA DE SEGURIDAD PERIMETRAL Y EQUIPOS ENRUTADORES".

OBSERVACIONES PRESENTADAS POR JOHN HINCAPIÉ DE LA EMPRESA ECOMIL

OBSERVACIÓN No. 1

Revisando las respuestas dadas a las observaciones realizadas por diferentes compañías al Pliego de Condiciones Definitivo, y teniendo en cuenta la adenda emitida por la entidad, quisiéramos observar al respecto lo siguiente:

- 1) *La entidad determina que la consola de administración y monitoreo debe ir embebida en la misma solución de Firewalls, especialmente por temas de espacio en rack (físico) e infraestructura (virtual), tal como se puede detallar aquí:*

OBSERVACIÓN No. 3

Se le solicita a la Universidad permitir que la consola de administración y monitoreo se ofrezca de modo virtual o appliance.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, dado que el espacio físico (en Rack) y lógico (ambiente virtual) destinado en el Data Center para esta solución responde al dimensionamiento del proyecto; en consecuencia, se ratifica lo solicitado en el pliego de condiciones en el ítem 2 del numeral 2.4.1.1 "ESPECIFICACIONES TÉCNICAS COMPONENTE 1".
"El sistema debe contar con máximo dos equipos con el fin de minimizar los puntos de falla, optimizar el espacio en el data center, optimizar el uso de las conexiones de red y facilitar la administración incluyendo el sistema de monitoreo y reportes. Estos deben trabajar de forma redundante entre sí en Alta disponibilidad (HA) soportando todos los servicios que presta el sistema de seguridad perimetral HA."

No obstante, existen soluciones en el mercado tipo appliance que no superarían el espacio en rack que la entidad presupuestó (6 Unidades para la solución total), de forma tal que se adaptan perfectamente al dimensionamiento del proyecto. Por lo tanto, solicitamos respetuosamente a la entidad considerar que la adenda tenga una nota adicional que indique:

"El sistema puede contar con una solución de monitoreo, reportes y consolidación de logs tipo appliance o virtual, siempre y cuando no supere los requerimientos de espacio dimensionados en el diseño del proyecto"



RESPUESTA DE LA UNIVERSIDAD: Se aclara que esta observación ya fue analizada y atendida por la entidad, dando origen al Adendo No. 1 a los pliegos, que fue publicado el pasado 4 de octubre, a las 16:57 en la página Web de la Universidad y en el SECOP, en el cual, tras considerar que, de acuerdo al ítem 80 del numeral 2.4.1.1 "ESPECIFICACIONES TÉCNICAS COMPONENTE 1", el sistema debe tener instalada la consola de administración y monitoreo incluida, de manera que ésta no puede estar instalada en un servidor físico o virtual, se modificó el ítem 80 del numeral 2.4.1.1 "ESPECIFICACIONES TÉCNICAS COMPONENTE 1", quedando de la siguiente manera: *"La consola de administración y monitoreo debe residir en el mismo appliance de seguridad de red, lo cual implica que ésta posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función."*

OBSERVACIÓN No. 2

2) En el documento "Informe de Dimensionamiento", la entidad proyecta unas métricas relacionadas a Nuevas Conexiones por Segundo, según la siguiente tabla:

Tipo de Usuario	Marca CheckPoint	Marca Hillstone Networks	Marca Palo Alto
-----------------	------------------	--------------------------	-----------------

1 de 2

	INFORME DE DIMENSIONAMIENTO PARA LA ADQUISICIÓN DE HARDWARE Y SOFTWARE EN CONJUNTO CON LOS SERVICIOS DE LICENCIAMIENTO, CONFIGURACIÓN, INSTALACIÓN, MIGRACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DEL SISTEMA DE SEGURIDAD PERIMETRAL EN ALTA DISPONIBILIDAD PARA LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS.	
	Fecha: 31-05-2018	

Administrativos	3,811	3,755	3,825
Estudiantes y Profesores	125,943	124,651	123,952
Administradores de TI y Sistemas de TI	1,502	1,625	1,452
TOTAL	131,256	130,031	129,229

Tabla 2. Total de nuevas conexiones en red por segundo por tipo de usuario.

A partir de la información de la tabla 2 y proyectando el aumento en la cantidad de nuevos usuarios a futuro en red que tendrá la Universidad, se establece que el equipo debe tener la capacidad de procesar mínimo 135.000 nuevas conexiones en red por segundo.

No obstante, es necesario considerar que, si la Universidad proyecta incrementar el canal de Internet de 2 Gbps a 4 Gbps, es posible que los usuarios realicen más actividades y, por lo tanto, se genere un mayor número de conexiones por segundo. Por lo tanto, sugerimos respetuosamente a la entidad ampliar la capacidad del sistema a 270.000 nuevas conexiones por segundo, teniendo en cuenta dicha proyección en ancho de banda, considerando que las 135.000 proyectadas pueden limitar el sistema en picos de operación máxima

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. De acuerdo al dimensionamiento, se tuvo en cuenta la totalidad de usuarios que hacen uso del acceso a internet dedicado con el que cuenta la Universidad y su crecimiento proyectado, por lo cual, se ratifica lo indicado en el ítem 18 del numeral 2.4.1.1 "ESPECIFICACIONES TÉCNICAS

umi

[Handwritten signature]

COMPONENTE 1": "Cada equipo debe tener la Capacidad de procesar mínimo 135.000 nuevas conexiones en red por segundo", la cual es un una especificación técnica mínima, luego el proponente puede ofertar un equipo con características técnicas superiores.

OBSERVACIONES PRESENTADAS POR GERMAN ZAMORA DE LA CONSULTORIAS TECNOLOGICAS

OBSERVACIÓN No. 1

Estimados Señores:

De manera atenta me permito realizar observaciones a la Adenda publicada por la Entidad el pasado miércoles:

La compañía PCM SAS hizo una observación al Pliego que fue aceptada por la Universidad Distrital y modificó el pliego, así:

OBSERVACIONES PRESENTADAS POR JULIETH ANDREA CANO PEDRAZA DE LA EMPRESA PCM SAS

OBSERVACIÓN No. 1

Con respecto al numeral 80 nuestra interpretación a la palabra "puede" en dicho párrafo es que la entidad aceptaría soluciones cuya consola de administración y monitoreo requieran ser instaladas en un servidor físico o virtual, agradecemos la validación de nuestra interpretación y si es correcta la ampliación de la redacción de dicho numeral en ese sentido a fin de mayor claridad y condiciones de participación de todos los proponentes.

80	La consola de administración y monitoreo puede residir en el mismo appliance de seguridad de red, desde que posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función.
----	---

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación, toda vez que, de acuerdo al ítem 80 del numeral 2.4.1.1 "ESPECIFICACIONES TÉCNICAS COMPONENTE 1", el sistema debe tener instalada la consola de administración y monitoreo incluida, de manera que ésta no puede estar instalada en un servidor físico o virtual, por lo tanto, se adendará lo pertinente en el ítem 80 del numeral 2.4.1.1 "ESPECIFICACIONES TÉCNICAS COMPONENTE 1", quedando de la siguiente manera:

"La consola de administración y monitoreo debe residir en el mismo appliance de seguridad de red, lo cual implica que ésta posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función."

SOLICITUD:

Consideramos que la aceptación por parte de la Universidad a este punto y por ende el cambio en la tabla de especificaciones técnicas del componente 1 del pliego a través de la Adenda 1 publicada el pasado 10 de Octubre, vulnera el derecho a la PLURALIDAD DE OFERENTES, a razón de que cambiar la palabra "puede" por "debe" en el numeral 80 de la tabla de especificaciones técnicas del componente 1 direcciona el proceso para que solo lo puedan cumplir Check Point y Palo Alto, esto se interpreta como que no hay transparencia en este proceso, por lo anterior solicito se mantenga el requerimiento como estaba originalmente permitiendo la pluralidad de oferentes.

Um,

[Handwritten signature]

80	La consola de administración y monitoreo puede residir en el mismo appliance de seguridad de red, desde que posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función.
----	---

La Universidad indica que tiene un recurso dispuesto de 6 espacios de rack para que sea instalada la solución y existen soluciones que disponiendo 2 equipos de FW y un sistema de administración residente en otro appliance ocuparía NO más de esos 6 espacios y permiten además separar físicamente los archivos LOG de los equipos FW como buena práctica de Seguridad, razón por la cual no se entiende el por qué se pretende limitar el punto 80 a que se "deba" estar incluido en el mismo Appliance de seguridad de red, nos sugiere preferencia de marcas que atenta contra la transparencia del proceso.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El cambio de la palabra "puede" por la palabra "debe" del ítem 80 mencionado en la observación, obedece a guardar coherencia con el ítem 2 del numeral 2.4.1.1. "ESPECIFICACIONES TÉCNICAS COMPONENTE 1" en donde se ha especificado que *"El sistema debe contar con máximo dos equipos... Estos deben trabajar de forma redundante entre sí en Alta disponibilidad (HA) soportando todos los servicios que presta el sistema de seguridad perimetral HA."*, en otras palabras, los dos equipos deben soportar **todos** los servicios, incluyendo, la consola de administración y monitoreo sin equipos adicionales.

En cuanto a la pluralidad de oferentes, se encuentra, en la documentación pública en las páginas Web de los fabricantes referenciados en el estudio de mercado, que esta característica puede ser ofrecida por los mismos, de tal forma que se mantiene la pluralidad de marcas y oferentes en el proceso. Entre las marcas relacionadas en el estudio de mercado, se encuentran las mencionadas por quien observa (check point y palo alto), pero no solo éstas.

De otra parte, la inclusión de un equipo adicional para la solución de monitoreo, reportes y logs, además de afectar el espacio en rack en el data center, también ocasionaría que se aumenten los puntos de falla en el sistema de seguridad perimetral, tendría más conexiones eléctricas, más conexiones de red y aumentaría la complejidad en la administración del mismo, de otra parte, los archivos LOG se mantendrán en cada uno de los dos equipos que conforman el sistema de seguridad perimetral en alta disponibilidad y adicionalmente tendrán una copia de respaldo en el sistema de almacenamiento masivo de la Universidad.

Dado lo anterior, se ratifica lo solicitado en el ítem 2 del numeral 2.4.1.1. "ESPECIFICACIONES TÉCNICAS COMPONENTE 1" y lo referido en el Adendo No. 1, numeral 2, que modifica el ítem 80 del numeral 2.4.1.1 "ESPECIFICACIONES TÉCNICAS COMPONENTE 1", el cual quedó de la siguiente manera:

"La consola de administración y monitoreo debe residir en el mismo appliance de seguridad de red, lo cual implica que esta posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función."

El Comité Asesor de Contratación de la Universidad Distrital Francisco José de Caldas, en sesión virtual de octubre 12 de 2018, avaló las anteriores respuestas, preparadas por el equipo de la Red de Datos UDNET, encabezado por la Jefe de la dependencia.

Javi
[Signature]

COMITÉ ASESOR DE CONTRATACIÓN

[Signature]