Dirección Nacional de Contrataciones Públicas
E.E.U.U. 961 c/ Tte. Fariña - Asunción, Paraguay
Tel. y Fax +595 21 4154000 - dncp@contrataciones.gov.py

Consultas Realizadas

Licitación 410715 - ADQUISICIÓN DE EQUIPOS TERMINALES Y ACCESORIOS PARA CLIENTES CORPORATIVOS.

Consulta 1 - Para el Lote 1 ítem 8.1 de Firewall Tipo A.

Consulta	Fecha de Consulta	13-09-2022
Para el Lote 1 ítem 8.1 de Firewall Tipo A. Sección Funcionalidades del Firewall, se mencionan las características y rendimiento de Firewall, no así el licenciamiento para estas funciones. Solicitamos a la convocante aclarar si se precisa de licencias para disponer las características funcionales de seguridad y el periodo contemplado del mismo.		

Respuesta	Fecha de Respuesta	07-10-2022
Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.		

Consulta 2 - Para el Lote 1 ítem 8.1 de Firewall Tipo A

Consulta	Fecha de Consulta	13-09-2022
Para el Lote 1 ítem 8.1 de Firewall Tipo A. de Características del Hardware en el ítem 8.1.15 se requiere "Fuente de alimentación: Auto-Ranging interno 220-110 VAC, 50-60Hz". Solicitamos a la convocante que este requerimiento sea opcional. Debido a que la fuente de alimentación podría ser interno o externo y no afectaría al rendimiento del Hardware		

Respuesta	Fecha de Respuesta	07-10-2022
Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.		

Consulta 3 - Para el Lote 1 ítem 8.2 de Firewall Tipo B

Consulta	Fecha de Consulta	13-09-2022
Para el Lote 1 ítem 8.2 de Firewall Tipo B. Sección Funcionalidades del Firewall, se mencionan las características y rendimiento de Firewall, no así el licenciamiento para estas funciones. Solicitamos a la convocante aclarar si se precisa de licencias para disponer las características funcionales de seguridad y el periodo contemplado del mismo.		

Respuesta	Fecha de Respuesta	07-10-2022
Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.		

Consulta 4 - Para el Lote 1 ítem 8.2 de Firewall Tipo B.

Consulta	Fecha de Consulta	13-09-2022
Para el Lote 1 ítem 8.2 de Firewall Tipo B. de Características del Hardware en el ítem 8.2.13 se requiere "Puertos Ethernet: 6 GbE cobre y al menos 2 puertos ópticos de 1Gbps y 2 puertos ópticos de 10Gbps, los cuales deben estar licenciados y activados para su funcionamiento inmediato, al menos 2 puertos deben poder ser configurados como puerto WAN". Solicitamos a la convocante que este requerimiento sea opcional. Debido a que se considera un factor crítico para nivelar el perfomance del equipo junto con las características Hardware.		

Respuesta	Fecha de Respuesta	29-09-2022
La cantidad de puertos solicitados es la mínima requerida por COPACO S.A y por lo tanto no puede ponerse como opcional por lo que se mantiene lo solicitado en el Pliego de Bases y Condiciones.		

Consulta 5 - FW tipo 1 y FW tipo dos

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo dos requiere la funcionalidad Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo.
Este requerimiento se refiere (según Fortinet lo explica) que, con la utilización de un ASIC, llamado NPU por Fortinet, puede incrementarse el desempeño VPN.
Se debe aclarar que dichos ASICs, no son incluidos como una opción ya que son fijos lo que determinan un rendimiento FIJO de desempeño VPN, es decir no puede ampliarse normalmente.
Solicitamos esta funcionalidad sea opcional o sea eliminada, ya que el desempeño VPN de cada equipo es Fijo y no puede modificarse en las marcas de FW mundialmente conocidas. Lo que permitirá la participación de otras marcas además de la mencionada.

Respuesta	Fecha de Respuesta	07-10-2022

Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.

Consulta 6 - El Pliego para el FW tipo 1

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 requiere 8 GbE cobre + 2 GbE óptico al menos 2 puertos deben poder ser configurados como puerto WAN. Atendiendo que un equipo normalmente de las capacidades de NGFW, IPS, VPN no requiere tal cantidad de puertos así como dicha distribución de tipos de puertos.
Encontramos que el modelo FG-80F coincide de manera idéntica a la distribución de puertos requeridos.
En la generalidad de las aplicaciones de PyME, solo son requeridos un máximo de 6 Puertos GE sin incluir puertos SFP. Ya que normalmente, el proveedor de conectividad, ya sea por GPON u otra tecnología, entregan conexiones de cobre
Solicitamos que las conexiones SFP sean opcionales de modo a no encarecer innecesariamente la oferta de dichos equipos

Respuesta	Fecha de Respuesta	07-10-2022

Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.

Consulta 7 - El Pliego para el FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 2 requiere 6 GbE cobre y al menos 2 puertos ópticos de 1Gbps y 2 puertos ópticos de 10Gbps, los cuales deben estar licenciados y activados para su funcionamiento inmediato, al menos 2 puertos deben poder ser configurados como puerto WAN
Atendiendo que un equipo normalmente de las capacidades de NGFW, IPS, VPN no requiere tal cantidad de puertos, así como dicha distribución de tipos de puertos.
Puertos 10G carecen de sentido, donde encontramos que el modelo FG-100F coincide de manera similar a la distribución de puertos requeridos.
En la generalidad de las aplicaciones de PyME, solo son requeridos un máximo de 8 Puertos GE sin incluir puertos SFP. Ya que normalmente, el proveedor de conectividad, ya sea por GPON u otra tecnología, entregan conexiones de cobre
Solicitamos que las conexiones SFP y SFP+ sean opcionales de modo a no encarecer innecesariamente la oferta de dichos equipos

Respuesta	Fecha de Respuesta	29-09-2022

Existen en el mercado diferentes marcas que cumplen con lo solicitado, que el equipo a ser suministrado tenga el arreglo de puertos ópticos solicitado es un requerimiento de los clientes corporativos de COPACO S.A. Por lo que se mantiene lo solicitado en el Pliego de Bases y Condiciones.

Consulta 8 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad El equipo de seguridad debe soportar el uso del protocolo ICAP.
El protocolo ICAP es para la redirección de contenidos con fines de filtrado y conversión
Es decir, redireccionar la funcionalidad de filtrado WEB
Los equipos de FW pueden operar en conjunto para filtrado WEB y conversión similar a ICAP sin soportar este protocolo.
Solicitamos este requerimiento sea opcional ya que dicha funcionalidad puede ser lograda con equipos adicionales

Respuesta	Fecha de Respuesta	29-09-2022

Se verifica en el Pliego de Bases y Condiciones que los puntos 8.1.5 y 8.2.5 son opcionales.

Consulta 9 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Soporte a etiquetas de VLAN (802.lq) y creación de zonas de seguridad en base a VLANs
Esta funcionalidad es utilizada por equipos FORTINET por medio de los puertos FortiLINK a través de su integración con Switches Fortinet.
Claramente direcciona a soluciones de dicha marca por lo que se limita la participación de otras soluciones.
Solicitamos dicha funcionalidad sea eliminada o considerada opcional.

Respuesta	Fecha de Respuesta	29-09-2022

Existen en el mercado diferentes marcas que cumplen con lo solicitado además de la marca mencionada en la consulta y el etiquetado de VLAN es una funcionalidad básica utilizada en la red de COPACO S.A.

Consulta 10 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Capacidad nativa de integrarse con directorios LDAP, Active Directory, eDirectory, RADIUS y TACACS +.
eDirectory son una gran cantidad de servicios diferentes, como los de Novell eDirectory, NetIQdirectory, eDirectory.com, son opciones particulares de validación de usuarios los cuales son diferentes y no constituyen un es estándar, ni son masivamente utilizados por lo que no puede ser requerida como requisito obligatorio.
Entendiendo que existe una variedad de soluciones eDirectory y que ninguno son soluciones estándares, solicitamos que dicho requerimiento sea considerado opcional

Respuesta	Fecha de Respuesta	29-09-2022

eDirectory permite controles de acceso tanto globales como específicos, los cuales pueden ser Novell eDirectory o NetIQ eDirectory, etc., la manera en que se solicita permite que cualquier fabricante pueda participar en el presente llamado sin citar específicamente el tipo de eDirectory.

Consulta 11 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022
El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Capacidad de poder asignar parámetros de traffic Shaping sobre reglas de firewall Solicitamos sea aceptable establecer políticas de IQoS en políticas independientes a la regla de Firewall de modo a que la granularidad sea superior		

Respuesta	Fecha de Respuesta	07-10-2022
Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.		

Consulta 12 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022
El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log Solicitamos sea aceptable Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear en una regla de firma estática o registrar en log		

Respuesta	Fecha de Respuesta	29-09-2022
La manera en que se expresa la opción de bloqueo es genérica no así la propuesta realizada en la consulta, por lo que se mantiene en el Pliego de Bases y Condiciones.		

Consulta 13 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022
El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping Solicitamos sea aceptable Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping o quality of service (QoS) que permite un mejor manejo de trafico		

Respuesta	Fecha de Respuesta	07-10-2022
Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.		

Consulta 14 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022
El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Deberá permitir configurar firmas nuevas para cualquier protocolo. Solicitamos sea aceptable Deberá permitir configurar firmas nuevas o lista de firmas para cualquier protocolo, lo que permite mejor capacidad de agregar firmas nuevas		

Respuesta	Fecha de Respuesta	07-10-2022
Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.		

Consulta 15 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022
El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Deberá ser capaz de crear firmas (signatures) personalizadas para proteger la red de objetos de red como servidores, direcciones web, protocolos y aplicaciones. Solicitamos sea aceptable Deberá ser capaz de crear firmas (signatures) o lista de firmas personalizadas para proteger la red de objetos de red como servidores, direcciones web, protocolos y aplicaciones.		

Respuesta	Fecha de Respuesta	07-10-2022
Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.		

Consulta 16 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022
El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Deberá contar con mecanismos de detección de ataques basados en Reconocimiento de patrones Solicitamos sea aceptable Deberá contar con mecanismos de detección de ataques basados en Reconocimiento de patrones o detección de anomalías de protocolo, lo que permite mejorar el tipo de reconocimiento de ataques desconocidos		

Respuesta	Fecha de Respuesta	07-10-2022
Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.		

Consulta 17 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022
El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Deberá contar con mecanismos de Protección contra ataques de Windows o NetBios Solicitamos sea aceptable Deberá contar con mecanismos de Protección contra ataques de Windows o NetBios o WinNuke attack lo que permite una mayor capacidad de protección		

Respuesta	Fecha de Respuesta	07-10-2022
Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.		

Consulta 18 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022
El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Deberá contar con la capacidad de poner en cuarentena o bloquear los mensajes de correo electrónico y hosts infectados. La misma debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma indefinida, hasta que un administrador tome una acción al respecto Solicitamos sea aceptable opcionalmente podría contar con la capacidad de cuarentena de mensajes de correo electrónico y de hosts infectados. La misma debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma indefinida, hasta que un administrador tome una acción al respecto		

Respuesta	Fecha de Respuesta	29-09-2022
La funcionalidad solicitada en los puntos 8.1.91 y 8.2.92 es necesaria para cada equipo de firewall y no puede considerarse como funcionalidad opcional por lo que se mantiene losolicitado en el Pliego de Bases y Condiciones.		

Consulta 19 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad EI equipo deberá poseer la capacidad de trabajar como un Proxy Cache o DNS Cache
Solicitamos sea aceptable opcionalmente EI equipo podrá contar con la capacidad de trabajar como un Proxy Cache o poder agregar DNS Cache.

Respuesta	Fecha de Respuesta	29-09-2022

La funcionalidad solicitada en los puntos 8.1.93 y 8.2.94 es necesaria y no puede considerarse como funcionalidad opcional por lo que se mantiene lo solicitado en el Pliego de Bases y Condiciones.

Consulta 20 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Capacidad de filtrado de scripts en páginas web.
Solicitamos sea aceptable Capacidad de filtrado de scripts en páginas web o con capacidad de análisis de script mediante sandbox en cloud. Ya que un análisis del tipo Sandbox resulta mas completo e intenso en relación de un análisis interno del equipo que esta más limitado

Respuesta	Fecha de Respuesta	07-10-2022

Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.

Consulta 21 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad La capacidad antispam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencial ausencia de combinaciones de palabras, decidir rechazar el mensaje. La capacidad AntiSpam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear).
Solicitamos sea aceptable La capacidad antispam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencial ausencia de combinaciones de palabras, decidir rechazar el mensaje. La capacidad AntiSpam incluida deberá permitir especificar listas blancas o excepciones de correo electrónico (confiables, a los cuales siempre se les deberá pasar) y listas negras o bloqueo por sender , recipient , email content (no confiables, a los cuales siempre les deberá bloquear).

Respuesta	Fecha de Respuesta	07-10-2022

Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.

Consulta 22 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address)
Solicitamos sea aceptable Las listas blancas o listas negras podrán ser o por dirección IP o por dirección de correo electrónico (e-mail address)

Respuesta	Fecha de Respuesta	29-09-2022

Se mantiene lo solicitado en el Pliego de Bases y Condiciones.

Consulta 23 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad La capacidad AntiSpam deberá poder consultar una base de datos (RBL o SPF) donde se revise por lo menos la dirección IP del emisor del mensaje y sea rechazado en caso de pertenecer a fuentes Spam
Solicitamos sea aceptable como opcionalmente podrá tener la capacidad AntiSpam de consultar una base de datos (RBL o SPF) donde se revise la dirección IP del emisor del mensaje y sea rechazado en caso de pertenecer a fuentes Spam

Respuesta	Fecha de Respuesta	29-09-2022

La funcionalidad solicitada en los puntos 8.1.103 y 8.2.104 es necesaria y no puede considerarse como funcionalidad opcional por lo que se mantiene lo solicitado en el Pliego de Bases y Condiciones.

Consulta 24 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser advertidos, puestos en cuarentena o rechazados
Solicitamos sea aceptado En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser advertidos o auditados, puestos en cuarentena o rechazados o bloqueados.

Respuesta	Fecha de Respuesta	07-10-2022

Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.

Consulta 25 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad La solución debe ser capaz de detectar información sensible desde una lista. En caso de que el email posea información sensible ésta debe ser rechazada con aviso o sin aviso al emisor
Solicitamos sea aceptado La solución debe ser capaz de detectar información sensible desde una lista o configuración de categorías de palabras clave. En caso de que el email posea información sensible esta debe ser rechazada con aviso o sin aviso al emisor

Respuesta	Fecha de Respuesta	07-10-2022

Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.

Consulta 26 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad que debe soportar el análisis de archivos del tipo MIME: doc, xls, PDF, ppt, xlsx, docx, exe, din, dll, archivos comprimidos, etc.
Solicitamos sea aceptable La funcionalidad debe soportar el análisis de archivos del tipo MIME: doc, xls, PDF, ppt, xlsx, docx, exe, din o dsn, dll, archivos comprimidos o otros.

Respuesta	Fecha de Respuesta	07-10-2022

Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.

Consulta 27 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad La solución debe contar con la funcionalidad de portal cautivo
Solicitamos sea aceptable La solución debe contar con la funcionalidad de portal cautivo o Autenticación web

Respuesta	Fecha de Respuesta	07-10-2022

Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.

Consulta 28 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad El portal cautivo debe poder configurarse en cualquier interfaz (LAN eléctrica u óptica) del equipo
Portal cautivo, es definido por varias marcas como Autenticación web
Solicitamos sea aceptables El portal cautivo o Autenticación web debe poder configurarse en todas las interfaces o cualquier interfaz (LAN eléctrica u óptica) del equipo

Respuesta	Fecha de Respuesta	07-10-2022

Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.

Consulta 29 - El Pliego para el FW tipo 1 y FW tipo 2

Consulta	Fecha de Consulta	15-09-2022

El Pliego para el FW tipo 1 y FW tipo 2 requiere la funcionalidad El equipo debe permitir la personalización de la página web de bienvenida del portal cautivo.
Portal cautivo, es definido por varias marcas como Autenticación web
Solicitamos sea aceptable El equipo debe permitir la personalización de la página web de bienvenida del portal cautivo o Autenticación web

Respuesta	Fecha de Respuesta	07-10-2022

Favor remitirse a la Versión 4 del Pliego de Bases y Condiciones - Adenda N° 3.

Consulta 30 - Para el lote 2 Routers tipo 2

Consulta	Fecha de Consulta	15-09-2022

Para el lote 2 Routers tipo 2 y tipo 2 se requiere capacidad de Firewall de 3 Gbps
Solicitamos sea aceptable una capacidad de mínima de 1 Gbps de modo a permitir una mayor participación de equipos con dichas capacidades

Respuesta	Fecha de Respuesta	29-09-2022

Se mantiene lo solicitado en el Pliego de Bases y Condiciones

Consulta 31 - Lote 2, ítem 2, punto 9.2.17

Consulta	Fecha de Consulta	15-09-2022
Se solicita a la convocante especificar en el Lote 2, ítem 2, punto 9.2.17 a que se refiere el requerimiento de soporte de 15 usuarios como mínimo.		

Respuesta	Fecha de Respuesta	29-09-2022
El punto 9.2.17 de la sección Conectividad WiFi se refiere a que el equipo debe ser capaz de dar conectividad inalámbrica a como mínimo 15 usuarios, todos conectados al mismo tiempo.		

Consulta 32 - Lote 1, ítem 2, punto 9.2.41

Consulta	Fecha de Consulta	15-09-2022
Se solicita a la convocante especificar en el Lote 1, ítem 2, punto 9.2.41 las funcionalidades solicitadas para el equipo de manera a poder escoger la/s licencia/s correcta/s, ya en las especificaciones del item 2 solo se detallan la capacidad del equipo y sus características.		

Respuesta	Fecha de Respuesta	29-09-2022
Todas las funcionalidades solicitadas en cuadro 9.2 Router tipo 2 así como las licencias para que los equipos necesarios cuenten con las especificaciones mínimas solicitadas deben ser provistas y las mismas deben ser permanentes.		

Consulta 33 - Lote 1, ítem 1, punto 9.1.28

Consulta	Fecha de Consulta	15-09-2022
Se solicita a la convocante especificar en el Lote 1, ítem 1, punto 9.1.28 las funcionalidades solicitadas para poder escoger la/s licencia/s correcta/s, ya en las especificaciones del item 1 solo se detallan la capacidad del equipo y sus características.		

Respuesta	Fecha de Respuesta	29-09-2022
Todas las funcionalidades solicitadas en cuadro 9.1 Router tipo 1 así como las licencias para que los equipos necesarios cuenten con las especificaciones mínimas solicitadas deben ser provistas y las mismas deben ser permanentes		

Consulta 34 - Lote 2, item 1, punto 9.1.28

Consulta	Fecha de Consulta	27-09-2022
Se solicita a la convocante que modifique en el Lote 2, item 1, punto 9.1.28 licencias del tipo permanentes a tipo suscripción y especificar el tiempo de adquisición ya que el modelo de licencias de las marcas como Fortinet,Cisco, Palo Alto trabajan con tipos de licencias del tipo de suscripción. Especialmente para habilitar funcionalidades de filtro web como lo solicitado en el punto 9.1.18 Debe contar con funcionalidad de control parental para el acceso a sitios web.		

Respuesta	Fecha de Respuesta	07-10-2022
Se mantiene lo establecido en el Pliego de Bases y Condiciones.		

Consulta 35 - Lote 2, item 2, punto 9.2.41

Consulta	Fecha de Consulta	27-09-2022
2- Se solicita a la convocante que modifique en el Lote 2, item 2, punto 9.2.41 licencias del tipo permanentes a tipo suscripción y especificar el tiempo de adquisición ya que el modelo de licencias de las marcas como Fortinet,Cisco, Palo Alto trabajan con tipos de licencias del tipo de suscripción. Especialmente para habilitar funcionalidades de filtro web como lo solicitado en el punto 9.2.31 Debe contar con funcionalidad de control parental para el acceso a sitios web..		

Respuesta	Fecha de Respuesta	07-10-2022
Se mantiene lo establecido en el Pliego de Bases y Condiciones.		