DOCUMENTO DIGITAL

Cumple con los requisitos de la Ley N° 18.600

Presidencia N° 89

Montevideo, 28 de marzo de 2025

VISTO: La necesidad de adquirir un (1) Firewall Perimetral de Próxima Generación o Next-Generation Firewall (NGFW) con licenciamiento e instalación incluida, prevista en el Plan Anual de Compras 2025 (expediente digital Vías N° 271103).

RESULTANDO: Que la Comisión Asesora de Adjudicaciones elaboró el borrador de pliego de condiciones particulares correspondiente para la realización del llamado a concurso de precios.

CONSIDERANDO: I) Que en virtud de los procedimientos de compra vigentes, procede la realización de un llamado a concurso de precios.

II) Que se considera adecuado el pliego de condiciones particulares elaborado.

III) Que se entiende pertinente cometer a la Comisión Asesora de Adjudicaciones la convocatoria al llamado a concurso de precios objeto de estas actuaciones.

ATENTO: A las disposiciones del Texto Ordenado de la Contabilidad y Administración Financiera del Estado (TOCAF) y a la normativa reglamentaria que le asiste,

El Presidente de la Cámara de Representantes,

R E S U E L V E :

1°.- Llámese a concurso de precios para la adquisición de un (1) Firewall Perimetral de Próxima Generación o Next-Generation Firewall (NGFW) con licenciamiento e instalación incluida, según las actuaciones contenidas en el expediente digital Vías 271.103, a través de la Plataforma de ARCE.

2°.- Autorízase a la Comisión Asesora de Adjudicaciones de la Cámara de Representantes a fijar el día y la hora para la apertura de las ofertas.

3°.- Apruébase el pliego de condiciones particulares que se agrega a continuación.

PLIEGO DE CONDICIONES PARTICULARES

Artículo 1º. Objeto del concurso de precios.- La Cámara de Representantes llama a concurso de precios Nº –/25 para la adquisición de un Firewall Perimetral de Próxima Generación o *Next-Generation Firewall* (NGFW), con licenciamiento e instalación incluida.

Situación actual: La Cámara de Representantes cuenta en la actualidad con una solución NGFW marca Dell, modelo SonicWall NSa 4600, que se encuentra en el fin de su vida útil determinada por el fabricante.

Se busca sustituir la solución por un nuevo equipo en modalidad *on-premise*, con las siguientes características:

- Se requiere de una solución de protección de redes con características de *Next Generation Firewall* (NGFW) para la seguridad de perímetro.
- El fabricante del NGFW debe ser miembro activo de la organización CTA (Cyber Threat Alliance), garantizando el intercambio de inteligencia de amenazas entre terceros.
- El equipo propuesto no debe estar listado, ni anunciado por el fabricante como fin de vida (end-of-life) o fin de venta (end-of-sale) o fin de soporte (end of support), se deberá adjuntar un link público o carta del fabricante dirigida al proceso que verifique que el modelo propuesto no está en ese listado.
- El equipo NGFW deberá tener soporte vigente directamente del fabricante durante la vigencia del servicio, el soporte directo del fabricante 24x7 deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo de mismas características en caso de falla de hardware.
- El oferente deberá indicar en su propuesta la marca, modelo y licenciamiento de los equipos ofrecidos para este proceso.
- El hardware debe estar diseñado exclusivamente para la función específica de seguridad. No se aceptarán equipos de propósito genérico (PC o servers).
- No se aceptarán equipos enrutadores con funcionalidad de Firewall.
- Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y/o SSL y/o UDP.
- El fabricante del firewall propuesto debe contar con certificación ICSA Labs para Firewall.
- Capacidad de realizar backups de la configuración automáticamente y también respaldarlos en la nube.

Características de rendimiento y hardware:

- Rendimiento de Prevención/Protección de Amenazas de al menos 9 Gbps, indicando la

metodología para la realización del test. Dicho rendimiento se deberá alcanzar con las siguientes funcionalidades habilitadas simultáneamente: control de aplicaciones, sistema de prevención de intrusos (IPS), Antivirus/Antimalware de red, antispyware/antibot. Se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242.

- Rendimiento de Antimalware o Antivirus o Antispyware como mínimo de 9.4 Gbps.
- Rendimiento de *Firewall* como mínimo de 17.5 Gbps.
- Rendimiento de IPS como mínimo de 6 Gbps.
- Rendimiento de IPSec VPN como mínimo de 10.5 Gbps.
- Rendimiento de Inspección SSL como mínimo de 4.9 Gbps.
- El equipo debe soportar como mínimo 4.000.000 de sesiones/conexiones simultáneas.
- El equipo debe soportar como mínimo 114.000 sesiones/conexiones por segundo.
- El equipo debe soportar como mínimo 350.000 sesiones/conexiones DPI SSL.
- El equipo deberá soportar como mínimo 4.000 túneles VPN Site to Site.
- Deberá incluir como mínimo 2 puertos 10GE SFP+.
- Deberá incluir como mínimo 8 puertos 1GE RJ45.
- Deberá incluir al menos 1 puerto de consola RJ45.
- Deberá incluir al menos 1 puerto USB 3.0.
- Deberá incluir al menos 1 puerto de gestión RJ45.
- Deberá incluir fuente de alimentación 100-240VAC/50-60Hz.
- Deberá incluir fuente de poder redundante.

Control por políticas de firewall:

- Reglas configurables basadas en red de origen, red de destino, protocolo, puerto de comunicación y acción posible.
- Las acciones posibles deberán incluir como mínimo permitir o denegar tráfico.
- Adicionalmente las reglas deberán ser configurables considerando grupos de usuarios pertenecientes a la base de datos local del equipo, externos vía LDAP y/o Radius y externos de forma transparente.
- Las reglas deberán poder ser configuradas según horarios, incluyendo día, mes y año.
- Deberá soportar reglas de firewall en IPv6.
- Inspección de Aplicaciones, IPS, antivirus y filtrado de páginas web sobre comunicaciones cifradas por TLS (Transport Layer Security), como HTTPS, sin importar si opera sobre el puerto 443 u otro.
- Inspección de tráfico cifrado sobre SSH.

- Se podrán definir excepciones al tráfico cifrado por dominios o por categorías de páginas web.

VPN IPSEC/SSL:

- La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
- La VPN IPSec debe ser compatible con AES (Advanced Encryption Standard) de 128, 192 y 256 bits.
- El software agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado al menos al menos los sistemas operativos Windows y Linux.
- Conexión para dispositivos móviles de agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado al menos al menos los sistemas iOS y Android.
- Deberá soportar autenticación vía AD/LDAP o base de usuarios local.
- Deberá soportar asignación de direcciones IP y DNS en los clientes remotos.
- Debe permitir configurar políticas de control de aplicaciones IPS o Antivirus para tráfico de los clientes remotos conectados en la VPN SSL.

Prevención de amenazas conocidas:

- El dispositivo de seguridad debe poseer módulo de IPS (*Intrusion Prevention System*), Antivirus/*Antimalware*, Antispyware/*Antibot*.
- Debe ser capaz de realizar DNS *Sinkhole* para la identificación de equipos comprometidos por spyware en entornos corporativos.
- Debe contar con un módulo IPS integrado en el propio dispositivo firewall, con una consola de administración unificada y monitoreo de los dispositivos de seguridad, con soporte para al menos 3.000 firmas.
- Debe contar con protección contra ataques de inundación (*flood)* a nivel de UDP, ICMP y SYN *Flood*.
- Deberá permitir al administrador ejecutar acciones sobre los eventos de IPS como bloquear el tráfico, registrar o capturar el tráfico generado por el ataque.
- El IPS deberá ser capaz de inspeccionar el tráfico entre las zonas internas de la red.
- Deberá contar con mecanismos de antievasión.
- Deberá contar con filtro de bloqueo hacia centros de comando y control de *botnets*.
- Deberá contar con filtro de bloqueo por localización geográfica granular por cada regla de firewall.
- Deberá permitir analizar, tráfico entrante y saliente de al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP, CIFS/NETBIOS, y su administración debe estar integrada a la administración del dispositivo.

- Debe soportar escaneo de virus o spyware sobre protocolos basados en *stream* TCP, como Mensajería Instantánea y P2P.
- Debe permitir el análisis antivirus sin limitación del tamaño del archivo transferido y sin que esto afecte la efectividad de la detección de amenazas.
- Deberá contar con actualizaciones automáticas con un intervalo mínimo de búsqueda de actualizaciones de una hora.

Análisis de *malware* moderno:

- El sistema deberá soportar tecnología de análisis de *malware* de códigos desconocidos en un sistema aislado (Sandbox) donde se ejecutará e inspeccionará el comportamiento del código.
- El sistema Sandbox deberá operar como un servicio basado en la nube sin necesidad de hardware adicional.
- El sistema de Sandbox deberá contar con múltiples motores de detección para reducir las técnicas de evasión.
- El sistema deberá hacer un bloqueo del código que se está descargando hasta que se defina un veredicto.
- Deberá contar con controles de localización geográfica basados en la dirección IP de origen para hacer reglas de conexión por país bien sea de manera general o por reglas de firewall.
- El sistema deberá ser capaz de prevenir ataques del tipo DNS Tunneling.
- Deberá soportar el envío manual de archivos para análisis a través del servicio Sandbox.
- El sistema deberá contar con reportes sobre los archivos enviados a análisis y su veredicto.

Licenciamiento:

Se deberá incluir suscripción para el equipamiento hasta el vencimiento de la garantía, incluyendo las siguientes funcionalidades:

- Gateway antivirus.
- IPS.
- Control de aplicaciones.
- Filtrado de contenido.
- Anti-spam.
- Funcionalidad de visibilidad de red.
- Seguridad DNS.

- Se deberá incluir además licenciamiento perpetuo para al menos 100 clientes VPN.

Se deberá además:

- Especificar el plan de trabajo y las etapas del mismo.
- Instalar el nuevo equipo y dejarlo operativo. La ubicación final del equipo será en el mismo rack que la solución actual, reemplazandolo cuando quede operativo el nuevo. Se prevé reutilizar los cables y conexiones por UTP y módulos SFP si corresponde.
- Migrar las rutas, reglas, etc. del actual firewall NSa 4600 al nuevo, verificando que queden operativas.
- Configurar los accesos necesarios para la conexión con Active Directory y migración de los accesos VPN configurados en el actual Firewall.
- Brindar un plan de capacitación para la operación del nuevo equipo, incluyendo al menos la generación de nuevas reglas, modificación de las existentes, creación de nuevos usuarios, manejo de los accesos por VPN y control de las actualizaciones del equipo.

Artículo 2º. Complementos del objeto.- Las especificaciones indicadas son realizadas en el sentido del artículo 10.2 del Pliego Único de Bases y Condiciones Generales que rige este llamado.

Los requisitos establecidos en el artículo 1° de este Pliego deben entenderse como los mínimos e indivisibles. Las propuestas deben cumplir con todos los requisitos. En caso de que no cumplan con alguno quedarán descalificadas.

Artículo 3º. Plazo.- La empresa que resulte adjudicataria deberá entregar e instalar el artículo licitado dentro del plazo de noventa (90) días corridos a contar del siguiente al día que quede firme el acto de adjudicación.

Artículo 4º. Garantía y servicio de mantenimiento.- En la oferta se deberá indicar el período de garantía on-site, el que no podrá ser inferior a tres (3) años. Se valorarán las garantías mayores.

Durante el plazo de garantía, el mantenimiento del equipo así como las eventuales reparaciones deberán ser realizadas en las dependencias de la Cámara de Representantes, salvo que sea imprescindible su traslado a un taller de reparación, en cuyo caso el adjudicatario deberá proporcionar un equipo de similares características hasta tanto se reinstale funcionando el equipo originalmente asignado.

En caso de solicitud de reparación, se deberá dar respuesta dentro de las veinticuatro (24) horas de notificados. La Administración hará la comunicación al contacto establecido por el adjudicatario a los números telefónicos fijos, móviles u otros medios, además de por correo electrónico a la dirección registrada en el RUPE.

Los costos generados por traslados e instalaciones serán de cargo del oferente.

Artículo 5°. Mantenimiento de oferta.- Los oferentes deberán establecer en la propuesta el plazo de mantenimiento de su oferta, el que no podrá ser menor a treinta (30) días corridos. En caso de que ello no ocurra, se entenderá que la oferta se mantiene hasta el día de notificación de la adjudicación.

El plazo de mantenimiento de la oferta contenido en las propuestas no podrá estar sujeto a condición alguna, en caso contrario la Administración podrá a su juicio desestimar la oferta.

Artículo 6º. Consultas.- Las consultas aclaratorias sobre el presente llamado a concurso de precios deberán dirigirse únicamente a la Secretaría de la Comisión Asesora de Adjudicaciones de la Cámara de Representantes, a través del correo electrónico secretariacaa@diputados.gub.uy hasta el día ** de ** de 2025 a la hora **.

Las mismas serán contestadas a través de correo electrónico a quien efectuó la consulta y en caso de que la Administración entienda necesaria una aclaración a todos los interesados, la dará a conocer realizando la correspondiente publicación en la página de ARCE.

Las respuestas a consultas efectuadas una vez vencido el plazo indicado en el inciso primero de este artículo o a través de los medios indicados al pie de este Pliego, no obligan a la Administración.

Artículo 7º. Solicitudes de prórroga.- Se podrá solicitar prórroga de la fecha de apertura a través del correo electrónico secretariacaa@diputados.gub.uy, hasta el día ** de ** de 2025 a la hora **, indicando claramente los motivos que se invocan.

La Administración resolverá sobre la solicitud, respondiendo a través de correo electrónico a quien la haya efectuado y en caso de resolución afirmativa lo hará conocer realizando la correspondiente comunicación general en la página de ARCE.

Artículo 8º. Forma de cotizar.- Se cotizará debiendo detallar el precio en pesos uruguayos, con los impuestos correspondientes incluidos.

El precio cotizado deberá incluir el objeto de llamado y todo costo que lo integre hasta su efectiva entrega e instalación en las dependencias de la Cámara de Representantes.

El precio se mantendrá firme hasta la entrega del objeto licitado.

Artículo 9°. Elementos esenciales que debe contener la propuesta.- La Cámara de Representantes no aceptará las ofertas que carezcan de alguno de los elementos que se señalan a continuación:

- Precio, conforme a la forma de cotizar solicitada en el artículo 8°.
- Información completa de la solución ofertada.
- Plan de trabajo con etapas y plan de capacitación.
- Certificado partner de la marca ofertada.
- Certificaciones de la empresa.

- Plazo de entrega de la solución.
- Plazo de garantía on-site (mínimo de 3 años) con indicación de días y horarios en que se brindará el servicio y el tiempo de respuesta ante un aviso de falla.
- Formulario de identificación del oferente con firma autógrafa del representante de la empresa oferente (Anexo I).
- Formulario de declaración de suministro y existencia permanente de repuestos y asistencia de técnicos especializados en el territorio nacional (Anexo II).
- Completar tabla de ponderación de la empresa y la solución (Anexo III). Se deberá especificar en la tabla si se cumple o no con cada concepto y en caso de requerir aclaraciones se podrá hacer por separado haciendo referencia al documento en la misma tabla. En caso de valores numéricos se deberá especificar el correspondiente en la tabla.
- Completar tabla de características técnicas (Anexo IV) completa para cada alternativa presentada.

Para estar en condiciones de ofertar las empresas deben estar inscriptas en el RUPE en calidad de ACTIVAS.

Artículo 10. Notificaciones.- Todas las notificaciones, incluidas las de adjudicación del llamado al adjudicatario y a los demás oferentes, se realizarán a través del Sistema de Notificaciones y Comunicaciones Electrónicas de AGESIC o al correo electrónico registrado en el RUPE, siendo de exclusiva responsabilidad de los oferentes comunicar fehacientemente a la Administración todo cambio en el mismo o, en su caso, la preferencia por otro medio de notificación.

Constituirá plena prueba de la notificación realizada y de su fecha, el reporte emitido por el correo electrónico utilizado para efectuarla.

Artículo 11. Información confidencial y datos personales.- Cuando los oferentes incluyan información confidencial, la misma deberá ser ingresada en el sistema en tal carácter y en forma separada a la parte pública de la oferta.

La clasificación de la documentación en carácter de confidencial es de exclusiva responsabilidad del proveedor. La Administración podrá descalificar la oferta o tomar las medidas que estime pertinentes, si considera que la información ingresada en carácter confidencial no reúne los requisitos establecidos en el artículo 12.2 del Pliego de Condiciones Generales.

Sólo se considerará información confidencial: la información relativa a clientes; la que pueda ser objeto de propiedad intelectual; la que refiera al patrimonio del oferente; la que comprenda hechos o actos de carácter económico, contable, jurídico o administrativo relativos al oferente y que pudieran ser útiles para un competidor; la que está amparada en una cláusula contractual de confidencialidad; y aquella de naturaleza similar conforme a lo dispuesto en la Ley Nº 18.381, de Acceso a la Información Pública, y demás normas concordantes y complementarias.

En ningún caso se considerará información confidencial: los precios, la descripción de los bienes ofertados y las condiciones generales de la oferta, todo lo cual debe quedar disponible para

los demás oferentes. Las ofertas que presenten estos datos como confidenciales podrán ser descartadas.

Los documentos que entregue un oferente en carácter confidencial no serán divulgados a los restantes oferentes. No obstante, el oferente deberá incluir en la parte pública de su oferta un resumen de la información confidencial que ingrese.

Artículo 12. Recepción de ofertas.- Las propuestas se recibirán exclusivamente en línea, a través de la plataforma de la Agencia Reguladora de Compras Estatales (ARCE).

A esos efectos, las propuestas completas deberán ingresarse en el sitio web **http://www.comprasestatales.gub.uy,** antes de la hora fijada para la apertura, en un todo de acuerdo con lo dispuesto en el Pliego de Condiciones Generales, especialmente en sus artículos 10 y 11, adjuntando y especificando los elementos solicitados en este Pliego.

La propuesta y los anexos, en caso de corresponder, deberán llevar firma responsable del oferente e incluirse en la propuesta como archivos adjuntos.

Artículo 13. Apertura de propuestas.- La apertura se realizará en forma electrónica el día ** de ** de 2025 a la hora **.

El acta de apertura será publicada automáticamente en la página web de ARCE y simultáneamente se comunicará a los oferentes a la dirección electrónica que hayan registrado previamente en el RUPE.

Artículo 14. Acceso a las ofertas.- A partir de la fecha y hora establecidas para la apertura de las ofertas, estas quedarán visibles para todos los oferentes, con excepción de aquella información que sea ingresada con carácter confidencial, de acuerdo con lo establecido en el artículo 12.2 del Pliego de Condiciones Generales.

Artículo 15. Plazo para salvar defectos, carencias o errores en las ofertas.- Las propuestas serán evaluadas en forma primaria, respecto del cumplimiento de los requisitos formales y de admisibilidad exigidas en el presente Pliego.

Si se constatan defectos formales insubsanables, la respectiva oferta no será considerada.

De constatarse defectos subsanables, la Administración podrá otorgar a los oferentes 2 (dos) días hábiles para salvar los defectos, carencias formales o errores evidentes o de escasa importancia, siempre que a su juicio ello no altere la igualdad de los oferentes o cuando se presuma la existencia de alguna maniobra destinada a obtener una ventaja indebida.

Este plazo podrá ampliarse para proveedores del exterior y en ese caso se aplicará todos los oferentes.

Artículo 16. Comentarios y observaciones sobre las propuestas.- Los oferentes dispondrán de un plazo de dos días hábiles a contar desde el día siguiente al de la apertura para efectuar los comentarios y observaciones que les merezcan las distintas propuestas, los que deberán enviarse al correo secretariacaa@diputados.gub.uy.

Artículo 17. Discrepancias.- Si en la oferta hubiera discrepancia entre los precios unitarios y los totales, valdrá el más beneficioso para la Administración.

Cuando exista diferencia entre la cantidad escrita en números y en letras, valdrá la escrita en letras.

De existir diferencia entre los precios expresados en el cuadro resumen de la página de ARCE y los establecidos en la propuesta presentada en archivo adjunto, se tendrán por válidos los primeros.

Artículo 18. Criterios para el análisis de las propuestas.- Las propuestas que cumplan con los aspectos formales y sustanciales exigidos, serán comparadas de acuerdo a los siguientes factores:

Factor	Puntaje máximo a asignar
Precio (i)	50
Características técnicas (ii)	35
Plazo de entrega (iii)	5
Plazo de garantía (iv)	5
Antecedentes con la Administración Pública (v)	5

(i) Se otorgará un puntaje de 50 (cincuenta) puntos al menor precio ofertado. Los precios mayores se ordenarán en forma decreciente e inversamente proporcional, de acuerdo a una regla de tres inversa.

(ii) La División Tecnología de la Información de la Cámara de Representantes establecerá la puntuación correspondiente a la valoración de empresa, la solución y las características técnicas, la que se adjudicará de acuerdo con lo descrito en los Anexos III y IV y tendrá un puntaje máximo de 35 (treinta y cinco) puntos.

(iii) Se otorgará 5 (cinco) puntos al menor plazo de entrega, el cual no podrá ser superior al establecido en el artículo 3° del presente Pliego. Los plazos mayores se ordenarán en forma decreciente e inversamente proporcional, de acuerdo a una regla de tres inversa.

(iv) Se otorgará 5 (cinco) puntos al mayor plazo de garantía. Los plazos menores se ordenarán en forma proporcional, de acuerdo a una regla de tres.

(v) Se otorgará 1 (un) punto por cada antecedente debidamente acreditado mediante documento emitido por el organismo correspondiente, firmado por funcionario con facultades suficientes, hasta un máximo de 5 (cinco) puntos. Para la consideración de los antecedentes presentados, no bastará la simple mención de los mismos, excepto respecto de aquellos correspondientes a la Cámara de Representantes.

Los incumplimientos de las empresas oferentes registrados en el RUPE darán lugar a un descuento de hasta 10 puntos en total. A efectos de determinar el puntaje a restar se aplicará la siguiente tabla:

Por cada advertencia registrada en los últimos 12 meses – 2 (dos) puntos.

Por cada multa registrada en los últimos 18 meses – 3 (tres) puntos.

Por cada suspensión - se considerará el plazo equivalente al doble del período correspondiente a la suspensión, con un mínimo de 18 meses – 5 (cinco) puntos.

Por eliminación de un organismo registrada en los últimos 10 años – 10 (diez) puntos.

Solo se considerarán aquellas ofertas que cumplan en su totalidad con los requerimientos técnicos detallados en el objeto del llamado, especificado en el artículo 1° y con los elementos esenciales especificados en el artículo 9° de este pliego.

Artículo 19. Valoración y consultas.- A efectos de la mejor valoración de las ofertas, la Administración podrá realizar las consultas que estime del caso a los oferentes solicitando las aclaraciones que estime pertinentes.

Artículo 20. Mejora de ofertas y negociaciones.- La Administración queda facultada para utilizar los mecanismos de mejora de ofertas y negociaciones indicados en los artículos 13.4 y 13.5 del Pliego de Condiciones Generales**,** a fin de obtener mejores condiciones de calidad o de precio.

Artículo 21. Anulación del llamado. Llamado sin efecto- La Administración podrá, en cualquier momento antes de la apertura de ofertas, anular el llamado.

En caso de anulación, la misma será comunicada a través de los mismos medios utilizados para la difusión del llamado sin que ello genere derecho a reclamación alguna de parte de los oferentes.

Asimismo, el organismo licitante se reserva el derecho a declarar sin efecto el llamado en la etapa en que se encuentre en caso de entenderlo conveniente.

Artículo 22. Perfeccionamiento del contrato.- El contrato se perfeccionará en el momento en que quede firme la notificación al oferente de la resolución de adjudicación.

En caso de que se interpongan recursos administrativos, la empresa adjudicataria no tendrá derecho a reembolso alguno por los gastos en los que haya incurrido mientras se mantenga el efecto suspensivo de los mismos.

Artículo 23. Adjudicación.- La Administración se reserva el derecho de adjudicar a la oferta que considere más conveniente a sus intereses y a las necesidades del servicio, así como de rechazar todas las ofertas recibidas si a su juicio no resultaren convenientes a sus intereses, no reúnen las condiciones requeridas, o no cumplen las especificaciones que se establecen en el presente Pliego.

El organismo licitante se reserva el derecho de no adjudicar, si así lo considerara conveniente, e incluso adjudicar al siguiente mejor oferente en caso de configurarse los extremos previsto en el inciso 3 del artículo 70 del TOCAF.

El ejercicio de la referida facultad por parte de la Administración no generará derechos a los oferentes para incrementar los precios unitarios propuestos.

La Administración no realizará reembolso ni restitución alguna por concepto de gastos generados por la elaboración de las propuestas presentadas, y no incurrirá en responsabilidad alguna si decidiera rechazar todas las propuestas en cualquier etapa del procedimiento, no generando derecho alguno a favor de los oferentes.

Al momento de la adjudicación, quienes resultaren seleccionados deberán estar inscriptos en el RUPE, con estado “Activo”. En caso contrario, la Administración podrá adjudicar al siguiente mejor oferente, de acuerdo al orden de prelación, o anular la adjudicación.

El adjudicatario no podrá ceder los créditos emergentes del contrato, salvo autorización expresa de la Cámara de Representantes.

Artículo 24. Recepción provisoria.- Se verificará en oportunidad que la solución requerida esté totalmente instalada y funcionando, a juicio de la División Tecnología de la Información de la Cámara de Representantes. Si luego de instalada se constatara que no cumple con alguna de las exigencias detalladas en este pliego, se podrá rechazar el equipo adjudicado.

Artículo 25. Recepción definitiva.- No mediando observaciones, o habiéndose subsanado las mismas, la recepción definitiva a los efectos previstos en el artículo siguiente, se verificará dentro de un plazo de diez (10) días hábiles contados a partir de la recepción provisoria o de subsanadas las observaciones. No obstante, ello no impedirá que se pueda realizar reclamos posteriores.

Artículo 26. Pago.- Configurada la recepción definitiva, el adjudicatario presentará la factura correspondiente al equipo adjudicado en moneda nacional, de acuerdo al precio estipulado en su oferta.

El pago se efectuará dentro de los veinte (20) días hábiles de presentada la factura, por transferencia bancaria a la cuenta registrada en el RUPE, siendo de exclusiva responsabilidad del adjudicatario comunicar fehacientemente a la Administración todo cambio en la misma.

Artículo 27. Mora automática y multas.- Se establece la mora automática para todos los casos de incumplimiento.

Toda demora en la entrega del objeto que le fuera imputable al adjudicatario, será multada en la cantidad equivalente al 5/1000 (cinco por mil) del precio total, por cada día hábil en que dure la misma, lo que en caso de corresponder se descontará del importe facturado.

La multa será aplicada previa vista al adjudicatario y será deducida en forma automática de las facturas presentadas para el cobro, sin que sea necesaria interpelación alguna.

Artículo 28. Sanciones.- Sin perjuicio de las multas por incumplimiento estipuladas en el artículo anterior, todos los incumplimientos podrán dar mérito a la aplicación de las siguientes sanciones, las que podrán ser acumulativas entre sí:

A) Advertencia.

B) Suspensión del proveedor por el tiempo que la Cámara de Representantes determine.

C) Eliminación del infractor como proveedor de la Cámara de Representantes.

Estas sanciones serán comunicadas al RUPE.

Artículo 29. Causales de rescisión.- La demora de la empresa adjudicataria en la entrega -de acuerdo al artículo 3° de este pliego- del objeto adjudicado por un plazo mayor a treinta (30) días corridos, se entenderá como incumplimiento grave, y podrá dar lugar a la rescisión unilateral de la relación contractual.

A esos efectos, si a juicio de la Administración se hubiera producido un incumplimiento, lo notificará al adjudicatario de la forma prevista en el artículo 9° de este Pliego, quien contará con un plazo de tres (3) días hábiles contados desde el siguiente al de la notificación, para formular sus descargos.

Transcurridos los plazos a que refieren los incisos anteriores, la Administración resolverá, y en caso de considerar no justificado debidamente el incumplimiento, podrá rescindir el contrato sin incurrir en ningún tipo de responsabilidad.

La rescisión por incumplimiento del adjudicatario podrá ser acumulativa con el cobro de los daños y perjuicios ocasionados y de la multa establecida en el artículo 27 de este pliego, a criterio de la Administración.

Artículo 30. Beneficios fiscales.- No se otorgarán beneficios fiscales.

Artículo 31. Normativa que rige el llamado.- Este llamado a concurso de precios se rige por:

•El Texto Ordenado de Contabilidad y Administración Financiera (TOCAF) aprobado por el Decreto Nº 150/012, de 11 de mayo de 2012.

•El Pliego Único de Bases y Condiciones Generales para los Contratos de Suministros y Servicios Personales en los Organismos Públicos, aprobado por el Decreto Nº131/014, de 28 de mayo de 2014 (Pliego de Condiciones Generales).

•El presente Pliego de Condiciones Particulares.

•El Decreto 202/024, de 23 de julio de 2024, reglamentario del funcionamiento del Registro Único de Proveedores (RUPE).

Artículo 32. Intervención preventiva del Tribunal de Cuentas.- La adjudicación del objeto de este concurso de precios está supeditada a la intervención preventiva de legalidad a cargo del Tribunal de Cuentas.

ANEXO I – Formulario de identificación del oferente.

El/los que suscribe/n _____ (nombre de quien Firme y tenga poderes suficientes para representar a la empresa oferente acreditados en RUPE, en representación de _____ (nombre de la empresa oferente), declara/n bajo juramento que la oferta ingresada en línea a través del sitio web www.comprasestatales.gub.uy vincula a la empresa en todos sus términos y que acepta sin condiciones las disposiciones del Pliego de Condiciones Particulares del llamado _____ (descripción del procedimiento de contratación), así como las restantes normas que rigen la contratación.

A su vez, la empresa oferente declara contar con capacidad para contratar con el Estado, no encontrándose en ninguna situación que expresamente le impida dicha contratación, conforme lo preceptuado por el artículo 46 del TOCAF y restantes normas concordantes y complementarias.

FIRMA: _____

Aclaración: _____

C.I.: _____

ANEXO II – Formulario de declaración de suministro y existencia permanente de repuestos originales y asistencia de técnicos especializados en el territorio nacional.

El/los que suscribe/n _____, en representación de _____ (nombre de la empresa oferente), declara/n bajo juramento que respecto a concurso de precios N° –/25 de la Cámara de Representantes, que en caso de resultar adjudicados, la empresa garantiza el suministro y la existencia de repuestos originales del equipo ofertado y la asistencia de técnicos especializados en el territorio nacional.

FIRMA: _____

Aclaración: _____

C.I.: _____

Anexo III

			50
Valoración de la empresa	**Especificar**	**Mínimo requerido**	**Max.**
Presencia en el mercado		**5 años**	**10**
Relación con la marca ofertada		**Marca avalada por Forrester y/o Gartner**	**10**
Presencia en cuadrante Gartner		**dentro de los últimos 5 años**	**10**
Partner de la marca ofertada		**Requerido**	**10**
Cartera de clientes		**Especificar**	**10**
			50
Valoración de la solución	**Especificar**	**Mínimo requerido**	**Max.**
Garantía del producto		**3 años mínimo - Especificar**	**10**
Tipo de Garantía		**On-Site (especificar)**	**10**
Asistencia telefónica, email u otra		**Especificar modalidad implementada**	**10**
Reposición frente a rotura		**Especificar tiempo estimado**	**10**
Respuesta a un reclamo		**Especificar modalidad y tiempo**	**10**

Se ponderarán cada fila de la tabla sobre una base de 10 puntos máximo, por lo que la tabla "Valoración de la empresa" tendrá como máximo 50 puntos y la tabla "Valoración de la solución" tendrá un máximo de 50 puntos, totalizando por lo tanto un máximo de 100 puntos entre ambas.

Anexo IV

Tabla de Valoración Técnica	Especificar	**154**
Características generales:		**13**
Se requiere de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de perímetro.		1
El fabricante del NGFW debe ser miembro activo de la organización CTA (Cyber Threat Alliance), garantizando el intercambio de inteligencia de amenazas entre terceros.		1
El equipo propuesto no debe estar listado, ni anunciado por el fabricante como fin de vida (end-of-life) o fin de venta (end-of-sale) o fin de soporte (end of support), se deberá adjuntar un link público o carta del fabricante dirigida al proceso que verifique que el modelo propuesto no está en ese listado.		2
El equipo Next Generation Firewall (NGFW) deberá tener soporte vigente directamente del fabricante durante la vigencia del servicio, el soporte directo del fabricante 24x7 deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo de mismas características en caso de falla de hardware.		2
El oferente deberá indicar en su propuesta la marca, modelo y licenciamiento de los equipos ofrecidos para este proceso.		1
El hardware debe estar diseñado exclusivamente para la función específica de seguridad. No se aceptarán equipos de propósito genérico (PC o servers).		1
No se aceptarán equipos enrutadores con funcionalidad de firewall.		1
Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y/o SSL y/o UDP.		1
El fabricante del firewall propuesto debe contar con certificación ICSA Labs para Firewall.		1
Especificar otras certificaciones del fabricante.		1
Capacidad de realizar backups de la configuración automáticamente también respaldarlos en la nube.		1
Características de rendimiento y hardware		**66**
Rendimiento de Prevención/Protección de Amenazas de al menos 9 Gbps, indicando la metodología para la realización del test. Dicho rendimiento se deberá alcanzar con las siguientes funcionalidades habilitadas simultáneamente: control de aplicaciones, sistema de prevención de intrusos (IPS), Antivirus/Antimalware de red, antispyware/antibot. Se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242.		4
Rendimiento de Antimalware o Antivirus o Antispyware como mínimo de 9.4 Gbps.		4
Rendimiento de Firewall como mínimo de 17.5 Gbps.		4
Rendimiento de IPS como mínimo de 6 Gbps.		4
Rendimiento de IPSec VPN como mínimo de 10.5 Gbps.		4
Rendimiento de Inspección SSL como mínimo de 4.9 Gbps.		4

Indicar rendimiento de Control de Aplicaciones en Gbps.		4
El equipo debe soportar como mínimo 4.000.000 de sesiones/conexiones simultáneas.		4
El equipo debe soportar como mínimo 114.000 sesiones/conexiones por segundo.		4
El equipo debe soportar como mínimo 350.000 sesiones/conexiones DPI SSL.		4
El equipo deberá soportar como mínimo 4.000 túneles VPN Site to Site.		4
Deberá incluir como mínimo 2 puertos 10GE SFP+.		4
Deberá incluir como mínimo 8 puertos 1GE RJ45.		4
Deberá incluir al menos 1 puerto de consola RJ45.		4
Deberá incluir al menos 1 puertos USB 3.0.		4
Deberá incluir al menos 1 puerto de gestión RJ45.		4
Deberá incluir fuente de alimentación 100-240VAC/50-60Hz.		1
Deberá incluir fuente de poder redundante.		1
Características de red		**10**
Especificar soporte de VLAN Tags 802.1q, ruteo multicast, jumbo frames, subinterfaces ethernet lógicas, NAT de origen y destino.		1
Especificar soporte en configuración de alta disponibilidad Activo/Pasivo.		1
Especificar soporte de enrutamiento estático y dinámico (RIPv2, OSPFv2, OSPFv3 y BGP).		1
Especificar soporte NAT de origen y NAT de destino de manera simultánea.		1
Especificar QoS. Garantizar comunicaciones críticas con 802.1p, etiquetado DSCP y reasignación de tráfico VoIP en la red.		1
Enrutamiento basado en políticas o PBR (Policy Based Routing) para que el tráfico sea enrutado a las diferentes interfaces basado en el servicio, las direcciones IP de origen o de destino.		1
Enrutamiento basado en políticas mediante FQDN (Full Qualified Domain Name).		1
Enrutamiento basado en la aplicación (por ejemplo encaminar diferentes aplicaciones por distintas interfaces de salida).		1
Especificar soporte de tecnología SD-WAN.		1
Especificar soporte de Link aggregation, tanto estático como dinámico.		1
Control por políticas de firewall		**11**
Reglas configurables basadas en red de origen, red de destino, protocolo, puerto de comunicación y acción posible.		1
Las acciones posibles deberán incluir como mínimo permitir o denegar tráfico.		1

Adicionalmente las reglas deberán ser configurables considerando grupos de usuarios pertenecientes a la base de datos local del equipo, externos vía LDAP y/o Radius y externos de forma transparente.		1
Especificar manejo de reglas con autenticación realizada de forma no transparente. Indicar si existe un portal de autenticación.		1
Las reglas deberán poder ser configuradas según horarios, incluyendo día, mes y año.		1
Deberá soportar reglas de firewall en IPv6.		1
Inspección de Aplicaciones, IPS, antivirus y filtrado de páginas web sobre comunicaciones cifradas por TLS (Transport Layer Security), como HTTPS, sin importar si opera sobre el puerto 443 u otro.		1
Indicar si el sistema de inspección profunda de paquetes opera bidireccionalmente.		1
Indicar si el sistema de inspección profunda de paquetes opera sin proxies para evitar problemas de latencia.		1
Inspección de tráfico cifrado sobre SSH.		1
Se podrán definir excepciones al tráfico cifrado por dominios o por categorías de páginas web.		1
VPN IPSEC/SSL		**14**
La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.		1
La VPN IPSec debe ser compatible con AES (Advanced Encryption Standard) de 128, 192 y 256 bits.		1
El software agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado en al menos los sistemas operativos Windows y Linux.		4
Conexión para dispositivos móviles de agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado en al menos los sistemas iOS y Android.		4
Indicar el soporte del uso de OTP (One Time Password) para el acceso a la VPN.		1
Deberá soportar autenticación vía AD/LDAP o base de usuarios local.		1
Deberá soportar asignación de direcciones IP y DNS en los clientes remotos.		1
Debe permitir configurar políticas de control de aplicaciones IPS o Antivirus para tráfico de los clientes remotos conectados en la VPN SSL.		1
Control de aplicaciones		**12**
Especificar capacidad de identificación, categorización, control y visualización del tráfico de aplicaciones.		3
Especificar si se identifican independientemente del Stack o del puerto utilizado (TCP, UDP, etc.).		2
Especificar capacidad de hacer el control granular por dirección IP, usuario, grupos de usuarios locales o de LDAP/Active Directory y basado en horarios.		4
Creación de reglas de control de ancho de banda de las aplicaciones soportadas.		1

Reportes en tiempo real de cuáles aplicaciones están siendo usadas, que usuario o dirección IP lo está haciendo y cuánto tráfico está cursando.		1
Indicar periodicidad en la actualización del listado de aplicaciones.		1
Filtrado de contenido web		**8**
Filtro de contenido integrado al NGFW para la clasificación de páginas web. Indicar categorías diferentes y si existe algún mecanismo automático de actualización y consulta.		3
Capacidad de forzar la navegación de los usuarios en el modo Safe Search Enforcement o “Búsqueda Segura” independientemente de la configuración en el navegador del usuario.		1
Soporte de mecanismos de autenticación: RADIUS, TACACS+, Active Directory, LDAP y base de datos interna entre otros.		1
Definición de cuota diaria, semanal o mensual de tiempo de conexión o de tráfico generado por cada usuario.		1
Capacidad de personalizar los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida).		1
Capacidad de definir cuotas de tiempo para la navegación por categoría y por grupos.		1
Prevención de amenazas conocidas		**20**
El dispositivo de seguridad debe poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.		3
Debe ser capaz de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos.		1
Indicar número de perfiles IPS predefinidos.		1
Debe contar con un módulo IPS integrado en el propio dispositivo firewall, con una consola de administración unificada y monitoreo de los dispositivos de seguridad, con soporte para al menos 3.000 firmas.		3
Debe contar con protección contra ataques de inundación (flood) a nivel de UDP, ICMP y SYN Flood.		1
Deberá permitir al administrador ejecutar acciones sobre los eventos de IPS como bloquear el tráfico, registrar o capturar el tráfico generado por el ataque.		1
El IPS deberá ser capaz de inspeccionar el tráfico entre las zonas internas de la red.		1
Deberá contar con mecanismos de antievasión.		1
Deberá contar con filtro de bloqueo hacia centros de comando y control de botnets.		1
Deberá contar con filtro de bloqueo por localización geográfica granular por cada regla de firewall.		1
Debe permitir analizar, tráfico entrante y saliente de al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP, CIFS/NETBIOS, y su administración debe estar integrada a la administración del dispositivo.		1
Debe soportar escaneo de virus o spyware sobre protocolos basados en		1

stream TCP, como Mensajería Instantánea y P2P.		
Debe permitir el análisis antivirus sin limitación del tamaño del archivo transferido y sin que esto afecte la efectividad de la detección de amenazas.		1
Indicar si el sistema antivirus cuenta con la certificación Antivirus ICSA Labs.		1
Deberá contar con actualizaciones automáticas con un intervalo mínimo de búsqueda de actualizaciones de 1 hora.		1
Indicar si la solución cuenta con una nube de inteligencia propietaria del fabricante donde éste se encarga de actualizar la base de seguridad de los dispositivos a través de firmas.		1
Análisis de malware moderno		**11**
Para las amenazas de día cero, la solución debe tener la capacidad de prevenir el ataque antes de que se creen las firmas.		1
El sistema deberá soportar tecnología de análisis de malware de códigos desconocidos en un sistema aislado (Sandbox) donde se ejecutará e inspeccionará el comportamiento del código.		1
El sistema Sandbox deberá operar como un servicio basado en la nube sin necesidad de hardware adicional.		1
El sistema de Sandbox deberá contar con múltiples motores de detección para reducir las técnicas de evasión.		1
Indicar el número de motores de Sandbox.		1
Indicar si el sandboxing incluye inspección en memoria en tiempo real.		1
El sistema deberá hacer un bloqueo del código que se está descargando hasta que se defina un veredicto.		1
Deberá contar con controles de localización geográfica basados en la dirección IP de origen para hacer reglas de conexión por país bien sea de manera general o por reglas de firewall.		1
El sistema deberá ser capaz de prevenir ataques del tipo DNS Tunneling.		1
Deberá soportar el envío manual de archivos para análisis a través del servicio Sandbox.		1

Se deberá completar la tabla indicando, según corresponda, el valor numérico o el grado de cumplimiento de cada ítem. Cualquier aclaración adicional se deberá presentar por separado. Se ponderarán los conceptos de cada fila de la tabla sobre el máximo de puntos indicado en la última columna. Se aplicará donde corresponda la proporcionalidad en función de las propuestas presentadas.

ESTE DOCUMENTO CONTIENE FIRMAS ELECTRÓNICAS AVANZADAS DE:

LIC. SEBASTIÁN VALDOMIR – Presidente

VIRGINIA ORTIZ – Secretaria

Escanee el código QR para acceder al original digital firmado