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 466786 - SBEN1922-25 Actualización de Licencias, Soporte y Mantenimiento para Equipo de Control de Amenazas Centralizadas (UTM Sonicwall)

Consulta 1 - EETT - Números de serie para renovación.

Consulta	Fecha de Consulta	23-10-2025
Solicitamos a la convocante que pueda proveer los datos del UTM Sonicwall, como ser modelo y los números de serie de los equipos para los cuales se debe realizar la actualización de las licencias. Este dato es necesario para que la marca verifique el estado de las mismas y nos puedan proveer los costos de las mismas. Agradeceremos la provisión de estos datos.		

Respuesta	Fecha de Respuesta	24-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado en el SICP. Por otra parte, se aclara lo siguiente: Los números de serie de los equipos SonicWall actualmente operativos constituyen información sensible vinculada a la infraestructura crítica de seguridad perimetral de la ANDE. Su divulgación pública podría comprometer la seguridad de la red institucional. No obstante, conforme a las buenas prácticas de contratación pública y de ciberseguridad (ISO/IEC 27001:2022, cláusulas 5.34 y 8.23), la ANDE verificará internamente el estado de las licencias ante el fabricante SonicWall. El oferente, en cambio, solo deberá cotizar la actualización de las licencias vigentes según las especificaciones técnicas y cantidades establecidas en el Pliego de Bases y Condiciones y la Planilla de Datos Garantizados.		

Consulta 2 - Certificacion ISO 27001

Consulta	**Fecha de Consulta**	23-10-2025

En el PBC en el aparado de Capacidad Técnica, solicitan Sistema de Gestión de Calidad e ISO 27001: Sistema de Gestión de Seguridad de la Información o similares.
El objeto del llamado es la renovación de licencias, soporte y mantenimiento de un equipo ya existente (UTM), y no la provisión de un servicio de outsourcing o gestión integral de la seguridad de la información. La certificación ISO 27001 se exige para asegurar la seguridad de la información que el proveedor procesa o gestiona a largo plazo. En un contrato de soporte, el acceso a información sensible es limitado y esporádico.
La exigencia de un SGSI certificado (ISO 27001) para un contrato de soporte estándar de hardware/ software es una restricción (barrera de entrada) que no añade valor significativo a la calidad del soporte técnico ofrecido, sino que solo incrementa el costo y restringe la participación. Idealmente, debería ser la ANDE quien cuente con esta certificación de SGSI y que ellos la apliquen a los proveedores de manera a que sea el proveedor el que se ajusta a las normas de la entidad y con esto se logra una mayor concurrencia de potenciales oferentes.
Solicitamos a la convocante que el requisito de la ISO 27001 se elimine o, en su defecto, se reemplace por una Declaración Jurada o un NDA que asegure la confidencialidad del proveedor.

Respuesta	**Fecha de Respuesta**	24-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado en el SICP.

Por otra parte, se aclara lo siguiente:

El requerimiento de certificación ISO/IEC 27001 se encuentra plenamente justificado conforme a la naturaleza del servicio. Si bien el objeto del contrato consiste en la renovación de licencias y soporte técnico especializado, el alcance incluye:

- Acceso administrativo remoto a la infraestructura UTM (firewall central de ANDE).

- Intervención sobre políticas de seguridad, VPN, inspección DPI-SSL, IPS y filtrado de contenidos.

- Gestión y Resguardo de configuraciones críticas de la red corporativa.

Estas actividades suponen la interacción directa con información sensible y confidencial, lo que exige que el proveedor cuente con un Sistema de Gestión de Seguridad de la Información (SGSI) certificado bajo estándares internacionales.

La norma ISO 27001 no es exclusiva de servicios de outsourcing, sino de cualquier organización que maneje activos de información críticos, tal como lo define la sección 4 de la norma. Por ello, el requisito no constituye una barrera de entrada, sino un mecanismo objetivo de aseguramiento de la integridad, confidencialidad y disponibilidad de los servicios contratados.

Consulta 3 - Certificacion CEH (Certified Ethical Hacker)

Consulta	**Fecha de Consulta**	23-10-2025

En el PBC en el aparado de Capacidad Técnica, solicitan Técnicos certificados con la certificación CEH o similar equivalente y vigentes relacionadas a configuraciones e implementación de equipos.
La certificación Certified Ethical Hacker (CEH) está diseñada para profesionales que realizan pruebas de penetración (hacking ético), análisis de vulnerabilidades profundas y simulación de ataques. El objeto del llamado de soporte y mantenimiento de un appliance UTM, requiere personal con certificaciones del Fabricante del UTM (ej. Fortinet NSE, Check Point CCSA/CCSE, Sonicwall SNSA, Palo Alto Networks PCNSE), no un especialista en hacking ético.
Exigir una certificación no directamente relacionada con el objeto contractual es un claro elemento direccionador. El personal requerido debe ser experto en la operación y resolución de problemas del equipo específico que se va a mantener (el appliance UTM). Un CEH no garantiza el conocimiento del appliance y una certificación del fabricante sí lo hace.
Solicitamos a la convocante que el requisito de CEH sea eliminado y, en su lugar, se exija una o más certificaciones directamente emitidas por el Fabricante del Equipo de Control de Amenazas Centralizadas (UTM) que se está actualizando, ya que estas son las que garantizan la capacidad de soporte y troubleshooting del appliance específico. De esta manera se podra lograr una mayor participacion de potenciales oferentes.

Respuesta	**Fecha de Respuesta**	24-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado en el SICP.

Por otra parte, se aclara lo siguiente:

El requerimiento de contar con un técnico certificado CEH o equivalente responde a la necesidad de que el personal técnico que acceda a la red de la ANDE comprenda los métodos, técnicas y vectores de ataque utilizados por actores maliciosos.

Si bien la certificación del fabricante (SonicWall) garantiza el conocimiento del producto, no acredita competencias en análisis de vulnerabilidades, explotación de debilidades ni medidas de defensa ofensiva, que son esenciales en la operación de un firewall de siguiente generación.

El CEH (Certified Ethical Hacker) es una certificación internacionalmente reconocida por el ANSI (ISO/IEC 17024) que valida el dominio de técnicas ofensivas aplicadas a la seguridad perimetral. Su exigencia no reemplaza, sino complementa la certificación del fabricante, garantizando que el técnico pueda identificar configuraciones inseguras o vulnerabilidades explotables.

Libre acceso a las certificaciones: Se considera que no existe impedimento alguno para que los técnicos de los oferentes obtengan las certificaciones solicitadas, asegurando así el cumplimiento de los requisitos.

Cabe resaltar que los oferentes también pueden formar alianzas (Consorcios), capacitar o contratar nuevos recursos para cumplir con los requisitos solicitados.

De acuerdo con el apartado "Técnicos Certificados" de las Especificaciones Técnicas, la combinación de ambas certificaciones responde a un enfoque integral de seguridad operativa:

- SonicWall Certified Technician: conocimiento del dispositivo.

- CEH o equivalente: conocimiento de las amenazas y ataques.

Por tanto, el requisito es técnicamente pertinente y proporcional, y su objetivo es fortalecer la resiliencia del entorno de red de la ANDE.

Consulta 4 - Direccionamiento del PBC para un proveedor

Consulta	**Fecha de Consulta**	23-10-2025

Revisando el PBC en el aparado de Capacidad Técnica, solicitan Sistema de Gestión de Calidad e ISO 27001: Sistema de Gestión de Seguridad de la Información o similares, Técnicos certificados con la certificación CEH o similar equivalente y vigentes relacionadas a configuraciones e implementación de equipos. Este mismo requerimiento de capacidad técnica fue requerido en el llamado “LP1873-24 ADQUISICIÓN Y ACTUALIZACIÓN DE SOFTWARE DE CIBERSEGURIDAD (KASPERSKY) A SOLUCIÓN DE DETECCIÓN Y RESPUESTA EXTENDIDA (XDR)” ID: 458987 de la ANDE este año en el cual fue adjudicada la firma Sekiura.
Solicitamos a la convocante que elimine los requerimientos de capacidad técnica de ISO 27001 y de CEH que favorecen directamente a la oferta de Sekiura que sería la única empresa que representa Sonicwall que cumple exactamente con lo solicitado en el PBC.

Respuesta	**Fecha de Respuesta**	24-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado en el SICP.

Por otra parte, se aclara lo siguiente:

El hecho de que un procedimiento licitatorio anterior -como el identificado con ID: 458987- haya incluido requerimientos similares, no constituye evidencia de direccionamiento.

Ambos llamados abordan proyectos distintos, con objetos técnicos diferenciados:

- El proceso anterior trató sobre la ADQUISICIÓN Y ACTUALIZACIÓN DE SOFTWARE DE CIBERSEGURIDAD (KASPERSKY) A SOLUCIÓN DE DETECCIÓN Y RESPUESTA EXTENDIDA (XDR).

- El presente llamado se orienta a la ACTUALIZACIÓN DE LICENCIAS, SOPORTE Y MANTENIMIENTO PARA EQUIPO DE CONTROL DE AMENAZAS CENTRALIZADAS (UTM SONICWALL).

La coincidencia en los requisitos de capacidad técnica se justifica por la naturaleza común del campo de la ciberseguridad, donde los estándares de calidad, seguridad y certificación profesional son internacionalmente reconocidos y adoptados de forma generalizada.

Cabe resaltar que los oferentes también pueden formar alianzas (Consorcios), capacitar o contratar nuevos recursos para cumplir con los requisitos solicitados. Un pliego no es direccional si existen múltiples caminos para cumplirlo.

Además, el propio Pliego de Bases y Condiciones establece que se aceptarán certificaciones "similares o equivalentes", ampliando la participación de empresas que cuenten con otras normas y acreditaciones reconocidas (por ejemplo, ISO 27002, NIST CSF, OSCP, CompTIA Security+, CISSP, entre otras).

Por tanto, los requisitos no limitan la concurrencia ni privilegian a un único proveedor, garantizando la igualdad de condiciones entre oferentes calificados.

Consulta 5 - Especificaciones técnicas modificadas para el equipo solicitado

Consulta	Fecha de Consulta	23-10-2025

Consultamos si este llamado es para la actualización de soporte de licencias o si es una adquisición de un nuevo equipo. Todo esto debido a que hemos verificado que en el llamado anterior “LP1831-24 SERVICIO DE ACTUALIZACIÓN DE LICENCIAS, SOPORTE TÉCNICO Y MANTENIMIENTO PARA EQUIPO DE CONTROL DE AMENAZAS CENTRALIZADAS (UTM SONICWALL)” ID: 442845 están indicadas las especificaciones técnicas del equipo con el que cuenta la ANDE. En el presente llamado encontramos que han cambiado las especificaciones técnicas, especificando un equipo de más capacidad. Estas son las diferencias que hemos verificado entre las EETTs de los llamados mencionados:
En la línea 22 de Content Filtering de las EETTs anteriores solicitaban al menos 55 categorías, ahora solicitan: al menos 56 categorías. En la línea 23 de Application Firewall Service and Networking solicitaban: Soportar Modo Firewall de al menos 8 millones y 129.000 conexiones por seg, ahora solicitan: Modo Firewall de al menos 10 millones, Soportar 130.000 conexiones por seg y Cantidad mínima de conexiones del sistema con los módulos de IPS, Antivirus, Antispyware y Control de Aplicaciones activados (DPI) será de cuatro (4) millones.
En la línea 24 para Intrusion Prevention solicitaban: soporte para al menos 3.000 firmas y ahora solicitan: El sistema IPS contará con al menos 4.800 firmas de ataques. En App Control solicitaban: El rendimiento mínimo del sistema de control de aplicaciones será de 10.5 Gbps y Identificar, categorizar, controlar y visualizar tráfico de más de 3600 aplicaciones agrupadas en al menos 25 Categorías., ahora solicitan: El rendimiento mínimo del sistema de control de aplicaciones será de 11 Gbps y Identificar, categorizar y controlar y visualizar tráfico de más de 4300 aplicaciones agrupadas en al menos 25 Categorías. Para DPI-L/TLS/SSH solicitaban: Soportar conexiones DPI SSL hasta 450 mil. Ahora solicitan: Manejar como mínimo 500000 conexiones concurrentes de tráfico cifrado usando los módulos de protección (IPS, Antimalware y control de aplicaciones) y Soportar conexiones DPI SSL hasta 200 mil. Para VPN SSL solicitaban: cantidad mínima de túneles VPN Site to Site soportados será 6.000 y mínimo 2000 Licencias de cliente VPN para acceso remoto y ahora solicitan: cantidad mínima de túneles VPN Site to Site soportados será 12.000 y mínimo 3000 Licencias de cliente VPN para acceso remoto.

Por favor confirmar si se va a adquirir un equipo nuevo o si van a usar las especificaciones técnicas del equipo actual de acuerdo con las especificaciones del llamado anterior que fue declarado desierto. Nos llama la atencion estos cambios y un direccionamiento a un solo proveedor(representante de la marca solicitada). No permite la lire competencia entre todos los canales que representan Sonicwall.

Respuesta	Fecha de Respuesta	24-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado en el SICP.

Por otra parte, se aclara lo siguiente:

El presente llamado corresponde efectivamente a la actualización de licencias y soporte, no a la adquisición de nuevos equipos. Sin embargo, las especificaciones técnicas mínimas fueron ajustadas y ampliadas conforme a:

1. Evolución del entorno de ciberamenazas, que exige mayores capacidades de inspección, filtrado y rendimiento DPI-SSL.

2. Nuevas versiones de firmware y módulos de seguridad de SonicWall, que incrementan los parámetros de rendimiento.

3. Recomendaciones derivadas del análisis de obsolescencia tecnológica.

En este contexto, los valores actualizados (por ejemplo, incremento de conexiones por segundo o firmas IPS) no representan un cambio de modelo de hardware, sino una actualización de parámetros de desempeño requeridos para mantener la cobertura de soporte y compatibilidad con las últimas licencias de seguridad. Además las Especificaciones Técnicas establecen que en caso de descontinuación o imposibilidad de soporte del fabricante, el proveedor deberá reemplazar los equipos sin costo adicional, manteniendo la vigencia del soporte comprometido - lo cual confirma el carácter de mantenimiento evolutivo, no de adquisición de nuevos equipos.

En resumen, las diferencias detectadas en los valores técnicos no constituyen un requerimiento de nuevo hardware, sino una actualización funcional y de seguridad del software y servicios asociados, con el objetivo de elevar el nivel de protección ante ciberamenazas modernas, por lo que no hay direccionamiento a un proveedor exclusivo.

Consulta 6 - EETTs - Modelo de equipo solicitado

Consulta	Fecha de Consulta	23-10-2025
Solicitamos a la convocante que nos pueda confirmar si el modelo solicitado en las especificaciones tecnicas corresponden a un Sonicwall NSA11700. Entendemos que no es el modelo de appliance con que cuentan actualmente.		

Respuesta	Fecha de Respuesta	24-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado en el SICP.		