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 464312 - LPN N° 39/2025 - SERVICIO DE SOPORTE TÉCNICO INFORMÁTICO

Consulta 1 - Fechas limites

Consulta	Fecha de Consulta	17-03-2026

Favor aclarar las fechas de consultas y apertura, ya que en el pliego figura : Fecha Límite de Consultas: 18/03/2026 12:00
Fecha de Entrega de Ofertas: Fecha de Entrega de Ofertas: 24/03/2026 10:00
y en el portal:
Fecha Límite de Consultas jueves, 19 de marzo de 2026 - 12:00
Fecha de Entrega de Ofertas miércoles, 25 de marzo de 2026 - 10:00

Respuesta	Fecha de Respuesta	17-03-2026

Al respecto, se informa que las fechas a tener en cuenta son las publicadas en el PORTAL - SICP.

Consulta 2 - Consulta N.º 1 – Requisitos de certificación técnica (Lote N.º 1)

Consulta	Fecha de Consulta	17-03-2026

En relación con el requisito establecido para el Lote N.º 1, donde se solicita que el oferente cuente con al menos una certificación de nivel experto (CCIE) en las especialidades indicadas, además de certificaciones de nivel profesional (CCNP), solicitamos respetuosamente a la convocante considerar la revisión de dicho requerimiento.

Al respecto, cabe señalar que las certificaciones de nivel profesional CCNP en sus distintas especialidades (Data Center, Security, Enterprise o Wireless) acreditan competencias técnicas avanzadas suficientes para el diseño, implementación, operación y soporte de infraestructuras de red complejas, alineadas con las tecnologías requeridas en el presente proceso. Las certificaciones de nivel CCNP (Cisco Certified Network Professional) acreditan de manera fehaciente la capacidad técnica para la implementación, configuración y resolución de problemas complejos en entornos corporativos de Data Center, Security y Enterprise. El nivel CCIE, por su parte, está orientado al diseño de arquitecturas de red a nivel de fabricante, excediendo las competencias necesarias para la ejecución de los servicios de soporte y mantenimiento objeto de este pliego.

Asimismo, la exigencia de certificaciones de nivel experto como CCIE podría restringir la participación de oferentes calificados, considerando la limitada disponibilidad de dichos perfiles en el mercado regional, sin que ello represente necesariamente una mejora proporcional en la calidad del servicio requerido.

En ese sentido, y en atención a los principios de igualdad, libre concurrencia y competitividad, solicitamos a la convocante evaluar la posibilidad de:

Eliminar el requisito de certificación CCIE,

Esta modificación permitiría una mayor participación de oferentes técnicamente competentes, garantizando al mismo tiempo el cumplimiento de los objetivos técnicos del proyecto.

Respuesta	Fecha de Respuesta	18-03-2026

En atención a la consulta formulada, y en concordancia con lo previamente establecido la Convocante aclara y precisa lo siguiente:
- Las certificaciones de nivel profesional (CCNP - Cisco Certified Network Professional) y experto (CCIE - Cisco Certified Internetwork Expert) requeridas responden directamente al nivel de especialización necesario para operar, mantener y optimizar infraestructuras de red complejas y de alta criticidad, incluyendo, entre otras, las siguientes tecnologías:

- Cisco ACI
- Cisco ISE
- Cisco DNA Center
- Cisco Meraki
- Infraestructura de Switching, Routing y Seguridad

Estas plataformas constituyen el núcleo de la arquitectura de red institucional, cuya indisponibilidad o degradación podría generar impactos operativos significativos, afectando servicios críticos y sensibles a la continuidad operativa.
En este contexto, la exigencia de contar con certificaciones de nivel profesional y experto no excede el alcance de los servicios requeridos, sino que resulta plenamente coherente y proporcional, considerando que el soporte solicitado contempla no solo tareas operativas, sino también:
- Diagnóstico avanzado y análisis de fallas complejas.
- Mitigación y resolución de incidentes en entornos de misión crítica.
- Optimización del desempeño y estabilidad de la infraestructura.
- Atención de contingencias y escalamiento técnico especializado.

Particularmente, el nivel CCIE garantiza experiencia práctica comprobada, criterio técnico y capacidad de resolución en escenarios de alta complejidad, complementando las competencias del nivel CCNP. Si bien las certificaciones de nivel profesional (CCNP - Cisco Certified Network Professional) acreditan conocimientos sólidos para la implementación, operación y soporte de redes empresariales, el nivel CCIE valida, además, habilidades avanzadas en diagnóstico, análisis profundo, resolución de incidentes de alta complejidad y toma de decisiones en entornos de misión crítica, donde los tiempos de indisponibilidad y el impacto operativo deben reducirse al mínimo.
Por tanto, su inclusión tiene como finalidad asegurar que el oferente disponga de un recurso altamente calificado que actúe como referente técnico ante situaciones críticas, sin que ello implique una exigencia desproporcionada.
Asimismo, se deja constancia de que este requisito:
- Garantiza una capacidad real y verificable de respuesta técnica ante incidentes complejos.
- Se encuentra alineado con el alcance y criticidad de los servicios requeridos.
- No limita la participación a un proveedor específico, dado que dichas certificaciones constituyen estándares ampliamente reconocidos y accesibles a múltiples integradores del mercado.

Adicionalmente, se contempla la posibilidad de contar con staff regional, siempre que se garantice el cumplimiento de los tiempos de atención establecidos y la disponibilidad de soporte in situ cuando corresponda, lo cual amplía la concurrencia y favorece la competitividad del proceso.
Por lo expuesto, la Convocante mantiene el requerimiento de certificaciones CCNP y CCIE, por considerarlo técnica y operativamente justificado, y alineado con los objetivos de calidad, continuidad del servicio y mitigación de riesgos del presente proceso.

Consulta 3 - Consulta N.º 2 – Requisitos de certificación técnica (Lote N.º 3)

Consulta	**Fecha de Consulta**	17-03-2026

En relación con los requisitos establecidos para el Lote N.º 3, específicamente aquellos vinculados a certificaciones técnicas del fabricante para equipos Next Generation Firewall (NGFW) Check Point, solicitamos respetuosamente a la convocante considerar la revisión de dicho requerimiento.

Al respecto, es importante señalar que las tecnologías de Next Generation Firewall (NGFW) comparten principios, arquitecturas y funcionalidades comunes entre distintos fabricantes del mercado, tales como control de aplicaciones, inspección profunda de paquetes (DPI), prevención de intrusiones (IPS), filtrado web y gestión centralizada de políticas de seguridad.

En ese sentido, la experiencia técnica en plataformas NGFW de distintos fabricantes permite a los profesionales adquirir competencias plenamente transferibles para la implementación, administración y soporte de soluciones de seguridad equivalentes, independientemente de la marca específica.

El objeto de la contratación se centra en el soporte de configuración y mantenimiento lógico, y no en la provisión o recambio de hardware. En este ámbito, los protocolos, arquitecturas de red y políticas de seguridad son estándares globales. Un profesional con certificaciones de seguridad profesional posee las competencias necesarias para gestionar la configuración de estos equipos de manera eficiente.

Limitar la participación exclusivamente a certificaciones de un solo fabricante restringe la libre concurrencia de empresas con amplia trayectoria en ciberseguridad que cuentan con personal altamente capacitado en los conceptos técnicos requeridos, cumpliendo con el mismo estándar de calidad.

Lo fundamental para el éxito del servicio es el dominio de los términos de seguridad y la gestión de vulnerabilidades, capacidades que son transversales a las distintas plataformas del mercado.

Asimismo, la exigencia exclusiva de certificaciones emitidas por un fabricante en particular podría limitar la participación de oferentes técnicamente calificados, afectando los principios de igualdad, libre concurrencia y competitividad.

En virtud de lo expuesto, solicitamos a la convocante evaluar las siguientes alternativas:

Eliminar la obligatoriedad de certificaciones específicas del fabricante, permitiendo en su lugar la participación de técnicos idóneos cuya experiencia pueda ser acreditada mediante declaración jurada, acompañada de documentación que respalde su experiencia en implementación y soporte de soluciones NGFW.

Alternativamente, permitir la presentación de certificaciones equivalentes de nivel profesional o experto en tecnologías NGFW, independientemente del fabricante (por ejemplo, certificaciones en otras plataformas líderes del mercado), considerando la equivalencia funcional y técnica entre dichas soluciones.

Esta flexibilización permitiría ampliar la participación de oferentes, garantizando al mismo tiempo la calidad técnica requerida para la correcta ejecución del servicio.

Respuesta	**Fecha de Respuesta**	18-03-2026

En atención a la Consulta N.º 2, y en concordancia con los criterios técnicos ya establecidos en el Pliego de Bases y Condiciones, la Convocante se permite aclarar y ampliar lo siguiente:
Los requisitos de certificación técnica asociados al Lote N.º 3, específicamente las certificaciones CCSA (Check Point Certified Security Administrator) y CCSE (Check Point Certified Security Expert) o superiores, responden al nivel de especialización necesario para la correcta administración, configuración y soporte de las soluciones de seguridad Next Generation Firewall (NGFW) de tecnología Check Point, las cuales forman parte del alcance directo de intervención del presente lote.
Si bien es correcto que las soluciones NGFW comparten principios generales de funcionamiento -tales como inspección profunda de paquetes (DPI), prevención de intrusiones (IPS), control de aplicaciones y gestión de políticas de seguridad-, cada fabricante implementa dichas funcionalidades mediante arquitecturas, motores de inspección, estructuras de políticas y herramientas de gestión propias. En el caso particular de Check Point, estas características incluyen elementos específicos como su sistema operativo, su arquitectura de políticas unificadas, el uso de SmartConsole, gateways de seguridad, blades de protección y mecanismos propios de gestión centralizada, los cuales requieren conocimientos especializados y experiencia directa en dicha plataforma.
En este sentido, el alcance del servicio no se limita a conceptos generales de ciberseguridad, sino que involucra la operación, mantenimiento lógico, diagnóstico y resolución de incidentes directamente sobre equipamiento instalado de tecnología Check Point, por lo que resulta técnicamente necesario que el personal asignado cuente con certificaciones específicas del fabricante que acrediten conocimiento profundo y experiencia práctica en dicha solución.
En relación con la solicitud de eliminar la obligatoriedad de certificaciones específicas del fabricante y sustituirlas por la acreditación de experiencia mediante declaración jurada, esta Convocante considera pertinente señalar que, precisamente, el requerimiento de certificaciones técnicas tiene como finalidad principal acreditar de manera objetiva, verificable y estandarizada la idoneidad del personal propuesto, a través de las certificaciones requeridas
Asimismo, se deja expresa constancia que la exigencia de certificaciones CCSA y CCSE (o superiores):
- Busca garantizar la capacidad real de administración, diagnóstico y resolución de incidentes sobre la plataforma específica implementada.
- Asegura el conocimiento de las mejores prácticas y herramientas propias del fabricante.
Resulta proporcional al alcance del servicio requerido, considerando la criticidad de la infraestructura de seguridad involucrada.
Adicionalmente, se establece que el equipo técnico propuesto cumpla en conjunto con las certificaciones solicitadas, lo cual introduce un criterio de flexibilidad, evitando que dicho requisito sea excluyente respecto de una sola persona y permitiendo la conformación de equipos complementarios.
Por otra parte, se aclara que este requerimiento no limita la participación a un único proveedor, puesto que las certificaciones mencionadas constituyen estándares del fabricante ampliamente disponibles en el mercado y accesibles a múltiples integradores y empresas especializadas en ciberseguridad.
Por lo expuesto, y considerando la naturaleza del servicio, la criticidad de los servicios involucrados, la necesidad de garantizar una operación segura, eficiente y alineada a las mejores prácticas, se mantiene el requerimiento de certificaciones CCSA y CCSE (o superiores) para el Lote N.º 3, por considerarlo técnica y operativamente justificado, además acorde al objeto y al alcance del equipamiento comprendido en el presente lote.

Consulta 4 - Lote 4- Alcance operativo del NOC

Consulta	Fecha de Consulta	19-03-2026
Considerando que el servicio de monitoreo incluye infraestructura on-premise, nubes públicas (OCI, Azure u otras) y servicios transaccionales, se solicita confirmar si el alcance del Lote N° 4 se limita exclusivamente a detección, notificación y escalamiento, o si incluye acciones de mitigación o intervención técnica directa por parte del proveedor.		

Respuesta	Fecha de Respuesta	20-03-2026
Se confirma que el alcance del Lote N° 4 se limita exclusivamente a la detección, correlación, notificación y escalamiento de eventos. Conforme al PBC, el objeto es que el proveedor "realice el monitoreo permanente e informe en tiempo y forma a través de un protocolo de escalamiento priorizado", siendo la atención y solución de los incidentes responsabilidad de los funcionarios del BCP. El servicio no incluye acciones de mitigación o intervención técnica directa por parte del proveedor.		

Consulta 5 - Lote 4 - Uso obligatorio de herramientas del BCP

Consulta	Fecha de Consulta	19-03-2026
Se solicita confirmar si el proveedor deberá utilizar exclusivamente las herramientas de monitoreo provistas por el BCP (PRTG, DCIM, Dynatrace, Grafana), o si se permite el uso complementario de herramientas propias del proveedor, siempre que no interfieran ni dupliquen funciones.		

Respuesta	Fecha de Respuesta	20-03-2026
Conforme al PBC, el Sistema de Monitoreo del BCP incluye las herramientas PRTG, DCIM, Dynatrace, Grafana y otros dispositivos que notifican alertas de manera independiente mediante protocolo TCP/IP. El PBC establece que el Personal de Monitoreo realizará sus funciones "mediante las herramientas de monitoreo provistas por el BCP". Adicionalmente, entre los recursos que proveerá el BCP se encuentran "los accesos necesarios y debidamente autorizados a las plataformas y herramientas de monitoreo" y el "acceso a herramientas de monitoreo relacionadas al Servicio de Monitoreo". Sin embargo, la Responsabilidad N° 5 del Proveedor establece que este deberá "proveer una herramienta para el registro y seguimiento de incidentes objeto del servicio a ser contratado", lo cual constituye una herramienta propia del proveedor complementaria al sistema de monitoreo del BCP		

Consulta 6 - Lote 4 - Medición de SLA de notificación

Consulta	Fecha de Consulta	19-03-2026
Para los tiempos de notificación establecidos (≤5 minutos al BCP), se solicita aclarar desde qué evento se computa el tiempo: a) desde la generación del evento en la herramienta b) desde la recepción del evento por el personal de monitoreo c) desde la validación manual del evento		

Respuesta	Fecha de Respuesta	20-03-2026
Dado que el PBC describe que el monitoreo se realiza "en un esquema de alertas mostradas y notificadas por el Sistema de Monitoreo" y que el Personal de Monitoreo es el "encargado del monitoreo 24x7 de los eventos mediante las herramientas de monitoreo provistas por el BCP", se entiende que el cómputo se inicia desde la generación/visualización del evento en la herramienta de monitoreo.		

Consulta 7 - Lote 4 - Cantidad mínima de operadores

Consulta	Fecha de Consulta	19-03-2026
Se solicita confirmar si la exigencia de “al menos 1 personal de monitoreo” es por turno o por servicio en total, y si se admite un esquema N:1 donde un operador atienda múltiples clientes, siempre que se cumplan los SLA.		

Respuesta	Fecha de Respuesta	20-03-2026
El PBC requiere "al menos 1 (un) Personal de Monitoreo asignado en forma remota", lo cual establece el mínimo de personal monitoreando en todo momento, no una dotación total. Al tratarse de un servicio 24x7x365, el proveedor deberá dimensionar la cantidad de operadores por turno necesaria para garantizar esa cobertura continua. El PBC indica expresamente que los trabajos "no requieren ser exclusivos para el Banco Central del Paraguay", admitiéndose un esquema compartido siempre que se cumplan los SLA. La dotación real queda a criterio del proveedor conforme a su Responsabilidad N° 1: "contar con la cantidad de personal técnico especializado necesario para cumplir con el servicio en tiempo y forma".		

Consulta 8 - Lote 4 - Responsabilidad sobre el enlace VPN

Consulta	Fecha de Consulta	19-03-2026
Considerando que el proveedor debe proveer el enlace de carrier para la VPN sitio a sitio, se solicita aclarar si las indisponibilidades del servicio ocasionadas por fallas del enlace de comunicaciones del BCP quedan excluidas del cómputo de SLA del proveedor.		

Respuesta	Fecha de Respuesta	20-03-2026
El PBC establece que el proveedor deberá "proveer el enlace de carrier para enlace VPN entre el BCP y el Proveedor". Por su parte, el BCP asume la responsabilidad de proveer "el acceso remoto seguro mediante herramientas a ser proveídas por el BCP" así como "el/los equipos de red para establecer los citados enlaces VPNs del lado del BCP". Dado que ambas partes tienen responsabilidades diferenciadas sobre los componentes de la conectividad, el cómputo de SLA del proveedor deberá evaluarse considerando el correcto cumplimiento de las obligaciones que el PBC asigna a cada parte para la operatividad del servicio.		

Consulta 9 - Lote 4 - Límite de responsabilidad del proveedor

Consulta	Fecha de Consulta	19-03-2026
Se solicita confirmar que el proveedor del Lote N° 4 no es responsable por la resolución técnica del incidente, sino únicamente por la correcta detección, notificación, seguimiento y escalamiento conforme a los procedimientos definidos por el BCP.		

Respuesta	Fecha de Respuesta	20-03-2026
Conforme al PBC, el proveedor del Lote N° 4 es responsable de la correcta detección, notificación, seguimiento y escalamiento de eventos conforme a los procedimientos del BCP. La resolución técnica de los incidentes corresponde a "los funcionarios responsables de dichos servicios de misión crítica de la GTIC", no al proveedor del servicio de monitoreo.		