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 484674 - LPN N° 40/2026 - SERVICIO DE RESPUESTA ANTE INCIDENTES CIBERNÉTICOS (CSIRT EXTERNO)

Consulta 1 - Consultas Técnicas - SISAP

Consulta	Fecha de Consulta	24-09-2026

Nos pueden indicar ¿que identifican a nivel del Banco como activo y qué identifican como fuentes de datos?

¿Cuántos activos en total tienen en la organización?, Entiéndase como activo cualquier dispositivo que se conecte a la red interna por medio de una dirección IP.

¿Cuántas direcciones IP en total tienen bajo alcance de monitoreo?

¿Se espera que se haga el monitoreo a través del SIEM de Qradar?

El SIEM de QRadar, para la gestión de la consola de ¿quién sería responsabilidad?

¿Nos pueden enviar el detalle de las fuentes de datos que se van a integrar a la solución SIEM, como cantidad y marca, tipo de integración al SIEM (Syslog o API)?

Se puede incluir un SIEM adicional para el monitoreo complementario de los activos de la organización? si la respuesta es sí:
- ¿Debe ser en premisa o puede estar en nube?
- ¿Puede ser en una instancia MSSP o debe estar a nombre del Banco?
- Hay alguna restricción para almacenamiento de logs, ¿cuánto tiempo en frío y cuánto en caliente?
- ¿Cuántos centros de datos tienen? En caso de tener más de uno, los servicios salen de forma independiente? o los centros de datos son réplicas en caso de fallas?
- Dentro de la infraestructura de red, ¿se puede contar con un puerto espejo hacia el colector de logs?

Tienen servicios o infraestructura a monitorear en nube?, si la respuesta es sí:
- ¿Cuáles nubes?
- ¿Cuántos activos?
- ¿Cuál es el throughput de la red de la o las nubes?

De la herramienta de EDR, nos pueden indicar si la solución es on premise o cloud?

¿La solución de EDR está desplegada en todas las máquinas de la compañía?

¿El SIEM que actualmente tienen (QRadar) se va tomar como una fuente de datos adicional para la integración y enriquecimiento con el nuevo SIEM?

Cuando indican cierre de brechas, a qué tipo de brechas se refiere, y es porque se requiere que el cierre las haga el proveedor?

Para la simulación anual de ciber incidentes:
- ¿Cuentan con un Plan de respuesta a incidentes ya documentado?
- ¿Para qué tipo de incidentes se tienen creados procedimientos de respuesta a incidentes?
- ¿Cuentan con procedimientos ya creados para ejecución del TableTop? Si la respuesta es sí: Nos pueden indicar un aproximado de cuantos tienen creados y sobre qué escenarios?

Respuesta	Fecha de Respuesta	30-09-2026

La información relativa a la cantidad de activos, direcciones IP, fuentes de datos, arquitectura tecnológica, infraestructura de red, centros de datos, herramientas de seguridad, servicios en nube y demás componentes de la infraestructura tecnológica de la Convocante constituye información sensible y, por razones de seguridad, no será divulgada durante la etapa de licitación. El servicio deberá prestarse conforme al alcance, requerimientos y condiciones establecidos en el PBC y en las Especificaciones Técnicas. La información adicional que resulte necesaria para la correcta ejecución del servicio será proporcionada al proveedor adjudicado durante la etapa de implementación y/o ejecución contractual, conforme a los procedimientos de seguridad y acuerdos de confidencialidad aplicables. Asimismo, las actividades de monitoreo, detección, análisis, respuesta ante incidentes, simulaciones y cierre de brechas deberán ejecutarse de conformidad con lo establecido en el PBC y sus Especificaciones Técnicas.

Consulta 2 - EXPERIENCIA REQUERIDA

Consulta	Fecha de Consulta	25-09-2026

Respecto al requisito de experiencia establecido en el PBC, entendemos que podrán ser considerados contratos de prestación de servicios SOC u otros servicios similares, siempre que de la documentación presentada se desprenda expresamente que su alcance incluyó actividades relacionadas con la contención, investigación, respuesta y recuperación ante incidentes de ciberseguridad, así como la detección y/o análisis de dichos incidentes.
Solicitamos a la Convocante confirmar si nuestra interpretación es correcta.

Respuesta	Fecha de Respuesta	30-09-2026

Serán considerados válidos contratos de servicios SOC u otros servicios equivalentes o similares, siempre que de la documentación respaldatoria presentada se pueda verificar fehacientemente la ejecución de actividades relacionadas con la detección, análisis, contención, investigación, respuesta, recuperación y gestión de incidentes de ciberseguridad, conforme a los requisitos establecidos en el PBC.

Consulta 3 - EETT / CAPACIDAD DEL EQUIPO TÉCNICO

Consulta	Fecha de Consulta	25-09-2026

Considerando que la adjudicación del llamado se realizará por la totalidad y que las Especificaciones Técnicas permiten que un mismo profesional cubra más de un perfil cuando acredite documentalmente los requisitos exigidos para cada uno, entendemos que un profesional podrá ser propuesto simultáneamente para un perfil del Ítem N.° 1 y otro del Ítem N.° 2. Por ejemplo, una misma persona podría ser propuesta como Líder de Servicio / Coordinador CSIRT del Ítem N.° 1 y como Líder de Respuesta ante Incidentes / Coordinador Técnico del Ítem N.° 2, siempre que cumpla íntegramente los requisitos de formación, certificaciones y experiencia establecidos para ambos perfiles, y que la acumulación de funciones no afecte la disponibilidad, capacidad de respuesta, continuidad ni calidad del servicio.
Solicitamos a la Convocante confirmar si nuestra interpretación es correcta.

Respuesta	Fecha de Respuesta	30-09-2026

La interpretación es correcta, favor adecuarse a lo establecido en el PBC.

Consulta 4 - EETT - Plataforma SaaS de gestión de tickets

Consulta	Fecha de Consulta	25-09-2026

Respecto de la plataforma SaaS de gestión de tickets requerida, solicitamos confirmar si se aceptará una plataforma empresarial de gestión de servicios y atención de casos que permita a veinte (20) usuarios autorizados del BCP registrar, consultar, actualizar, dar seguimiento y auditar los tickets gestionados, y que cuente con MFA, RBAC, registros de auditoría, cifrado en tránsito y en reposo y capacidades de exportación.
Asimismo, solicitamos confirmar si las certificaciones ISO/IEC 27001 y los informes SOC 2 o SOC 1 podrán corresponder al fabricante o proveedor de servicios en la nube de la plataforma ofertada, siempre que esta se encuentre expresamente incluida dentro de su alcance y el oferente presente documentación vigente y verificable.
En tal caso, solicitamos confirmar que no será obligatorio que el oferente o integrador posea adicionalmente un informe SOC 1 o SOC 2 propio.
Finalmente, solicitamos aclarar si las veinte (20) licencias podrán acreditarse conforme al esquema oficial de licenciamiento del fabricante, siempre que garanticen a veinte usuarios del BCP las funciones de seguimiento, consulta, actualización y auditoría exigidas.

Respuesta	Fecha de Respuesta	30-09-2026

Se confirma que serán aceptadas plataformas SaaS de gestión de tickets que cumplan con los requisitos funcionales y de seguridad establecidos en el PBC. Las certificaciones ISO/IEC 27001 y los informes SOC 1 y/o SOC 2 podrán corresponder al fabricante de la solución o al proveedor de infraestructura que la soporte, siempre que la solución ofertada forme parte de su alcance. Las licencias serán aceptadas conforme al esquema oficial del fabricante, debiendo garantizar las funcionalidades requeridas para los veinte (20) usuarios previstos en el PBC.