

Consultas Realizadas

Licitación 485892 - SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Consulta 1 - Consulta sobre PBC

Consulta	Fecha de Consulta	15-06-2026
En relación con el requisito que establece que el oferente debe contar con al menos un Centro de Operaciones de Seguridad (SOC) en la República del Paraguay y al menos otro ubicado a una distancia mínima de 500 km del primero, solicitamos amablemente se sirvan aclarar el fundamento técnico y operativo de dicha exigencia. En particular, agradeceríamos conocer cuál es el objetivo específico que se busca garantizar mediante la distancia mínima requerida entre ambos SOC, así como los criterios técnicos utilizados para determinar el umbral de 500 km. La presente consulta tiene por finalidad comprender de mejor manera el alcance del requerimiento y verificar su relación con la continuidad operativa, redundancia, recuperación ante desastres u otros aspectos técnicos asociados a la prestación del servicio, a efectos de asegurar una correcta interpretación de las Especificaciones Técnicas por parte de los potenciales oferentes. Asimismo, agradeceríamos confirmar si el objetivo del requisito podría ser igualmente satisfecho mediante mecanismos alternativos de alta disponibilidad, redundancia geográfica, planes de continuidad del negocio o recuperación ante desastres debidamente documentados, independientemente de la distancia física específica entre los centros de operación. Agradecemos desde ya la aclaración que puedan brindar.		

Consulta 2 - Sobre la Maestría obligatoria para el Director General

Consulta	Fecha de Consulta	18-06-2026
Solicitamos justificar técnicamente la exigencia de una maestría obligatoria para el Director General del Servicio, considerando que certificaciones internacionales especializadas como CISSP, CISM o CCISO son reconocidas globalmente como credenciales de mayor especialización práctica en ciberseguridad que muchos programas académicos de posgrado.		

Consulta 3 - Sobre la Maestría obligatoria para el Director General

Consulta	Fecha de Consulta	18-06-2026
Solicitamos aclarar por qué no se contempla la posibilidad de compensar la exigencia de maestría mediante experiencia profesional comprobada adicional o certificaciones internacionales de alto nivel, lo que podría ampliar la concurrencia sin afectar la calidad del servicio.		

Consulta 4 - Sobre la acumulación excesiva de certificaciones

Consulta	Fecha de Consulta	18-06-2026
Solicitamos justificar la necesidad de exigir simultáneamente múltiples certificaciones de gestión y técnicas para un mismo recurso, considerando que certificaciones como CISSP, CISM, CCISO, ISO 27032 Lead Cybersecurity Manager e ISO 27035 Lead Incident Manager presentan amplios solapamientos de contenido y competencias.		

Consulta 5 - Estudio de mercado a fin de solicitar ciertos requisitos excesivos

Consulta	Fecha de Consulta	18-06-2026
Solicitamos aclarar si la convocante realizó un estudio de mercado que determine cuántos profesionales residentes permanentes en Paraguay cumplen simultáneamente con los requisitos de maestría, certificaciones internacionales y experiencia solicitados.		

Consulta 6 - Sobre el requisito de formar parte del staff

Consulta	Fecha de Consulta	18-06-2026
Solicitamos justificar la necesidad de que la totalidad de los especialistas formen parte del staff permanente del oferente desde la presentación de ofertas, considerando que la contratación de especialistas para proyectos específicos es una práctica habitual en la industria de ciberseguridad.		

Consulta 7 - Sobre el Especialista Threat Hunting

Consulta	Fecha de Consulta	18-06-2026
Solicitamos justificar la necesidad de exigir cuatro certificaciones específicas de Blue Team o Threat Hunting para un único recurso, considerando que la experiencia práctica en operaciones SOC suele tener mayor relevancia operativa que la acumulación de múltiples certificaciones teóricas.		

Consulta 8 - Sobre los Analistas de Ciberseguridad

Consulta	Fecha de Consulta	18-06-2026
Solicitamos aclarar por qué se exige específicamente ISO 27001 Lead Auditor, CEH o Security+, excluyendo otras certificaciones equivalentes ampliamente reconocidas en el mercado internacional.		

Consulta 9 - Consulta sobre especificaciones técnicas

Consulta	Fecha de Consulta	18-06-2026
Solicitamos confirmar que serán aceptadas arquitecturas basadas en software libre, plataformas open source o soluciones híbridas, siempre que cumplan con los niveles de servicio requeridos.		

Consulta 10 - SOC EN PARAGUAY Y CENTRO ALTERNO

Consulta	Fecha de Consulta	18-06-2026
Solicitamos justificar técnicamente la exigencia de contar previamente con: "un SOC en Paraguay y otro a más de 500 km" considerando que el servicio solicitado es gestionado y no implica necesariamente la instalación de infraestructura física en dependencias de la Convocante.		

Consulta 11 - Estudio de mercado a fin de solicitar ciertos requisitos excesivos

Consulta	Fecha de Consulta	18-06-2026
Solicitamos informar si se realizó un relevamiento de mercado que determine cuántos proveedores cumplen actualmente con la exigencia simultánea de poseer dos SOC operativos bajo dichas condiciones geográficas.		

Consulta 12 - SOC

Consulta	Fecha de Consulta	18-06-2026
Solicitamos aclarar si se aceptarán SOC regionales o internacionales certificados que acrediten alta disponibilidad y continuidad operativa equivalente.		

Consulta 13 - Finalidad del requisito de contar con dos SOC separados por 500 km

Consulta	Fecha de Consulta	26-06-2026
Se solicita a la Convocante aclarar cuál es el objetivo técnico y operativo que persigue el requisito de que el oferente cuente con un Centro de Operaciones de Seguridad (SOC) en la República del Paraguay y otro adicional ubicado a una distancia mínima de 500 km. En particular, se solicita indicar qué riesgo específico se busca mitigar mediante esta separación geográfica y de qué manera dicho requisito contribuye a la continuidad operativa del servicio solicitado.		

Consulta 14 - Definición de qué será considerado un SOC

Consulta	Fecha de Consulta	26-06-2026
Se solicita a la Convocante establecer una definición objetiva de qué será considerado un Centro de Operaciones de Seguridad (SOC) a efectos del presente proceso. En particular, se solicita aclarar si será suficiente la existencia de un inmueble declarado como SOC o si deberá tratarse de un centro operativo con infraestructura tecnológica, personal especializado, herramientas SIEM/SOAR, capacidad real de monitoreo 24x7 y procesos documentados. Lo anterior a fin de evitar interpretaciones subjetivas durante la evaluación de las ofertas.		

Consulta 15 - Documentación probatoria

Consulta	Fecha de Consulta	26-06-2026
Se solicita a la Convocante indicar expresamente cuál será la documentación que deberá presentar el oferente para acreditar que el sitio ubicado a más de 500 km constituye efectivamente un Centro de Operaciones de Seguridad (SOC) plenamente operativo y no únicamente una oficina administrativa o un inmueble arrendado. Asimismo, se solicita indicar si serán requeridos documentos tales como: Contratos de propiedad o alquiler. Fotografías de las instalaciones. Inventario de infraestructura. Relación de personal asignado. Diagramas de arquitectura. Certificaciones. Evidencias de operación 24x7. Otros documentos que la Convocante considere pertinentes.		

Consulta 16 - Forma de acreditar la distancia

Consulta	Fecha de Consulta	26-06-2026
Se solicita aclarar cuál será el criterio que utilizará la Convocante para verificar el cumplimiento de la distancia mínima de 500 km entre ambos SOC. Asimismo, indicar si dicha distancia será medida en línea recta (coordenadas geográficas), por vía terrestre o mediante algún otro criterio técnico.		

Consulta 17 - Relación entre el requisito y la continuidad operativa

Consulta	Fecha de Consulta	26-06-2026
Considerando que el numeral corresponde al apartado "Continuidad operativa del servicio", se solicita aclarar cómo el requisito de separación geográfica de los SOC garantiza por sí mismo la continuidad operativa del servicio, considerando que dicha continuidad depende además de la disponibilidad de las comunicaciones entre ambos centros.		

Consulta 18 - Redundancia de telecomunicaciones

Consulta	Fecha de Consulta	26-06-2026
En caso de que la finalidad del requisito sea garantizar la continuidad operativa del servicio ante contingencias, se observa que el Pliego no establece requisitos mínimos respecto de la redundancia de los enlaces de telecomunicaciones que interconectan ambos SOC. En ese sentido, se solicita aclarar si la Convocante considera necesario exigir, entre otros aspectos: - enlaces redundantes; - proveedores de telecomunicaciones distintos; - trayectos físicos diferenciados; - múltiples salidas internacionales; - mecanismos de conmutación automática ante fallas. Lo anterior considerando que estos elementos constituyen prácticas ampliamente aceptadas para garantizar la disponibilidad continua de los servicios de monitoreo y respuesta ante incidentes.		

Consulta 19 - Capacidad de operación del SOC alterno

Consulta	Fecha de Consulta	26-06-2026
Se solicita aclarar si el SOC ubicado a más de 500 km deberá contar con capacidad para asumir el 100% de la operación en caso de indisponibilidad del SOC principal o si únicamente se requiere su existencia física. Asimismo, indicar si deberá contar con infraestructura, personal y licencias equivalentes al SOC principal para garantizar la continuidad del servicio.		

Consulta 20 - Aplicación durante toda la vigencia contractual

Consulta	Fecha de Consulta	26-06-2026
Se solicita aclarar si ambos SOC deberán permanecer plenamente operativos durante toda la ejecución contractual y cuál será el mecanismo mediante el cual la Convocante verificará el mantenimiento de dicho requisito durante la vigencia del contrato.		

Consulta 21 - Consulta

Consulta	Fecha de Consulta	26-06-2026
La separación geográfica de dos SOC constituye únicamente uno de los componentes de un esquema de continuidad del negocio. Sin embargo, por sí sola no garantiza la disponibilidad del servicio si no se complementa con una arquitectura de alta disponibilidad que contemple redundancia de infraestructura, replicación de datos, enlaces de comunicaciones independientes, proveedores de telecomunicaciones distintos, rutas físicas diferenciadas y procedimientos de recuperación ante desastres (DRP). En consecuencia, se solicita a la Convocante aclarar el fundamento técnico por el cual únicamente se exige la separación geográfica de los SOC, sin establecer requisitos mínimos respecto de los demás componentes esenciales para asegurar la continuidad operativa.		

Consulta 22 - Experiencia requerida — período y forma de acreditación

Consulta	Fecha de Consulta	30-06-2026
Sección: Requisitos de Participación — Experiencia Requerida Respecto del requisito de experiencia, que conforme al pliego puede acreditarse mediante facturaciones y/o contratos de los ejercicios 2023, 2024 y 2025, solicitamos se considere ampliar el período computable para incluir también los ejercicios 2021 y 2022.		

Consulta 23 - Antigüedad IPS de los perfiles de conducción

Consulta	Fecha de Consulta	30-06-2026
Sección: Requisitos de Participación — Capacidad Técnica (Perfiles) En relación con la exigencia de que los perfiles se encuentren inscriptos en la planilla del IPS del oferente con una antigüedad mínima de un (1) año, solicitamos se considere, específicamente para los perfiles de conducción (Director General y Coordinador de SOC / Líder Operativo), la aceptación de una antigüedad mínima de seis (6) meses, atendiendo a la limitada disponibilidad en plaza de profesionales con el nivel de especialización requerido para dichos cargos.		

Consulta 24 - Condición de estudiante — acreditación

Consulta	Fecha de Consulta	30-06-2026
Sección: Requisitos documentales para evaluar la Capacidad Técnica Consulta: En los requisitos documentales se solicita constancia de estudiante “debiendo encontrarse en los últimos años de la carrera”. Considerando que el cuerpo de las especificaciones exige la condición de “estudiante o egresado” sin distinción de año cursado, solicitamos se confirme que será admitida la condición de estudiante de carreras informáticas o afines con independencia del año en curso, acreditable mediante historial académico y/o constancia o proforma de inscripción universitaria vigente.		

Consulta 25 - Horario de la modalidad presencial in situ

Consulta	Fecha de Consulta	30-06-2026
Sección: Especificaciones Técnicas — numeral 1.3 (Modalidad de atención remota y presencial) Consulta: Solicitamos aclarar el horario de la modalidad presencial in situ, considerando que el pliego presenta dos referencias distintas: la descripción de perfiles indica de 08:00 a 18:00 horas, mientras que el numeral 1.3 de las EETT indica de 08:00 a 16:00 horas. Agradeceríamos confirmar cuál es el horario aplicable.		

Consulta 26 - Certificaciones equivalentes y en proceso de renovación

Consulta	Fecha de Consulta	30-06-2026
Sección: Requisitos de Participación — Capacidad Técnica (Perfiles) Consulta: Solicitamos aclarar si serán aceptadas certificaciones equivalentes emitidas por otros organismos de reconocido prestigio internacional, así como certificaciones que se encuentren en proceso de renovación con constancia de vigencia, para los distintos perfiles requeridos, a fin de no restringir indebidamente la concurrencia.		

Consulta 27 - Maestría del Director General del Servicio

Consulta	Fecha de Consulta	30-06-2026
Sección: Requisitos de Participación — Capacidad Técnica (Perfiles) Consulta: Solicitamos aclarar si, para el cargo de Director General del Servicio, será admitida la maestría en áreas afines a la ciberseguridad (gestión de la seguridad de la información, gestión de TI o gestión de riesgos), así como la formación de posgrado en curso debidamente acreditada, en atención al principio de amplitud de la participación.		

Consulta 28 - Consulta

Consulta	Fecha de Consulta	30-06-2026
Respecto a los perfiles exigidos en la Sección de Capacidad Técnica (Pág. 16 y 17), se solicita de forma simultánea un (1) Director General del Servicio y un (1) Coordinador de SOC / Líder Operativo. Dado que el objeto del llamado es un "Servicio de Centro de Operaciones de Seguridad (SOC)" bajo la modalidad de servicio gestionado continuo, las tareas de supervisión macro, control contractual y enlace operativo pueden ser absorbidas perfectamente por un único perfil gerencial de alta calificación. En virtud del principio de eficiencia y economía de la Ley N° 7021/22, se solicita a la convocante: a) Justificar técnicamente qué funciones operativas específicas del Director General no pueden ser ejecutadas por el Coordinador de SOC, y b) Evaluar la unificación de ambos perfiles en una sola figura de "Gerente / Director de Proyecto", a fin de evitar un encarecimiento artificial de los costos de la estructura de personal que terminará impactando negativamente en la oferta económica final.		

Consulta 29 - Consulta

Consulta	Fecha de Consulta	30-06-2026
El pliego establece como requisito obligatorio que tanto el Director General como el Coordinador de SOC se encuentren inscriptos en la planilla de IPS del oferente con una antigüedad mínima comprobable de un (1) año. Si bien se comprende la necesidad de garantizar personal propio para las tareas críticas del SOC, aplicar esta restricción temporal de forma idéntica a los dos roles de mayor jerarquía administrativa limita severamente la participación de empresas solventes que legítimamente contratan o asignan directores de proyecto según la adjudicación de nuevos contratos. Atendiendo a que esto restringe la libre competencia, se solicita a la convocante: a) Eliminar o flexibilizar la exigencia de un (1) año de antigüedad en IPS para el perfil del Director General , permitiendo que su relación de dependencia con el oferente se perfeccione al momento del inicio del servicio, o en su defecto, b) Permitir la unificación de las capacidades exigidas para optimizar la estructura de costos.		

Consulta 30 - Consulta

Consulta	Fecha de Consulta	30-06-2026
De acuerdo con los criterios de adjudicación declarados en el pliego, el procedimiento busca asegurar el mayor "valor por dinero". Sin embargo, la obligación de financiar de manera concurrente dos salarios de nivel ejecutivo (un Director con maestría y certificaciones CISM/CCISO y un Coordinador con diplomado y certificaciones Blue/Red Team), sumado a un Analista In-Situ y seis técnicos adicionales en el SOC, rompe la proporcionalidad financiera para un monitoreo automatizado. Se solicita a la convocante arrimar las justificaciones técnicas y los estudios de mercado que demuestren que la ausencia de uno de estos dos perfiles gerenciales (Director o Coordinador) comprometería la continuidad operativa del SOC , considerando que las herramientas tecnológicas de orquestación y automatización (SOAR) requeridas en el mismo pliego ya reducen drásticamente los tiempos de reacción y la necesidad de intervención manual de alta gerencia.		

Consulta 31 - Consulta

Consulta	Fecha de Consulta	30-06-2026
El pliego exige que la totalidad de los 10 perfiles técnicos requeridos (incluyendo directores, coordinadores y analistas) cuenten con una antigüedad mínima comprobable de 1 (un) año de vínculo laboral en la Planilla de IPS de la empresa oferente . Considerando la alta rotación y dinámica del talento especializado en ciberseguridad a nivel nacional, esta exigencia limita de forma desproporcionada la libre competencia. ¿Permitirá la convocante que la experiencia de los perfiles se demuestre mediante sus Currículums Vitae y certificaciones internacionales individuales, permitiendo la incorporación de profesionales al staff del oferente mediante contratos de compromiso de incorporación en caso de resultar adjudicados, garantizando así el cumplimiento del Principio de Economía y Libre Competencia establecido en la Ley N° 7021/22? En caso negativo, favor justificar técnicamente el impacto operativo de restringir el empleo de analistas que no posean un año de antigüedad en la misma firma.		

Consulta 32 - Consulta

Consulta	Fecha de Consulta	30-06-2026
El ítem 10.2 exige una retención histórica mínima de 110 Terabytes (110 TB) de información de seguridad disponible para análisis operativo inmediato, mientras que el ítem 10.8 prohíbe expresamente esquemas basados en copias de seguridad no indexadas. Pero no se especifica periodos de retención. Mantener 110 TB de telemetría indexada y en caliente en una plataforma analítica durante 24 meses representa un costo de licenciamiento e infraestructura que supera el precio de mercado razonable para el presupuesto total de este llamado. A fin de salvaguardar el equilibrio económico del contrato, ¿permitirá la convocante un esquema híbrido de almacenamiento (Tiered Storage), donde la telemetría se mantenga indexada en caliente por un periodo inicial de 90 días, y luego sea trasladada a almacenamiento frío (Cold Storage) comprimido pero recuperable para análisis forense, disminuyendo así el costo artificial de la solución?		

Consulta 33 - Consulta

Consulta	Fecha de Consulta	30-06-2026
El pliego exige que el oferente cuente con un SOC en la República del Paraguay y al menos un segundo SOC a una "distancia mínima de 500Km de este". Considerando las dimensiones geográficas del territorio nacional y que el modelo requerido es de servicio gestionado en entornos cloud e híbridos , una restricción lineal de 500 km obliga de facto a los oferentes a disponer de infraestructura transfronteriza fuera del país para un llamado de carácter Nacional. ¿Se considerará conforme el cumplimiento de este requisito mediante una arquitectura de Centro de Operaciones distribuida en la nube con alta disponibilidad (Multi-AZ) y redundancia lógica geográficamente dispersa que garantice un Acuerdo de Nivel de Servicio (SLA) equivalente, sin importar la distancia física en kilómetros? En caso negativo, favor indicar el fundamento técnico que conecte la distancia física de 500 km con la efectividad de la detección de incidentes digitales.		

Consulta 34 - Consulta

Consulta	Fecha de Consulta	30-06-2026
Existe una contradicción explícita en el pliego: en la página 21 (Ítem 7, Perfiles) se exige para el Analista SOC In-Situ un horario presencial de 08:00 a 18:00 horas (10 horas diarias) , mientras que en la misma página (Ítem 1.3, Modalidad) se indica que la modalidad presencial In-Situ será de lunes a viernes de 08:00 a 16:00 horas (8 horas diarias). Favor aclarar cuál es el horario definitivo que regirá para el personal presencial a efectos de calcular correctamente los costos de la nómina laboral.		

Consulta 35 - Consulta

Consulta	Fecha de Consulta	30-06-2026
El llamado utiliza el método de adjudicación basado únicamente en el precio más bajo. Teniendo en cuenta que el presupuesto referencial interno está significativamente por debajo de los costos de mercado para la provisión simultánea de 10 profesionales senior dedicados, licenciamiento EDR/XDR para 800 activos y retención de 110 TB indexados, ¿cuál será el procedimiento o rango que utilizará el Comité de Evaluación para identificar y rechazar ofertas con precios anormalmente bajos que pongan en riesgo la seguridad nacional del Banco mediante la simulación de capacidades técnicas inexistentes?		

Consulta 36 - Especificaciones Técnicas - 1.2 Continuidad Operativa del Servicio

Consulta	Fecha de Consulta	30-06-2026
Respecto al requisito establecido en el numeral 1.2 Continuidad Operativa del Servicio, que dispone: "El oferente debe contar con al menos un Centro de Operaciones de Seguridad (SOC) en la República del Paraguay, y al menos uno más que se encuentre a una distancia mínima de 500 km de este." Solicitamos la eliminación del requisito que exige una distancia mínima de 500 km entre ambos SOC, por constituir una especificación técnica restrictiva que carece de sustento técnico y de razonabilidad respecto del objeto de la contratación. La continuidad operativa, la alta disponibilidad y la recuperación ante desastres no dependen de una distancia geográfica predeterminada, sino de la arquitectura de redundancia, los mecanismos de replicación, los planes de continuidad y la resiliencia de la infraestructura, aspectos ya exigidos en el Pliego. La imposición de una distancia mínima de 500 km no aporta un beneficio técnico demostrable y genera un efecto excluyente, restringiendo artificialmente la concurrencia al limitar la participación a un número reducido de proveedores con una configuración específica de infraestructura, en abierta contradicción con los principios de libre competencia, igualdad, razonabilidad y máxima concurrencia que rigen las contrataciones públicas. Las especificaciones técnicas deben responder exclusivamente a necesidades funcionales de la Convocante y no incorporar condiciones que, sin justificación objetiva, produzcan una limitación injustificada de la competencia o favorezcan indirectamente a determinados operadores económicos. Por lo expuesto, solicitamos suprimir dicho requisito y reemplazarlo por la exigencia de acreditar mecanismos efectivos de continuidad operativa y recuperación ante desastres, independientemente de la ubicación geográfica de los SOC, siempre que se garantice el cumplimiento de los niveles de servicio requeridos.		

Consulta 37 - Especificaciones Técnicas - 1.3 – Modalidad de atención remota y presencial

Consulta	Fecha de Consulta	30-06-2026
Respecto al punto 1.3 – Modalidad de atención remota y presencial, que establece: “El servicio de SOC deberá ser de forma híbrida 24x7 de los cuales en la modalidad presencial In-Situ deberá ser presentada de lunes a viernes de 08:00 a 16:00 horas...” Observamos que existe una discrepancia con lo indicado en la sección correspondiente a los perfiles técnicos, específicamente para el cargo de Analista de Seguridad SOC, in-situ, donde se menciona que el servicio deberá prestarse en modalidad presencial de lunes a viernes en el horario de 08:00 a 18:00 horas (pág. 21 del PBC). Considerando que ambas disposiciones establecen horarios distintos para la prestación presencial del servicio, solicitamos respetuosamente aclarar cuál es el horario que deberá considerarse como válido a los efectos de la elaboración de la propuesta técnica y económica.		

Consulta 38 - Especificaciones Técnicas - 1.2 Continuidad Operativa del Servicio

Consulta	Fecha de Consulta	30-06-2026
Respecto al requisito establecido en el numeral 1.2 Continuidad Operativa del Servicio, que dispone: “El oferente debe contar con al menos un Centro de Operaciones de Seguridad (SOC) en la República del Paraguay, y al menos uno más que se encuentre a una distancia mínima de 500 Km de este.” Solicitamos respetuosamente aclarar si nuestra interpretación es correcta, entendemos que el segundo SOC requerido tiene como finalidad exclusiva actuar como sitio de contingencia, respaldo o recuperación ante desastres del servicio, siendo utilizado solamente en situaciones donde el SOC principal no pueda operar total o parcialmente debido a incidentes, fallas o eventos que afecten su disponibilidad, orientada a garantizar la continuidad operativa y recuperación del servicio ante contingencias.		

Consulta 39 - Especificaciones Técnicas - Punto 9.12 Prohibición de investigación puramente manual

Consulta	Fecha de Consulta	30-06-2026
EETT - Punto 9.12 Prohibición de investigación puramente manual Donde exige: “No se aceptarán ofertas donde las capacidades de investigación y análisis forense dependan exclusivamente de actividades manuales, herramientas aisladas o servicios profesionales no integrados al SOC. Debe contar con capacidades de análisis forense con herramientas certificadas ante procesos judiciales.” Solicitamos respetuosamente que este requisito pueda cumplirse mediante herramientas forenses open source reconocidas en la industria, tales como DFIR-IRIS, Velociraptor, Autopsy y The Sleuth Kit, siempre que sean utilizadas dentro de un procedimiento formal de preservación de evidencia digital que incluya cadena de custodia, generación y verificación de hashes criptográficos SHA-256/SHA-512, control de acceso, bitácora de acciones, almacenamiento seguro/inmutable y documentación técnica reproducible. En caso contrario, solicitamos especificar qué “herramientas certificadas” serán consideradas válidas para cumplir este requisito. Adicionalmente, considerando que el objeto de la presente contratación corresponde a un servicio gestionado de SOC, el resultado esperado debería centrarse en las capacidades efectivas de investigación, análisis y respuesta ante incidentes, y no en la utilización de herramientas determinadas o en la posesión de productos específicos por parte del oferente.		

Consulta 40 - Especificaciones Técnicas - Punto 12. SERVICIOS DE PREVENCIÓN Y PROTECCIÓN PARA ACTIVOS CRÍTICOS

Consulta	Fecha de Consulta	30-06-2026
En el punto 12.1 donde dice: “Las capacidades definidas en este apartado aplicarán exclusivamente a activos críticos definidos por la Entidad, hasta un máximo de 800 (ochocientos), incluyendo servidores Windows y Linux, sistemas críticos y otros activos tecnológicos compatibles” Considerando que la infraestructura tecnológica del Banco Nacional de Fomento está compuesta por una cantidad significativamente superior de activos tecnológicos en comparación al máximo establecido, y que el propio pliego establece que las capacidades aplicadas sobre dichos activos deberán integrarse operativamente al SOC y CSIRT, solicitamos respetuosamente que la Convocante indique con mayor precisión cuáles serán considerados activos críticos dentro del alcance del servicio. La presente aclaración resulta necesaria a los efectos de que todos los oferentes puedan dimensionar adecuadamente el alcance real de la solución, estimar los recursos tecnológicos requeridos, prever las capacidades de integración, monitoreo y protección necesarias, así como elaborar sus propuestas técnicas y económicas en igualdad de condiciones. Asimismo, la definición de criticidad puede variar significativamente entre organizaciones, por lo que la sola referencia a un máximo de 800 activos no permite determinar con precisión el cumplimiento de todo lo exigido en el apartado 12.1.		

Consulta 41 - Especificaciones Técnicas - Punto 3.3 Protección base en endpoints

Consulta	Fecha de Consulta	30-06-2026
Respecto al punto 3.3 - Protección base en endpoints, donde se exige que el servicio incluya una capa de protección preventiva en los endpoints con capacidades de prevención de malware, protección contra ransomware, amenazas en memoria y comportamiento malicioso, solicitamos respetuosamente la eliminación de dicho apartado o, en su defecto, aclarar que estas capacidades serán cubiertas mediante las soluciones de seguridad actualmente disponibles en la Entidad. Consideramos que las capacidades requeridas en el punto 3.3 corresponden, en la práctica, a funcionalidades propias de soluciones de Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR) o tecnologías equivalentes, cuya provisión implica el suministro de licencias de software especializadas para los activos protegidos. Sin embargo, el objeto de la presente contratación corresponde a la prestación de servicios de SOC y CSIRT, cuyo alcance principal consiste en la operación, monitoreo, detección, análisis y respuesta ante incidentes de ciberseguridad, y no en la adquisición o provisión de licenciamiento de herramientas de protección endpoint, cuyo objeto de gasto es totalmente diferente al previsto en esta contratación. Asimismo, se observa que el Banco Nacional de Fomento ya ha realizado recientemente la contratación de licencias de ciberseguridad, conforme al proceso ID N.º 472694 - Adquisición de Licenciamiento de Software de Soporte Técnico Antivirus, destinado a cubrir un total de 2.500 dispositivos, incluyendo capacidades avanzadas de protección, EPP, EDR y XDR. En ese contexto, exigir nuevamente la provisión de capacidades que presumiblemente ya se encuentran cubiertas por licencias adquiridas por la Entidad podría generar una duplicación de costos para la Institución y trasladar a los oferentes la necesidad de incorporar componentes tecnológicos que no guardan relación directa con el objeto principal de la contratación. Lo solicitado se fundamenta además en los principios de Economía, Eficacia y Eficiencia previstos en la Ley N.º 7021/22, procurando evitar la duplicación de capacidades ya adquiridas por la Entidad y optimizar el uso de los recursos públicos.		

Consulta 42 - EETT – PUNTO 1.2

Consulta	Fecha de Consulta	30-06-2026
Donde dice: “El oferente debe contar con al menos un Centro de Operaciones de Seguridad (SOC) en la República del Paraguay, y al menos uno más que se encuentre a una distancia mínima de 500 Km de este.” La exigencia de contar con un segundo SOC ubicado a una distancia mínima de 500 km del SOC establecido en Paraguay no responde necesariamente a un requerimiento técnico para garantizar la continuidad operativa, ya que actualmente la resiliencia de este tipo de servicios se sustenta en mecanismos de alta disponibilidad, redundancia, replicación de información, recuperación ante desastres y continuidad de negocio, independientemente de una distancia geográfica específica. Asimismo, considerando la extensión territorial de la República del Paraguay y la modalidad de la presente convocatoria, correspondiente a una Licitación Pública Nacional, la exigencia de una separación mínima de 500 km implica que, en la práctica, el segundo SOC deba encontrarse fuera del territorio nacional en la mayoría de los casos. Esta situación podría generar desafíos adicionales relacionados con la supervisión operativa, auditoría, cumplimiento normativo, gestión contractual y control de la información procesada. Adicionalmente, tratándose de una entidad financiera pública que administra información sensible y crítica para el Estado y los ciudadanos, resulta recomendable privilegiar esquemas que favorezcan la soberanía de la información, permitiendo que las actividades de monitoreo, análisis y tratamiento de eventos de seguridad puedan desarrollarse dentro de jurisdicción nacional siempre que sea técnicamente viable. Por lo expuesto, solicitamos eliminar la condición de distancia mínima, ya que consideramos que el objetivo de continuidad operativa y recuperación ante contingencias debería medirse a través de capacidades efectivas de redundancia, resiliencia y recuperación ante desastres, y no mediante la imposición de una distancia geográfica mínima que, en la práctica, condiciona la prestación parcial del servicio desde el extranjero y restringe innecesariamente la participación de potenciales oferentes.		

Consulta 43 - Capacidad Técnica / Para todos los perfiles tecnicos

Consulta	Fecha de Consulta	30-06-2026
Donde dice: “Debe encontrarse inscripto en la Planilla de IPS del oferente y contar con una antigüedad mínima comprobable de 1 (un) año de vínculo laboral con la empresa oferente” Solicitamos respetuosamente que se admita la acreditación del vínculo profesional mediante Planilla de IPS y/o contrato laboral, manteniéndose el requisito de antigüedad mínima exigido. La industria de tecnología y ciberseguridad posee dinámicas laborales particulares, donde es habitual que profesionales altamente especializados presten servicios bajo modalidades distintas a la relación de dependencia tradicional, incluyendo contratos de prestación de servicios profesionales, consultorías especializadas y esquemas de asignación dedicados de recursos técnicos. Asimismo, la inscripción exclusiva en la Planilla de IPS no constituye necesariamente el único mecanismo válido para demostrar la existencia de una relación profesional estable y verificable entre el oferente y el recurso propuesto. Existen otros documentos contractuales que permiten acreditar fehacientemente el vínculo, la dedicación y la experiencia requerida para la ejecución del servicio. Adicionalmente, existen antecedentes en procedimientos de contratación de servicios tecnológicos del propio Banco Nacional de Fomento (id 438167) donde se han aceptado mecanismos alternativos para acreditar el vínculo entre el oferente y los recursos técnicos propuestos, como el contrato laboral, sin requerir exclusivamente la inscripción en la Planilla de IPS.		

Consulta 44 - EETT – PUNTO 7.8

Consulta	Fecha de Consulta	30-06-2026
Donde dice: “El servicio deberá permitir la demostración funcional de los playbooks de respuesta incluidos, en un entorno controlado, a solicitud de la Entidad durante la fase de evaluación técnica.” Solicitamos respetuosamente que dicho requisito sea considerado opcional o, alternatively, que su verificación sea realizada únicamente al oferente adjudicado durante la etapa de implementación del servicio. La realización de demostraciones funcionales durante la fase de evaluación técnica implica la preparación de entornos, recursos y configuraciones específicas por parte de los oferentes, generando una carga operativa adicional que podría limitar la participación de potenciales competidores, sin constituir un elemento indispensable para la evaluación de la capacidad técnica del proveedor.		

Consulta 45 - Capacidad Técnica / Punto 3. a) 1 (un) Director General del Servicio de Ciberseguridad

Consulta	Fecha de Consulta	30-06-2026
Donde dice: "Debe ser un profesional egresado de carreras informáticas o afines." Solicitamos respetuosamente que este requisito sea modificado para exigir únicamente que el profesional sea egresado universitario, manteniendo los requisitos de experiencia y competencias técnicas exigidos en el Pliego, sin restringir la formación académica a carreras informáticas o afines. El rol de Director General del Servicio de Ciberseguridad posee un enfoque eminentemente estratégico, orientado al gobierno de la ciberseguridad, gestión de riesgos, continuidad operativa, dirección de equipos multidisciplinarios y toma de decisiones. En la práctica, estas funciones son desempeñadas por profesionales con diversas formaciones universitarias, complementadas con experiencia específica y certificaciones internacionales en ciberseguridad, requisitos que el propio Pliego ya contempla. La limitación exclusiva a carreras informáticas o afines carece de una justificación técnica objetiva para el desempeño del cargo y restringe injustificadamente la participación de profesionales altamente calificados, particularmente de especialistas extranjeros cuyos títulos universitarios no poseen una denominación equivalente a la utilizada por las universidades nacionales, pese a contar con amplia experiencia y reconocidas certificaciones internacionales. De mantenerse esta exigencia, se generará una restricción innecesaria de la competencia, limitando la participación de oferentes que cuentan con personal plenamente idóneo para cumplir las funciones requeridas, en contravención de los principios de razonabilidad, igualdad de participación y máxima concurrencia que deben regir las especificaciones técnicas en los procedimientos de contratación pública. Por lo expuesto, solicitamos la modificación del requisito, privilegiando la experiencia profesional, las competencias técnicas y las certificaciones especializadas por sobre la denominación específica del título universitario.		

Consulta 46 - Capacidad Técnica / Punto 3. a) 1 (un) Director General del Servicio de Ciberseguridad

Consulta	Fecha de Consulta	30-06-2026
Donde dice: "Debe contar con al menos 1 (una) de las siguientes certificaciones vigentes de gestión de ciberseguridad: ISACA CISM, ECCouncil CCISO." Solicitamos respetuosamente que se incorpore también la certificación Certified Ethical Hacker (CEH) de EC-Council como certificación válida para el cumplimiento de este requisito. La certificación CEH es una de las credenciales más reconocidas internacionalmente en el ámbito de la ciberseguridad y acredita conocimientos avanzados sobre técnicas de ataque, identificación de vulnerabilidades, gestión de riesgos y medidas de protección aplicables a entornos corporativos. Su enfoque práctico permite comprender en profundidad las amenazas actuales y fortalecer las capacidades de prevención y respuesta ante incidentes. La incorporación de esta certificación favorecerá una mayor concurrencia de oferentes y profesionales calificados, sin afectar el objetivo de garantizar la idoneidad técnica del responsable del servicio.		

Consulta 47 - Capacidad Técnica / Punto 3. a) 1 (un) Director General del Servicio de Ciberseguridad

Consulta	Fecha de Consulta	30-06-2026
Donde dice: "Debe contar con al menos 1 (una) de las siguientes certificaciones vigentes de ciberseguridad: ISC2 CISSP, PECB ISO 27032 Senior Lead Cybersecurity Manager, PECB ISO 27035 Senior Lead Incident Manager." Solicitamos respetuosamente que se incorpore también la certificación ISACA CISA (Certified Information Systems Auditor) como certificación válida para el cumplimiento de este requisito. La certificación CISA constituye una de las credenciales más reconocidas internacionalmente en materia de gobierno, gestión de riesgos, auditoría y control de sistemas de información. Sus dominios de conocimiento se encuentran estrechamente relacionados con la gestión de la seguridad de la información, la evaluación de controles de ciberseguridad, la gestión de incidentes y la mejora continua de la postura de seguridad organizacional.		

Consulta 48 - Capacidad Técnica / Punto 3. b) 1 (un) Coordinador de SOC / Líder Operativo

Consulta	Fecha de Consulta	30-06-2026
Donde dice: “Debe contar con al menos 2 (dos) capacitaciones y/o certificaciones en seguridad o ciberseguridad, de organizaciones reconocidas internacionalmente como: ISC2, ISACA, ECCouncil, PECB, Certiprof” y; “Debe contar con al menos 1 (una) certificación específicamente relacionada a seguridad ofensiva y/o defensiva (RedTeam / BlueTeam)” En lugar de estos requisitos, solicitamos respetuosamente que, para este perfil, se acepten cursos de especialización, programas de formación profesional o especializaciones en ciberseguridad debidamente acreditados, sin que sea obligatoria la presentación de certificaciones específicas de Red Team o Blue Team. Considerando que el perfil requerido corresponde a un cargo de coordinación y liderazgo operativo, sus funciones principales se encuentran orientadas a la gestión del servicio, coordinación de equipos, seguimiento de incidentes, escalamiento técnico y enlace operativo con la convocante, más que a la ejecución directa de actividades especializadas de seguridad ofensiva o defensiva. Asimismo, el pliego ya exige que este profesional cuente con un diplomado en ciberseguridad o seguridad de la información, además de experiencia comprobable en roles de TI, ciberseguridad o seguridad de la información, requisitos que ya permiten acreditar una formación sólida en la materia, Adicionalmente, las certificaciones técnicas especializadas solicitadas resultan parcialmente redundantes con los requisitos exigidos para otros perfiles del equipo, tales como analistas SOC, especialistas en Threat Hunting, arquitectos de ciberseguridad y demás recursos técnicos encargados de la ejecución operativa y especializada del servicio		

Consulta 49 - Capacidad Técnica / Punto 3. f) 2 (dos) Analistas de Ciberseguridad

Consulta	Fecha de Consulta	30-06-2026
Donde dice: “Deben contar con al menos 2 (dos) de las siguientes certificaciones: ISO 27001 Lead Auditor, CEH, Security+” Solicitamos respetuosamente que se incorporen también las certificaciones ISO/IEC 27001 Foundation (Certiprof) y/o EC-Council Incident Handler (ECIH) como certificaciones válidas para el cumplimiento de este requisito. La certificación ISO/IEC 27001 Foundation proporciona conocimientos fundamentales sobre Sistemas de Gestión de Seguridad de la Información (SGSI), gestión de riesgos, controles de seguridad y buenas prácticas alineadas con estándares internacionales, competencias plenamente aplicables a las funciones de los Analistas de Ciberseguridad. Por su parte, la certificación ECIH (EC-Council Incident Handler) está específicamente orientada a la gestión y respuesta ante incidentes de seguridad, incluyendo análisis, contención, erradicación y recuperación, actividades que guardan una relación directa con las responsabilidades que este perfil deberá desempeñar dentro del servicio requerido.		

Consulta 50 - Capacidad Técnica / Punto 3. f) 2 (dos) Analistas de Ciberseguridad

Consulta	Fecha de Consulta	30-06-2026
Donde dice: “Deben contar con al menos 2 (dos) de las siguientes certificaciones: ISO 27001 Lead Auditor, CEH, Security+” Solicitamos respetuosamente que se incorporen también las certificaciones ISO/IEC 27001 Foundation (Certiprof) y/o EC-Council Incident Handler (ECIH) como certificaciones válidas para el cumplimiento de este requisito. La certificación ISO/IEC 27001 Foundation proporciona conocimientos fundamentales sobre Sistemas de Gestión de Seguridad de la Información (SGSI), gestión de riesgos, controles de seguridad y buenas prácticas alineadas con estándares internacionales, competencias plenamente aplicables a las funciones de los Analistas de Ciberseguridad. Por su parte, la certificación ECIH (EC-Council Incident Handler) está específicamente orientada a la gestión y respuesta ante incidentes de seguridad, incluyendo análisis, contención, erradicación y recuperación, actividades que guardan una relación directa con las responsabilidades que este perfil deberá desempeñar dentro del servicio requerido.		

Consulta 51 - Capacidad Técnica / Punto 3. g) 1 (un) Analista de Seguridad SOC, in-situ

Consulta	Fecha de Consulta	30-06-2026
Donde dice: "El personal debe contar con al menos 3 certificaciones y/o cursos de ciberseguridad de organizaciones reconocidas internacionalmente, tales como ISC2, ISACA, ECCOUNCIL, ISO, FORTINET, CISCO, MICROSOFT" Solicitamos respetuosamente que se amplíen las organizaciones aceptadas para acreditar dicho requisito, incorporando también certificaciones y/o capacitaciones emitidas por Certiprof, Hack The Box, PortSwigger Academy y TryHackMe. Observamos que para el perfil c) Analistas de Seguridad SOC, el propio pliego admite certificaciones y capacitaciones emitidas por organizaciones como Certiprof, Hack The Box, PortSwigger Academy y TryHackMe, entre otras. Considerando que ambos perfiles desarrollan funciones estrechamente relacionadas con la operación del SOC, monitoreo de eventos, análisis de alertas e incidentes de seguridad, resulta razonable mantener criterios homogéneos de evaluación respecto a las capacitaciones y certificaciones admitidas. La incorporación de estas alternativas no disminuye el nivel técnico exigido, sino que permite reconocer trayectorias formativas ampliamente utilizadas en el mercado y favorece una mayor participación de profesionales calificados, manteniendo el objetivo de contar con personal idóneo para la prestación del servicio.		

Consulta 52 - Capacidad Tecnica

Consulta	Fecha de Consulta	30-06-2026
Respecto al requisito del Pliego que exige que el personal técnico afectado al servicio se encuentre vinculado exclusivamente mediante relación de dependencia e inscripción al Instituto de Previsión Social (IPS), solicitamos respetuosamente que también se admita la participación de profesionales vinculados mediante contratos de prestación de servicios profesionales u otras modalidades legales de contratación, siempre que el oferente acredite su disponibilidad efectiva, dedicación y responsabilidad durante toda la ejecución contractual. La operación de un Centro de Operaciones de Seguridad (SOC) de nivel empresarial requiere la participación de profesionales altamente especializados en disciplinas como monitoreo avanzado, respuesta a incidentes, inteligencia de amenazas, análisis forense digital, ingeniería de seguridad, arquitectura de ciberseguridad y gestión de plataformas especializadas. Estos perfiles, por la naturaleza de su especialización y la dinámica del mercado, son frecuentemente contratados bajo la modalidad de prestación de servicios profesionales, tanto a nivel nacional como internacional. Limitar la conformación del equipo exclusivamente a personal en relación de dependencia e inscripto en el IPS constituye una restricción innecesaria que no guarda relación directa con la capacidad técnica del oferente ni con la calidad del servicio a prestar. La modalidad de contratación del recurso humano no determina su idoneidad, experiencia, disponibilidad ni el cumplimiento de las obligaciones contractuales, las cuales recaen íntegramente sobre el adjudicatario. Asimismo, esta exigencia restringe la participación de empresas que cuentan con equipos consolidados de especialistas nacionales e internacionales, incluyendo profesionales con certificaciones y experiencia altamente demandadas en el ámbito de la ciberseguridad, reduciendo artificialmente la concurrencia de oferentes sin aportar un beneficio técnico objetivo para la Convocante. Por lo expuesto, solicitamos que el Pliego admita indistintamente personal en relación de dependencia o vinculado mediante contratos de prestación de servicios profesionales, siempre que el oferente acredite documentalmente la disponibilidad del personal propuesto y asuma la responsabilidad por su permanencia durante toda la ejecución del contrato, privilegiando la capacidad técnica e idoneidad del equipo por sobre la modalidad jurídica de su contratación.		