

Consultas Realizadas

Licitación 490431 - SERVICIO DE CONSULTORIA PARA EL FORTALECIMIENTO DE INFRAESTRUCTURA CRÍTICA TECNOLÓGICA

Consulta 1 - Posible duplicación/superposición entre el 40% general y el 40% específico

Consulta	Fecha de Consulta	22-09-2026
Texto actual: Experiencia General exige 40% en "servicios y/o consultorías en el área de tecnología"; Experiencia Específica a) exige 40% en "consultoría en ciberseguridad, seguridad de la información o infraestructura tecnológica". Conflicto: No se aclara si se trata de dos exigencias independientes y acumulables (es decir, el oferente debe sumar contratos por 40% en tecnología en general Y adicionalmente 40% en ciberseguridad específicamente, pudiendo llegar a exigir un 80% combinado o incluso duplicar el mismo contrato para ambos rubros), o si el 40% específico es un subconjunto que también satisface el general. Esta falta de claridad puede generar interpretaciones arbitrarias al momento de evaluar ofertas. Consulta: Solicitamos a la Convocante aclarar si los contratos presentados para acreditar el 40% de Experiencia Específica (ciberseguridad/seguridad de la información/infraestructura tecnológica) pueden utilizarse simultáneamente para acreditar el 40% de Experiencia General (tecnología en general), o si por el contrario se requieren contratos diferenciados y no superpuestos para cada índice, dado que el texto actual no lo especifica y ello genera incertidumbre sobre el volumen real de facturación acumulada que deberá demostrar el oferente, en contravención del Principio de Transparencia; solicitamos se confirme expresamente el criterio de acumulación (independiente vs. subsumido) a aplicar.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada se aclara que los mismos antecedentes podrán acreditar ambos requisitos si cumplen las condiciones de cada uno. Los porcentajes se verifican por separado: 40% del monto referenciado en el llamado para la experiencia general y 40% del monto ofertado para la específica, por lo que solicitamos remitirse a lo solicitado en el PBC.		

Consulta 2 - Experiencia específica de la empresa:

Consulta	Fecha de Consulta	22-09-2026
En relación a los Requisitos Documentales para la evaluación de la Experiencia (contratos, facturas y/o actas de recepción final), solicitamos a la Convocante aclarar lo siguiente: 1) si el cumplimiento de los índices de experiencia (general y específica) se acredita mediante la presentación de una cantidad mínima determinada de contratos, o si por el contrario basta con alcanzar el monto/porcentaje de facturación indicado independientemente de la cantidad de documentos presentados; 2) si es admisible presentar un único contrato, factura o acta de recepción que, por su naturaleza y monto, acredite simultáneamente más de uno de los requisitos solicitados (por ejemplo, un mismo contrato de consultoría en ciberseguridad que a la vez cubra el porcentaje de Experiencia General y el de Experiencia Específica inciso a), o que sirva además para acreditar el literal b) o c) si el objeto del servicio lo comprende); y 3) si para los literales b) y c) de la Experiencia Específica se exige un contrato específico por cada servicio mencionado (SIEM, Ethical Hacking, SOC/CSIRT, ISO 27001, CIS, gestión de riesgos) o si un mismo contrato integral que abarque varios de esos servicios es suficiente para tener por acreditados todos ellos. Lo anterior a fin de contar con reglas claras y objetivas para la conformación de la oferta, en resguardo de los Principios de Transparencia e Igualdad de Condiciones entre oferentes.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada se aclara que para acreditar los porcentajes no se establece una cantidad mínima de contratos; deben cumplirse los montos y demás condiciones exigidas. Un contrato integral podrá respaldar varios requisitos si acredita los servicios correspondientes a cada uno. La asignación de puntos se rige por la matriz de evaluación, por lo que solicitamos remitirse a lo solicitado en el PBC.		

Consulta 3 - La "factura" queda fuera del puntaje

Consulta	Fecha de Consulta	22-09-2026
La Matriz describe que la Experiencia Específica a) se acredita con "copias de contratos, facturas y/o actas de recepción final" (tres opciones), pero la regla de puntaje solo otorga puntos por "cada contrato y/o acta de cierre final" — sin mencionar factura. Es decir, según cómo está redactado, un oferente que solo presente facturas (documento válido según la descripción) podría no sumar puntos, porque la fórmula de puntaje no la contempla. Esta es la más sólida y concreta, en línea con lo que ya veníamos analizando.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada se aclara que las facturas son admitidas como respaldo documental de la experiencia. Para la asignación de puntos, atenerse a la matriz, que establece un punto por contrato y/o acta de cierre final. La presentación de facturas no genera, por sí sola, puntos adicionales, por lo que solicitamos remitirse a lo solicitado en el PBC.		

Consulta 4 - Matriz de Evaluación Técnica

Consulta	Fecha de Consulta	22-09-2026
En la Matriz de Evaluación Técnica, la Experiencia Específica de la Consultora se puntúa mediante tres rubros independientes: a) consultoría en ciberseguridad/seguridad de la información/infraestructura tecnológica (4 puntos), b) soluciones SIEM con soporte multitenencia, Ethical Hacking y servicios SOC/CSIRT (4 puntos), y c) auditorías ISO 27001, implementación CIS o gestión de riesgos (4 puntos), otorgándose 1 punto por cada contrato y/o acta de cierre final presentado en cada rubro. Sin embargo, el pliego no aclara si un mismo contrato o factura, cuyo objeto de servicio abarque simultáneamente varios de estos rubros (por ejemplo, un contrato de consultoría que incluya de forma conjunta trabajos de auditoría ISO 27001 y servicios SOC/CSIRT), puede ser presentado y puntuado en cada uno de los rubros que efectivamente cubre, o si por el contrario cada contrato solo puede computarse para un único rubro aun cuando su objeto abarque más de uno. Asimismo, tampoco se aclara si dicho contrato o factura, presentado para acreditar la Experiencia Específica, puede utilizarse también para acreditar la Experiencia General de la Consultora, dado que ambos índices se evalúan mediante documentación de naturaleza similar (contratos, facturas y/o actas de recepción/cierre final) sin que el pliego establezca si se trata de documentación exclusiva y no superponible entre índices, o si un mismo respaldo documental puede computarse en más de un rubro de la matriz. Ante esta falta de precisión, que puede derivar en aplicación discrecional y desigual entre oferentes al momento de la calificación técnica, solicitamos a la Convocante aclarar expresamente: 1) si un mismo contrato, factura o acta de recepción/cierre final cuyo objeto abarque más de uno de los rubros de la Experiencia Específica (literales a, b y c) puede computarse y puntuarse en cada uno de dichos rubros de forma simultánea; y 2) si la documentación presentada para acreditar la Experiencia Específica puede utilizarse también para acreditar la Experiencia General de la Consultora, o si se requiere documentación diferenciada y no superpuesta para cada índice de la matriz.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada se aclara que un mismo antecedente podrá considerarse en los rubros cuyo cumplimiento acredite, incluida la experiencia general, con los respaldos exigidos para cada caso. Cada rubro se evaluará por separado, respetando sus condiciones y puntaje máximo, sin multiplicar el puntaje por presentar varios documentos de una misma contratación, por lo que solicitamos remitirse a lo solicitado en el PBC.		

Consulta 5 - Experiencia específica y documental

Consulta	Fecha de Consulta	22-09-2026
En el numeral de Experiencia Específica, literal a), el PBC exige demostrar la experiencia mediante "facturaciones de venta y recepciones finales" (redacción conjuntiva, que exigiría ambos documentos de forma simultánea para cada contrato); sin embargo, en el numeral de Requisitos Documentales para la evaluación de la experiencia, punto 1, se establece que dicha experiencia podrá acreditarse mediante "copias de contratos, facturas y/o actas de recepción final" (redacción disyuntiva, que admite cualquiera de los tres documentos de forma independiente). Ante esta discrepancia entre ambas cláusulas del mismo pliego, solicitamos a la Convocante unificar el criterio documental aplicable y precisar expresamente si, para acreditar el literal a) de la Experiencia Específica, resulta suficiente la presentación de uno solo de los documentos indicados (contrato, factura o acta de recepción final, indistintamente), conforme al criterio disyuntivo del punto 1 de Requisitos Documentales, o si por el contrario se exige la presentación conjunta de factura y acta de recepción final para cada contrato acreditado, conforme al literal a). Lo anterior a fin de evitar interpretaciones ambiguas al momento de conformar la oferta y garantizar el resguardo del Principio de Transparencia e Igualdad de Condiciones entre oferentes.		
Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada atenderse al literal a) de Experiencia Específica, que exige facturaciones de venta y recepciones finales. La enumeración general de documentos admisibles no deja sin efecto esa exigencia particular; un contrato por sí solo no acredita la facturación y recepción requeridas, por lo que solicitamos remitirse a lo solicitado en el PBC.		

Consulta 6 - Discrepancia terminológica: "acta de recepción final" vs "acta de cierre final"

Consulta	Fecha de Consulta	22-09-2026
En la Matriz, la descripción del requisito dice "actas de recepción final", pero la regla de puntaje de la misma matriz dice "acta de cierre final". ¿Son el mismo documento o dos documentos distintos? Esto afecta directamente qué papel presentar para sumar puntos.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada se aclara que a los efectos de este requisito, ambas denominaciones se refieren al documento que acredita la finalización y aceptación del servicio. No se requieren dos actas distintas por una diferencia de denominación, por lo que solicitamos remitirse a lo solicitado en el PBC.		

Consulta 7 - Formación Académica y Experiencia de Profesionales, Especialista en Ciberseguridad

Consulta	Fecha de Consulta	22-09-2026
- Experiencia Específica sin umbral cuantitativo ni período definido Consulta: El requisito de Experiencia Específica del perfil Especialista en Ciberseguridad exige "contar con experiencias demostrables en trabajos de test de penetración (pentesting), implementación de controles críticos o infraestructura", sin establecer cantidad mínima de trabajos o proyectos, años de experiencia específica, ni período de ejecución (a diferencia de otros requisitos del pliego que sí fijan años mínimos o el trienio 2023-2025), lo que convierte a este requisito en un criterio subjetivo no homologable entre oferentes; asimismo, el uso de la conjunción disyuntiva "o" entre pentesting, implementación de controles críticos e infraestructura genera duda sobre si basta con acreditar experiencia en uno solo de dichos rubros o si se exige experiencia en los tres de forma conjunta. Solicitamos a la Convocante establecer un parámetro objetivo y verificable (cantidad mínima de trabajos, años de experiencia y/o período de ejecución) para este requisito, y confirmar expresamente si basta con acreditar experiencia en uno solo de los rubros mencionados o si se exige experiencia acumulada en los tres.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada se aclara que debe acreditarse experiencia en pentesting, implementación de controles críticos o infraestructura. La redacción admite experiencia en cualquiera de esos rubros. No se incorporan cantidades, años ni períodos adicionales a los previstos para este requisito. Remitirse a lo solicitado en el PBC		

Consulta 8 - Formación Académica y Experiencia de Profesionales, Especialista en Ciberseguridad

Consulta	Fecha de Consulta	22-09-2026
- Falta de documentación exigida para acreditar Experiencia General y Experiencia Específica Consulta: En los requisitos correspondientes al perfil de Especialista en Ciberseguridad, el pliego exige acreditar Experiencia General mínima de 6 años en el área de ciberseguridad y/o seguridad de la información (4 puntos) y Experiencia Específica en trabajos de test de penetración (pentesting), implementación de controles críticos o infraestructura, sin especificar en ningún caso qué documentación respaldatoria será admitida para tener por acreditados dichos puntajes (por ejemplo, certificados laborales, constancias de IPS, contratos de servicios profesionales, cartas de referencia u otro medio idóneo), a diferencia de otros índices de la matriz que sí detallan expresamente los medios de prueba aceptados. Solicitamos a la Convocante precisar la documentación mínima admisible para acreditar tanto la Experiencia General como la Experiencia Específica del Especialista en Ciberseguridad, a fin de que los oferentes puedan conformar su oferta con certeza sobre el respaldo documental exigido.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, el apartado Equipo de Trabajo exige presentar el currículum y certificados que avalen la experiencia general y específica. Estos deben permitir verificar los trabajos y períodos declarados. Asimismo, deberán cumplirse los requisitos de vinculación laboral y acreditación ante el IPS establecidos en Capacidad Técnica. Favor remitirse a lo solicitado en el PBC		

Consulta 9 - Formación Académica y Experiencia de Profesionales, Coordinador de Proyecto

Consulta	Fecha de Consulta	22-09-2026
Consulta: En los requisitos de Formación Académica y Experiencia de Profesionales para el perfil de Coordinador de Proyecto, el pliego exige acreditar Experiencia General mínima de 7 años en el área de ciberseguridad y/o seguridad de la información (4 puntos), Experiencia Específica mínima de 5 años en gestión de proyectos de seguridad de la información y/o auditorías ISO 27001 (4 puntos), y haber logrado la certificación ISO 27001 de al menos 2 empresas en el rol de Implementador o como miembro del equipo implementador (3 puntos), sin especificar en ningún caso qué documentación respaldatoria será admitida para tener por acreditados dichos puntajes, a diferencia de otros índices de la matriz que sí detallan expresamente los medios de prueba aceptados (contratos, facturas, actas de recepción o cierre final); adicionalmente, respecto del requisito de haber logrado la certificación ISO 27001 de al menos 2 empresas, no se aclara si dicha experiencia puede acreditarse habiendo el profesional participado en el proceso de implementación y certificación de manera interna, es decir, en relación de dependencia dentro de la propia empresa certificada (formando parte de su plantel permanente durante el proceso de implementación), o si por el contrario se exige exclusivamente haber participado como consultor externo contratado por dicha empresa para dicho fin. Ante esta falta de precisión documental y de alcance del requisito, que puede derivar en criterios de evaluación discrecionales y desiguales entre oferentes, solicitamos a la Convocante: 1) precisar la documentación mínima admisible para acreditar la Experiencia General y la Experiencia Específica del Coordinador de Proyecto (por ejemplo, certificados laborales, constancias de IPS, contratos de servicios profesionales, cartas de referencia u otro medio idóneo); y 2) confirmar expresamente si la experiencia de haber logrado la certificación ISO 27001 de al menos 2 empresas resulta válida cuando el profesional participó en dicho proceso como personal interno de la empresa certificada, o si se exige necesariamente su participación como consultor externo.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se deberán presentar el currículum y certificados que avalen los períodos, funciones y experiencias exigidos. La participación como personal interno es válida si acredita el rol previsto en el PBC y la certificación ISO 27001 lograda por al menos dos empresas; no se exige participación exclusiva como consultor externo. Se solicita favor remitirse a lo solicitado en el PBC.		

Consulta 10 - Formación Académica y Experiencia de Profesionales, Especialista en Ciberseguridad

Consulta	Fecha de Consulta	22-09-2026
- Certificaciones "u otras equivalentes" sin criterio objetivo de equivalencia Consulta: El requisito de certificación técnica exigido para el perfil de Especialista en Ciberseguridad admite "Certificación técnica relacionada con seguridad informática, administración de redes o gestión de incidentes (por ejemplo, CompTIA Security+, CEH, CISSP u otras equivalentes)", sin que el pliego defina un criterio técnico objetivo para determinar qué certificaciones califican como "equivalentes" a las citadas a modo de ejemplo, quedando dicha valoración librada a la discrecionalidad del comité de evaluación al momento de calificar la oferta, lo cual genera inseguridad jurídica y riesgo de trato desigual entre oferentes que presenten certificaciones distintas pero de nivel y alcance técnico comparable. Solicitamos a la Convocante precisar el criterio de equivalencia aplicable (por ejemplo, certificaciones que acrediten competencias en pentesting, hardening, análisis de vulnerabilidades o gestión de incidentes, emitidas por organismos reconocidos internacionalmente) o, en su defecto, proporcionar un listado enunciativo de certificaciones adicionales que serán aceptadas como equivalentes a las mencionadas, a fin de garantizar un criterio de evaluación objetivo y no discrecional.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se aclara que en el PBC, se solicita certificaciones técnicas mínimas de cumplimiento. La equivalencia se valorará según el alcance y las competencias acreditadas en esas áreas. Las certificaciones mencionadas son ejemplos y no constituyen una lista cerrada. Solicitamos favor remitirse a lo solicitado en el PBC.		

Consulta 11 - Formación Académica y Experiencia de Profesionales, Experto en Ciberseguridad

Consulta	Fecha de Consulta	22-09-2026
Consulta: En los requisitos correspondientes al perfil de Experto en Ciberseguridad, el pliego exige acreditar Experiencia General mínima de 5 años en trabajos de ciberseguridad y/o seguridad de la información (2 puntos), Experiencia Específica mínima de 5 años en test de penetración (3 puntos) y Experiencia Específica de al menos 4 años de trabajo en hardening (2 puntos), sin especificar en ningún caso qué documentación respaldatoria será admitida para tener por acreditados dichos puntajes (por ejemplo, certificados laborales, constancias de IPS, contratos de servicios profesionales, cartas de referencia u otro medio idóneo), a diferencia de otros índices de la matriz que sí detallan expresamente los medios de prueba aceptados. Solicitamos a la Convocante precisar la documentación mínima admisible para acreditar tanto la Experiencia General como las Experiencias Específicas del perfil de Experto en Ciberseguridad.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, conforme al apartado Equipo de Trabajo, se deberán presentar el currículum y certificados que acrediten la experiencia general y los períodos específicos exigidos en pentesting y hardening. Se mantienen, además, los requisitos de vinculación laboral y acreditación ante el IPS establecidos en Capacidad Técnica. Solicitamos favor remitirse a lo solicitado en el PBC.		

Consulta 12 - Formación Académica y Experiencia de Profesionales, Experto en Ciberseguridad

Consulta	Fecha de Consulta	22-09-2026
Ausencia de requisito de formación académica (título universitario) Consulta: A diferencia de los perfiles de Coordinador de Proyecto y Especialista en Ciberseguridad, en los cuales el pliego exige expresamente contar con título universitario en carreras afines (Ingeniería en Informática, Ingeniería en electrónica, Ingeniería en Sistemas Informáticos, Licenciatura en Informática, entre otras) como requisito puntuable independiente, el perfil de Experto en Ciberseguridad no contempla ítem alguno de Formación Académica, comenzando la matriz de evaluación de dicho perfil directamente con el requisito de certificaciones. Esta omisión genera incertidumbre sobre si para el perfil de Experto en Ciberseguridad se exige o no título universitario como condición habilitante, o si por el contrario dicho perfil puede completarse únicamente con certificaciones técnicas y experiencia laboral, sin formación universitaria de base, criterio que resultaría inconsistente respecto del tratamiento dado a los demás perfiles del Equipo de Trabajo. Solicitamos a la Convocante aclarar expresamente si el perfil de Experto en Ciberseguridad requiere formación universitaria como condición habilitante y, en caso afirmativo, precisar dicho requisito y su correspondiente ponderación dentro de la matriz; o, en caso negativo, confirmar que dicho perfil puede acreditarse exclusivamente mediante certificaciones y experiencia laboral demostrable.		

Respuesta	Fecha de Respuesta	02-10-2026
Se aclara que en el PBC no establece título universitario como requisito para el perfil de Experto en Ciberseguridad. Se evaluarán las certificaciones y experiencias previstas para ese perfil, sin incorporar exigencias académicas adicionales y manteniendo las condiciones generales del Equipo de Trabajo. Se solicita favor remitirse a lo solicitado en el PBC		

Consulta 13 - Formación Académica y Experiencia de Profesionales, Experto en Ciberseguridad

Consulta	Fecha de Consulta	22-09-2026
Exigencia de experiencia en test de penetración (pentesting) desvinculada del objeto de la contratación Consulta: El perfil de Experto en Ciberseguridad exige contar con Experiencia Específica mínima de 5 años en test de penetración (pentesting), requisito que resulta desvinculado del objeto de la presente contratación, orientado a servicios de consultoría en ciberseguridad, seguridad de la información e infraestructura tecnológica con énfasis en auditorías ISO 27001, implementación de controles CIS y gestión de riesgos, sin que en ninguna otra sección del pliego (objeto de la contratación, alcance de los servicios, especificaciones técnicas) se mencione la ejecución de servicios de pentesting como parte del objeto contractual. Esta discordancia entre el perfil profesional exigido y el objeto real del servicio a contratar genera dudas sobre la pertinencia y proporcionalidad del requisito, y podría constituir una exigencia desvinculada de las necesidades reales de la Convocante, restringiendo innecesariamente la concurrencia de oferentes cuyo equipo técnico, aun estando altamente calificado en los servicios efectivamente requeridos (ISO 27001, CIS, gestión de riesgos, SIEM, SOC/CSIRT), no cuente específicamente con 5 años de experiencia en test de penetración. Solicitamos a la Convocante fundamentar la pertinencia de exigir experiencia específica en test de penetración para el perfil de Experto en Ciberseguridad, aclarando si dicho servicio forma parte del alcance y objeto de la presente contratación; en caso negativo, solicitamos se reconsidere o elimine dicho requisito por no guardar relación con el objeto contractual, en resguardo de los Principios de Economía, Razonabilidad y Libre Concurrencia.		

Respuesta	Fecha de Respuesta	02-10-2026
Se mantiene el requisito. La justificación técnica del PBC incluye expresamente pruebas de intrusión, además de la identificación de vulnerabilidades y medidas correctivas. Por ello, la experiencia en pentesting guarda relación con los trabajos previstos para el fortalecimiento de la infraestructura tecnológica. Se solicita favor remitirse a lo solicitado en el PBC.		

Consulta 14 - ¿El proveedor debe suministrar una nueva solución SIEM/XDR?

Consulta	Fecha de Consulta	22-09-2026
El PBC exige entregar un SIEM/XDR operativo, con integración de fuentes y casos de uso. Sin embargo, no se determina expresamente si ESSAP ya dispone de una plataforma que deberá utilizarse o si el adjudicado deberá suministrar una nueva solución con sus licencias. Tampoco especifica cantidad de GB/día, EPS, período de retención ni plazo de licenciamiento. Estos datos son fundamentales para dimensionar y cotizar el servicio por lo que se solicita amablemente a la convocante aclarar este punto.		

Respuesta	Fecha de Respuesta	02-10-2026
Adecuarse al numeral 2.3 de las especificaciones técnicas. El PBC no precisa la existencia de una plataforma disponible ni fija GB/día, EPS, retención o plazo de licenciamiento. Se solicita favor remitirse a lo solicitado en el PBC.		

Consulta 15 - Cuál es el dimensionamiento completo de la infraestructura?

Consulta	Fecha de Consulta	22-09-2026
Se establece un máximo de 500 endpoints, pero no se especifican las cantidades exactas de servidores físicos, máquinas virtuales, dispositivos de red, sedes ni plataformas críticas. Se necesita conocer esa infraestructura para estimar el esfuerzo de consultoría, las integraciones y las herramientas necesarias.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se solicita favor remitirse a lo solicitado en el PBC.		

Consulta 16 - Los tres perfiles profesionales deben corresponder a personas distintas?

Consulta	Fecha de Consulta	22-09-2026
El pliego identifica un coordinador, un especialista y un experto en ciberseguridad, pero no aclara si es posible acreditar más de un perfil mediante un mismo profesional. También solicitamos confirmar si todos los requisitos detallados en la matriz constituyen condiciones excluyentes o si su incumplimiento parcial únicamente afecta la puntuación técnica.		

Respuesta	Fecha de Respuesta	02-10-2026
Atenerse a los requisitos de perfiles y condiciones del Equipo de Trabajo; el PBC no regula expresamente la acumulación de perfiles en una misma persona. Los requisitos mínimos de capacidad técnica son obligatorios y la puntuación se asigna conforme a la matriz. La existencia de puntajes no exime de cumplir los mínimos exigidos. Solicitamos favor remitirse al PBC.		

Consulta 17 - cantidad mínima de reglas y casos de uso exigidos

Consulta	Fecha de Consulta	29-09-2026
Consulta: En el ítem 2.3 se requiere la entrega de "10-15 reglas/casos de uso iniciales", expresado como un rango sin precisar cuál es la cantidad mínima exigible para dar por cumplido el entregable, ni cuáles son los escenarios de detección prioritarios, ni el porcentaje de reducción de falsos positivos que se espera del ajuste (tuning). Un rango abierto genera incertidumbre en la cotización y en la recepción, ya que el cumplimiento quedaría sujeto a apreciaciones subjetivas del evaluador. Solicitamos a la Convocante precisar que la cantidad mínima exigible para la aceptación es de diez (10) reglas o casos de uso, indicar si ESSAP definirá los escenarios a cubrir o si serán propuestos por el Proveedor, y establecer un criterio objetivo y medible de aceptación del proceso de tuning.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se aclara que el rango previsto es de 10 a 15 reglas o casos de uso iniciales; su límite inferior es 10. La propuesta deberá responder al relevamiento y a los riesgos identificados. La aceptación se verificará mediante dashboards activos y recepción de eventos, conforme al numeral 2.3. El PBC no fija un porcentaje de reducción de falsos positivos. Solicitamos favor remitirse al PBC.		

Consulta 18 - Alcance del entregable "SIEM/XDR operativo"

Consulta	Fecha de Consulta	29-09-2026
Consulta: En el ítem 2.3 del Detalle del Servicio se exige como entregable un "SIEM/XDR operativo + guía de operación + 10-15 reglas/casos de uso iniciales", con criterio de aceptación basado en "dashboards activos, eventos llegando". Sin embargo, el llamado se denomina "Servicio de Consultoría" y el PBC no indica si la plataforma SIEM/XDR, sus licencias, el hardware o la infraestructura cloud, los agentes de endpoint y el almacenamiento serán provistos por ESSAP o deberán ser suministrados por el Proveedor. Tampoco se informan parámetros de dimensionamiento como volumen de eventos por segundo (EPS) o GB/día de ingesta, período de retención de logs, cantidad de fuentes por tipo ni modalidad de despliegue (on-premise, cloud o híbrido). Esta omisión impide cotizar sobre bases homogéneas, pues algunos oferentes podrían incluir el costo de una plataforma completa y otros únicamente servicios profesionales, lo cual afecta la comparabilidad de las ofertas y el principio de igualdad de condiciones previsto en la Ley N° 7021/2022 de Suministro y Adquisiciones Públicas. Asimismo, si ESSAP ya cuenta con una plataforma instalada, la omisión de la marca y versión otorgaría ventaja al oferente que la conoce. Solicitamos a la Convocante aclarar expresamente si el suministro de la plataforma SIEM/XDR y sus licencias forma parte del alcance del Proveedor; en caso afirmativo, publicar los parámetros de dimensionamiento, retención y período de licenciamiento exigidos y admitir cualquier solución de mercado que los cumpla; y en caso negativo, informar la marca, versión y capacidad de la plataforma existente sobre la cual se realizará la integración.		

Respuesta	Fecha de Respuesta	02-10-2026
Atenerse al numeral 2.3, que exige una plataforma operativa, integración de fuentes, guía de operación y reglas iniciales. Solicitamos favor remitirse al PBC		

Consulta 19 - Contradicción en el alcance del hardening de servidores

Consulta	Fecha de Consulta	29-09-2026
Consulta: En la sección de Generalidades, apartado "Hardening, vulnerabilidades y cambios", se establece que "el hardening se verificará contra CIS Benchmark vigente o guía equivalente, mediante reporte pass/fail por control", con registro de excepciones, riesgo residual y aprobación de ESSAP, lo cual implica una ejecución y verificación técnica sobre los servidores. Sin embargo, en el ítem 2.4 del Detalle del Servicio, las acciones se limitan a "Baseline hardening por rol, recomendaciones", el entregable es un "Checklist hardening" y el criterio de aceptación es la "Entrega de Playbook para recomendaciones", es decir, un alcance meramente consultivo. Ambas cláusulas describen alcances sustancialmente distintos, con impacto directo en el esfuerzo, las horas-hombre y el costo ofertado. Solicitamos a la Convocante unificar el criterio y aclarar si el alcance comprende únicamente la elaboración del baseline y recomendaciones o si incluye la aplicación efectiva de configuraciones sobre los servidores y la emisión de reportes pass/fail por control; en este último caso, informar la cantidad de servidores y sistemas operativos alcanzados, e indicar si la aplicación de cambios será ejecutada por el Proveedor o por personal de ESSAP.		

Respuesta	Fecha de Respuesta	02-10-2026
Se mantienen el baseline por rol, las recomendaciones, el checklist y el playbook del numeral 2.4, junto con la verificación por control prevista en Generalidades. Favor remitirse a lo solicitado en el PBC		

Consulta 20 - Contradicción entre SLA de remediación predefinidos y SLA a definir

Consulta	Fecha de Consulta	29-09-2026
Consulta: En la sección de Generalidades se establece que "las vulnerabilidades críticas deberán contar con corrección o mitigación en un máximo de 72 horas y las altas en quince días"; no obstante, en el ítem 2.5 se indica como acción "Definir SLA por severidad (críticas/altas)" y como criterio de aceptación "SLA documentados; reporte con % cumplimiento". Existe contradicción entre SLA ya fijados en el pliego y SLA que deben ser definidos como parte del servicio. Adicionalmente, no se precisa si el plazo de 72 horas y 15 días constituye una obligación de resultado del Proveedor, lo cual resultaría desproporcionado en un servicio de consultoría, dado que la corrección depende de la disponibilidad de parches por parte de los fabricantes, de las ventanas de mantenimiento, de la aprobación de cambios de ESSAP y de la ejecución por parte de los administradores de la Convocante. Solicitamos a la Convocante unificar el criterio, aclarar si los plazos de 72 horas y 15 días son exigibles al Proveedor o constituyen un objetivo del proceso a definir en el ítem 2.5, precisar quién ejecuta la remediación, y establecer que los plazos se computan a partir de la autorización del cambio por ESSAP y quedan suspendidos ante causas no imputables al Proveedor.		

Respuesta	Fecha de Respuesta	02-10-2026
Adecuarse al PBC. La ejecución se organizará mediante la matriz RACI y las autorizaciones de cambio; no se incorpora el inicio diferido ni la suspensión automática solicitados. Solicitamos favor remitirse al PBC.		

Consulta 21 - Generalidades (Respaldo y recuperación)

Consulta	Fecha de Consulta	29-09-2026
Consulta: En la sección de Generalidades, apartado "Respaldo y recuperación", se exige al menos una restauración controlada por cada plataforma crítica, la comparación de resultados contra "los RTO y RPO aprobados" y se establece expresamente que "no se considerará suficiente la sola evidencia de jobs exitosos". Sin embargo, en el ítem 2.7 el criterio de aceptación es precisamente "Evidencia jobs OK; retención documentado", la acción consiste en "Definir RPO/RTO para sistemas críticos" y se utiliza la expresión "Documentar y o verificar backups automatizados". Existen por tanto tres incongruencias: el criterio de aceptación del ítem 2.7 es el mismo que la sección de Generalidades declara insuficiente; los RTO/RPO se presentan como ya aprobados en un apartado y como pendientes de definición en otro; y la expresión "y o" no permite determinar si la verificación es obligatoria u opcional. Solicitamos a la Convocante unificar el criterio de aceptación del ítem 2.7, aclarar si las pruebas de restauración forman parte del alcance obligatorio, informar la cantidad de plataformas críticas y la solución de respaldo existente (marca, versión y medios), y precisar si los RTO/RPO serán definidos durante el proyecto o si ESSAP ya cuenta con valores aprobados que deban comunicarse a los oferentes.		

Respuesta	Fecha de Respuesta	02-10-2026
Los RTO y RPO deberán definirse conforme al numeral 2.7 y contar con aprobación para contrastar los resultados. El PBC no identifica la solución de respaldo existente ni cuantifica las plataformas críticas. Favor remitirse a lo solicitado en el PBC.		

Consulta 22 - Notificación y responsabilidad por incidentes

Consulta	Fecha de Consulta	29-09-2026
Consulta: En el apartado "Notificación y responsabilidad por incidentes" se establece que el Proveedor "será responsable por incidentes atribuibles a su operación, configuración, negligencia, accesos o incumplimiento de controles, aunque el escenario específico no se encuentre enumerado en el PBC". Esta cláusula establece una responsabilidad abierta, sin límite económico, sin procedimiento de determinación de la atribución y extensible a supuestos no previstos en el pliego, lo que impide a los oferentes cuantificar el riesgo contractual y desalienta la participación, en contradicción con los principios de libre competencia, proporcionalidad y seguridad jurídica que rigen las contrataciones bajo la Ley N° 7021/2022. Además, en un servicio de consultoría en el que ESSAP aprueba cada cambio y mantiene la administración de su infraestructura, la atribución de responsabilidad requiere un procedimiento objetivo. Solicitamos a la Convocante modificar la cláusula a fin de limitar la responsabilidad del Proveedor a daños directos debidamente comprobados y atribuibles a su dolo o culpa, establecer un tope de responsabilidad vinculado al monto del contrato, definir el procedimiento de análisis de causa raíz y descargo previo a la imputación, y excluir expresamente los incidentes derivados de cambios aprobados por ESSAP o de condiciones preexistentes.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, solicitamos favor remitirse a lo solicitado en el PBC.		

Consulta 23 - Edición de la norma ISO/IEC 27000:2026

Consulta	Fecha de Consulta	29-09-2026
Consulta: En la lista de estándares y mejores prácticas se menciona la norma "ISO/IEC 27000:2026 - Sistema de Gestión de Seguridad de la Información - Visión General y Vocabulario". La edición ampliamente utilizada y de referencia de dicha norma es la ISO/IEC 27000:2018, por lo que resulta necesario confirmar si la referencia a una edición 2026 es correcta y si la misma se encuentra efectivamente publicada y disponible, dado que no puede exigirse el cumplimiento de un documento que los oferentes no puedan consultar. Asimismo, se hace referencia al "Plan Nacional de Ciberseguridad y la Guía de Controles Críticos de Ciberseguridad" sin indicar versión, año ni organismo emisor. Solicitamos a la Convocante aclarar la edición exigida de la norma ISO/IEC 27000 o, en su caso, sustituirla por la edición vigente publicada, e identificar con precisión la versión y el organismo emisor de las normas nacionales citadas.		

Respuesta	Fecha de Respuesta	02-10-2026
Se mantienen los requerimientos exigidos por el PBC. La guía nacional corresponde a la aprobada por Resolución MITIC N.º 277/2020. El Plan Nacional citado fue aprobado por Decreto N.º 7052/2017 y actualizado por la Estrategia Nacional de Ciberseguridad 2025-2028, aprobada por Decreto N.º 3900/2025, bajo coordinación del MITIC. Favor remitirse a lo solicitado en el PBC.		

Consulta 24 - Marco de referencia para el baseline IG2

Consulta	Fecha de Consulta	29-09-2026
Consulta: Los ítems 2.2 y 2.5 hacen referencia a un "baseline IG2" y a un "proceso IG2", terminología propia de los Implementation Groups de los CIS Critical Security Controls; sin embargo, dicho marco no figura en la lista de estándares y mejores prácticas de la sección de Generalidades, donde únicamente se menciona el CIS Benchmark para hardening. Por otra parte, se incluye el modelo SOC-CMM como estándar de referencia, aunque el alcance del servicio no contempla la implementación, operación ni evaluación de madurez de un Centro de Operaciones de Seguridad. Solicitamos a la Convocante aclarar si el término IG2 refiere a los CIS Critical Security Controls v8/v8.1 e incorporarlo expresamente como marco de referencia, y precisar el alcance concreto de la aplicación de SOC-CMM, indicando si se exige una evaluación formal de madurez como entregable o si solo constituye una referencia metodológica.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se aclara que IG2 se refiere al Grupo de Implementación 2 de los CIS Critical Security Controls. El PBC no individualiza una versión. Favor remitirse a lo solicitado en el PBC.		

Consulta 25 - Capacidad Técnica en Consorcio

Consulta	Fecha de Consulta	29-09-2026
El texto exige que "todos los integrantes deben cumplir la experiencia mínima requerida" / "todos los integrantes del Consorcio deberán cumplir la capacidad técnica mínima requerida", es decir el 100% para cada miembro		

Respuesta	Fecha de Respuesta	02-10-2026
Atenerse a las disposiciones específicas para consorcios: Ello no elimina las condiciones que el PBC exige individualmente a cada miembro. Favor remitirse a lo solicitado en el PBC.		

Consulta 26 - Indefinición de la "Norma Corporativa Básica"

Consulta	Fecha de Consulta	29-09-2026
Consulta: El PBC establece que todos los documentos e informes deberán ser padronizados y normalizados "de acuerdo a la Norma Corporativa Básica", sin que dicha norma se encuentre adjunta al pliego ni identificada, lo que impide a los oferentes conocer los requisitos de formato que condicionan la aceptación de los entregables. Asimismo, se indica que la documentación deberá estar redactada "en idioma español y/o inglés", redacción que admitiría la entrega de documentos exclusivamente en inglés, lo cual resulta incongruente con una institución pública paraguaya y con la necesidad de que el personal de ESSAP apruebe y utilice dichos documentos. Solicitamos a la Convocante publicar o poner a disposición de los oferentes la Norma Corporativa Básica referida, y aclarar si los entregables deben presentarse obligatoriamente en español, admitiéndose documentación técnica de fabricantes en inglés.		

Respuesta	Fecha de Respuesta	02-10-2026
La Norma Corporativa Básica no está adjunta ni identificada en el PBC. En cuanto al idioma, las Generalidades admiten español y/o inglés para la documentación técnica. El contrato y la correspondencia contractual se rigen por la cláusula de idioma del modelo de contrato, que exige castellano y las traducciones allí previstas. Favor remitirse a lo solicitado en el PBC.		

Consulta 27 - Omisión de cantidades de activos necesarias para dimensionar el servicio

Consulta	Fecha de Consulta	29-09-2026
Consulta: El PBC únicamente cuantifica el alcance de endpoints ("hasta 500"), pero no informa la cantidad de sedes, servidores físicos, máquinas virtuales, bases de datos, dispositivos de red (routers, switches, firewalls, APs), subredes/VLAN ni aplicaciones web a relevar, a pesar de que los ítems 2.1 y 2.8 exigen inventario, clasificación de criticidad, mapa de red y escaneo de puertos, y el criterio de aceptación del ítem 2.1 fija una "cobertura inventario $\geq$ 95% de activos en alcance". Sin estos datos los oferentes no pueden dimensionar horas-hombre ni cotizar sobre bases comparables, y el porcentaje de cobertura carece de base de cálculo. Solicitamos a la Convocante informar las cantidades estimadas de activos por tipo y la cantidad y ubicación de sedes incluidas, y aclarar que el porcentaje de cobertura se medirá sobre el universo de activos efectivamente puestos a disposición y con acceso habilitado por ESSAP.		

Respuesta	Fecha de Respuesta	02-10-2026
Atenerse a los numerales 1, 2.1 y 2.8 del PBC. Favor remitirse a lo solicitado en el PBC		

Consulta 28 - Agentes de endpoint y telemetría a validar

Consulta	Fecha de Consulta	29-09-2026
Consulta: El ítem 2.2 requiere "validar agentes/telemetría" y reportar cobertura por plataforma sobre hasta 500 endpoints Windows, macOS y Linux, pero no informa si ESSAP cuenta actualmente con solución de EDR, antivirus o gestión de endpoints, ni su marca y versión, ni si el Proveedor debe suministrar e instalar agentes. En caso de que el despliegue de agentes forme parte del alcance, ello implicaría el suministro de licencias no descriptas en el pliego. Solicitamos a la Convocante informar las soluciones de endpoint existentes y la distribución aproximada por sistema operativo, y aclarar si el suministro, licenciamiento y despliegue de agentes está incluido en el alcance del Proveedor.		

Respuesta	Fecha de Respuesta	02-10-2026
Se aclara que el numeral 2.2 no identifica las soluciones existentes, sus versiones ni la distribución por sistema operativo, y tampoco detalla un suministro separado de licencias de agentes. Se mantiene el alcance de lo establecido en el PBC. Favor remitirse a lo solicitado en el PBC.		

Consulta 29 - Descripción incompleta de la sensibilización y de las simulaciones de phishing

Consulta	Fecha de Consulta	29-09-2026
Consulta: El ítem 3.2 se encuentra redactado de forma incompleta ("Sensibilización (1 sesiones.\"", sin indicar con certeza la cantidad de sesiones, su duración, la cantidad de participantes, ni la distribución entre modalidad presencial y virtual. Asimismo, exige "simulaciones de phishing" sin especificar cantidad de campañas, número de usuarios destinatarios, ni si la plataforma de simulación y su licenciamiento corren por cuenta del Proveedor, siendo además el único criterio de aceptación la "Asistencia". Respecto del ítem 3.1, no se indica si la infraestructura de laboratorio será provista por ESSAP o por el Proveedor. Solicitamos a la Convocante precisar la cantidad de sesiones de sensibilización, su duración y el número de participantes, la cantidad de campañas y usuarios alcanzados por las simulaciones de phishing, quién provee la plataforma de simulación y el entorno de laboratorio, y un criterio de aceptación objetivo para ambos ítems.		

Respuesta	Fecha de Respuesta	02-10-2026
Adecuarse a los requerimientos de los numerales 3.2 y 3.1., del PBC. Favor remitirse a lo solicitado en el PBC.		

Consulta 30 - Disponibilidad actual de plataforma SIEM/XDR

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar si la ESSAP cuenta actualmente con una solución SIEM y/o XDR licenciada y disponible para la ejecución del servicio previsto en el punto 2.3. En caso afirmativo, favor indicar fabricante, producto, versión y alcance o capacidad actualmente disponible.		

Respuesta	Fecha de Respuesta	02-10-2026
El PBC no identifica fabricante, producto, versión ni capacidad de una plataforma SIEM/XDR existente. Se mantiene el entregable operativo exigido en el numeral 2.3. Se solicita favor remitirse al PBC.		

Consulta 31 - Provisión de licenciamiento SIEM/XDR

Consulta	Fecha de Consulta	29-09-2026
En caso de que la ESSAP no cuente actualmente con una solución SIEM/XDR disponible para la ejecución del servicio, favor aclarar si el adjudicado deberá incluir dentro de su oferta la provisión del software, suscripciones y/o licenciamiento necesario para cumplir con el entregable "SIEM/XDR operativo".		

Respuesta	Fecha de Respuesta	02-10-2026
Atenerse al numeral 2.3 y a la disposición sobre los bienes y servicios razonablemente necesarios para cumplir el suministro. Se solicita favor remitirse al PBC.		

Consulta 32 - Alcance del licenciamiento requerido

Consulta	Fecha de Consulta	29-09-2026
En caso de que corresponda al adjudicado proveer una solución SIEM/XDR, favor indicar la cantidad de activos, endpoints, servidores, usuarios, volumen estimado de eventos por segundo y/o GB diarios, así como el período durante el cual deberá permanecer vigente el licenciamiento.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada , solicitamos favor remitirse al PBC.		

Consulta 33 - Cantidad de servidores y máquinas virtuales

Consulta	Fecha de Consulta	29-09-2026
Favor indicar la cantidad aproximada de servidores físicos y máquinas virtuales comprendidos dentro del alcance de la consultoría, discriminando, de ser posible, por sistema operativo y plataforma de virtualización.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada se solicita, adecuarse al numeral 2.1., con el alcance y la cobertura previstos. Favor remitirse a lo solicitado en el PBC.		

Consulta 34 - Cantidad y ubicación de sedes

Consulta	Fecha de Consulta	29-09-2026
Favor indicar la cantidad de sedes de ESSAP comprendidas dentro del alcance del servicio y su ubicación geográfica, aclarando cuáles requerirán trabajos presenciales.		

Respuesta	Fecha de Respuesta	02-10-2026
El Plan de Prestación de Servicios identifica como lugar de entrega la Dirección de Tecnología y Desarrollo Informático, José Berges 516 entre Brasil y San José. Favor remitirse a lo solicitado en el PBC.		

Consulta 35 - Modalidad de ejecución de los trabajos

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar qué actividades deberán ser ejecutadas obligatoriamente de manera presencial en las instalaciones de ESSAP y cuáles podrán realizarse de manera remota. Esto incide directamente en horas, traslados y costos internos, y cuyos valores son necesarios para establecer nuestra oferta.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada se solicita, favor remitirse a lo solicitado en el PBC.		

Consulta 36 - Infraestructura de red comprendida en el alcance

Consulta	Fecha de Consulta	29-09-2026
Favor indicar la cantidad aproximada de routers, switches, firewalls, access points, VLAN y demás dispositivos de red comprendidos dentro de la evaluación prevista en el punto 2.8.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se solicita adecuarse a lo contemplado en el numeral 2.8. Favor remitirse a lo solicitado en el PBC.		

Consulta 37 - Implementación de cambios de segmentación de red

Consulta	Fecha de Consulta	29-09-2026
En relación con el punto 2.8, favor aclarar si el adjudicado deberá ejecutar efectivamente cambios de configuración y segmentación/DMZ sobre la infraestructura de ESSAP o si el alcance se limitará a la evaluación, diseño y presentación de recomendaciones y plan de implementación.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se solicita adecuarse a lo contemplado en el numeral 2.8. Favor remitirse a lo solicitado en el PBC		

Consulta 38 - Herramientas para gestión de vulnerabilidades

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar si ESSAP dispone actualmente de una plataforma de gestión y escaneo de vulnerabilidades para la ejecución del servicio. En caso afirmativo, favor indicar fabricante y producto. En caso negativo, aclarar si el adjudicado deberá proveer las herramientas necesarias durante la vigencia del proyecto.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, el proveedor deberá contemplar las herramientas necesarias para cumplir el numeral 2.5., como se establece en el PBC.		

Consulta 39 - Alcance de las pruebas de penetración

Consulta	Fecha de Consulta	29-09-2026
Favor detallar el alcance previsto para las pruebas de penetración, indicando cantidad aproximada de direcciones IP, aplicaciones web, servicios expuestos, ambientes internos y externos que deberán ser evaluados.		

Respuesta	Fecha de Respuesta	02-10-2026
Las pruebas de intrusión están previstas en la justificación técnica, y el numeral 2.8 incluye escaneo interno y, cuando corresponda, de borde/DMZ. El PBC no cuantifica direcciones IP, aplicaciones o servicios a evaluar. Se solicita favor remitirse a lo solicitado en el PBC.		

Consulta 40 - Herramientas para simulación de phishing

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar si ESSAP dispone actualmente de una plataforma para simulación de campañas de phishing o si el adjudicado deberá proveer la herramienta necesaria para realizar las simulaciones requeridas.		

Respuesta	Fecha de Respuesta	02-10-2026
El PBC no identifica una plataforma de phishing disponible en la institución, ni se establece una licencia permanente como entregable independiente. Favor remitirse a lo solicitado en el PBC.		

Consulta 41 - Alcance de la campaña de phishing

Consulta	Fecha de Consulta	29-09-2026
Favor indicar la cantidad aproximada de usuarios que deberán participar de la campaña de simulación de phishing prevista en el servicio.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se solicita favor remitirse a lo solicitado en el PBC.		

Consulta 42 - Alcance del hardening de servidores

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar si el servicio de hardening comprende únicamente la evaluación y elaboración de recomendaciones/checklists o si el adjudicado deberá realizar modificaciones efectivas sobre las configuraciones de los servidores de ESSAP.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, atenerse a la respuesta de la consulta 19. Favor remitirse a lo solicitado en el PBC.		

Consulta 43 - Cantidad de servidores sujetos a hardening

Consulta	Fecha de Consulta	29-09-2026
Favor indicar la cantidad aproximada de servidores y plataformas que deberán ser sometidos al proceso de hardening conforme a CIS Benchmark o guía equivalente.		

Respuesta	Fecha de Respuesta	02-10-2026
El PBC no fija una cantidad de servidores o plataformas para hardening. Favor remitirse a lo solicitado en el PBC		

Consulta 44 - Responsabilidad sobre remediación de vulnerabilidades

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar si la corrección o mitigación de vulnerabilidades críticas y altas deberá ser ejecutada directamente por el adjudicado o si el adjudicado deberá identificar, recomendar y acompañar técnicamente las acciones que serán ejecutadas por el personal de ESSAP.		

Respuesta	Fecha de Respuesta	02-10-2026
El numeral 2.5 incluye un ciclo inicial de remediación para activos críticos; no se limita a la identificación de hallazgos. La distribución de tareas deberá reflejarse en la matriz RACI del Plan de Trabajo, respetando las autorizaciones de la institución y las obligaciones del proveedor. Se mantienen los plazos de corrección o mitigación del PBC. Favor remitirse a lo solicitado en el PBC.		

Consulta 45 - Sistemas de backup actualmente utilizados

Consulta	Fecha de Consulta	29-09-2026
Favor indicar las plataformas o soluciones de respaldo actualmente utilizadas por ESSAP y la cantidad aproximada de plataformas críticas sobre las cuales deberán realizarse pruebas controladas de restauración.		

Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se solicita favor remitirse a lo solicitado en el PBC		

Consulta 46 - Definición de plataformas críticas

Consulta	Fecha de Consulta	29-09-2026
Favor indicar la cantidad aproximada de plataformas que ESSAP considera críticas y que estarán comprendidas dentro de las pruebas de respaldo, recuperación, RPO y RTO.		

Respuesta	Fecha de Respuesta	02-10-2026
El PBC no establece una cantidad de plataformas críticas. Se aclara que para cada plataforma crítica seleccionada se exige la restauración controlada y la comparación de resultados con los RTO y RPO aprobados. Favor remitirse a lo solicitado en el PBC.		

Consulta 47 - Integraciones requeridas con Active Directory

Consulta	Fecha de Consulta	29-09-2026
Favor indicar la cantidad de dominios, controladores de dominio y/o bosques de Active Directory actualmente existentes y que deberán ser considerados dentro de la integración SIEM/XDR.		

Respuesta	Fecha de Respuesta	02-10-2026
El PBC no detalla la cantidad de dominios, controladores o bosques existentes. Se mantiene la integración prevista, sin presumir una cantidad de componentes. Favor remitirse a lo solicitado en el PBC		

Consulta 48 - Fuentes de logs a integrar al SIEM/XDR

Consulta	Fecha de Consulta	29-09-2026
Favor indicar la cantidad y tipo aproximado de fuentes que deberán integrarse a la plataforma SIEM/XDR, incluyendo servidores, dispositivos de red, Active Directory, aplicaciones web, bases de datos y demás fuentes relevantes.		
Respuesta	Fecha de Respuesta	02-10-2026
El PBC no cuantifica las fuentes por tipo. Se mantienen la integración, normalización y etiquetado exigidos. Favor remitirse a lo solicitado en el PBC		

Consulta 49 - Casos de uso SIEM/XDR

Consulta	Fecha de Consulta	29-09-2026
Respecto de los 10 a 15 casos de uso iniciales solicitados, favor aclarar si los mismos serán definidos por ESSAP durante la ejecución del proyecto o deberán ser propuestos íntegramente por el adjudicado en función del relevamiento realizado.		
Respuesta	Fecha de Respuesta	02-10-2026
Su validación corresponderá a la institución al verificar los entregables y criterios de aceptación previstos en el PBC. Favor remitirse a lo solicitado en el PBC		

Consulta 50 - Operación posterior del SIEM/XDR

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar si, una vez realizada la implementación e integración del SIEM/XDR, el adjudicado deberá prestar servicios posteriores de monitoreo, operación, SOC y/o atención de incidentes, o si el alcance finaliza con la transferencia de conocimiento y aceptación de los entregables del proyecto.		
Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se solicita favor remitirse a lo solicitado en el PBC.		

Consulta 51 - Servicio de monitoreo 24x7

Consulta	Fecha de Consulta	29-09-2026
Favor confirmar si dentro del alcance de la presente contratación se requiere algún servicio de monitoreo continuo de seguridad bajo modalidad 24x7, 8x5 u otra modalidad. En caso afirmativo, favor indicar período y nivel de servicio requerido.		
Respuesta	Fecha de Respuesta	02-10-2026
El PBC no establece un servicio de monitoreo 24x7, 8x5 ni otra cobertura horaria permanente. Favor remitirse a lo solicitado en el PBC		

Consulta 52 - Cantidad de profesionales requeridos

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar la cantidad mínima de profesionales que deberá integrar el equipo de trabajo durante la ejecución contractual y si los perfiles de Coordinador de Proyecto, Especialista en Ciberseguridad y Experto en Ciberseguridad deberán corresponder necesariamente a personas diferentes.		
Respuesta	Fecha de Respuesta	02-10-2026
Se aclara que se deberán cubrir los perfiles de Coordinador de Proyecto, Especialista en Ciberseguridad y Experto en Ciberseguridad, con los requisitos del PBC. El pliego no establece expresamente que deban corresponder a tres personas distintas. Atenerse a las condiciones del Equipo de Trabajo y a la respuesta de la consulta 16. Favor remitirse a lo solicitado en el PBC		

Consulta 53 - Acumulación de perfiles profesionales

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar si un mismo profesional podrá acreditar y desempeñar más de uno de los perfiles requeridos, siempre que cumpla integralmente con los requisitos académicos, certificaciones y experiencia establecidos para cada perfil.		
Respuesta	Fecha de Respuesta	02-10-2026
Atenerse a la respuesta de la consulta 16. Se mantienen íntegros los requisitos de cada perfil y las condiciones del Equipo de Trabajo. Favor remitirse a lo solicitado en el PBC.		

Consulta 54 - Dedicación mínima de los profesionales

Consulta	Fecha de Consulta	29-09-2026
Favor indicar si existe un porcentaje o cantidad mínima de horas de dedicación requerida para cada uno de los profesionales propuestos durante los 180 días de ejecución del proyecto.		
Respuesta	Fecha de Respuesta	02-10-2026
El PBC no fija un porcentaje ni una cantidad mínima de horas por profesional. Favor remitirse a lo solicitado en el PBC.		

Consulta 55 - Certificaciones técnicas equivalentes

Consulta	Fecha de Consulta	29-09-2026
Considerando que el PBC admite determinadas certificaciones "o similares/equivalentes", favor confirmar que serán aceptadas certificaciones de ciberseguridad que acrediten competencias equivalentes a las requeridas, aun cuando correspondan a fabricantes u organismos certificadores distintos de los mencionados como ejemplo.		
Respuesta	Fecha de Respuesta	02-10-2026
Siempre se admiten certificaciones similares o equivalentes en los requisitos que expresamente contemplan esa posibilidad, según su alcance y competencias acreditadas. La equivalencia no depende únicamente del nombre o del organismo emisor y no se extiende automáticamente a requisitos que contienen una enumeración específica sin esa alternativa. Favor remitirse a lo solicitado en el PBC		

Consulta 56 - Presentación del Plan de Trabajo

Consulta	Fecha de Consulta	29-09-2026
Respecto del Plan de Trabajo "llave en mano" requerido con la oferta, favor confirmar si el cronograma Gantt deberá elaborarse tomando como fecha inicial referencial el día 1 desde la Orden de Servicio, considerando que la fecha efectiva de inicio aún no se conoce al momento de presentación de ofertas.		
Respuesta	Fecha de Respuesta	02-10-2026
Para elaborar el Gantt de la oferta, el apartado Plan de Trabajo permite tomar como referencia el inicio desde la Orden de Servicio, con un máximo de 180 días corridos. Ello no modifica el Plan de Prestación de Servicios, que consigna el cómputo desde la firma del contrato; ambas referencias constan en el PBC. Favor remitirse a lo solicitado en el PBC		

Consulta 57 - Nivel de detalle del Plan de Trabajo

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar el nivel de detalle esperado para el Plan de Trabajo a ser presentado con la oferta y si los alcances, RACI, riesgos e hitos podrán ser ajustados de común acuerdo con ESSAP durante la fase inicial de relevamiento, sin alterar el alcance contractual.		
Respuesta	Fecha de Respuesta	02-10-2026
Se aclara que el relevamiento podrá precisar la organización operativa de los trabajos, con validación de la institución, sin alterar el alcance, los entregables ni las condiciones contractuales. Para los demás puntos, adecuarse al PBC.		

Consulta 58 - Aceptación de entregables

Consulta	Fecha de Consulta	29-09-2026
Favor indicar el plazo máximo con que contará ESSAP para revisar, observar y aprobar cada entregable presentado por el adjudicado, así como el plazo otorgado al proveedor para realizar eventuales ajustes, de tal manera a evitar que los 180 días se consuman esperando aprobaciones.		
Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta realizada, se solicita adecuarse a los requerimientos de plazos establecidos en el PBC.		

Consulta 59 - Cronograma y dependencia de aprobaciones

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar si los tiempos utilizados por ESSAP para revisión, aprobación, provisión de accesos o disponibilidad de infraestructura serán computados dentro del plazo contractual de 180 días.		
Respuesta	Fecha de Respuesta	02-10-2026
Se mantiene el plazo de 180 días corridos. Favor remitirse a lo solicitado en el PBC		

Consulta 60 - Disponibilidad de accesos e información

Consulta	Fecha de Consulta	29-09-2026
Favor confirmar que ESSAP proporcionará oportunamente los accesos, credenciales, VPN, información técnica, personal de apoyo y autorizaciones necesarias para la ejecución de las actividades previstas.		
Respuesta	Fecha de Respuesta	02-10-2026
El PBC exige accesos nominales, temporales y previamente autorizados, VPN institucional con MFA y PAM cuando esté disponible. La habilitación de credenciales e información deberá respetar esos controles; no se prevé acceso irrestricto. Favor remitirse a lo solicitado en el PBC		

Consulta 61 - Disponibilidad de accesos e información

Consulta	Fecha de Consulta	29-09-2026
Favor confirmar que ESSAP proporcionará oportunamente los accesos, credenciales, VPN, información técnica, personal de apoyo y autorizaciones necesarias para la ejecución de las actividades previstas.		
Respuesta	Fecha de Respuesta	02-10-2026
Remitirse a la consulta 60 y su respuesta.		

Consulta 62 - Uso de herramientas propias del adjudicado

Consulta	Fecha de Consulta	29-09-2026
Favor aclarar si el adjudicado podrá utilizar herramientas propias de diagnóstico, inventario, análisis, escaneo de vulnerabilidades, pentesting y generación de evidencias durante la ejecución del servicio, siempre que se cumplan los requisitos de seguridad y confidencialidad establecidos por ESSAP.		
Respuesta	Fecha de Respuesta	02-10-2026
Teniendo en cuenta la consulta se solicita favor adecuarse a lo solicitado en el PBC.		