Dirección Nacional de Contrataciones Públicas
E.E.U.U. 961 c/ Tte. Fariña - Asunción, Paraguay
Tel. y Fax +595 21 4154000 - dncp@contrataciones.gov.py

Consultas Realizadas

Licitación 477705 - SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN Y CONTROLES CRITICOS DE CIBERSEGURIDAD

Consulta 1 - Consulta sobre adecuación del PBC a las necesidades de CONATEL

Consulta	**Fecha de Consulta**	28-08-2026

Del análisis del PBC se observa una elevada similitud con la Licitación ID N.º 473102 del SNPP, no solo en aspectos técnicos generales, sino también en parámetros específicos y requisitos de capacidad técnica.

En el presente llamado incluso permanecen referencias ajenas a la CONATEL, tales como “objetivos del SNPP” y “datos sensibles del sector educativo”. Asimismo, coinciden parámetros como el procesamiento aproximado de 5 GB/día de logs, operación SOC 8x5 con monitoreo remoto 24x7, capacidad mínima para gestionar 1.000 activos y varios requisitos relativos a perfiles técnicos, certificaciones y experiencia.

Por lo expuesto, solicitamos aclarar si el presente PBC fue elaborado y dimensionado específicamente conforme a las necesidades e infraestructura actuales de la CONATEL, o si determinados apartados corresponden a una reutilización, copy-paste o adaptación del PBC de la Licitación ID N.º 473102 del SNPP.

En caso de haberse utilizado dicho procedimiento como referencia, solicitamos confirmar que los parámetros técnicos, perfiles profesionales, años de experiencia, certificaciones y demás requisitos fueron revisados y justificados específicamente para la realidad de la CONATEL.

Finalmente, solicitamos aclarar si las referencias al “SNPP” y al “sector educativo” serán corregidas mediante adenda.

Respuesta	**Fecha de Respuesta**	31-08-2026

Utilización de documentos de referencia: Confirmamos que el PBC de la Licitación ID N° 473102 del SNPP fue analizado y utilizado como marco de referencia para la estructuración de este llamado. Esta práctica obedece a que dicho documento contempla exigencias alineadas con buenas prácticas y estándares internacionales de ciberseguridad aplicables al sector público.

Dimensionamiento técnico: Confirmamos que los parámetros técnicos, requisitos de capacidad, perfiles profesionales y certificaciones solicitadas fueron revisados, analizados, validados y dimensionados de manera específica para la infraestructura y las necesidades de infraestructura tecnológica y ciberseguridad actuales de la CONATEL. Aprovechamos para aclarar que los requerimientos solicitados de procesar 5GB/día de logs, gestión de al menos 1.000 activos y la operación de un SOC 8x5 con monitoreo remoto 24x7 no son arbitrarios; representan la volumetría real de nuestra red, se ajustan a nuestras necesidades y constituyen medidas estándares de la industria para garantizar una detección, gestión y respuesta temprana a incidentes cibernéticos. Así también, los perfiles técnicos solicitados son totalmente acordes a las capacidades necesarias para ejecutar las labores requeridas en el pliego de bases y condiciones. En otras palabras, estas necesidades técnicas y perfiles técnicos son usualmente requeridos por infraestructuras tecnológicas.

Correcciones de forma (Adenda): Reconocemos que, producto de un error material de edición y revisión documental, permanecieron en el texto menciones ajenas a nuestra institución, tales como referencias a objetivos del SNPP y al "sector educativo". Confirmamos que dichas referencias de forma serán subsanadas y adecuadas estrictamente al contexto de la CONATEL mediante la emisión de una Adenda al presente llamado.

Consulta 2 - Capacidad Técnica - Lider de proyecto

Consulta	Fecha de Consulta	07-09-2026

Superposición de certificaciones, por una parte, dice "Certificación en Auditoría de Sistemas y/o Seguridad de la Información vigente" y por otra parte dice "Certificación en Seguridad de la Información y/o Continuidad de Negocio vigente".
Se entiende entonces con una sola certificación de seguridad de la información ya cumplís con el requisito propuesto en el pliego de bases y condiciones. ¿Estoy en lo correcto?

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que una misma certificación vigente en Seguridad de la Información podrá acreditar ambos requisitos, siempre que su alcance corresponda a lo exigido en los dos apartados.

Consulta 3 - Capacidad Técnica - Lider de proyecto (Certificación muy específica)

Consulta	Fecha de Consulta	07-09-2026

Las Reglas para los Pliegos de Bases y Condiciones (Artículo 45). La ley determina que las instituciones convocantes violan la libre participación si redactan pliegos con "dedicatoria". En este caso habla de "Diplomado en Gestión y Dirección de Proyectos". En este caso solicitamos cordialmente a la convocante, que libere lo del diplomado y deje "Certificación o Diplomado en Gestión de Proyectos o Dirección de Proyectos."

Respuesta	Fecha de Respuesta	14-09-2026

La exigencia del diplomado responde a las responsabilidades del Líder de Proyecto en la planificación, coordinación y seguimiento del servicio, incluyendo la gestión de plazos, recursos, riesgos y entregables. Se aclara que no se exige una denominación literal del programa ni una institución educativa determinada, sino que el contenido del diplomado comprenda formación en gestión y dirección de proyectos.

Consulta 4 - Capacidad Técnica - Implementación de Solución

Consulta	Fecha de Consulta	10-09-2026

Para este apartado: "Curso de seguridad de la información o curso de manejo de la información",
"Curso en respuesta a incidentes, gestión de incidentes o gestión de crisis cibernética"
"Al menos 3 talleres, cursos, entrenamientos, conferencias o congresos en Ciberseguridad y/o Seguridad de la Información y/o Hacking Ético".
Se solicita amablemente a la convocante considerar diplomados en ciberseguridad o certificación en auditoria ISO 27001, ya que prácticamente abarca lo mismo de lo que están solicitando.
En caso contrario se violaría el 1. Art. 4° — Principios rectores (los más directamente vulnerados)
Inciso d) Igualdad y Libre Competencia: todo oferente con solvencia técnica que cumpla los requisitos "tendrá la posibilidad de participar sin restricciones y en igualdad de oportunidades en los procedimientos de contratación pública". Un perfil hecho a medida de un candidato puntual restringe de hecho esa posibilidad, aunque formalmente esté "abierto".

Respuesta	Fecha de Respuesta	14-09-2026

Se acepta la solicitud. El PBC dicta el cumplimiento minimo de formación. Podrán ser considerados los diplomados en Ciberseguridad o las certificaciones en Auditoría ISO/IEC 27001, siempre que la documentación presentada permita acreditar conocimientos equivalentes a los cursos y actividades de formación requeridos para el perfil.

Consulta 5 - Capacidad Técnica - Implementación de Solución

Consulta	Fecha de Consulta	10-09-2026

Para este apartado "Curso MGCTI y/o SCRUM y/o PM4R y/o gestión de proyectos", también se considere la certificación internacional PMP. Ya que es refiere a la gestión de proyectos también.
En caso contrario violarían el Inciso e) Imparcialidad: los documentos de la contratación deben dictarse "en atención a criterios técnicos que permitan objetividad en el tratamiento a los sujetos del Sistema Nacional de Suministro Público". Combinar certificaciones exóticas, cursos específicos y años exactos de experiencia sin justificación técnica rompe la objetividad exigida.

Respuesta	Fecha de Respuesta	14-09-2026

Se acepta la solicitud. El PBC exige el cumplimiento de un nivel mínimo de formación. Una certificación internacional PMP podrá ser considerada, por guardar correspondencia directa con los conocimientos requeridos para el perfil.

Consulta 6 - Capacidad Técnica - Implementación de Solución

Consulta	Fecha de Consulta	10-09-2026

Sobre este apartado "Certificación en el área de ciberseguridad: FCA, FCF o CCNA Security". No se entiende que estan requiriendo acá o para que? Certificación en redes sobre seguridad?
Ya que por ejemplo: -La certificación FCA más común se refiere a Fortinet Certified Associate in Cybersecurity.
-La certificación Fortinet Training and Certification FCF (Fortinet Certified Fundamentals)
- La certificación CCNA Security fue retirada por Cisco y reemplazada por enfoques modernos como el examen general CCNA 200-301.
Con este apartado en el perfil, están direccionando EXCLUSIVAMENTE a dos fábricantes.
Violando así Normativa vulnerada lo siguiente:
Art. 4°, inc. d) Igualdad y Libre Competencia (Ley N° 7021/2022): se restringe la participación a profesionales certificados por dos marcas puntuales, sin habilitar certificaciones equivalentes de otros fabricantes o entidades neutrales (CompTIA, ISC², EC-Council, ISACA), pese a que el objeto de la contratación no requiere, según el propio pliego, productos de esos fabricantes.
Art. 4°, inc. e) Imparcialidad: la exigencia no responde a "criterios técnicos que permitan objetividad", sino a la elección arbitraria de credenciales de marca.
Art. 4°, inc. k) Razonabilidad: exigir una certificación discontinuada por el propio fabricante carece de razonabilidad técnica y cualitativa.
Art. 45, 4° párrafo (Ley N° 7021/2022): la convocante tiene la obligación de elaborar las bases "con la mayor amplitud... con el objeto de que concurra el mayor número de Oferentes", debiendo ser "suficientemente claras, objetivas e imparciales para evitar favorecer a algún participante".
Art. 45, 5° párrafo: prohíbe expresamente establecer "elementos que no resulten técnicamente indispensables en los pliegos de bases y condiciones si con ello se limitan las posibilidades de concurrencia a eventuales proveedores o contratistas" — estándar que este requisito no supera, al no derivarse de ninguna de las soluciones tecnológicas objeto del llamado.

Se solicita a la convocante, aceptar certificaciones o diplomados enfocados en seguridad en redes en general, si eso es lo que está buscando.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que las certificaciones FCA, FCF y CCNA Security fueron citadas como referencias del nivel mínimo requerido y no con carácter exclusivo. Se admitirán otras certificaciones vigentes y equivalentes en ciberseguridad o seguridad de redes. El requisito se mantiene conforme al PBC.

Consulta 7 - Capacidad Técnica — Perfiles y Certificaciones del Personal

Consulta	Fecha de Consulta	10-09-2026

SE SOLICITA SUPRIMIR O AMPLIAR LAS CERTIFICACIONES SOLICITADAS, admitiendo equivalencias en ambos casos, por los siguientes motivos:

CCNA Security es una certificación descontinuada por Cisco, actualmente reemplazada por el examen general CCNA 200-301.
FCA (Fortinet Certified Associate in Cybersecurity) y FCF (Fortinet Certified Fundamentals) son certificaciones puntuales y exclusivas del fabricante Fortinet.

Tal como está redactado, el apartado direcciona la exigencia a dos fabricantes específicos, sin admitir certificaciones equivalentes de entidades neutrales y reconocidas en seguridad de redes (CompTIA, ISC², EC-Council, ISACA, entre otras), pese a que el objeto de la contratación no exige, según el propio pliego, productos de esas marcas.

Esto podría vulnerar los principios de igualdad y libre competencia, imparcialidad y razonabilidad (Art. 4°, incs. d), e) y k) de la Ley N° 7021/2022), así como la obligación de elaborar las bases con la mayor amplitud posible para favorecer la concurrencia de oferentes y evitar exigencias no indispensables técnicamente (Art. 45, párrafos 4° y 5°).

En consecuencia, se solicita a la convocante:

Suprimir las certificaciones puntuales de marca (FCA, FCF y CCNA Security) y admitir certificaciones o diplomados equivalentes en seguridad de redes en general; o bien
En caso de mantener y ampliar el requisito, indicar expresamente cuáles son las certificaciones equivalentes aceptadas, o cuáles serán los criterios de validación para admitir certificaciones distintas a las mencionadas.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que la expresión "como FCA, FCF o CCNA Security" es enunciativa. Podrán presentarse certificaciones vigentes equivalentes en ciberseguridad o seguridad de redes, emitidas por fabricantes u organismos reconocidos, siempre que acrediten el nivel mínimo exigido. No se acepta su sustitución por diplomados

Consulta 8 - Capacidad Técnica — Evidencia de Operación del SOC

Consulta	Fecha de Consulta	10-09-2026

SE SOLICITA FUNDAMENTAR O AJUSTAR EL PLAZO DE "32 MESES" exigido para acreditar la operación del SOC, por los siguientes motivos:

El plazo de 32 meses no corresponde a una unidad de medición estándar en la práctica de mercado ni en pliegos comparables, donde habitualmente se exigen 24 o 36 meses (2 o 3 años).
Esta particularidad numérica genera la apariencia de un requisito diseñado en función del historial contractual específico de un proveedor determinado, lo que contraviene el principio de transparencia y no direccionamiento que debe regir la elaboración de especificaciones técnicas.

Esto podría vulnerar los principios de transparencia e imparcialidad (Art. 4°, incs. d) y e) de la Ley N° 7021/2022), así como el estándar de razonabilidad exigido para las condiciones del pliego (Art. 45, párrafos 4° y 5°).

En consecuencia, se solicita a la Convocante:

Fundamentar el criterio técnico u objetivo que justifica el número específico de "32" meses; o bien
Ajustar el plazo a un estándar de mercado razonable (24 o 36 meses) que no limite injustificadamente la pluralidad de oferentes.

Respuesta	Fecha de Respuesta	14-09-2026

No se acepta la modificación. El periodo de 32 meses fue establecido para verificar experiencia operativa reciente y reiterada en la prestación de servicios SOC, atendiendo a la rápida evolución de las amenazas y tecnologías de ciberseguridad. El requisito se mantiene.

Consulta 9 - Capacidad Técnica — Perfiles y Certificaciones del Personal

Consulta	Fecha de Consulta	10-09-2026

SE SOLICITA ELIMINAR O MODIFICAR LA EXIGENCIA DE ANTIGÜEDAD MÍNIMA DE 6 MESES EN IPS para todo el plantel propuesto, por los siguientes motivos:

Esta exigencia, aplicada de manera indiscriminada a todo el personal propuesto —incluyendo perfiles altamente especializados como el Líder de Proyecto y los Técnicos de Monitoreo SOC—, no guarda relación de proporcionalidad con el objeto contractual, ya que la idoneidad técnica de un profesional depende de su formación y experiencia acreditada, no de su antigüedad en la planilla de un empleador determinado.
El requisito puede operar como barrera de entrada para oferentes que, cumpliendo sobradamente la capacidad técnica exigida, tercericen, contraten o incorporen personal especializado específicamente para el proyecto.

Esto podría vulnerar los principios de libre competencia e igualdad (Art. 4°, Ley N° 7021/2022).

En consecuencia, se solicita a la Convocante:

Eliminar la exigencia de antigüedad mínima en IPS; o subsidiariamente
Permitir que el vínculo laboral se acredite hasta la fecha de inicio de la prestación del servicio, y no a la fecha de presentación de la oferta.

Respuesta	Fecha de Respuesta	14-09-2026

La antigüedad mínima requerida de inscripción en el Insituto de Previsión Social busca acreditar la vinculación previa, estabilidad y disponibilidad efectiva del plantel propuesto para un servicio continuo y sensible, evitando equipos conformados únicamente para la presentación de la oferta. El requisito se mantiene.

Consulta 10 - Capacidad Técnica — Observación sobre Oferentes en Consorcio

Consulta	Fecha de Consulta	10-09-2026

SE SOLICITA ACLARAR Y RECTIFICAR EL CRITERIO DE EVALUACIÓN DE CAPACIDAD TÉCNICA PARA CONSORCIOS, por los siguientes motivos:

La cláusula, que exige que "todos los integrantes del Consorcio deberán cumplir la capacidad técnica mínima requerida", contradice el principio de complementariedad propio de la figura del consorcio, en virtud del cual los integrantes suman y complementan capacidades técnicas, financieras y de personal para alcanzar en conjunto el mínimo exigido.
Exigir que cada consorciado cumpla, por sí solo, la totalidad de la capacidad técnica mínima anula la utilidad práctica y el objeto mismo de la figura asociativa, restringiendo injustificadamente la conformación de consorcios y, con ello, la libre concurrencia.

Esto podría vulnerar los principios de libre competencia e igualdad (Art. 4°, Ley N° 7021/2022), así como la obligación de elaborar bases con la mayor amplitud de concurrencia posible (Art. 45, párrafo 4°).

En consecuencia, se solicita a la Convocante aclarar y, en su caso, rectificar el pliego para que la capacidad técnica mínima se evalúe de forma conjunta y complementaria entre los integrantes del consorcio, conforme a la práctica habitual en la normativa de contrataciones públicas.

Respuesta	Fecha de Respuesta	14-09-2026

Por el carácter del servicio crítico y sensible, se requiere que cada integrante del consorcio cuente con la capacidad técnica mínima necesaria para asumir las obligaciones y responsabilidades derivadas del contrato. La complementariedad prevista para otros criterios no sustituye esta condición mínima

Consulta 11 - Capacidad Técnica — Perfiles y Certificaciones del Personal — Perfil "Líder de Proyecto"

Consulta	Fecha de Consulta	10-09-2026

SE SOLICITA JUSTIFICAR O REDUCIR LA ACUMULACIÓN DE CERTIFICACIONES EXIGIDAS AL LÍDER DE PROYECTO, por los siguientes motivos:

Se exige simultáneamente, en una única persona física: certificación en Gestión de Riesgos vigente, certificación en Auditoría de Sistemas y/o Seguridad de la Información vigente, certificación en Auditoría ISO/IEC 27001 (40 hs o más) vigente, certificación en Seguridad de la Información y/o Continuidad de Negocio vigente, y diplomado en Gestión y Dirección de Proyectos, además de 15 años de experiencia general y 5 años de experiencia específica.
Esta combinación acumulativa de cinco (5) certificaciones vigentes distintas podría no encontrarse disponible en el mercado más que en un número muy reducido de profesionales, afectando la pluralidad de oferentes sin una justificación técnica proporcional al objeto contractual.

Esto podría vulnerar los principios de razonabilidad y proporcionalidad (Art. 4°, inc. k), Ley N° 7021/2022).

En consecuencia, se solicita a la Convocante:

Justificar, en términos de proporcionalidad y necesidad respecto del objeto contractual, la exigencia acumulativa de las cinco certificaciones; y
Confirmar si se aceptarán: a) certificaciones internacionales equivalentes a las mencionadas (por nomenclatura distinta pero de igual alcance técnico); y b) combinaciones alternativas de certificaciones que acrediten competencias equivalentes, a fin de no limitar la concurrencia a una única marca o esquema de certificación.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que el PBC exige acreditar competencias diferenciadas en riesgos, auditoría, ISO/IEC 27001, seguridad o continuidad y gestión de proyectos. No se exige una marca ni un organismo emisor determinado. Una misma credencial podrá ser considerada para más de un requisito cuando su alcance lo demuestre claramente; cada competencia deberá quedar íntegramente acreditada.

Consulta 12 - Capacidad Técnica — Características mínimas del SOC

Consulta	Fecha de Consulta	10-09-2026

SE SOLICITA FUNDAMENTAR EL UMBRAL DE "1.000 ACTIVOS" exigido como capacidad mínima de gestión del SOC, por el siguiente motivo:

No surge del pliego una justificación objetiva de que dicho umbral guarde relación de proporcionalidad con el volumen real de endpoints/servidores del organismo a ser monitoreados bajo el presente contrato.

Esto podría vulnerar el principio de razonabilidad (Art. 4°, inc. k), Ley N° 7021/2022), en la medida en que el parámetro haya sido fijado muy por encima de la necesidad real, en desmedro de oferentes con capacidad instalada suficiente para el objeto contractual pero por debajo del umbral fijado.

En consecuencia, se solicita a la Convocante fundamentar objetivamente el criterio técnico utilizado para fijar el umbral de 1.000 activos en relación con el volumen real a monitorear.

Respuesta	Fecha de Respuesta	14-09-2026

El umbral de 1.000 activos acredita la capacidad operativa y de escalabilidad mínima del SOC, considerando crecimiento, concurrencia de eventos y continuidad del servicio. No representa la cantidad inicial exacta de activos de la institución. El umbral mide escalabilidad operativa del SOC y no necesariamente coincide con el inventario inicial.

Consulta 13 - Capacidad Técnica — "Perfiles y Certificaciones del Personal" — Perfil "Técnicos de Monitoreo SOC"

Consulta	Fecha de Consulta	10-09-2026

SE SOLICITA ACLARAR LA FORMA DE ACREDITACIÓN DE LA "CERTIFICACIÓN AVANZADA SOLUCIÓN OFERTADA", por el siguiente motivo.: al no estar aún definida la solución tecnológica a ofertar —que es de libre elección del oferente—, no resulta claro cómo se acreditará este requisito en la etapa de oferta.

Esto podría vulnerar el principio de libre competencia (Art. 4°, Ley N° 7021/2022), en la medida en que el requisito favorezca —de manera encubierta— una marca o fabricante específico si no se aclara adecuadamente.

En consecuencia, se solicita a la Convocante aclarar y confirmar si se aceptará que dicha certificación se presente sobre la herramienta/plataforma que cada oferente efectivamente proponga en su oferta, evitando así el direccionamiento encubierto hacia un fabricante determinado.

Respuesta	Fecha de Respuesta	14-09-2026

Sí. La certificación avanzada deberá corresponder a la herramienta o plataforma que cada oferente proponga. No se exige una marca predeterminada; se evaluará la certificación aplicable a la solución efectivamente ofertada.

Consulta 14 - Especificaciones Técnicas — Ítem 1

Consulta	Fecha de Consulta	10-09-2026

Ítem 1: Herramienta para Monitoreo y Remediación de Vulnerabilidades (500 dispositivos)
SE SOLICITA FUNDAMENTAR O REDUCIR EL UMBRAL DE "MÁS DE 11.000 APLICACIONES DE TERCEROS", por los siguientes motivos:

La cifra de "más de 11.000 aplicaciones de terceros" para administración de parches en Windows, Linux y Mac coincide con la cobertura publicitada específicamente por el fabricante Vicarius, en su producto vRx, y supera ampliamente la de otras soluciones reconocidas del mercado (Qualys VMDR ~300+, ManageEngine ~1.100+, Automox ~580, ConnectWise ~7.000+, NinjaOne ~6.000+).
Ninguna de estas alternativas —todas idóneas y de reconocida trayectoria— alcanzaría el umbral tal como está redactado, lo que genera la apariencia de una especificación técnica direccionada a un único fabricante.

Esto podría vulnerar los principios de igualdad y libre competencia e imparcialidad (Art. 4°, incs. d) y e) de la Ley N° 7021/2022), así como la prohibición de incluir en los pliegos elementos no técnicamente indispensables que limiten la concurrencia de oferentes (Art. 45, párrafo 5°).

En consecuencia, se solicita a la Convocante:

Confirmar si el requisito fue tomado de la ficha técnica/comercial de Vicarius vRx;
Fundamentar objetivamente, en función del inventario real de software de la institución (a proteger en 500 dispositivos), por qué se requiere específicamente ese umbral y no uno inferior; y
Reducir el umbral exigido a un número proporcional a la necesidad real (por ejemplo, 500 a 1.000 aplicaciones de terceros), de forma que no quede excluida, por una cifra propia de un único fabricante, la generalidad de soluciones idóneas del mercado.

Respuesta	Fecha de Respuesta	14-09-2026

La cobertura exigida constituye una capacidad mínima de cobertura y escalabilidad para entornos heterogéneos y no identifica una marca determinada. Se admitirán soluciones de cualquier fabricante que acrediten el cumplimiento del umbral exigido.

Consulta 15 - Especificaciones Técnicas — Ítem 1

Consulta	Fecha de Consulta	10-09-2026

Ítem 1: Herramienta para Monitoreo y Remediación de Vulnerabilidades (500 dispositivos) (pág. 40/93)

SE SOLICITA ACLARAR LA NEUTRALIDAD TECNOLÓGICA DEL REQUISITO "PROTECCIÓN SIN PARCHES", por los siguientes motivos:

Las cláusulas "la plataforma debe ofrecer mecanismos de protección para vulnerabilidades sin parches disponibles, aplicaciones heredadas o sistemas con ventanas de mantenimiento restringidas" y "...una única consola unificada para descubrimiento, priorización de riesgos, aplicación de parches, protección sin parches y ejecución de scripts..." utilizan la expresión "protección sin parches", que corresponde a la traducción literal de "Patchless Protection™", denominación de la función vShield del producto Vicarius vRx, del fabricante Vicarius.
La inclusión textual de esta función, con esa denominación específica, como requisito "Exigido" (obligatorio), sugiere que el pliego fue redactado tomando como base la ficha técnica de dicho fabricante en particular.

Esto podría vulnerar los principios de igualdad y libre competencia e imparcialidad (Art. 4°, incs. d) y e) de la Ley N° 7021/2022).

En consecuencia, se solicita a la Convocante:

Confirmar si el requisito fue tomado de la ficha técnica/comercial de Vicarius vRx;
Confirmar que el requisito es tecnológicamente neutro y que se aceptarán mecanismos funcionalmente equivalentes de mitigación de vulnerabilidades sin parche disponible, cualquiera sea su denominación comercial o técnica (virtual patching, parcheo virtual mediante IPS, controles compensatorios basados en EDR/exploit prevention, shielding en memoria, u otros de eficacia equivalente); y
Aclarar que no se exigirá que dicha función se denomine o esté empaquetada exactamente como "Patchless Protection", ni que replique la arquitectura de módulos de Vicarius vRx.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que "protección sin parches" describe una capacidad funcional y no una denominación comercial. Se admitirán mecanismos equivalentes de mitigación de vulnerabilidades sin parche disponibles, cualquiera sea su nombre o arquitectura, siempre que cumplan la finalidad y eficacia exigidas

Consulta 16 - Especificaciones Técnicas — Ítem 1

Consulta	Fecha de Consulta	10-09-2026

Suministros Requeridos - Especificaciones Técnicas — Ítem 1: Herramienta para Monitoreo y Remediación de Vulnerabilidades (500 dispositivos)

SE SOLICITA CONFIRMAR LA NEUTRALIDAD DE LA ESTRUCTURA DE "CONSOLA ÚNICA" EXIGIDA, por los siguientes motivos:

La cláusula "la plataforma debe ofrecer una única consola unificada para descubrimiento, priorización de riesgos, aplicación de parches, protección sin parches y ejecución de scripts, sin la necesidad de múltiples módulos o consolas adicionales" establece una secuencia de cinco funciones exactas —descubrimiento, priorización, parcheo, protección sin parche y scripts— que reproduce, en el mismo orden, la arquitectura publicada de los cinco módulos de Vicarius vRx: vRadar (descubrimiento) → vScore (priorización) → vPatch (parcheo) → vShield (protección sin parche) → vScript (scripts).
Este patrón de correspondencia exacta, tanto en el número de funciones como en su secuencia, resulta poco probable que se dé por azar en una redacción técnica genérica, lo que sugiere que la especificación fue elaborada tomando como plantilla la arquitectura modular de ese producto puntual.

Esto podría vulnerar los principios de igualdad y libre competencia e imparcialidad (Art. 4°, incs. d) y e) de la Ley N° 7021/2022).

En consecuencia, se solicita a la Convocante confirmar expresamente que:

La especificación no fue redactada tomando como plantilla la arquitectura de módulos de Vicarius vRx;
El requisito se refiere únicamente a que la solución ofrezca dichas capacidades de forma integrada (sin exigir múltiples licencias o consolas separadas), y no a que replique la nomenclatura o el diseño modular de ese producto puntual; y
Se aceptarán arquitecturas alternativas de igual o mayor integración funcional propuestas por otros fabricantes, aun cuando organicen dichas capacidades de manera distinta.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que el requisito busca una gestión integrada desde una única consola, sin exigir nomenclatura ni arquitectura modular específica. Se admitirán arquitecturas alternativas que reúnan las capacidades exigidas en una sola consola y sin licencias o consolas adicionales para su operación.

Consulta 17 - Especificaciones Técnicas — Ítem 1

Consulta	Fecha de Consulta	10-09-2026

Ítem 1: Herramienta para Monitoreo y Remediación de Vulnerabilidades (500 dispositivos)

SE SOLICITA FUNDAMENTAR EL UMBRAL DE "160.000 VULNERABILIDADES HEREDADAS SEGÚN EL NIST", por los siguientes motivos:

La cláusula "debe admitir al menos el número de vulnerabilidades heredadas igual o superior a 160.000 que se presentan en el NIST" fija una cifra puntual que coincide con valores de cobertura histórica de vulnerabilidades utilizados en material comercial del fabricante Vicarius.
Se trata de un dato dinámico —el total de CVEs publicados en el NVD (National Vulnerability Database) varía constantemente según la fecha de consulta—, por lo que fijarlo como umbral fijo sin indicar metodología ni fecha de corte genera la apariencia de una cifra extraída de la ficha comercial de un fabricante determinado, y no de un criterio técnico objetivo y verificable.

Esto podría vulnerar los principios de igualdad y libre competencia e imparcialidad (Art. 4°, incs. d) y e) de la Ley N° 7021/2022).

En consecuencia, se solicita a la Convocante:

Confirmar si el número "160.000" fue tomado de la ficha técnica/comercial de Vicarius vRx;
Precisar la metodología y fuente objetiva utilizada para fijarlo, indicando si corresponde al total histórico de CVEs publicados en el NVD a una fecha determinada, y en tal caso, cuál es dicha fecha de corte; y
Fundamentar por qué dicho número —que varía constantemente y depende de la fecha de consulta— es un criterio técnico objetivo y no una cifra extraída de la ficha comercial de un fabricante determinado, capaz de excluir soluciones igualmente robustas que midan o reporten su cobertura de otra manera.

Respuesta	Fecha de Respuesta	14-09-2026

No se acepta la modificación. La cifra constituye un umbral mínimo de cobertura histórica de vulnerabilidades y no una referencia a un fabricante. El oferente deberá acreditar, mediante documentación técnica verificable, una base igual o superior al mínimo establecido.

Consulta 18 - EETT - Item N° 01 - Librería de "más de 1000 scripts públicos de múltiples fuentes"

Consulta	Fecha de Consulta	10-09-2026

SE SOLICITA FUNDAMENTAR O FLEXIBILIZAR EL REQUISITO DE "MÁS DE 1.000 SCRIPTS PÚBLICOS DE MÚLTIPLES FUENTES", por los siguientes motivos:

Las cláusulas "librería de scripts públicos con más de 1000 scripts" y "librería de scripts públicos de múltiples fuentes" coinciden con las características de la biblioteca de scripts de la comunidad "vSociety" de Vicarius vRx.
Fijar un número mínimo exacto de scripts como criterio de idoneidad técnica, sin admitir mecanismos funcionalmente equivalentes, puede direccionar el requisito hacia un único proveedor con una biblioteca de ese volumen específico.

Esto podría vulnerar los principios de igualdad y libre competencia e imparcialidad (Art. 4°, incs. d) y e) de la Ley N° 7021/2022).

En consecuencia, se solicita a la Convocante:

Confirmar si el requisito fue tomado de la ficha técnica/comercial de Vicarius vRx;
Fundamentar la exigencia de un número mínimo de 1.000 scripts públicos como criterio de idoneidad técnica; y
Confirmar si se aceptarán soluciones con bibliotecas de menor tamaño numérico pero de eficacia equivalente (por ejemplo, generación asistida de scripts mediante IA, scripts propios del fabricante con soporte y validación garantizados, o integración con bibliotecas de terceros), a fin de no limitar la concurrencia a un único proveedor con una biblioteca de ese volumen específico.

Respuesta	Fecha de Respuesta	14-09-2026

El mínimo requerido busca asegurar disponibilidad inmediata, variedad y madurez de automatizaciones para remediación y respuesta. Se admitirán bibliotecas de cualquier origen o fabricante que acrediten al menos la cantidad y condiciones previstas en el PBC.

Consulta 19 - Solicitud de pronunciamiento expreso sobre direccionamiento hacia Vicarius vRx

Consulta	Fecha de Consulta	10-09-2026

SE SOLICITA PRONUNCIAMIENTO EXPRESO SOBRE EL POSIBLE DIRECCIONAMIENTO HACIA VICARIUS vRx, por los siguientes motivos:

Las consultas anteriormente formuladas respecto de este mismo Ítem 1, tomadas en conjunto, señalan coincidencias que reproducen, con alto grado de precisión, cifras y la arquitectura de cinco módulos propios del producto Vicarius vRx del fabricante Vicarius: el umbral de más de 11.000 aplicaciones de terceros, la función "protección sin parches" (traducción de Patchless Protection™), la secuencia exacta de cinco funciones en consola única (que replica el orden de los módulos vRadar → vScore → vPatch → vShield → vScript), el umbral de 160.000 vulnerabilidades NIST, y la librería de más de 1.000 scripts públicos (coincidente con la comunidad "vSociety").
La acumulación de estas coincidencias, cada una individualmente observada, configura en conjunto un patrón que excede la probabilidad de coincidencia azarosa y amerita un pronunciamiento expreso y no genérico por parte de la Convocante.

Esto podría vulnerar los principios de igualdad y libre competencia e imparcialidad (Art. 4°, incs. d) y e) de la Ley N° 7021/2022), así como la obligación de elaborar las bases con la mayor amplitud posible para favorecer la concurrencia de oferentes (Art. 45, párrafo 4°).

En consecuencia, se solicita formalmente a la Convocante que se pronuncie de manera expresa sobre lo siguiente:

Confirmar o negar si las especificaciones técnicas del Ítem 1 fueron elaboradas tomando como referencia la ficha técnica o el material comercial de Vicarius vRx;
En caso afirmativo, o si no puede acreditar una fuente técnica objetiva distinta para cada uno de los parámetros observados (11.000 aplicaciones, protección sin parches/Patchless Protection, las cinco funciones en consola única, 160.000 vulnerabilidades NIST, 1.000+ scripts), incorporar en el pliego la cláusula de equivalencia habitual en la contratación pública ("o equivalente técnico"), permitiendo que cualquier oferente demuestre, mediante prueba de concepto, ficha técnica comparativa o certificación independiente, que su solución cumple la finalidad funcional perseguida (gestión de vulnerabilidades, priorización de riesgos y remediación integradas), sin necesidad de replicar cifras ni terminología propias de Vicarius; y
De no aceptarse lo anterior, se deja planteada expresamente la reserva del derecho de impugnar/protestar el pliego por direccionamiento hacia un fabricante determinado y restricción indebida a la libre competencia, conforme al Art. 4° de la Ley N° 7021/2022.

Respuesta	Fecha de Respuesta	14-09-2026

La Convocante aclara que no exige la marca Vicarius vRx ni una arquitectura o nomenclatura comercial determinada. Las especificaciones definen capacidades mínimas vinculadas con la necesidad institucional. Podrá ofertarse cualquier solución que demuestre el cumplimiento integral de las funcionalidades y umbrales establecidos. Existen diversas otras soluciones en el mercado, con similares caracteristicas

Consulta 20 - Sistema de adjudicación total

Consulta	Fecha de Consulta	10-09-2026

Considerando que el llamado reúne cinco prestaciones técnica y comercialmente diferenciables —gestión de vulnerabilidades, protección EDR/XDR, gestión de eventos/SIEM, diseño y operación asistida de SOC y diseño e implementación de SGSI—, solicitamos a la Convocante justificar técnica, operativa y económicamente por qué se estableció la adjudicación por la TOTALIDAD y no por ítems o lotes independientes. La agrupación obliga a que un único oferente reúna simultáneamente relaciones comerciales con fabricantes distintos, capacidades de SOC, consultoría SGSI y perfiles altamente específicos, reduciendo de forma sustancial el universo de competidores. Por tanto se solicita a la Convocante modificar el sistema de adjudicación a la modalidad: POR ÍTEM o, subsidiariamente, por LOTES funcionales, a fin de preservar la igualdad y libre competencia.

Respuesta	Fecha de Respuesta	14-09-2026

La adjudicación por la totalidad responde a la necesidad de integración, interoperabilidad, responsabilidad única, soporte coordinado y cumplimiento uniforme de niveles de servicio entre las herramientas, el SOC y el SGSI. La división por ítems incrementaría los riesgos de incompatibilidad y fragmentación de responsabilidades. No se acepta la modificación.

Consulta 21 - Estudio de mercado y competencia efectiva

Consulta	Fecha de Consulta	10-09-2026

En atención a que la Ley N° 7021/22 exige que el estudio de mercado permita identificar proveedores y determinar si existe competencia, solicitamos informar cuántas marcas y cuántos oferentes locales fueron identificados por la Convocante como capaces de cumplir, en forma simultánea y literal, la totalidad de las EETT de los Ítems 1, 2 y 3 y, además, los requisitos de SOC y SGSI. Solicitamos individualizar, al menos por cantidad, las soluciones técnicamente equivalentes verificadas durante el estudio de mercado.

Respuesta	Fecha de Respuesta	14-09-2026

El estudio de mercado consideró proveedores, cotizaciones y antecedentes disponibles para verificar la existencia de oferta y estimar el precio referencial, en cumplimimento con la Ley N° 7021/22. El procedimiento no establece una lista cerrada de marcas u oferentes; podrá participar cualquier interesado cuya solución cumpla integralmente el PBC.

Consulta 22 - Metodología de precios referenciales

Consulta	Fecha de Consulta	10-09-2026

El dictamen de precios referenciales evidencia solicitudes de cotización a LEGACY ROOTS, TECCOM y SISTECO, con respuestas documentadas de una cantidad limitada de empresas, complementadas con adjudicaciones anteriores de objetos no necesariamente idénticos. Solicitamos justificar cómo se verificó que la muestra utilizada refleja competencia suficiente y precios comparables para un llamado que integra cinco componentes heterogéneos. Asimismo, solicitamos aclarar por qué no se realizó una estimación independiente por ítem con mayor pluralidad de fuentes de mercado.

Respuesta	Fecha de Respuesta	14-09-2026

La estimación no solo considera a tres cotizaciones referenciales de empresas sino tambien antecedentes de contrataciones comparables adjudicadas, conforme a la información disponible durante el estudio de mercado, en cumplimiento con la Ley N° 7021/22. La valoración se realizó sobre la solución integral requerida, en concordancia con el sistema de adjudicación por la totalidad

Consulta 23 - Experiencia específica del 50% exclusivamente en SOC

Consulta	Fecha de Consulta	10-09-2026

El PBC exige demostrar experiencia en servicios de diseño, implementación y operación de SOC por un monto mínimo equivalente al 50% del monto total ofertado. Considerando que una parte sustancial del llamado corresponde a licencias y herramientas de ciberseguridad de los Ítems 1, 2 y 3, y otra parte a SGSI, solicitamos justificar por qué la experiencia requerida se concentra exclusivamente en SOC y se calcula sobre el monto TOTAL ofertado. ¿Se aceptará acreditar el 50% mediante experiencia acumulada en ciberseguridad, SIEM, EDR/XDR, gestión de vulnerabilidades, SOC/MDR/MSSP, seguridad de la información, SGSI o servicios equivalentes, en proporción a los ítems ofertados?

Respuesta	Fecha de Respuesta	14-09-2026

El diseño, implementación y operación del SOC constituye el componente central e integrador del servicio, dentro del cual convergen las herramientas y actividades requeridas. El porcentaje puede acreditarse mediante la suma de contratos o facturaciones de los periodos establecidos. No se acepta la modificación.

Consulta 24 - Periodo limitado a 2023-2025

Consulta	Fecha de Consulta	10-09-2026

Solicitamos justificar la restricción de la experiencia a los ejercicios 2023, 2024 y 2025, excluyendo contratos ejecutados con anterioridad que demuestran capacidad técnica plenamente vigente. ¿Se ampliará el período de acreditación a los últimos cinco años o, como mínimo, hasta el último mes anterior a la apertura, de forma acumulativa?

Respuesta	Fecha de Respuesta	14-09-2026

Negativo. Los ejercicios 2023, 2024 y 2025 fueron definidos para acreditar experiencia reciente mediante periodos cerrados, completos y comparables. La antigüedad general de la empresa se evalúa separadamente.

Consulta 25 - SOC activo en Paraguay al momento de ofertar

Consulta	Fecha de Consulta	10-09-2026

El PBC exige que el oferente cuente, antes de la presentación de la oferta, con un SOC activo y operativo en territorio paraguayo. Solicitamos indicar la razón objetiva por la cual dicha infraestructura debe encontrarse ya operativa antes de la adjudicación, en vez de admitirse la capacidad de implementación y disponibilidad comprometida para el inicio contractual. Este requisito transforma una condición de ejecución en una barrera de acceso previa. ¿Se aceptará acreditar capacidad mediante SOC propio, SOC de empresa vinculada, partner, fabricante o MSSP, acompañado de compromiso contractual de disponibilidad?

Respuesta	Fecha de Respuesta	14-09-2026

No se aceptará.. El requisito busca verificar capacidad instalada, disponibilidad inmediata, continuidad operativa 24x7 y atención local desde la presentación de la oferta. Un compromiso de implementación futura no acredita la existencia ni la operación efectiva del SOC requerido

Consulta 26 - Consorcios

Consulta	Fecha de Consulta	10-09-2026
El PBC permite, para determinados requisitos financieros y de experiencia, una distribución 60%/40% entre líder y demás miembros, pero exige que todos los integrantes cumplan íntegramente la capacidad técnica. Solicitamos justificar esta diferencia de tratamiento y aclarar por qué no se admite la complementariedad técnica entre consorciados. Solicitamos aplicar una regla combinada y proporcional también a la capacidad técnica.		

Respuesta	Fecha de Respuesta	14-09-2026
Remitirse a la respuesta de consulta Nro.: 10.		

Consulta 27 - Líder de proyecto: 15 años de experiencia

Consulta	Fecha de Consulta	10-09-2026
Solicitamos justificar mediante criterio técnico verificable la exigencia de quince años de experiencia general en seguridad de la información para el líder de proyecto. ¿Qué función del alcance no podría ser ejecutada por un profesional con, por ejemplo, 8 o 10 años de experiencia y certificaciones vigentes? Solicitamos reducir el requisito a un período razonable y proporcional al alcance contractual.		

Respuesta	Fecha de Respuesta	14-09-2026
El Líder deberá integrar seguridad, riesgos, auditoría, SGSI, continuidad, coordinación institucional y toma de decisiones sobre un servicio crítico. Los quince años responden al nivel de responsabilidad y experiencia sénior requerido para conducir integralmente el proyecto.		

Consulta 28 - Curso de Auditoría ISO 27001 de 40 horas

Consulta	Fecha de Consulta	10-09-2026
Solicitamos justificar por qué se fija específicamente una duración mínima de 40 horas para la certificación/curso de Auditoría ISO/IEC 27001. La competencia técnica se acredita normalmente por certificaciones y esquemas de evaluación del organismo emisor, no por una cantidad rígida de horas. ¿Se aceptarán certificaciones de auditor líder, auditor interno o implementador ISO/IEC 27001 reconocidas, independientemente de la duración nominal del curso?		

Respuesta	Fecha de Respuesta	14-09-2026
La carga mínima de 40 horas fue establecida para asegurar profundidad suficiente en los contenidos de auditoría ISO/IEC 27001. Se admitirán certificaciones de auditor reconocidas siempre que permitan acreditar la carga horaria mínima exigida.		

Consulta 29 - Subcontratación

Consulta	Fecha de Consulta	10-09-2026
El apartado de subcontratación figura como ‘No Aplica’, aunque el objeto incluye consultoría, pentesting, operación SOC, soporte especializado, capacitación y herramientas de varios fabricantes. Solicitamos justificar la prohibición práctica de subcontratar componentes especializados y permitir subcontratación parcial controlada, especialmente para servicios profesionales especializados y soporte de fabricante, manteniendo el adjudicatario la responsabilidad integral.		

Respuesta	Fecha de Respuesta	14-09-2026
: La restricción responde a la necesidad de responsabilidad directa, control del personal, confidencialidad y trazabilidad en la ejecución de prestaciones críticas. El soporte ordinario del fabricante no se considerará subcontratación cuando no implique delegar obligaciones esenciales del adjudicatario.		

Consulta 30 - Ítem 2 - especificaciones con terminología propietaria

Consulta	Fecha de Consulta	10-09-2026

El Ítem 2 incorpora terminología y funcionalidades altamente específicas, entre ellas XEDR, Endpoint Risk Management, Human Risks Analytics, PowerShell Defense, Exploit Defense, reducción dinámica de superficie de ataque, agrupación inteligente de usuarios y hardening personalizado. Solicitamos informar cuántos fabricantes distintos cumplen literalmente la totalidad de estas características y confirmar que se aceptarán mecanismos equivalentes que logren el mismo objetivo de seguridad aunque utilicen denominaciones técnicas o arquitecturas diferentes; Favor especificar las soluciones aceptadas o los requisitos para su aceptación.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que las denominaciones utilizadas describen capacidades funcionales y no marcas determinadas. Se admitirán mecanismos técnicamente equivalentes, cualquiera sea su nomenclatura o arquitectura, siempre que la solución demuestre el cumplimiento integral de los objetivos y funcionalidades exigidos.

Consulta 31 - Ítem 2 - Gartner + Forrester + MITRE

Consulta	Fecha de Consulta	10-09-2026

El fabricante del Ítem 2 debe encontrarse posicionado simultáneamente en análisis de Gartner y Forrester y demostrar resultados públicos en MITRE ATT&CK Evaluations. Solicitamos justificar por qué se exige acumulativamente la presencia en organizaciones privadas de análisis de mercado como condición técnica, cuando existen fabricantes con capacidad demostrable que pueden no participar por decisión comercial en alguno de esos estudios. ¿Se eliminará esta exigencia o se aceptarán evaluaciones independientes equivalentes?

Respuesta	Fecha de Respuesta	14-09-2026

Los requisitos aportan validaciones complementarias sobre presencia de mercado, capacidad tecnológica y desempeño técnico independiente. No se exige una posición específica ni una marca determinada, sino evidencia acumulativa de madurez y eficacia del fabricante.

Consulta 32 - Ítem 2 - SOC 2 Type 2 + ISO 27001 + ISO 9001 del fabricante

Consulta	Fecha de Consulta	10-09-2026

Solicitamos justificar la exigencia acumulativa de SOC 2 Type 2, ISO 27001 e ISO 9001 al fabricante. ¿Qué riesgo específico del contrato no podría mitigarse mediante certificaciones de seguridad y calidad equivalentes? Solicitamos aceptar certificaciones equivalentes o demostrar únicamente controles de seguridad y calidad aplicables al producto ofertado.

Respuesta	Fecha de Respuesta	14-09-2026

No se acepta la solicitud. Las acreditaciones solicitadas cubren ámbitos distintos y complementarios: controles operativos auditados, gestión de seguridad de la información y gestión de calidad. Su exigencia conjunta reduce riesgos de seguridad, continuidad y calidad asociados a la solución ofertada

Consulta 33 - Ítem 2 - responsable directo del fabricante con visitas periódicas

Consulta	Fecha de Consulta	11-09-2026
Se exige que el oferente cuente con un responsable directo del fabricante que efectúe visitas periódicas. Solicitamos justificar por qué una condición comercial interna del fabricante se convierte en requisito de participación. ¿Se aceptará soporte remoto, ejecutivo de cuenta regional, distribuidor autorizado o canal oficial, siempre que se garantice escalamiento y soporte durante la vigencia del contrato?		

Respuesta	Fecha de Respuesta	14-09-2026
El soporte remoto, ejecutivo regional, distribuidor o canal oficial podrá complementar, pero no sustituir, el requisito establecido		

Consulta 34 - Ítem 3 - acumulación SIEM/SOAR/UEBA/forense/vulnerabilidades/IoT/air-gap

Consulta	Fecha de Consulta	11-09-2026
El Ítem 3 acumula funciones propias de SIEM, SOAR, UEBA, threat intelligence, vulnerabilidad, análisis forense, multi-cloud, SDN, contenedores, IoT, inventario y operación air-gapped. Solicitamos indicar cuántas plataformas únicas fueron identificadas que cumplan literalmente la totalidad de estas capacidades. ¿Se permitirá una solución compuesta e integrada o el uso de componentes complementarios del mismo fabricante o de terceros mediante API?		

Respuesta	Fecha de Respuesta	14-09-2026
Se aclara que el PBC no exige una marca determinada, sino el cumplimiento integral de las capacidades requeridas. Podrán utilizarse componentes integrados, siempre que conformen una solución unificada, incluyan todas las licencias necesarias y no generen limitaciones operativas ni costos adicionales para la Convocante.		

Consulta 35 - Ítem 3 - air-gapped y multi-cloud

Consulta	Fecha de Consulta	11-09-2026
Solicitamos justificar la exigencia simultánea de operación en entornos air-gapped y capacidades nativas multi-cloud AWS/Azure/GCP. ¿CONATEL posee ambos escenarios dentro del alcance real del proyecto? Solicitamos limitar las EETT al entorno efectivamente existente y a necesidades comprobadas, evitando funcionalidades hipotéticas que reduzcan la competencia.		

Respuesta	Fecha de Respuesta	14-09-2026
El oferente deberá ajustarse al PBC		

Consulta 36 - Ítems 1, 2 y 3 - carta y cadena de autorización hasta fabricante

Consulta	Fecha de Consulta	11-09-2026
Para los Ítems 1, 2 y 3 se exige autorización del representante o distribuidor y documentación de la cadena hasta el fabricante. Solicitamos permitir carta directa del fabricante, representante regional, distribuidor mayorista autorizado, canal oficial o evidencia verificable del programa de partners, sin imponer una cadena documental rígida que dependa de terceros ajenos al oferente. Asimismo, solicitamos que las cartas puedan ser subsanables cuando su autenticidad pueda verificarse directamente con el fabricante.		

Respuesta	Fecha de Respuesta	14-09-2026
La documentación deberá presentarse conforme al PBC; su eventual subsanación será evaluada según su carácter sustancial o formal y la normativa aplicable.		

Consulta 37 - Documentación técnica en idioma inglés

Consulta	Fecha de Consulta	11-09-2026

El PBC no habilita la presentación de catálogos, anexos técnicos o folletos en idioma distinto al castellano. Considerando que la documentación oficial de fabricantes internacionales de ciberseguridad se emite habitualmente en inglés y que exigir traducción pública de decenas de manuales técnicos incrementa costos y plazos sin mejorar la evaluación, solicitamos admitir documentación técnica oficial en inglés, acompañada de matriz de cumplimiento en castellano.

Respuesta	Fecha de Respuesta	14-09-2026

El oferente deberá ajustarse a las condiciones establecidas en el PBC.

Consulta 38 - Ítem 4 - SIEM sin costos adicionales ni renovaciones

Consulta	Fecha de Consulta	11-09-2026

El Ítem 4 exige implementar un SIEM que permita incorporar nuevos dispositivos sin costos adicionales de licenciamiento ni renovaciones posteriores al contrato, según capacidad del hardware de la Convocante. Solicitamos aclarar si esta condición implica una licencia perpetua e ilimitada y justificar su compatibilidad con el Ítem 3, que contempla una herramienta específica de gestión de eventos. ¿Se aceptarán modelos de licenciamiento por capacidad, EPS, almacenamiento o suscripción, siempre que los costos correspondientes al período contractual estén incluidos?

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que la condición no implica una licencia ilimitada, sino la posibilidad de incorporar dispositivos, dentro de la capacidad del hardware de la Convocante, sin costos adicionales de licenciamiento o renovación. Podrán proponerse distintos modelos comerciales únicamente cuando cumplan íntegramente esta condición.

Consulta 39 - Ítem 4 - métricas rígidas MTTD/MTTR/MTTC/FPR/MITRE

Consulta	Fecha de Consulta	11-09-2026

Solicitamos aclarar la metodología de medición, línea de base, severidades, exclusiones, dependencias y responsabilidades de CONATEL para los KPI MTTD, MTTR, MTTC, FPR, cobertura MITRE, deduplicación y escalamiento. Sin una metodología objetiva, los KPI pueden convertirse en obligaciones indeterminadas. Solicitamos establecer métricas medibles y atribuibles al proveedor, sujetas a disponibilidad de logs, integraciones, accesos y colaboración institucional.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que la línea de base, metodología de medición, severidades, exclusiones y dependencias de los KPI serán definidas durante la etapa de planificación, conforme al entorno relevado. Las métricas serán aplicadas sobre actividades atribuibles al proveedor y estarán sujetas a la disponibilidad de registros, accesos e integraciones bajo responsabilidad de la Convocante

Consulta 40 - Ítem 4 - cobertura MITRE

Consulta	Fecha de Consulta	11-09-2026

El PBC exige porcentajes de cobertura MITRE ATT&CK. Solicitamos definir exactamente la versión de MITRE ATT&CK, las tácticas/técnicas consideradas críticas, la metodología para calcular cobertura y si la medición se realizará sobre capacidades nativas, reglas configuradas o escenarios de prueba. En ausencia de una metodología objetiva, solicitamos eliminar el porcentaje rígido.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que la cobertura será evaluada sobre la matriz MITRE ATT&CK Enterprise vigente durante la implementación y las técnicas aplicables al entorno institucional. El proveedor deberá demostrarla mediante el mapeo de capacidades, reglas de detección configuradas y escenarios de validación. No se acepta eliminar el porcentaje exigido.

Consulta 41 - Ítem 5 - alcance SGSI y eventual certificación

Consulta	Fecha de Consulta	11-09-2026
El Ítem 5 contempla diseño e implementación de SGSI conforme a ISO/IEC 27001:2022, auditorías internas, capacitación, SIEM, inventario automatizado y procesos continuos. Solicitamos aclarar expresamente si el alcance incluye obtener certificación ISO/IEC 27001 para CONATEL o únicamente preparar e implementar el SGSI. Si no incluye certificación, solicitamos que los entregables y obligaciones se delimiten para evitar interpretaciones extensivas durante la ejecución.		

Respuesta	Fecha de Respuesta	14-09-2026
Se aclara que el alcance comprende el diseño, preparación e implementación del SGSI conforme a ISO/IEC 27001:2022, pero no incluye la obtención de la certificación institucional por un organismo externo. Los entregables se limitarán a las obligaciones expresamente previstas en el PBC		

Consulta 42 - Solapamiento entre Ítems 4 y 5

Consulta	Fecha de Consulta	11-09-2026
Se observan actividades repetidas entre los Ítems 4 y 5, incluyendo gestión de riesgos, políticas, inventario, SIEM, incidentes, capacitación, auditoría, continuidad y cumplimiento ISO 27001. Solicitamos identificar de manera precisa los entregables exclusivos de cada ítem, eliminar duplicidades y explicar cómo se evitará el doble cómputo económico y operativo de las mismas actividades.		

Respuesta	Fecha de Respuesta	14-09-2026
Las actividades relacionadas son complementarias y deberán ejecutarse conforme a los entregables de cada ítem.		

Consulta 43 - Plazos y secuencia de implementación

Consulta	Fecha de Consulta	11-09-2026
Solicitamos que la Convocante publique un cronograma consolidado que identifique hitos, dependencias y plazos de los cinco ítems, especialmente la relación entre despliegue de herramientas, operación SOC y SGSI. La ausencia de una secuencia inequívoca puede trasladar al proveedor riesgos de demoras atribuibles a accesos, infraestructura o aprobaciones de CONATEL.		

Respuesta	Fecha de Respuesta	14-09-2026
El cronograma consolidado forma parte de la planificación que deberá presentar el adjudicatario, respetando los plazos e hitos establecidos en el PBC.		

Consulta 44 - EETT y principio de equivalencia

Consulta	Fecha de Consulta	11-09-2026
El propio PBC establece que las especificaciones deben ser amplias, evitar referencias que limiten a un fabricante y admitir equivalencias sustanciales. Solicitamos confirmar expresamente que todas las características funcionales de los Ítems 1, 2 y 3 serán evaluadas por resultado y equivalencia técnica, y no por coincidencia literal con nomenclaturas comerciales, nombres de módulos o arquitectura particular de una marca.		

Respuesta	Fecha de Respuesta	14-09-2026
Se confirma. Las características funcionales serán evaluadas por su cumplimiento técnico y resultado, sin exigir coincidencia con nombres comerciales, módulos o arquitecturas particulares. Las soluciones equivalentes deberán cumplir integralmente las capacidades y valores mínimos establecidos en el PBC.		

Consulta 45 - Solicitud de adenda

Consulta	Fecha de Consulta	11-09-2026

En atención al conjunto de restricciones expuestas —adjudicación total, experiencia exclusiva SOC, SOC preexistente, 32 meses, 1.000 activos, IPS seis meses, requisitos acumulativos de personal, consorcios sin complementariedad, cartas de fabricante y especificaciones altamente particulares— solicitamos la emisión de una ADENDA integral que restablezca condiciones de competencia efectiva. En caso de mantenerse las exigencias, solicitamos que la Convocante exponga para cada una su justificación técnica objetiva y el estudio de mercado que demuestre la existencia de pluralidad real de oferentes capaces de cumplirlas.

Respuesta	Fecha de Respuesta	14-09-2026

Cada observación fue analizada y respondida conforme a su alcance. La Convocante mantiene los requisitos establecidos por considerarlos necesarios para asegurar la capacidad técnica, integración, continuidad y correcta ejecución del servicio

Consulta 46 - Ítem 2 - Nombre propio "Control Center" como requisito de la consola de administración

Consulta	Fecha de Consulta	11-09-2026

Se advierte que "Control Center" no es una descripción genérica de funcionalidad, sino el nombre propio y comercial de la consola de administración del producto GravityZone de Bitdefender. Ningún otro fabricante del mercado (CrowdStrike Falcon, Microsoft Defender, SentinelOne Singularity, Trend Micro Vision One, Palo Alto Cortex XDR, Kaspersky, ESET PROTECT, etc.) denomina así a su consola.
Se solicita a la Convocante eliminar la referencia al nombre propio "Control Center" y sustituirla por una descripción funcional neutra (por ejemplo, "consola de administración centralizada basada en la nube"), de modo que cualquier fabricante pueda ofertar su propia consola bajo su denominación comercial.

Respuesta	Fecha de Respuesta	14-09-2026

La expresión "Control Center" no pretende identificar ni exigir una solución o fabricante determinado. El requisito se refiere a una consola web de administración centralizada, alojada en la nube, que permita gestionar integralmente la solución de seguridad. Se admitirán consolas con cualquier denominación comercial, siempre que cumplan las funcionalidades y condiciones técnicas establecidas en el PBC.

Consulta 47 - Ítem 2 - Módulo "Human Risk Analytics" con lista de verificaciones específicas

Consulta	Fecha de Consulta	11-09-2026

Esta descripción reproduce, punto por punto, el módulo "Human Risk Analytics" de Bitdefender GravityZone, incluyendo el mismo conjunto específico de verificaciones.
Se solicita a la Convocante confirmar que se aceptarán módulos de análisis de riesgo humano/comportamiento de usuario de otros fabricantes que cubran de manera equivalente (aunque no idéntica en cada verificación puntual) el objetivo de identificar prácticas de riesgo de los usuarios, sin exigir la replicación exacta de cada uno de los ítems listados.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que la denominación "Human Risk Analytics" no constituye una exigencia de marca. Se aceptarán soluciones equivalentes que permitan identificar, evaluar y gestionar los riesgos asociados al comportamiento de los usuarios, siempre que acrediten el cumplimiento de las capacidades mínimas requeridas en el PBC

Consulta 48 - Ítem 2 - Término "XEDR" como tecnología exigida

Consulta	Fecha de Consulta	11-09-2026

El acrónimo "XEDR" no es un estándar de la industria (el término genérico y ampliamente reconocido es EDR o XDR); es una denominación propia utilizada específicamente en el material comercial de Bitdefender GravityZone Business Security Enterprise.
Se solicita a la Convocante aclarar que el requisito se refiere a la capacidad funcional de correlación de eventos extendida entre terminales (EDR/XDR), independientemente de cómo cada fabricante denomine internamente a dicha tecnología, para no excluir soluciones EDR/XDR equivalentes de otros proveedores por una diferencia puramente nominal.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que la expresión "XEDR" se utiliza en sentido funcional. Serán aceptadas soluciones EDR o XDR equivalentes, independientemente de su denominación comercial, siempre que cumplan las capacidades de detección, correlación, investigación y respuesta exigidas en el PBC.

Consulta 49 - Ítem 2 - "ERM" y exigencia de "al menos 300 indicadores de Hardening"

Consulta	Fecha de Consulta	11-09-2026

Se solicita a la Convocante: a) Fundamentar objetivamente por qué se exige ese número mínimo de indicadores y no un umbral menor, considerando que la eficacia de un módulo de hardening depende de la calidad y relevancia de los indicadores, no exclusivamente de su cantidad; y b) Confirmar que se aceptarán soluciones equivalentes con un número distinto de indicadores, siempre que se demuestre una cobertura funcional comparable (CIS Benchmarks, hardening de OS, aplicaciones, configuraciones de red, etc.).

Respuesta	Fecha de Respuesta	14-09-2026

El número de indicadores establecido representa la cobertura mínima requerida para asegurar una evaluación amplia de configuraciones y riesgos. Se admitirán diferentes metodologías de organización o contabilización, siempre que el oferente demuestre una cobertura equivalente y el cumplimiento del alcance mínimo exigido en el PBC.

Consulta 50 - Ítem 2 - Descripción del add-on "PHASR" de Bitdefender como requisito genérico

Consulta	Fecha de Consulta	11-09-2026

Este bloque completo de requisitos coincide, casi en su literalidad —incluyendo la cifra del 70%— con la nota de prensa oficial de Bitdefender sobre su tecnología GravityZone PHASR (Proactive Hardening and Attack Surface Reduction), lanzada como add-on de GravityZone XDR. Se trata de una tecnología relativamente nueva y, según el propio fabricante, "pionera" en el mercado, lo que sugiere que pocos o ningún otro competidor podría cumplir este bloque de requisitos en su totalidad.
Se solicita a la Convocante: a) Fundamentar por qué se exige específicamente esta tecnología (de adopción reciente y limitada en el mercado) como requisito obligatorio ("Si"), y no como una característica deseable adicional; y b) Precisar qué otras soluciones de mercado —además de Bitdefender GravityZone PHASR— cumplirían actualmente esta combinación específica de capacidades, a fin de acreditar que existe pluralidad real de oferentes.

Respuesta	Fecha de Respuesta	14-09-2026

: La Convocante no exige una tecnología, módulo o denominación comercial específica. Se aceptarán soluciones técnicamente equivalentes que permitan reducir proactivamente la superficie de ataque y acreditar objetivamente el nivel de efectividad requerido, sin limitarse a la tecnología mencionada por el consultante.

Consulta 51 - Ítem 2 - Consumo de recursos "mínimos (>~220MB)"

Consulta	Fecha de Consulta	11-09-2026
La redacción de esta cláusula es ambigua (el símbolo ">~220MB" podría leerse como "menor a aproximadamente 220MB" o resulta contradictorio con la idea de "recursos mínimos"). Se solicita: a) Aclarar el valor exacto y si se trata de un techo máximo o un valor de referencia; y b) Fundamentar la relación de proporcionalidad de esa cifra específica con el hardware real de los 500 dispositivos a proteger, para no excluir soluciones igualmente eficientes con un consumo distinto.		

Respuesta	Fecha de Respuesta	14-09-2026
Se aclara que el valor indicado corresponde al consumo máximo aproximado de memoria del agente durante su operación normal. La solución ofertada deberá demostrar un consumo eficiente y compatible con los equipos de la Convocante, sin afectar significativamente su desempeño		

Consulta 52 - Ítem 2 - Acumulación de certificaciones y reconocimientos de mercado exigidos al fabricante

Consulta	Fecha de Consulta	11-09-2026
a) Aclarar si se exige "cuadrante de liderazgo" (Leaders) de forma literal, lo cual excluiría a fabricantes reconocidos y técnicamente idóneos posicionados en otros cuadrantes (Visionaries, Challengers, Niche Players) de la misma matriz Gartner, sin que ello implique necesariamente una menor capacidad técnica para el objeto de esta contratación; y b) Justificar la proporcionalidad de exigir simultáneamente los cuatro criterios reputacionales (certificación de procesos, analistas de mercado, evaluación técnica independiente y laboratorio propio), en lugar de aceptar cualquiera de ellos como evidencia suficiente e independiente de idoneidad, en resguardo de la pluralidad de oferentes.		

Respuesta	Fecha de Respuesta	14-09-2026
Los antecedentes y reconocimientos requeridos buscan acreditar la madurez, calidad y confiabilidad de la solución. No se exige exclusivamente la categoría "Leader" ni una denominación particular, salvo disposición expresa del PBC. Se admitirán documentos equivalentes emitidos por entidades independientes y reconocidas que permitan acreditar objetivamente dichas condiciones.		

Consulta 53 - Ítem 3 - Redundancia funcional con el Ítem 2 (acciones de respuesta a nivel de endpoint)

Consulta	Fecha de Consulta	11-09-2026
Estas mismas capacidades (aislamiento de host, terminación de procesos, cuarentena, bloqueo de IP) ya están exigidas de manera nativa en el Ítem 2 (herramienta EDR/XDR) del presente proceso. Exigir que la herramienta de gestión de eventos (SIEM) del Ítem 3 realice también, de forma nativa, estas mismas acciones de respuesta a nivel de endpoint implica que el oferente deba disponer de dos soluciones distintas con capacidades EDR superpuestas, o bien de una única plataforma "todo en uno" (SIEM+SOAR+EDR nativamente integrados) que muy pocos fabricantes ofrecen bajo una sola licencia y consola. Se solicita a la Convocante: a) Aclarar si la ejecución de estas acciones de respuesta puede satisfacerse mediante integración/orquestación (vía API, webhook o conector SOAR) entre la herramienta del Ítem 3 y la herramienta EDR/XDR del Ítem 2, en lugar de exigir que el Ítem 3 las ejecute de forma nativa y autónoma; y b) Fundamentar, en caso de mantener la exigencia nativa, por qué es necesaria esta duplicación de capacidades entre dos ítems distintos del mismo proceso, en términos de economía y eficiencia (Art. 4°, Ley N° 7021/2022)		

Respuesta	Fecha de Respuesta	14-09-2026
Se aclara que las acciones de respuesta podrán ejecutarse mediante integración u orquestación entre las soluciones de los Ítems 2 y 3, utilizando API, conectores, webhook u otros mecanismos equivalentes. El oferente deberá incluir todos los componentes y licencias necesarios para garantizar su funcionamiento integral.		

Consulta 54 - Ítem 3 - Exigencia de gestión de vulnerabilidades dentro de la herramienta SIEM/SOAR

Consulta	Fecha de Consulta	11-09-2026

Esta capacidad de gestión de vulnerabilidades (escaneo continuo, priorización, correlación con exploits) corresponde típicamente a una categoría de producto independiente (VM/RBVM), distinta de SIEM/SOAR, y coincide además con el objeto específico ya licitado en el Ítem 1 de este mismo proceso ("Herramienta para Monitoreo y Remediación de Vulnerabilidades"). Se solicita a la Convocante:
a) Aclarar si esta funcionalidad puede satisfacerse mediante integración con la solución de gestión de vulnerabilidades adquirida en el Ítem 1, en lugar de exigir capacidad nativa de escaneo de vulnerabilidades dentro del Ítem 3; y b) Fundamentar la necesidad de exigir esta capacidad por triplicado entre ítems (Ítem 1: gestión de vulnerabilidades; Ítem 2: protección de endpoint con detección de CVE en protocolos; Ítem 3: automatización de gestión de vulnerabilidades), en resguardo del principio de economía y eficiencia.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que las capacidades de gestión de vulnerabilidades del Ítem 3 podrán satisfacerse mediante integración con la solución del Ítem 1, siempre que se aseguren el intercambio de información, la priorización, correlación y automatización requeridas, sin costos adicionales para la Convocante

Consulta 55 - Ítem 3 - Amplitud de categorías de producto exigidas como capacidad nativa única

Consulta	Fecha de Consulta	11-09-2026

Se solicita a la Convocante: a) Confirmar si el requisito admite una solución compuesta por un núcleo SIEM/SOAR con integraciones certificadas hacia módulos o soluciones complementarias (propias o de terceros) para cubrir capacidades especializadas (por ejemplo, forense digital, seguridad IoT/OT, seguridad de contenedores), o si exige que absolutamente todas las capacidades sean nativas de un único producto y una única consola; y b) En caso de exigir capacidad 100% nativa en un único producto, identificar al menos tres soluciones de mercado, de fabricantes distintos, que a la fecha cumplan la totalidad de las capacidades listadas de forma nativa, a fin de acreditar que existe pluralidad real de oferentes y que el requisito no es, en la práctica, alcanzable por un número extremadamente reducido de fabricantes.

Respuesta	Fecha de Respuesta	14-09-2026

Se aceptará una solución compuesta e integrada, conformada por un núcleo SIEM/SOAR y componentes propios o de terceros, siempre que cumpla integralmente las funcionalidades exigidas, opere de manera interoperable y contemple todas las licencias, conectores y servicios necesarios. No se exige que todas las capacidades pertenezcan a un único producto o fabricante

Consulta 56 - Ítem 3-Ausencia de parámetros de dimensionamiento (EPS, volumen de datos, retención, fuentes de log)

Consulta	Fecha de Consulta	11-09-2026

La falta de estos parámetros de dimensionamiento impide a los oferentes calcular un licenciamiento y una arquitectura de infraestructura ajustados a la necesidad real de la institución, lo cual puede derivar en ofertas no comparables entre sí (unas subdimensionadas y otras sobredimensionadas) y afecta la transparencia y economía del proceso. Se solicita a la Convocante precisar, como mínimo: a) El número estimado de eventos por segundo (EPS) o de GB de logs por día a procesar; b) El período mínimo de retención de datos exigido (en línea caliente y en archivo/cold storage); y c) La cantidad aproximada de fuentes de log/dispositivos a integrar (equivalente a los "500 dispositivos" mencionados en los Ítems 1 y 2, si aplica también a este ítem), a fin de que los oferentes puedan dimensionar y cotizar la solución de manera objetiva y comparable.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que el PBC establece como parámetros de dimensionamiento el monitoreo de aproximadamente 500 activos y el procesamiento aproximado de 5 GB de datos/logs por día, con capacidad para futuros incrementos. El periodo de retención deberá ser definido en el diseño de la arquitectura, conforme a las normativas aplicables y a la capacidad del hardware provisto por la Convocante. Favor considerar las especificaciones establecidas en el PBC.

Consulta 57 - Ítem 4 - Valor incoherente del KPI "MTTA" (Mean Time to Acknowledge)

Consulta	Fecha de Consulta	11-09-2026

El valor "< 4530 minutos" equivale a aproximadamente 75,5 horas (más de 3 días), cifra manifiestamente incongruente con los demás KPIs de la misma tabla: MTTD < 4 horas, MTTR < 4 horas (P1/Crítico) y MTTC < 4 horas (Crítico). Dado que, por definición, el reconocimiento de un incidente (Acknowledge) debe ocurrir antes de su respuesta (Respond) y contención (Contain), un MTTA de hasta 3 días resulta operativamente incompatible con un MTTR de 2 a 4 horas. Se solicita a la Convocante: a) Confirmar si el valor "4530" corresponde a un error de tipeo (por ejemplo, "45" o "30" minutos, o un rango "45-30" mal transcripto) y, en su caso, corregir el pliego mediante circular aclaratoria; y b) Publicar el valor correcto del KPI MTTA antes del vencimiento del plazo para la presentación de ofertas, de modo que los oferentes puedan dimensionar correctamente la dotación de personal y las herramientas de automatización necesarias para cumplirlo.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que la expresión "< 4530 minutos" contiene un error de tipeo, identificable por la naturaleza del indicador y su relación con los demás KPI. El requisito (<45 30) se interpreta: MTTA inferior a 30 minutos para incidentes críticos e inferior a 45 minutos para incidentes de alta complejidad. Esta aclaración no modifica el alcance ni las condiciones técnicas previstas en el PBC.

Consulta 58 - Ítem 4 - Metodología de medición y verificación de los KPIs de desempeño

Consulta	Fecha de Consulta	11-09-2026

El pliego no especifica la metodología de cálculo, la fuente de datos, la periodicidad de medición ni el mecanismo de auditoría/verificación de estos KPIs, ni las consecuencias contractuales (multas, penalidades, causal de resolución) en caso de incumplimiento sostenido. Se solicita a la Convocante precisar:
a) La metodología y periodicidad de cálculo de cada KPI (mensual, trimestral, acumulado); b) Quién audita o verifica el cumplimiento (la propia contratante, un tercero independiente, o autodeclaración del proveedor); y c) El régimen de consecuencias (multas u otras penalidades conforme al Art. correspondiente de la Ley N° 7021/2022 y su reglamentación) aplicable ante el incumplimiento reiterado de cada KPI, a fin de que los oferentes puedan valorar el riesgo contractual al momento de cotizar.

Respuesta	Fecha de Respuesta	14-09-2026

Los KPI serán medidos mensualmente utilizando los registros auditables del SIEM, del sistema de gestión de incidentes y de las herramientas integradas. La metodología, línea de base, exclusiones y responsabilidades serán documentadas en la etapa de planificación y aprobadas por la Convocante. Su incumplimiento será tratado conforme a las condiciones y penalidades establecidas en el PBC y el contrato.

Consulta 59 - Ítem 4 - Exigencia implícita de tecnología "XDR + IA" para el KPI de MTTD

Consulta	Fecha de Consulta	11-09-2026

La redacción condiciona el cumplimiento del objetivo más exigente (MTTD < 1 hora) al uso específico de tecnología "XDR + IA", lo que podría interpretarse como una orientación hacia un enfoque tecnológico particular en lugar de un objetivo de resultado neutro. Se solicita a la Convocante aclarar:
a) Si el objetivo exigible y evaluable a efectos contractuales es el de "< 4 horas" (aplicable independientemente de la tecnología utilizada), y el valor "< 1 hora con XDR + IA" es meramente indicativo/aspiracional; o b) Si, por el contrario, se exige contractualmente alcanzar el MTTD < 1 hora, en cuyo caso deberá aceptarse que dicho objetivo sea alcanzado mediante cualquier combinación tecnológica equivalente (no limitada a soluciones específicamente etiquetadas como "XDR" o basadas en "IA"), evaluando el resultado y no la tecnología empleada.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que el objetivo general de MTTD es inferior a cuatro horas para incidentes críticos o altos. El objetivo inferior a una hora será aplicable cuando se utilicen capacidades de correlación extendida y automatización. Se admitirán tecnologías equivalentes, independientemente de su denominación comercial, siempre que permitan alcanzar y acreditar dicho resultado.

Consulta 60 - Modelo de licenciamiento SIEM "sin costos adicionales"

Consulta	Fecha de Consulta	11-09-2026

La exigencia de que el SIEM permita incorporar dispositivos ilimitados "sin costos adicionales de licenciamiento ni renovaciones posteriores al contrato" coincide con el modelo comercial específico de soluciones SIEM de código abierto — en particular, Wazuh, que se publicita expresamente como una plataforma "sin costo de licencia" ("no license cost"), "sin cargo por agente" ("no per-agent fee") y "sin cobro por volumen de datos ingeridos" ("no ingestion-based pricing"), permitiendo escalar a un número ilimitado de agentes/dispositivos sin costo de licenciamiento. Esta característica es propia de muy pocas soluciones del mercado, dado que la generalidad de los SIEM comerciales reconocidos (Splunk, IBM QRadar, Microsoft Sentinel, LogRhythm, Exabeam, Securonix, entre otros) licencian por volumen de datos ingeridos (GB/día o EPS) o por dispositivo, con costos que se incrementan a medida que crece el entorno monitoreado.
La combinación de (i) la exigencia de licenciamiento gratuito e ilimitado y (ii) la referencia explícita a "opciones open source" en la misma sección del pliego constituye un indicio de que el requisito fue modelado sobre una solución de código abierto específica, lo cual —aunque no implique un costo de licencia para el Estado— restringe igualmente la libre competencia, al excluir en la práctica a la generalidad de los fabricantes de SIEM comerciales, que no pueden ofertar licenciamiento perpetuo ilimitado sin costo bajo su modelo de negocio habitual.
Se solicita a la Convocante:
a) Confirmar si el requisito fue elaborado tomando como referencia el modelo de licenciamiento de Wazuh u otra solución SIEM de código abierto en particular;
b) Aclarar si la gratuidad exigida aplica exclusivamente a la incorporación de nuevos dispositivos/endpoints dentro del volumen de datos ya contemplado (5 GB/día aproximados) y del hardware provisto, o si se extiende a cualquier incremento de volumen de datos, cantidad de fuentes o EPS, independientemente de la capacidad de hardware; y
c) Confirmar que se aceptarán ofertas con soluciones SIEM comerciales de licenciamiento por volumen/consumo, siempre que el oferente garantice contractualmente que el costo total del servicio no se incrementará durante los 24 meses de vigencia dentro de los límites de capacidad de hardware indicados, sin exigir que el modelo comercial subyacente sea necesariamente de tipo "gratuito" o "de código abierto".

Respuesta	Fecha de Respuesta	14-09-2026

La Convocante no exige Wazuh ni un modelo de licenciamiento de código abierto. Se aceptarán soluciones comerciales, open source o equivalentes, siempre que permitan incorporar nuevos dispositivos sin costos adicionales de licenciamiento o renovación, dentro del volumen previsto y de la capacidad del hardware provisto por la Convocante. El oferente deberá incluir en su precio todos los componentes y derechos de uso necesarios para cumplir esta condición.

Consulta 61 - Ítem 4 - Ambigüedad en el modelo de dotación de personal del SOC (8x5 on-site vs. 24x7 remoto)

Consulta	Fecha de Consulta	11-09-2026

La redacción es ambigua respecto de quién provee y quién supervisa al personal en cada franja horaria. Se solicita a la Convocante aclarar expresamente, mediante una matriz de dotación:
a) Si el personal que presta el servicio 8x5 en sitio es provisto por el oferente adjudicado o por la propia contratante (la frase "con personal de la institución" sugiere esto último, lo cual debe confirmarse); b) Cuántos analistas/técnicos, con qué perfil y dedicación (full-time/part-time), debe aportar el oferente para el esquema 8x5 en sitio y para el monitoreo remoto 24x7; y c) Si el "analista de la contratante" que supervisa el servicio 8x5 sustituye o complementa al personal técnico exigido en las especificaciones de personal técnico del proceso (Líder de Proyecto, Técnicos de Monitoreo SOC), a fin de evitar superposiciones o vacíos de responsabilidad entre el personal de la contratante y el del oferente.
Esta aclaración es indispensable para que los oferentes puedan dimensionar y cotizar correctamente la dotación de personal requerida durante los 24 meses del contrato.

Respuesta	Fecha de Respuesta	14-09-2026

Se aclara que la operación presencial 8x5 se realizará con personal de la institución, bajo supervisión de CONATEL. El adjudicado deberá prestar el monitoreo remoto 24x7 fuera del horario presencial y aportar, como mínimo, el líder del proyecto, el responsable de implementación y los dos técnicos de monitoreo SOC exigidos en el PBC. Estos perfiles complementan al personal institucional y no lo sustituyen.

Consulta 62 - Ítem 5 - Mención textual de "Wazuh" y "ELK" como contenido curricular obligatorio

Consulta	Fecha de Consulta	11-09-2026

Se solicita a la Convocante:
a) Confirmar si la mención de "ELK" y "Wazuh" en el temario exigido para los cursos especializados obedece a que estas son las herramientas SIEM que la institución ya tiene previsto implementar (en los Ítems 3 y/o 4 del presente proceso), o si se trata únicamente de ejemplos ilustrativos de herramientas de monitorización de eventos de seguridad;
b) En caso de tratarse de ejemplos ilustrativos, confirmar que se aceptarán cursos especializados que cubran el mismo objetivo de competencia (monitorización y detección proactiva de amenazas mediante sistemas de gestión de eventos de seguridad) utilizando otras herramientas de mercado igualmente reconocidas (por ejemplo, Splunk, IBM QRadar, Microsoft Sentinel, Graylog, LogRhythm), sin exigir que el proveedor de capacitación acredite específicamente laboratorios prácticos sobre ELK y Wazuh; y
c) En caso de que la mención sea vinculante y no ilustrativa, ello reforzaría la necesidad de que la Convocante se pronuncie de manera expresa sobre la Consulta N° 4 del Ítem 4, dado que ambas referencias (capacitación en este Ítem 5 y licenciamiento gratuito/ilimitado en el Ítem 4) apuntan de manera consistente hacia la misma solución de código abierto.

Respuesta	Fecha de Respuesta	14-09-2026

Las referencias a ELK y Wazuh claramente se utilizan como ejemplos. No constituyen exigencias de marca o producto. Se aceptarán cursos que utilicen otras herramientas reconocidas de gestión y monitorización de eventos, siempre que cumplan los contenidos, laboratorios y objetivos de aprendizaje establecidos en el PBC.

Consulta 63 - Ítem 5 - Redundancia de la exigencia de "sistema SIEM" entre los Ítems 3, 4 y 5

Consulta	Fecha de Consulta	11-09-2026

El presente proceso exige la implementación de un "sistema SIEM" (o equivalente) en tres ítems distintos: el Ítem 3 ("Herramienta para Gestión de Eventos"), el Ítem 4 ("Implementar un servicio SIEM" dentro del SOC) y ahora el Ítem 5. El pliego no aclara si se trata de:
(i) el mismo sistema SIEM, adquirido en el Ítem 3, operado en el Ítem 4 y utilizado como insumo de monitorización en el Ítem 5; o (ii) sistemas SIEM independientes por cada ítem, lo cual implicaría una triplicación de licenciamiento, infraestructura y esfuerzo de implementación para el mismo objetivo funcional.
Se solicita a la Convocante:
a) Confirmar si los Ítems 3, 4 y 5 se refieren a un único sistema SIEM compartido entre los tres ítems, o si se trata de sistemas independientes; y
b) En caso de tratarse del mismo sistema, aclarar cómo se coordinará la adjudicación entre estos ítems si son adjudicados a oferentes distintos (por ejemplo, si el oferente del Ítem 4 u 5 debe integrarse obligatoriamentecon el SIEM adquirido en el Ítem 3, o si cada oferente puede proponer su propia solución), en resguardo de la economía y eficiencia del proceso y de la claridad necesaria para que los oferentes coticen correctamente sus ofertas.

Respuesta	Fecha de Respuesta	14-09-2026

La consulta confunde funciones complementarias con tres adquisiciones. Además, el procedimiento tiene adjudicación por la totalidad. Corresponde al adjudicado garantizar la integración y funcionamiento coordinado de todos los componentes, sin duplicación de licencias ni costos.