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 484832 - LPN N° 10/26 - SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

## Consulta 1 - Capacidad Técnica, Numeral 3 – Arquitecto

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En el Numeral 3 de Capacidad Técnica, el perfil “Arquitecto / Ingeniero de Ciberseguridad” exige tres años de experiencia en el rubro y al menos tres certificaciones de la lista “CISSP, CND, C)SWAE, SSCP, PenTest+, CEH o similares”. La lista contiene dos inconsistencias. Primero, la certificación CISSP de ISC2 exige como requisito previo un mínimo de cinco años de experiencia profesional acumulada, lo que no es coherente con los tres años establecidos para el perfil. Segundo, la certificación C)SWAE (Certified Secure Web Application Engineer) es emitida exclusivamente por el proveedor de formación Mile2, tiene escasa difusión en el mercado regional y su inclusión favorece a los profesionales formados con dicho proveedor. Además, la expresión “o similares” no tiene un criterio que permita determinar qué certificaciones serán consideradas equivalentes. Solicitamos a la Convocante eliminar la mención específica de la certificación C)SWAE o declarar expresamente la aceptación de equivalentes en seguridad de aplicaciones, como GWEB (GIAC), CSSLP (ISC2), OSWE (OffSec) o BSCP (PortSwigger). Solicitamos también publicar un listado indicativo de certificaciones consideradas “similares”, que incluya entre otras CompTIA Security+, CySA+, CASP+/SecurityX, GIAC (GSEC, GCIH, GCIA), OSCP, eJPT/eCPPT y CCSP, a fin de garantizar los Principios de Transparencia y Libre Competencia.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 2 - Requisitos Documentales puntos 1 y 2 - Duplicidad de requisitos

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En los Requisitos Documentales para la evaluación de la experiencia, el PBC incluye en un primer punto 1 la “Copia de facturaciones, contratos y/o recepciones finales que avalen la experiencia requerida”. A continuación vuelve a numerar un punto 1 (“Fotocopia simple de Acta de Constitución”) y un punto 2 (“Copia de contratos y/o facturaciones y/o recepciones finales que avalen la experiencia requerida”). Esto genera duplicidad de numeración y de contenido. Además, la primera redacción (“facturaciones, contratos y/o recepciones finales”) puede interpretarse como conjuntiva para facturas y contratos, mientras que la segunda (“contratos y/o facturaciones y/o recepciones finales”) es plenamente disyuntiva. Solicitamos a la Convocante eliminar el requisito duplicado y corregir la numeración. Solicitamos además confirmar expresamente que, para acreditar la experiencia del índice 2, basta con presentar cualquiera de los tres documentos (contrato, factura o recepción final) por cada experiencia declarada, conforme al criterio disyuntivo. Lo anterior a fin de evitar interpretaciones ambiguas en la etapa de evaluación.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 3 - Capacidad Técnica, Numeral 3

| **Consulta** | **Fecha de Consulta** | 12-10-2026 |
|---|---|---|

En el Numeral 3 de Capacidad Técnica, el perfil “Analista de Ciberseguridad L1” exige “certificaciones en ciberseguridad”, en plural, y acepta las emitidas por plataformas como Hack The Box, PortSwigger Academy o TryHackMe. Sin embargo, el PBC no establece una cantidad mínima. En cambio, para el perfil L2 sí se fija expresamente “al menos 2 (dos) certificaciones” y para el Arquitecto “al menos 3 (tres)”. Esta omisión genera incertidumbre sobre si una sola certificación es suficiente para el perfil L1. Solicitamos a la Convocante precisar la cantidad mínima de certificaciones exigidas para cada Analista L1. Solicitamos también aclarar si los certificados de finalización de rutas o módulos formativos de estas plataformas (por ejemplo, “paths” de TryHackMe o “labs” de PortSwigger) se consideran certificaciones válidas, o si se requieren exclusivamente certificaciones con examen, como HTB CPTS, HTB CDSA o BSCP.

| **Respuesta** | **Fecha de Respuesta** | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 4 - Experiencia, índice 2 - Contradicción

| **Consulta** | **Fecha de Consulta** | 12-10-2026 |
|---|---|---|

En el índice 2 de los criterios de experiencia, el PBC establece primero que la experiencia deberá acreditarse “dentro de los 5 últimos años (2021, 2022, 2023, 2024 y 2025)”. Sin embargo, el mismo índice señala después que “el método de evaluación será la suma de todos los montos de los contratos y/o facturaciones (IVA incluido) hasta llegar al 50% solicitado dentro de los años 2023, 2024 y 2025”, y además se refiere a “la presentación de documentaciones de los 3 años”. Las dos redacciones definen períodos distintos de cinco y de tres años para un mismo requisito. Esto genera incertidumbre sobre qué documentos serán computados y expone a los oferentes a criterios de evaluación dispares, en contra de los Principios de Transparencia e Igualdad de Condiciones. Solicitamos a la Convocante unificar el criterio y confirmar expresamente que el período válido es 2021 a 2025, conforme a la primera redacción del índice. Solicitamos también modificar la referencia a “los años 2023, 2024 y 2025” y a “los 3 años” para que sea coherente con dicho período.

| **Respuesta** | **Fecha de Respuesta** | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 5 - Capacidad Técnica, Numeral 3

| **Consulta** | **Fecha de Consulta** | 12-10-2026 |
|---|---|---|

En el Numeral 3 de Capacidad Técnica, el perfil “Analista de Ciberseguridad L1” exige “certificaciones en ciberseguridad”, en plural, y acepta las emitidas por plataformas como Hack The Box, PortSwigger Academy o TryHackMe. Sin embargo, el PBC no establece una cantidad mínima. En cambio, para el perfil L2 sí se fija expresamente “al menos 2 (dos) certificaciones” y para el Arquitecto “al menos 3 (tres)”. Esta omisión genera incertidumbre sobre si una sola certificación es suficiente para el perfil L1. Solicitamos a la Convocante precisar la cantidad mínima de certificaciones exigidas para cada Analista L1. Solicitamos también aclarar si los certificados de finalización de rutas o módulos formativos de estas plataformas (por ejemplo, “paths” de TryHackMe o “labs” de PortSwigger) se consideran certificaciones válidas, o si se requieren exclusivamente certificaciones con examen, como HTB CPTS, HTB CDSA o BSCP.

| **Respuesta** | **Fecha de Respuesta** | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 6 - Capacidad Técnica, Numeral 3 – Definición de “experiencia en el rubro”

| **Consulta** | **Fecha de Consulta** | 12-10-2026 |
|---|---|---|

En el Numeral 3 de Capacidad Técnica, todos los perfiles técnicos exigen una cantidad mínima de años de “experiencia en el rubro”: cinco años para el SOC Manager, tres para el Coordinador y el Arquitecto, y dos para los Analistas L1 y L2. En el caso de los Analistas L1 se agrega además el calificativo de experiencia “relevante”. El PBC no define si “el rubro” se refiere exclusivamente a ciberseguridad, a seguridad de la información o, en general, a tecnologías de la información. Tampoco indica con qué documentos debe acreditarse esta experiencia. Esta indefinición puede generar criterios de evaluación dispares entre oferentes. Solicitamos a la Convocante precisar el alcance del término “rubro” para cada perfil y aclarar si la diferencia entre “experiencia relevante” (L1) y “experiencia” (L2) responde a criterios distintos. Solicitamos también indicar expresamente qué documentos son válidos para acreditar la experiencia: CV firmado, constancias laborales, certificados de trabajo emitidos por empleadores anteriores o planillas de IPS.

| **Respuesta** | **Fecha de Respuesta** | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 7 - Capacidad Técnica, Numeral 3 – SOC Manager

| **Consulta** | **Fecha de Consulta** | 12-10-2026 |
|---|---|---|

En el Numeral 3 de Capacidad Técnica, el perfil “SOC Manager / CSIRT Director” exige “habilidades avanzadas en Cyber Defensa y Threat Hunting”. Sin embargo, el PBC no establece qué documento acredita dichas habilidades ni qué parámetro objetivo usará el Comité de Evaluación para calificarlas de “avanzadas”. La falta de un criterio verificable deja la evaluación a la discrecionalidad del evaluador y vulnera los Principios de Transparencia e Igualdad de Condiciones. Solicitamos a la Convocante aclarar qué documentación será válida para acreditar estas habilidades (certificaciones específicas, constancias laborales, CV con detalle de funciones u otros). En caso de no poder establecerse un criterio objetivo, solicitamos eliminar el requisito como condición de cumplimiento.

| **Respuesta** | **Fecha de Respuesta** | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 8 - Capacidad Técnica, Numeral 3 – SOC Manager

| **Consulta** | **Fecha de Consulta** | 12-10-2026 |
|---|---|---|

En el Numeral 3 de Capacidad Técnica, el perfil “SOC Manager / CSIRT Director” exige un “título de maestría en Ciberseguridad”. Esta denominación de posgrado es reciente en la oferta académica nacional. Muchos profesionales con amplia trayectoria en la dirección de centros de operaciones de seguridad cuentan con maestrías en Seguridad Informática, Seguridad de la Información, Tecnologías de la Información, Ingeniería de Sistemas o Auditoría de Sistemas, cuyos contenidos curriculares abarcan las mismas competencias. Restringir la exigencia a una única denominación limita la cantidad de oferentes capaces de cumplirla sin que esto aporte una mejora objetiva en la calidad del servicio. Esto contraviene los Principios de Igualdad y Libre Competencia. Solicitamos a la Convocante modificar el requisito para que diga “título de maestría en Ciberseguridad, Seguridad de la Información, Seguridad Informática, Tecnologías de la Información o áreas afines”.

| **Respuesta** | **Fecha de Respuesta** | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 9 - Experiencia, índice 3 - Servicios exigidos ajenos

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En el índice 3 de los criterios de experiencia, el PBC exige certificados de al menos cinco instituciones que acrediten “Servicios de auditorías de vulnerabilidades o pentesting”, “Servicios de gestión y respuesta ante incidentes cibernéticos” y “Servicios de asesorías en ciberseguridad relacionadas arquitecturas de ciberseguridad y/o desarrollo de documentación”. El objeto de la presente contratación es un servicio de monitoreo, gestión y respuesta ante incidentes, como el propio índice 2 lo reconoce. Las auditorías de pentesting y las asesorías en arquitectura o documentación son líneas de servicio distintas, por lo que exigirlas como requisito habilitante amplía la experiencia requerida más allá del objeto. Esta exigencia, sumada a la cantidad mínima de cinco instituciones emisoras, constituye una barrera de entrada desproporcionada que restringe la concurrencia. Solicitamos a la Convocante limitar la experiencia exigida en el índice 3 a servicios directamente vinculados al objeto, es decir, monitoreo, gestión y respuesta ante incidentes. En su defecto, solicitamos reducir la cantidad mínima de instituciones emisoras a tres, en resguardo de los Principios de Libre Competencia y Razonabilidad.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 10 - Capacidad Técnica, Numeral 3 – Coordinador de Ciberseguridad

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En el Numeral 3 de Capacidad Técnica, el perfil “Coordinador de Ciberseguridad” exige contar con “certificaciones en sistema de gestión y auditoría conforme a la norma ISO/IEC 27001”. La redacción es conjuntiva (“gestión y auditoría”) y plural (“certificaciones”), lo que podría interpretarse como la exigencia simultánea de dos certificaciones distintas: una de implementación (ISO/IEC 27001 Lead Implementer) y otra de auditoría (ISO/IEC 27001 Lead Auditor). Además, el PBC no precisa si se aceptan las certificaciones de Auditor Interno ni qué tipo de entidad debe emitirlas. Solicitamos a la Convocante aclarar si basta con acreditar una sola certificación, sea de implementación o de auditoría, o si se exigen ambas. Solicitamos también precisar si se acepta la certificación de Auditor Interno ISO/IEC 27001 y si la certificación debe ser emitida por una entidad acreditada (por ejemplo, PECB, IRCA/CQI, BSI, TÜV, Bureau Veritas o SGS).

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 11 - Experiencia, índice 2 - Alcance

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|
| En el índice 2 de los criterios de experiencia, el PBC exige “demostrar la experiencia en servicios de monitoreo, gestión y respuesta ante incidentes de seguridad de la presente contratación”, sin precisar qué denominaciones o modalidades de servicio se consideran equivalentes. En el mercado, estos servicios se contratan habitualmente bajo denominaciones como SOC (Security Operations Center), SOC as a Service, MDR (Managed Detection and Response), NDR, monitoreo SIEM, servicios gestionados de seguridad (MSSP) o respuesta a incidentes (IR). Además, muchos contratos incluyen estos servicios junto con otros componentes de seguridad o de TI. La falta de definición podría llevar al rechazo de experiencias que son técnicamente equivalentes al objeto de la contratación. Solicitamos a la Convocante aclarar que serán aceptados como experiencia válida los contratos, facturas o recepciones finales de servicios SOC, MDR, NDR, monitoreo SIEM, servicios gestionados de seguridad y respuesta a incidentes, cualquiera sea su denominación comercial. Solicitamos también precisar si, en contratos con alcance mixto, se computará el monto total del contrato o solo la porción correspondiente a estos servicios, y en este último caso, qué documento servirá para acreditar dicha porción. | | |

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|
| El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.- | | |

## Consulta 12 - Experiencia, índice 2 - Omisión del criterio aplicable a consorcios

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|
| En los índices 1 y 3 de los criterios de experiencia, el PBC define expresamente cómo deben cumplir los requisitos los consorcios. Para el índice 1 exige que “TODOS LOS INTEGRANTES deberán cumplir en forma independiente”, y para el índice 3 establece que “la sumatoria total de las experiencias de los integrantes deberá cumplir el (100)% de este requisito”. Sin embargo, el índice 2, referido a la experiencia en facturación equivalente al 50% del monto ofertado, no indica qué criterio se aplicará en caso de consorcios. Esta omisión deja librado a la interpretación del comité evaluador un requisito de cumplimiento esencial. Solicitamos a la Convocante aclarar que, para el índice 2, en caso de consorcios se admitirá la sumatoria de los montos acreditados por todos los integrantes para alcanzar el 50% exigido, en coherencia con el criterio del índice 3. Lo anterior en resguardo de los Principios de Transparencia e Igualdad de Condiciones. | | |

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|
| El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.- | | |

## Consulta 13 - Capacidad Técnica, Numeral 3 – Arquitecto

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En el Numeral 3 de Capacidad Técnica, el perfil “Arquitecto / Ingeniero de Ciberseguridad” exige “certificaciones oficiales o acreditaciones técnicas equivalentes en la plataforma SIEM a ser utilizada, emitidas por el fabricante, comunidad o programas reconocidos”. Sin embargo, el PBC no identifica en esta sección cuál es la plataforma SIEM a la que se refiere. Tampoco aclara si se trata de una plataforma existente en la infraestructura de la Convocante, en cuyo caso el oferente necesitaría conocer la marca para certificar a su personal, o de la plataforma que cada oferente proponga en su oferta. Si se trata de una plataforma preexistente de la Convocante, el requisito favorecería a los proveedores que ya trabajan con dicho fabricante. Solicitamos a la Convocante aclarar si la plataforma SIEM es la propuesta por el oferente o una preexistente de la institución. En este último caso, solicitamos informar la marca y versión. Solicitamos también aclarar si se aceptan las acreditaciones de formación gratuita del fabricante (por ejemplo, Splunk Core Certified User, Wazuh, Microsoft SC-200, IBM QRadar, Elastic, Fortinet FCP FortiSIEM u otras) como “acreditaciones técnicas equivalentes”.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 14 - Capacidad Técnica, Numeral 3

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En el Numeral 3 de Capacidad Técnica se exige que el personal técnico cuente con “certificaciones reconocidas internacionalmente” para todos los perfiles. Sin embargo, el PBC no indica si las certificaciones deben estar vigentes a la fecha de apertura de ofertas. Varias de las certificaciones mencionadas (CompTIA, ISC2, EC-Council) tienen una vigencia limitada, generalmente de tres años, y requieren créditos de educación continua para su renovación. Otras, como las de plataformas de formación técnica, no tienen fecha de vencimiento. Solicitamos a la Convocante aclarar si se exige la vigencia de las certificaciones a la fecha de apertura de ofertas o si se aceptan certificaciones vencidas como evidencia de formación. Solicitamos también precisar qué documento se considera prueba válida de vigencia, por ejemplo una verificación en línea del emisor o una credencial digital tipo Credly.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 15 - Capacidad Técnica, Numeral 3 – Posibilidad de que un mismo profesional cubra más de un perfil

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En el Numeral 3 de Capacidad Técnica se exigen siete profesionales distribuidos en cinco perfiles. Sin embargo, el PBC no aclara si un mismo profesional que cumpla con los requisitos de más de un perfil puede ser presentado para cubrir más de uno de ellos, por ejemplo, el SOC Manager que además cuenta con certificación ISO/IEC 27001 cubriendo también el rol de Coordinador. Solicitamos a la Convocante aclarar expresamente si los perfiles deben ser cubiertos por personas distintas o si se admite la acumulación de roles en un mismo profesional cuando éste cumpla con los requisitos de ambos.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 16 - Antigüedad mínima de 12 meses

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En el párrafo final del Numeral 3 de Capacidad Técnica se exige que todo el personal técnico tenga una antigüedad mínima de doce meses en el staff permanente del oferente. Este requisito no guarda relación con la idoneidad técnica del profesional, que ya se acredita mediante los años de experiencia en el rubro y las certificaciones exigidas para cada perfil. Además, el requisito obliga a los oferentes a mantener en planilla, al menos durante un año antes de la convocatoria, un equipo completo de siete profesionales especializados. Esto restringe la participación a las empresas que ya prestan servicios SOC en el mercado y constituye una barrera de entrada desproporcionada, contraria a los Principios de Igualdad y Libre Competencia. Solicitamos a la Convocante eliminar el requisito de antigüedad mínima o, en su defecto, reducirlo a seis meses. Alternativamente, solicitamos admitir que los profesionales sean presentados mediante carta de compromiso, con la obligación del adjudicado de acreditar la relación laboral al momento de la firma del contrato.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 17 - Planilla de Especificaciones Técnicas

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En la Planilla de Especificaciones Técnicas, apartado Generalidades, el PBC exige conectividad redundante de “mínimo 200 MBPS de subida y 40 MBPS de bajada”. En un servicio SOC el flujo principal de datos es la recepción de logs y eventos desde la infraestructura del CAH, lo que técnicamente corresponde al canal de bajada (ingreso) en las instalaciones del oferente. La relación indicada, con subida cinco veces mayor que la bajada, parece invertida respecto a la naturaleza del servicio y genera incertidumbre sobre el dimensionamiento de enlaces. Solicitamos a la Convocante aclarar si los valores consignados son correctos o si existe una inversión involuntaria, precisar si los anchos de banda se refieren a los enlaces del SOC del oferente o a los enlaces entre el CAH y el SOC, e indicar si la redundancia exigida implica dos proveedores de conectividad distintos.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 18 - Numeral 6 Inventario de Equipos y Servicios Existentes

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

El Numeral 6 detalla 700 usuarios, 70 servidores, 500 estaciones de trabajo y dispositivos, 82 sucursales y 2 firewalls de borde, y la Planilla de Especificaciones Técnicas exige que el SOC procese y correlacione todas esas fuentes con un crecimiento de al menos 30% sin pérdida de eventos. Sin embargo, el PBC no indica el volumen estimado de eventos por segundo (EPS) ni de ingesta diaria en GB, ni precisa si las 500 estaciones de trabajo y las 82 sucursales deben ser monitoreadas individualmente como fuentes de log o si sus eventos llegan consolidados a través de servidores, controladores de dominio o firewalls. Tampoco se identifica si las sucursales cuentan con equipamiento de red propio (firewalls, routers, switches) que deba integrarse. Dado que el dimensionamiento del SIEM, del almacenamiento de 12 meses en línea y de los 36 meses de custodia depende directamente de estos datos, solicitamos a la Convocante informar el volumen promedio y pico de EPS o GB diarios, el detalle de las fuentes de log a integrar por tipo, y aclarar si los endpoints y sucursales se monitorean de forma directa o consolidada, a fin de que todos los oferentes coticen sobre una base técnica común conforme al Principio de Igualdad de Condiciones.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 19 - Numeral 6 Inventario y Capacidades de Contención

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

La Planilla de Especificaciones Técnicas exige que las listas dinámicas de indicadores de inteligencia de amenazas se sincronicen en tiempo real con todos los dispositivos conectados automatizando bloqueos, que el SOAR sea interoperable con los elementos existentes, que se integren las vulnerabilidades detectadas por el CAH, y que el SOC cumpla tiempos máximos de contención de hasta 2 horas. No obstante, el Numeral 6 no identifica la marca, modelo y versión de los 2 firewalls de borde, ni si el CAH cuenta con una solución EDR o antivirus corporativo, servicio de directorio (Active Directory u otro), plataforma de correo o nube (por ejemplo Microsoft 365), ni la herramienta de escaneo de vulnerabilidades que utiliza. Sin esta información no es posible verificar la viabilidad de los conectores e integraciones exigidos ni cotizar herramientas adicionales que pudieran ser necesarias. Solicitamos a la Convocante informar las marcas, modelos y versiones de dichas plataformas y aclarar si el oferente deberá proveer una solución EDR propia para los 500 endpoints o si la contención se ejecutará sobre las herramientas existentes del CAH.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 20 - Numeral 4.3 literal C y Planilla de Especificaciones Técnicas

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

El Numeral 4, Cláusula 3, literal C exige conservar los logs por un período mínimo de 36 meses de custodia total incluyendo almacenamiento en frío, mientras que la Planilla de Especificaciones Técnicas exige 12 meses de información en línea como mínimo, y el ítem se contrata por 21 meses. Ello genera dudas respecto a la distribución entre almacenamiento en caliente y en frío, y respecto a la obligación de custodia una vez finalizado el contrato, considerando que los logs más recientes deberían conservarse hasta 15 meses después de la culminación del servicio sin contraprestación prevista. Solicitamos a la Convocante aclarar si el esquema esperado es de 12 meses en línea más 24 meses en frío, precisar si al finalizar el contrato el oferente deberá entregar la totalidad de los logs al CAH en un formato y medio determinados, transfiriendo así la responsabilidad de custodia, o si deberá mantener la custodia posterior, y en este último caso indicar cómo se remunerará dicho período.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 21 - Planilla de Especificaciones Técnicas, apartado Servicio

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En el apartado Servicio se exige que los componentes de recolección realicen “desde el origen, la normalización completa de los eventos”, enviando únicamente eventos previamente estructurados en campos, utilicen TCP con verificación constante mediante “pulso o Heartbeat”, almacenen eventos en una caché de tamaño configurable ante pérdida de conexión, apliquen compresión, permitan controles de ancho de banda y priorización de transacciones críticas, y filtren eventos en origen. Este conjunto de características, en su redacción y combinación, corresponde a la arquitectura de conectores del fabricante OpenText (ex Micro Focus) ArcSight, mediante sus SmartConnectors con normalización a formato CEF. Numerosas plataformas SIEM equivalentes del mercado (Splunk, Microsoft Sentinel, Google SecOps, Elastic Security, IBM QRadar, Wazuh, entre otras) garantizan la misma confiabilidad de recolección, sin pérdida de eventos, con buffering, cifrado y compresión, pero realizan el parsing y la normalización en la capa de ingesta o indexación y no necesariamente en el agente de origen. Solicitamos a la Convocante modificar el requisito para admitir arquitecturas en las que la normalización se realice en el recolector o en la plataforma de ingesta indistintamente, siempre que se garantice la no pérdida de eventos, el almacenamiento temporal ante desconexión, el monitoreo del estado del recolector y el cifrado en tránsito, a fin de garantizar la libre competencia.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 22 - Exigencia de simulación de propagación de malware y explotación de vulnerabilidades

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

El PBC exige que el servicio permita correlacionar accesos perimetrales de firewalls con vulnerabilidades detectadas en equipos “con el fin de simular propagaciones de malware y explotaciones (exploits) de vulnerabilidades”. La simulación de rutas de ataque es una funcionalidad propia de módulos específicos de modelado de topología y riesgo, como IBM QRadar Risk Manager o herramientas de attack path management, y no forma parte de la correlación estándar de un SIEM. Esta exigencia limita la concurrencia sin que el PBC defina los criterios de cumplimiento. Solicitamos a la Convocante aclarar si el requisito se considera cumplido mediante reglas de correlación que crucen tráfico permitido en firewall con vulnerabilidades de los activos destino para priorizar alertas, o si se exige una herramienta de simulación de rutas de ataque, y en ese caso modificar el requisito para aceptar soluciones equivalentes de cualquier fabricante.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 23 - Planilla de Especificaciones Técnicas, apartado Servicio

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

El mismo apartado exige por un lado que el SOC tenga capacidad de “recibir logs en formato crudo (RAW)” mediante Syslog, SCP, SFTP, NFS, CIFS y APIs, y por otro lado establece que los componentes de recolección “únicamente enviarán hacia el servicio de monitoreo los eventos previamente estructurados en campos específicos”. Ambas cláusulas resultan contradictorias, ya que una exige la recepción del dato crudo y la otra prohíbe su envío sin normalización previa. Asimismo, la conservación del log crudo original es relevante para fines forenses y de cadena de custodia exigidos en el Numeral 4. Solicitamos a la Convocante unificar el criterio y aclarar si se requiere la conservación y envío del log RAW original, del evento normalizado, o de ambos, y precisar cuál de ellos debe estar sujeto a los requisitos de retención de 36 meses.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 24 - Planilla de Especificaciones Técnicas, Generalidades

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En el apartado Generalidades se establece que el Proveedor mantendrá inventario de software y exposición “de la infraestructura utilizada para prestar el SOC”, ejecutará descubrimiento de activos cada 7 días, enumeración autenticada cada 14 días, y corregirá vulnerabilidades del catálogo CISA KEV en 7 días y las de CVSS igual o superior a 7,0 en 14 días, además de una prueba de intrusión anual. Por otro lado, en el apartado Servicio se exige que el oferente realice “pruebas de vulnerabilidad periódicas y, de corresponder, pruebas de intrusión planificadas, con una frecuencia mínima anual o a requerimiento de la institución”. La redacción no permite determinar con certeza si las obligaciones de escaneo y corrección recaen sobre la plataforma propia del SOC del oferente o sobre los activos del CAH, siendo que la corrección de vulnerabilidades en sistemas del CAH depende de su personal y ventanas de cambio. Asimismo, la expresión “a requerimiento de la institución” deja indeterminada la cantidad de pruebas de intrusión a cotizar. Solicitamos a la Convocante aclarar si los plazos de corrección aplican exclusivamente a la infraestructura del oferente, precisar el alcance de las pruebas de vulnerabilidad e intrusión sobre activos del CAH (cantidad de IPs, aplicaciones, modalidad externa y/o interna, caja negra, gris o blanca) y fijar la cantidad máxima de pruebas de intrusión incluidas durante los 21 meses del contrato.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 25 - Inteligencia sectorial frente a Cláusula de segregación de información

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

La Planilla exige que el servicio integre “inteligencia derivada de incidentes similares en el sector o región relacionada al CAH”, mientras que el Numeral 4, Cláusula 2, exige que los datos y eventos de cada cliente no sean accesibles ni visibles por otros clientes. Solicitamos a la Convocante confirmar que el requisito de inteligencia sectorial se cumple mediante el uso de indicadores de compromiso, tácticas y técnicas anonimizadas y desvinculadas de la identidad de otros clientes, sin que ello constituya incumplimiento de la cláusula de segregación, y que este mismo criterio aplica al uso de los observables propios del SOC.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 26 - Contradicción entre Syslog UDP

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

El PBC admite la recepción de logs mediante “Syslog (TCP o UDP)”, pero a continuación establece que la remisión de eventos hacia el SOC “debe ser realizada a través del protocolo de transporte TCP” con cifrado TLS 1.3 o mínimo TLS 1.2, y además que toda la comunicación debe estar encriptada mediante VPN SSL o IPsec redundante. Solicitamos a la Convocante aclarar si es admisible que los dispositivos del CAH envíen Syslog UDP hacia un recolector ubicado dentro de la red del CAH y que sea este recolector el que transmita hacia el SOC mediante TCP con TLS, precisar si se exige de forma conjunta el cifrado TLS y el túnel VPN o si cualquiera de ambos mecanismos es suficiente, e indicar si la redundancia de la VPN requiere enlaces de distintos proveedores en el extremo del CAH y quién asume dicho costo.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 27 - Integración de vulnerabilidades del CAH y declaración de incidentes

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

El PBC establece que el servicio debe integrar las vulnerabilidades detectadas por el CAH con el monitoreo y la correlación, y que “se deben declarar incidentes ante vulnerabilidades detectadas”. La declaración de un incidente por cada vulnerabilidad identificada, sin evidencia de explotación, distorsionaría la gestión de incidentes y el cómputo de los SLA definidos. Solicitamos a la Convocante aclarar si la declaración de incidente aplica únicamente cuando exista evidencia de intento o explotación efectiva de la vulnerabilidad, o a qué criterio de severidad corresponde, e informar la herramienta de escaneo de vulnerabilidades utilizada por el CAH y el formato de exportación de sus resultados.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 28 - Solicitud de flexibilización del requisito de residencia del personal técnico

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En relación con el requisito que establece que todos los profesionales del equipo técnico deberán residir en el país, solicitamos reconsiderar dicha exigencia, permitiendo que determinados perfiles especializados puedan prestar servicios de manera remota desde el exterior, siempre que se garantice la cobertura 24x7x365, el cumplimiento de los SLA y la disponibilidad de personal técnico local para intervenciones presenciales cuando sean necesarias.
Consideramos que la prestación de servicios SOC, por su naturaleza tecnológica, permite esquemas de operación remota e híbrida sin comprometer la calidad ni la seguridad del servicio. La modificación solicitada permitiría ampliar la participación de empresas con profesionales especializados de reconocida trayectoria internacional.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 29 - 2. Solicitud de flexibilización de la antigüedad laboral del personal técnico

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

Solicitamos respetuosamente reconsiderar la exigencia de que la totalidad de los profesionales propuestos cuenten con una antigüedad mínima de 12 meses en el plantel permanente del oferente.
Se propone admitir profesionales vinculados mediante contratos laborales o de prestación de servicios profesionales vigentes, debidamente documentados, sin exigir una antigüedad mínima determinada, siempre que acrediten la formación, certificaciones y experiencia requeridas y garanticen su disponibilidad durante la ejecución contractual. Esta modificación permitiría conformar equipos especializados sin comprometer las capacidades técnicas exigidas por la institución.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

El equipo técnico de la Convocante ha analizado los criterios de evaluación y los requisitos técnicos, confirmando que fueron previamente verificados y no observados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), favor adecuarse a las especificaciones técnicas.-

## Consulta 30 - Aclaración del período válido para acreditar experiencia comercial

| Consulta | Fecha de Consulta | 12-10-2026 |
|---|---|---|

En el apartado de experiencia requerida se establece inicialmente que podrán presentarse contratos y/o facturaciones correspondientes a los ejercicios 2021, 2022, 2023, 2024 y 2025. Sin embargo, posteriormente se indica que la evaluación considerará la suma de los montos correspondientes a los años 2023, 2024 y 2025.
Solicitamos aclarar cuál de los períodos será efectivamente considerado para acreditar el porcentaje mínimo del 50% del monto total ofertado, y confirmar si serán válidos los documentos correspondientes a todos los ejercicios comprendidos entre 2021 y 2025.

| Respuesta | Fecha de Respuesta | 12-10-2026 |
|---|---|---|

Se emitirá la Adenda N.º 01, a fin de corregir el apartado de experiencia requerida y unificar los criterios establecidos para el período válido de acreditación de la experiencia.