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 487310 - SUSCRIPCIÓN DE LICENCIAS VARIAS PARA LA AFD

Consulta 1 - Suscripción a PRTG Network Monitor (500 sensores)

Consulta	Fecha de Consulta	24-09-2026

Consulta: En el Ítem 5 de la Lista de Bienes y Servicios, el PBC requiere la "Suscripción a PRTG Network Monitor (incluye 500 sensores)" por una cantidad de 1 y un plazo de 36 meses; sin embargo, no se precisa si se trata de la renovación de una licencia o suscripción actualmente vigente en la Convocante o de una primera adquisición. Esta distinción afecta directamente la cotización, ya que el fabricante Paessler aplica condiciones comerciales, procedimientos de activación y eventuales cargos de reinstalación distintos según el caso, y en caso de renovación resulta indispensable contar con el identificador de licencia (License Key / License Name), la edición actual, la cantidad de sensores vigente y la fecha de vencimiento para gestionar la continuidad ante el fabricante. La omisión de esta información impide a los oferentes formular propuestas comparables y precisas. Solicitamos a la Convocante aclarar si el Ítem 5 corresponde a una renovación o a una nueva adquisición y, en caso de tratarse de una renovación, informar el identificador de licencia actual, la edición, la cantidad de sensores vigente y la fecha de vencimiento de la suscripción, a fin de garantizar el resguardo de los Principios de Transparencia e Igualdad de Condiciones.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que el Lote 05, Ítem 1 "Suscripción a PRTG Network Monitor (incluye 500 sensores)" NO corresponde a la renovación de una suscripción vigente, sino a la SUSCRIPCIÓN NUEVA de PRTG Network Monitor, conforme al objetivo de las Especificaciones Técnicas.

Consulta 2 - Suscripción a PRTG Network Monitor – Modalidad de despliegue y arquitectura requerida

Consulta	Fecha de Consulta	24-09-2026

Consulta: En el Ítem 5 no se especifica la modalidad de despliegue de la solución, siendo que el fabricante Paessler ofrece PRTG en versión on-premise (PRTG Network Monitor) y en versión alojada en la nube (PRTG Hosted Monitor), con condiciones de licenciamiento distintas. Asimismo, no se indica si se requiere un único servidor central (core server), la cantidad de sondas remotas (remote probes) previstas, ni si se contempla alta disponibilidad (cluster/failover), aspectos que inciden en la edición a cotizar y en su costo. Solicitamos a la Convocante aclarar la modalidad de despliegue requerida (on-premise o en la nube), la cantidad de servidores core y sondas remotas previstas y si se requiere configuración en alta disponibilidad, a fin de garantizar el resguardo de los Principios de Transparencia e Igualdad de Condiciones.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que lo requerido en el Lote 05, Ítem 1 es la suscripción que dé continuidad a la licencia de PRTG Network Monitor actualmente en uso en la Convocante, cuyo mantenimiento vence el 17/12/2026. Conforme a la política comercial vigente del fabricante Paessler, la continuidad de las licencias perpetuas se gestiona mediante el esquema de suscripción de PRTG Network Monitor, que mantiene la instalación on-premise existente. No se requiere provisión de hardware ni servidores, ya que la plataforma se encuentra operativa en la Convocante. Las obligaciones de soporte técnico, SLA y garantía de buen funcionamiento son las establecidas en los apartados 3 y 4 de las Especificaciones Técnicas para los Lotes 01 al 05.

Consulta 3 - Suscripción a PRTG Network Monitor – Alcance de servicios

Consulta	Fecha de Consulta	24-09-2026

Consulta: En el Ítem 5 se requiere únicamente la "Suscripción a PRTG Network Monitor (incluye 500 sensores)" por 36 meses, sin indicar si el alcance se limita a la provisión y entrega de la licencia o si comprende además servicios de instalación, configuración, migración, parametrización de sensores, alertas, mapas o reportes, integración con la infraestructura existente, capacitación o transferencia de conocimiento. La ausencia de esta definición genera una asimetría entre oferentes, dado que algunos podrían cotizar exclusivamente la licencia y otros incluir servicios profesionales, afectando la comparabilidad de las ofertas y la posterior ejecución contractual. Solicitamos a la Convocante aclarar si el Ítem 5 comprende únicamente el suministro de la suscripción o si incluye servicios de implementación y, en este último caso, detallar el alcance mínimo requerido (instalación, cantidad de dispositivos a monitorear, configuración de sensores, alertas, reportes, capacitación y horas de soporte técnico local), así como los entregables y criterios de recepción aplicables, a fin de garantizar el resguardo de los Principios de Transparencia e Igualdad de Condiciones.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que el soporte técnico comprenderá, como mínimo, la atención de incidentes, la corrección de fallos, ajustes de configuración razonables vinculados a la operación normal del software y el acompañamiento en la aplicación de actualizaciones, nuevas versiones y parches de seguridad recomendados por el fabricante durante la vigencia de la suscripción, conforme se indica expresamente en el Pliego de Bases y Condiciones.

Consulta 4 - Definición de "canal autorizado", forma de acreditación

Consulta	Fecha de Consulta	24-09-2026

Consulta: En el requisito aplicable a los Lotes 01, 04 y 05 se establece que "el oferente deberá contar con al menos un técnico certificado por el fabricante de la solución ofertada, o que el canal autorizado que respalda la oferta garantice disponibilidad de personal certificado durante la vigencia de la suscripción, mediante certificado vigente emitido por el fabricante o declaración expresa del canal autorizado". Para el Lote 05 (PRTG), el PBC no define qué se entiende por "canal autorizado", pudiendo corresponder al distribuidor mayorista de Paessler, al partner o revendedor registrado en su programa de canales, o al propio oferente en caso de ser partner del fabricante; tampoco se indica el documento mediante el cual se comprobará dicha condición (carta o constancia del fabricante, constancia del distribuidor, registro en el portal de partners de Paessler u otro). Asimismo, no se precisa la forma que debe revestir la "declaración expresa del canal autorizado", es decir, si será suficiente una nota simple firmada por el representante del canal o si se requiere una declaración jurada, con o sin certificación de firma, ni si dicha declaración deberá individualizar al personal certificado. La indefinición de estos aspectos puede dar lugar a criterios dispares en la evaluación y al rechazo de ofertas por cuestiones formales no previstas en el pliego. Solicitamos a la Convocante aclarar qué se entenderá por "canal autorizado" para el Lote 05, especificar el documento con el cual se acreditará dicha condición, y confirmar si la "declaración expresa del canal autorizado" podrá presentarse en formato de declaración jurada firmada por su representante legal, indicando los requisitos formales y el contenido mínimo que deberá contener, a fin de garantizar el resguardo de los Principios de Transparencia e Igualdad de Condiciones.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que la expresión "canal autorizado" se refiere al fabricante, representante o distribuidor, que forme parte de la cadena de comercialización autorizada por el fabricante, para el territorio nacional. Dicha condición se acreditará conforme al formato requerido en el apartado de formularios del PBC.

Consulta 5 - LOTE 8 - Ítem 1 - Especificaciones Técnicas

Consulta	Fecha de Consulta	29-09-2026

Consulta: El PBC exige con carácter EXIGIDO que "La solución debe ser capaz de recopilar, procesar y analizar los datos de los buzones de spam de Office 365 para identificar quién y cómo intenta atacar a la organización". Esta capacidad es característica de una funcionalidad específica del fabricante Lumu Technologies y no constituye una función estándar de las soluciones de detección de compromiso basadas en metadatos de red. Asimismo, el propio PBC indica que la AFD posee una solución de correo electrónico ANTISPAM, la cual ya genera telemetría sobre intentos de ataque vía correo. Solicitamos a la Convocante modificar este requisito para admitir como equivalente el análisis de metadatos o registros provenientes de la plataforma antispam o de Microsoft 365 (por ejemplo, mediante Microsoft Graph API, Message Trace o el registro de auditoría), o bien convertirlo en requisito deseable no excluyente.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que el objetivo del requisito es que la solución pueda incorporar y analizar información proveniente del ecosistema de correo electrónico de la AFD con el propósito de identificar, contextualizar y contribuir a la detección de intentos de ataque dirigidos a la organización. Por tanto, el cumplimiento será evaluado en función de la capacidad efectiva de la solución para recopilar, procesar y analizar la información requerida, conforme a las especificaciones establecidas en el PBC y a los objetivos de seguridad definidos por la Convocante. Asimismo, se informa que el requisito fue definido con base en el análisis técnico realizado por la convocante y en coordinación con el Ministerio de Tecnologías de la Información y Comunicación (MITIC) Órgano competente de control y facultado a dictar los lineamientos y condiciones para la contratación de este tipo de servicios al Estado, considerando las necesidades operativas y de seguridad de la institución. En consecuencia, favor, remitirse a lo solicitado en el PBC.

Consulta 6 - lote 8 - Ítem 1 - Certificación SOC 2 Tipo 2

Consulta	Fecha de Consulta	29-09-2026

Consulta: En las especificaciones técnicas del Ítem 1 se exige con carácter EXIGIDO que "El producto ofertado deberá poseer una certificación SOC2 Tipo 2". Sin embargo, en el apartado "Acreditación de madurez técnica, seguridad y adopción de la solución", literal b), la certificación SOC 2 Tipo II figura como una opción más entre "ISO/IEC 27001:2022, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, SOC 2 Tipo II, CSA STAR o equivalentes vigentes", siendo a su vez dicho literal b) sólo uno de los cuatro medios alternativos a elección del oferente. Asimismo, el apartado de Transferencia internacional admite de forma alternativa las mismas certificaciones. Esta discrepancia genera incertidumbre sobre si la SOC 2 Tipo II es un requisito excluyente o una alternativa. Solicitamos a la Convocante unificar el criterio modificando el requisito del Ítem 1 para que admita SOC 2 Tipo II, ISO/IEC 27001:2022, ISO/IEC 27017, ISO/IEC 27018, CSA STAR u otras certificaciones equivalentes vigentes del servicio SaaS, conforme al criterio amplio establecido en el mismo pliego.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que para el servicio SaaS objeto del presente ítem es requerida únicamente la certificación SOC 2 Tipo II, conforme se encuentra expresamente establecido en las especificaciones técnicas del requisito correspondiente. Por otro lado, en cuanto a las condiciones de acreditación de madurez técnica, seguridad y adopción de la solución, así como las relacionadas con transferencia internacional, privacidad y tratamiento de datos previstas en el PBC, se admiten certificaciones equivalentes conforme a lo expresamente establecido para dichos apartados. En consecuencia, no existe contradicción ni discrepancia entre los requisitos. Asimismo, se informa que dicha condición fue analizada y validada técnicamente en coordinación con el Ministerio de Tecnologías de la Información y Comunicación (MITIC), en su carácter de órgano rector en materia de tecnologías de la información y comunicación para los organismos y entidades del Estado, considerándose adecuada a las necesidades de seguridad, confiabilidad y operación del servicio requerido. Por tanto, favor, remitirse a lo establecido en el Pliego de Bases y Condiciones.

Consulta 7 - LOTE 8 Ítem 1 - Especificaciones Técnicas

Consulta	**Fecha de Consulta**	29-09-2026

Consulta: Del análisis conjunto de las especificaciones técnicas del Ítem 1 se observa que numerosos requisitos EXIGIDOS reproducen funcionalidades, métricas y terminología propias de la plataforma de Medición Continua de Compromiso (Continuous Compromise Assessment) del fabricante Lumu Technologies (productos Lumu Insights, Lumu Defender y Lumu Autopilot), entre ellos el análisis de buzones de spam de Office 365, la métrica de "ahorro operacional expresado en horas de trabajo de los analistas" visible "sin ninguna configuración", la identificación automática del "primer dispositivo de la red que se vio afectado", la distribución del compromiso por día y hora de la semana, el módulo de inteligencia artificial que itera automáticamente sobre la incidencia hasta el cierre o escalamiento, la cantidad de IOCs incluidos en los últimos 30 días y la incorporación futura de "otro producto del mismo fabricante". La acumulación de estas características, varias de ellas denominaciones comerciales o métricas propietarias sin estándar de mercado, limita la concurrencia a un único fabricante y excluye a soluciones equivalentes de detección y respuesta de red (NDR), análisis de DNS o medición de compromiso de otros fabricantes que cumplen el objetivo funcional del llamado. Solicitamos a la Convocante modificar dichas especificaciones redactándolas en términos funcionales y de resultado, admitir expresamente soluciones equivalentes que cumplan el objetivo de detectar, priorizar y responder a indicadores de compromiso en tiempo cercano al real, y aclarar que las métricas de desempeño podrán presentarse mediante indicadores equivalentes o reportes configurables, en resguardo de los Principios de Libre Competencia e Igualdad de Condiciones.

Respuesta	**Fecha de Respuesta**	05-10-2026

Se aclara que las especificaciones técnicas del Ítem 1 tienen por objeto establecer las capacidades y resultados funcionales requeridos por la AFD y no limitar la participación a un fabricante, producto, denominación comercial o arquitectura tecnológica específica. A efectos de la evaluación, el oferente deberá demostrar documental y/o técnicamente que las funcionalidades propuestas satisfacen los objetivos y resultados exigidos en el PBC.
Asimismo, se aclara que las especificaciones técnicas han sido definidas a partir de las necesidades operativas y de seguridad identificadas por la AFD, considerando criterios de razonabilidad, proporcionalidad y disponibilidad de soluciones en el mercado. Dichos requisitos fueron elaborados y analizados técnicamente con la participación y validación del Ministerio de Tecnologías de la Información y Comunicación (MITIC), en su carácter de órgano rector en materia de tecnologías de la información y comunicación para los organismos y entidades del Estado.
En consecuencia, la Convocante considera que los requerimientos establecidos mantienen una amplitud técnica razonable que permite la participación de oferentes cuyas soluciones acrediten el cumplimiento de las capacidades solicitadas, sin perjuicio de las particularidades tecnológicas que cada fabricante adopte para su implementación. Por tanto, favor, remitirse a las especificaciones técnicas establecidas en el Pliego de Bases y Condiciones.

Consulta 8 - LOTE 8 EETT

Consulta	Fecha de Consulta	29-09-2026

Consulta: El PBC exige con carácter EXIGIDO que la solución cuente con "capacidades de incorporación de forma modular de componentes que permitan a través del uso de la inteligencia artificial, una vez que se ha generado la respuesta automática (bloqueo) desde la propia plataforma, iterar igualmente de forma automatizada sobre la incidencia tantas veces como sea necesario hasta poder llegar a la conclusión que no existe presencia de comunicación con el adversario... y en consecuencia proceder de forma automática con el cierre del incidente". Esta descripción corresponde de manera específica al flujo operativo de un producto particular (Lumu Autopilot) y no a una capacidad estándar de mercado. Asimismo, la expresión "capacidades de incorporación de forma modular" sugiere que el componente puede no estar incluido en la suscripción, generando ambigüedad sobre si debe cotizarse. Solicitamos a la Convocante aclarar si este componente debe estar incluido y operativo durante los 12 meses del contrato o si constituye una capacidad de escalabilidad futura, y modificar la redacción admitiendo como equivalentes soluciones que realicen verificación post-contención y cierre automatizado o asistido de incidentes mediante SOAR, automatizaciones nativas o integraciones con el SIEM existente.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que el requisito mencionado forma parte del conjunto de capacidades técnicas requeridas por la AFD para fortalecer los procesos de detección, análisis, contención y gestión de incidentes de seguridad en tiempo cercano al real. La descripción establecida en el PBC tiene por finalidad definir el resultado funcional esperado por la Convocante y el nivel de automatización requerido para la operación de la solución, sin que ello implique la referencia exclusiva a un fabricante, producto o denominación comercial específica.
Asimismo, se aclara que las especificaciones técnicas fueron definidas sobre la base de las necesidades institucionales identificadas por la AFD, considerando criterios de razonabilidad, proporcionalidad y disponibilidad de soluciones en el mercado. Dichos requisitos fueron elaborados, analizados y validados técnicamente con la participación del Ministerio de Tecnologías de la Información y Comunicación (MITIC), en su carácter de órgano rector en materia de tecnologías de la información y comunicación para los organismos y entidades del Estado.
En cuanto a la consulta sobre la incorporación modular de componentes, se aclara que el requisito forma parte de las capacidades funcionales exigidas para la solución ofertada, por lo que el oferente deberá contemplar en su propuesta todos los elementos, componentes, licencias, funcionalidades e integraciones necesarias para acreditar el cumplimiento de las especificaciones técnicas requeridas durante la vigencia de la licencia.
En consecuencia, la Convocante considera que el requisito se encuentra debidamente justificado y mantiene una amplitud técnica razonable para la participación de oferentes que acrediten el cumplimiento de las capacidades exigidas. Por tanto, favor, remitirse a lo establecido en el Pliego de Bases y Condiciones.

Consulta 9 - LOTE 8

Consulta	Fecha de Consulta	29-09-2026

Consulta: El PBC exige que la solución recolecte información mediante un agente o colector "hacia el cual se haga reenvío (forward) de los logs requeridos para realizar la detección de compromisos", e incluso admite el análisis de "registros de seguridad provenientes de diversas fuentes". Sin embargo, otro requisito EXIGIDO establece que "El proceso de recolección de datos para medir el compromiso debe basarse en metadatos, es decir, no debe incluir los paquetes de datos completos (logs, pcaps, taps)", clasificando a los logs como paquetes completos, lo cual es técnicamente impreciso, dado que los logs de firewall, proxy o DNS constituyen justamente registros de metadatos y no captura de paquetes. Esta redacción genera una contradicción que podría utilizarse para descalificar soluciones que procesan logs como fuente de metadatos. Solicitamos a la Convocante corregir la redacción eliminando el término "logs" de la lista de elementos prohibidos, limitando la restricción a la captura completa de paquetes (full packet capture, PCAP y TAPs), y confirmar expresamente que el procesamiento de logs de dispositivos de red y seguridad es admitido.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que el procesamiento de logs y registros de seguridad provenientes de dispositivos y fuentes tales como DNS, firewall, proxy, VPN, correo electrónico y demás fuentes contempladas en el PBC se encuentra admitido y forma parte de las capacidades de recolección y análisis requeridas.
A los efectos del requisito indicado, los logs o registros de seguridad no deberán interpretarse como equivalentes a la captura completa de paquetes de red (Full Packet Capture).
En consecuencia, la restricción establecida respecto de la recolección de datos deberá entenderse referida a la captura y procesamiento del contenido completo de los paquetes de red (Full Packet Capture/PCAP), y no al procesamiento de logs, registros de seguridad o metadatos generados por dispositivos, aplicaciones y servicios.

Consulta 10 - LOTE 8 ITEM 1 - Contradicción en las fuentes de telemetría

Consulta	Fecha de Consulta	29-09-2026

Consulta: El PBC exige con carácter EXIGIDO que "La telemetría utilizada por la solución debe basarse en metadata de red y la misma debe ser colectada exclusivamente sobre los siguientes elementos de la red: DNS, netflow, firewall, proxy, email". No obstante, el párrafo inmediatamente siguiente establece que la solución deberá operar "mediante el análisis de metadatos de red y registros de seguridad provenientes de diversas fuentes", y otros requisitos EXIGIDOS contemplan la recolección de metadatos de nubes AWS y Azure vía API, de plataformas VPN, de agentes en endpoints y de buzones de spam de Office 365, fuentes que no se encuentran dentro de la lista taxativa. El término "exclusivamente" restringe indebidamente las arquitecturas de detección y contradice el resto de las exigencias del mismo ítem. Solicitamos a la Convocante eliminar el término "exclusivamente" y reemplazarlo por "como mínimo", admitiendo soluciones que analicen metadatos y registros de seguridad de fuentes adicionales, en resguardo de los Principios de Libre Competencia e Igualdad de Condiciones.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que las especificaciones técnicas han sido definidas a partir de las necesidades operativas y de seguridad identificadas por la AFD, considerando criterios de razonabilidad, proporcionalidad y disponibilidad de soluciones en el mercado. Dichos requerimientos fueron elaborados y validados técnicamente con la participación del Ministerio de Tecnologías de la Información y Comunicación (MITIC), en su carácter de órgano rector en materia de tecnologías de la información y comunicación para los organismos y entidades del Estado.
Asimismo, la Convocante aclara que la redacción del requisito citado responde a una definición técnica específica de las fuentes de telemetría requeridas para la solución objeto de contratación, conforme al modelo de análisis y correlación de eventos que se pretende implementar en la institución. En consecuencia, la interpretación del requisito deberá realizarse conforme a los términos expresamente establecidos en el Pliego de Bases y Condiciones.

Consulta 11 - LOTE 8 ITEM 1

Consulta	Fecha de Consulta	29-09-2026

Consulta: En las especificaciones técnicas del Ítem 1, el PBC establece como EXIGIDO que "La solución no requiere de la instalación de agentes en ningún elemento del ecosistema tecnológico de la AFD on premise para la realización de las actividades de detección, reportaje y atención de actividad maliciosa en la red". Sin embargo, el mismo apartado exige también, con carácter EXIGIDO, que la solución debe "proveer la capacidad de recolectar la información a través de la instalación de un agente dentro de la red de la organización y hacia el cual se haga reenvío (forward) de los logs", que debe "permitir la implantación mediante la instalación de un colector pasivo dentro de la AFD" y que debe "permitir la ingesta de metadatos mediante un agente para la medición remota del compromiso del dispositivo", además de exigir la recolección en dispositivos Windows, macOS y Linux. Ambas exigencias son mutuamente excluyentes en su redacción literal, ya que una prohíbe los agentes on premise y las otras los requieren de forma obligatoria, lo que impide a los oferentes determinar con certeza la arquitectura que cumple el pliego. Solicitamos a la Convocante aclarar y unificar el criterio, precisando si la prohibición se refiere exclusivamente a agentes instalados en endpoints como condición para la detección, y si se admiten tanto colectores virtuales on premise como agentes opcionales para dispositivos remotos, a fin de garantizar los Principios de Transparencia e Igualdad de Condiciones.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que la disposición que establece que la solución no requiere la instalación de agentes en elementos del ecosistema tecnológico on premise de la AFD se refiere a que las capacidades principales de detección, análisis, reportaje y atención de actividad maliciosa en la red no deberán depender de la instalación obligatoria de agentes en los endpoints de la AFD.
Lo anterior no excluye la utilización de colectores pasivos, físicos y/o virtuales, instalados dentro de la infraestructura de la AFD para la recolección, concentración o reenvío (forwarding) de logs, metadatos y demás información necesaria para las funcionalidades previstas en el PBC.
Asimismo, se admite la utilización de agentes en dispositivos Windows, macOS y Linux cuando estos sean necesarios para funcionalidades específicas, tales como la recolección de información o metadatos y la medición remota del compromiso de dispositivos, incluyendo equipos remotos, siempre que dichos agentes no constituyan una condición obligatoria para las capacidades principales de detección de actividad maliciosa en la red on premise.
En consecuencia, deberán entenderse los requisitos de manera complementaria: la arquitectura deberá permitir la detección de red sin requerir el despliegue obligatorio de agentes en los endpoints on premise, pudiendo utilizar colectores y, para las funcionalidades específicas que correspondan, agentes compatibles con los sistemas operativos exigidos en el PBC.

Consulta 12 - LOTE 8

Consulta	Fecha de Consulta	29-09-2026

Consulta: El PBC exige con carácter EXIGIDO que la solución incorpore "integración nativa para funciones de bloqueo automático con los proveedores más reconocidos del sector utilizados por la AFD como ser Fortinet, además Palo Alto Networks, Checkpoint y Cisco, entre otros". Según el apartado de Consideraciones Generales, la AFD utiliza soluciones Fortinet para red, comunicaciones, CASB y SASE, sin mencionar Palo Alto Networks, Check Point ni Cisco. Exigir integración nativa con fabricantes que no forman parte de la infraestructura de la AFD no aporta valor funcional al objeto del llamado y restringe innecesariamente la concurrencia. Solicitamos a la Convocante modificar el requisito limitando la integración nativa obligatoria a Fortinet (FortiGate y demás componentes existentes en la AFD) y convirtiendo la integración con otros fabricantes en requisito deseable, o admitiendo la integración mediante API documentada o SOAR.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que el requisito tiene por finalidad garantizar la capacidad de la solución para ejecutar acciones automatizadas de bloqueo y contención mediante su integración con los controles de seguridad utilizados por la AFD.
En consecuencia, la integración con las soluciones Fortinet actualmente utilizadas por la AFD deberá ser soportada por la solución ofertada. Dicha integración podrá realizarse mediante mecanismos nativos y/o mediante APIs documentadas y soportadas oficialmente, siempre que permitan ejecutar las funciones de bloqueo automático y respuesta requeridas en el PBC.
Las referencias a Palo Alto Networks, Check Point, Cisco y otros fabricantes deberán entenderse como ejemplos de interoperabilidad con soluciones reconocidas del mercado y no como la obligación de disponer de integración nativa con todos los fabricantes mencionados.

Consulta 13 - LOTE 8 ITEM 2

Consulta	Fecha de Consulta	29-09-2026

Consulta: En el Ítem 2 se exige con carácter EXIGIDO que la solución permita consultar información de usuarios comprometidos en la dark web que "debe incluir: email, password, teléfono, data leak, última fecha de exposición" con posibilidad de exportación en CSV, así como información de infostealers que incluya "credenciales, cookies" también exportables a CSV. Sin embargo, el apartado de Transferencia internacional, privacidad y tratamiento de datos establece que "La solución no deberá capturar, revelar, almacenar ni exportar contraseñas en texto claro" y que ante credenciales, cookies o tokens comprometidos "deberá aplicar mecanismos de enmascaramiento, acceso restringido, trazabilidad y finalidad exclusiva de remediación". Ambas exigencias son contradictorias. Solicitamos a la Convocante unificar el criterio y aclarar expresamente que el requisito del Ítem 2 se considera cumplido con la presentación de contraseñas y cookies en forma enmascarada, parcial o mediante hash, y que la exportación a CSV podrá realizarse con dichos datos enmascarados, en coherencia con el apartado de privacidad.

Respuesta	Fecha de Respuesta	05-10-2026

Los requisitos establecidos en el Ítem 2 deberán aplicarse en concordancia con las disposiciones de "Transferencia internacional, privacidad y tratamiento de datos" previstas en el PBC.
En consecuencia, la solución deberá permitir identificar y consultar la existencia de credenciales, cookies y/o tokens comprometidos, así como la información asociada requerida en el Ítem 2, aplicando los mecanismos de protección establecidos en el PBC.

Consulta 14 - LOTE 8 EETT INTEGRACIÓN SIEM

Consulta	Fecha de Consulta	29-09-2026

Consulta: El PBC exige con carácter EXIGIDO que la solución tenga "la capacidad de integrarse con soluciones de respuesta a incidentes y/o SIEMs para la gestión de incidentes que posee la AFD", y en Consideraciones Generales se menciona que la AFD posee SPLUNK, Tenable SC y Manage Engine. Solicitamos a la Convocante precisar con cuáles plataformas específicas es obligatoria la integración, la versión y modalidad de despliegue de Splunk (Enterprise on premise o Splunk Cloud) y de ManageEngine (producto específico), y aclarar si la integración mediante syslog, API REST o webhook es aceptada como cumplimiento, o si se exige una aplicación o conector nativo publicado por el fabricante.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que el requisito de integración deberá contemplar las herramientas de seguridad actualmente utilizadas por la AFD mencionadas en el PBC, en la medida en que resulte aplicable a las capacidades objeto del llamado.
A efectos del cumplimiento del requisito, no será obligatorio que la integración se realice exclusivamente mediante una aplicación o conector nativo publicado por el fabricante. Serán aceptados mecanismos de integración estándar soportados por la solución, siempre que permitan el intercambio de la información necesaria para la gestión de incidentes y el cumplimiento de las funcionalidades exigidas en el PBC.
Las versiones, modalidades de despliegue y demás parámetros técnicos específicos de las plataformas de la AFD que resulten necesarios para la implementación serán proporcionados al oferente adjudicado durante la etapa de implementación e integración.

Consulta 15 - LOTE 8 - Ítem 1 - Especificaciones Técnicas

Consulta	Fecha de Consulta	29-09-2026

Consulta: El PBC exige con carácter EXIGIDO que "Las capacidades de detección y respuesta automatizadas ofrecidas por la solución no pueden estar basadas en la creación de playbooks, casos de uso o reglas". No obstante, el mismo pliego exige que la solución muestre "los playbooks para cada tipo de ataque detectado" y que "deberá soportar mecanismos modernos de respuesta automatizada mediante APIs, integración con herramientas de seguridad o controles de red, sin limitarse a un único método de contención". La prohibición absoluta de reglas o playbooks excluye a la gran mayoría de soluciones NDR, XDR y SOAR del mercado, que combinan legítimamente modelos de aprendizaje automático con reglas y playbooks, y resulta contradictoria con los requisitos citados. Solicitamos a la Convocante eliminar dicho requisito o modificarlo en el sentido de que la solución no requiera que la AFD cree manualmente reglas o playbooks para operar, admitiendo soluciones cuyo motor combine inteligencia artificial, analítica de comportamiento, inteligencia de amenazas y reglas o playbooks gestionados por el fabricante.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que el requisito no pretende excluir soluciones que utilicen reglas, casos de uso o playbooks como componentes complementarios de su arquitectura, ni aquellas que incorporen playbooks predefinidos o gestionados por el fabricante.
El alcance del requisito es que las capacidades de detección y respuesta automatizadas exigidas no dependan de la creación y mantenimiento manual de reglas, casos de uso o playbooks por parte de la AFD para su funcionamiento.

Consulta 16 - Capacidad Técnica / Lote 6

Consulta	Fecha de Consulta	29-09-2026

Considerando que el PBC exige, para el Lote 06, al menos un profesional con certificación Fortinet Certified Professional Network y dos profesionales con certificación Fortinet Certified Associate in Cybersecurity, entendemos que estas constituyen exigencias mínimas y que podrán aceptarse certificaciones oficiales vigentes de nivel superior, tales como FCSS o certificaciones NSE 5, NSE 6 o NSE 7 vinculadas con las soluciones ofertadas. Solicitamos confirmar si nuestra interpretación es correcta.
La solicitud se fundamenta en que Fortinet organiza sus certificaciones mediante niveles progresivos y especializaciones tecnológicas, por lo que una certificación superior o específica acredita competencias iguales o mayores para la instalación, configuración y soporte de las soluciones. Su aceptación no reduciría el nivel técnico requerido, sino que ampliaría razonablemente las formas de acreditar la capacidad del personal y favorecería la participación de profesionales calificados.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que la capacidad técnica será evaluada conforme a los requisitos expresamente establecidos en el Pliego de Bases y Condiciones. En tal sentido, para el Lote 06 el oferente deberá acreditar que el personal propuesto cuenta con las certificaciones indicadas en el PBC, vigentes al momento de la presentación de la oferta. En consecuencia, la Convocante realizará la evaluación de conformidad con los requisitos expresamente establecidos en el Pliego de Bases y Condiciones.

Consulta 17 - Lote 6

Consulta	**Fecha de Consulta**	29-09-2026

Respecto del Lote 06 (Fortinet), entendemos que el adjudicatario deberá prestar el servicio de soporte técnico conforme a los niveles de servicio (SLA) detallados en la sección “Descripción por Lote de lo solicitado”. En ese sentido, agradeceremos aclarar el alcance esperado de dicho soporte, particularmente en los siguientes aspectos:
1. Considerando que el pliego establece que “todas las licencias de software deberán incluir las actualizaciones a nuevas versiones del producto ofertado, soporte de funcionamiento, y la posibilidad de escalar problemas al fabricante”, solicitamos confirmar si se espera que el adjudicatario realice durante la vigencia contractual actividades proactivas de actualización, instalación e implementación de nuevas versiones de las soluciones, o si el requisito se limita a garantizar el derecho de acceso a dichas versiones y brindar asistencia ante requerimientos específicos de la AFD vinculados únicamente a soporte de incidencias.
2. En relación con el Nivel 2 de soporte técnico especializado, el cual indica que abordará “incidentes de mayor complejidad, problemas de desempeño y configuraciones avanzadas”, agradeceremos confirmar si las configuraciones avanzadas se encuentran exclusivamente vinculadas a la resolución de incidentes o problemas operativos, o si también contemplan actividades de consultoría, optimización o implementación de nuevas configuraciones requeridas por la AFD de manera proactiva durante la vigencia del contrato.
Lo anterior a efectos de dimensionar correctamente el alcance de los servicios profesionales asociados a la propuesta técnica y económica.

Respuesta	**Fecha de Respuesta**	05-10-2026

Se aclara que el servicio de soporte técnico correspondiente al Lote 06 deberá prestarse conforme a los niveles de servicio (SLA) establecidos en el PBC y comprenderá el soporte necesario para mantener el correcto funcionamiento de las soluciones contratadas durante la vigencia de la licencia.
1. Respecto de las actualizaciones y nuevas versiones, el requisito implica que las licencias y suscripciones ofertadas deberán mantener vigente el derecho de acceso a actualizaciones, parches, correcciones y nuevas versiones liberadas por el fabricante durante el periodo de suscripción, así como la posibilidad de escalar al fabricante los incidentes que así lo requieran.
La instalación o implementación de actualizaciones y nuevas versiones por parte del adjudicatario se realizará cuando resulte necesaria para la resolución de incidentes, corrección de vulnerabilidades, mantenimiento del correcto funcionamiento de la solución o cuando sea expresamente requerida y coordinada por la AFD. El requisito no deberá interpretarse como una obligación de ejecutar automáticamente toda nueva versión liberada por el fabricante, debiendo cualquier actualización que pueda afectar el ambiente productivo ser previamente evaluada y coordinada con la AFD.
2. Respecto del Nivel 2 de soporte técnico especializado, las "configuraciones avanzadas" comprenden aquellas actividades técnicas necesarias para el diagnóstico y resolución de incidentes, problemas de desempeño, errores de configuración y ajustes requeridos para restablecer o mantener el funcionamiento adecuado de las soluciones contratadas.
Asimismo, durante la vigencia de la suscripción podrán requerirse ajustes y optimizaciones razonables sobre las configuraciones existentes cuando sean necesarios para mantener la seguridad, estabilidad y correcto funcionamiento de las soluciones. Por último, se aclare que el PBC no indica el servicio de soporte recurrente proyectos independientes de consultoría.

Consulta 18 - Lote 6

Consulta	Fecha de Consulta	29-09-2026

Para el Lote 6, favor especificar el alcance esperado del soporte técnico que deberá proveer el adjudicatario durante la vigencia de la suscripción. Solicitamos aclarar, entre otros aspectos:
o Requerimiento de soporte remoto y/o presencial.
o Cantidad aproximada de tickets mensuales
o Vigencia

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que el soporte técnico correspondiente al Lote 06 deberá cubrir las soluciones objeto del lote durante toda la vigencia de las respectivas suscripciones, conforme a los niveles de servicio (SLA) establecidos en el PBC.
El soporte deberá contemplar asistencia técnica remota para la atención, diagnóstico, seguimiento y resolución de incidentes, problemas de funcionamiento, desempeño y configuraciones relacionadas con las soluciones contratadas, incluyendo, cuando corresponda, el escalamiento de casos al fabricante.
El adjudicatario deberá atender los requerimientos que se presenten durante la vigencia del servicio y que se encuentren comprendidos dentro del alcance del soporte técnico establecido en el PBC, respetando los tiempos y niveles de servicio definidos.
La vigencia del soporte deberá corresponder al periodo establecido para cada solución, licencia o suscripción del Lote 06. Durante dicho periodo deberán mantenerse disponibles los servicios de soporte, el derecho de acceso a actualizaciones y nuevas versiones conforme a las condiciones del fabricante, y la posibilidad de escalamiento de incidentes cuando corresponda.

Consulta 19 - Lote 3

Consulta	Fecha de Consulta	29-09-2026

En el Lote 3 se solicita la provisión de licencias Microsoft 365 Copilot Business. Sin embargo, conforme al esquema oficial de licenciamiento de Microsoft, dicho producto requiere como prerrequisito determinadas suscripciones de la familia Microsoft 365 Business y no resulta compatible con usuarios que dispongan de licencias base Office 365 E3. Considerando que la AFD utiliza actualmente servicios de Office 365, solicitamos confirmar la corrección del requerimiento, dado que para usuarios con licencias Office 365 E3 el producto compatible corresponde a Microsoft Copilot (licencia empresarial) y no a Microsoft Copilot Business. Solicitamos se rectifique la denominación del producto requerido a efectos de asegurar la compatibilidad con el esquema oficial de licenciamiento de Microsoft. Ref: https://learn.microsoft.com/en-us/microsoft-365/copilot/microsoft-365-copilot-licensing#microsoft-copilot-licenses

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que la descripción del Lote 3 corresponde a requisitos mínimos solicitados, en consecuencia, el oferente deberá tener en cuenta al momento de la preparación de su oferta la garantía de su correcta instalación, configuración y operación, conforme a lo establecido en las Especificaciones Técnicas.

Consulta 20 - Lote 3

Consulta	Fecha de Consulta	29-09-2026

El pliego establece para todos los lotes la responsabilidad del adjudicatario respecto de instalación, configuración, operación, actualizaciones y soporte durante toda la vigencia de la suscripción. Para el caso específico del Lote 3, solicitamos confirmar si el alcance requerido corresponde exclusivamente y solamente a la provisión y asignación de las licencias Microsoft Copilot o si se prevé adicionalmente la realización de actividades de configuración avanzada, adopción, capacitación, gobierno, integración o servicios profesionales asociados a la plataforma. En caso afirmativo, favor detallar el alcance esperado, vigencia y la cantidad de horas solicitadas a efectos de una correcta elaboración de la oferta.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que el alcance del Lote 3 es el establecido en las Especificaciones Técnicas. Comprende la provisión de las suscripciones a nombre de la AFD, su asignación en el entorno de la Convocante y el soporte técnico durante toda la vigencia de la suscripción, conforme a los requisitos y niveles de servicio establecidos para todos los lotes.

Consulta 21 - Lote 3

Consulta	Fecha de Consulta	29-09-2026

Para el Lote 3, favor especificar el alcance esperado del soporte técnico que deberá proveer el adjudicatario durante la vigencia de la suscripción. Solicitamos aclarar, entre otros aspectos:
o Alcance funcional esperado del soporte.
o Requerimiento de soporte remoto y/o presencial.
o Niveles de Servicio (SLA)
o Cantidad aproximada de tickets mensuales
o Vigencia
La información resulta necesaria para dimensionar adecuadamente el esfuerzo de servicios requerido y garantizar condiciones comparables entre todos los oferentes.

Respuesta	Fecha de Respuesta	05-10-2026

El soporte técnico del Lote 3 es el establecido en las Especificaciones Técnicas para todos los lotes, que definen su alcance, la forma de reportar incidentes y los niveles de servicio (SLA), durante los 12 meses de vigencia de la suscripción, por tanto el oferente deberá tener en cuenta las condiciones citadas del PBC para la preparación de su oferta.

Consulta 22 - Cierre automatizado de incidentes (Lote 8. Item1)

Consulta	Fecha de Consulta	29-09-2026

En el Ítem 1 del Lote 8, el pliego describe como EXIGIDO que la solución realice "el cierre automatizado de los incidentes reportados" e itere automáticamente sobre cada incidente hasta su cierre o escalamiento a un operador. Entendemos que se trata de una capacidad requerida desde el inicio de la suscripción. La mención "a futuro, con la incorporación de otro producto del mismo fabricante", entendemos que se refiere a acciones de respuesta adicionales sobre firewalls, EDR o DNS, etc. y no a la gestión y el cierre de incidentes. Se solicita confirmar que el componente que realiza el cierre automatizado y el escalamiento debe estar incluido y operativo durante los 12 meses del contrato.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que, para el alcance de la presente contratación, no se requiere la incorporación de módulos o productos adicionales a la solución objeto del Ítem 1 del Lote 8 para implementar capacidades avanzadas de iteración autónoma y cierre automatizado de incidentes.
La solución ofertada deberá contar, durante los 12 meses de vigencia contractual, con las capacidades de detección, gestión y respuesta a incidentes contempladas dentro del alcance de la suscripción requerida, incluyendo las integraciones y mecanismos de respuesta previstos en el PBC.
La referencia a capacidades que permitan iterar de manera automatizada sobre una incidencia hasta su cierre o escalamiento deberá entenderse como una capacidad de evolución o escalabilidad futura, susceptible de ser incorporada mediante componentes o productos adicionales, y no como la obligación de incluir en la presente contratación una licencia o módulo adicional que no forme parte del alcance establecido, siempre que se cumplan las funcionalidades de detección y respuesta establecidas para la solución objeto del Ítem 1 del Lote 8.

Consulta 23 - Sobre la acreditación de autorización del canal

Consulta	Fecha de Consulta	29-09-2026

El PBC establece que “El Oferente deberá acreditar estar autorizado para la comercialización de la solución de la marca ofertada en el territorio paraguayo mediante documento emitido por la Marca y/o los canales autorizados correspondientes”. Se solicita pueda acreditarse dicho requisito mediante una Declaración Jurada del Oferente, en la cual manifieste su condición de canal autorizado y su capacidad para proveer, instalar, configurar y brindar soporte de la solución ofertada en tiempo y forma.

Respuesta	Fecha de Respuesta	05-10-2026

Se aclara que dicha condición se acreditará unicamente conforme al formato requerido en el apartado de formularios del PBC, y deberá acreditar la cadena de autorizaciones, hasta el fabricante, productor o prestador de servicios.Cada autorización debe indicar a que ítem corresponde.

Consulta 24 - Visualización de Contraseñas - Lote 8

Consulta	Fecha de Consulta	29-09-2026

Lote 8, Ítem 2, el pliego exige como EXIGIDO que la información de los usuarios de la AFD comprometidos en la dark web incluya "email, password, teléfono, data leak, última fecha de exposición", con posibilidad de exportarla en formato CSV. Además, exige la evidencia de la data exfiltrada en data leaks y las credenciales asociadas a infostealers. Entendemos que esta información es necesaria para que la AFD valide si la credencial expuesta sigue vigente o fue reutilizada y ejecute la remediación correspondiente.
Por su parte, el apartado del Ítem 1 "Transferencia internacional, privacidad y tratamiento de datos" del mismo lote establece que, al identificar credenciales comprometidas, la solución deberá aplicar mecanismos de enmascaramiento, acceso restringido, trazabilidad y finalidad exclusiva de remediación.
Entendemos que ambos requisitos se cumplen de forma armónica cuando la contraseña se visualiza en la consola únicamente por usuarios autorizados de la AFD, con control de acceso por roles, doble factor de autenticación y trazabilidad, con finalidad exclusiva de remediación, y se presenta enmascarada en los reportes en PDF. Se solicita confirmar dicha interpretación.

Respuesta	Fecha de Respuesta	05-10-2026

Ambos requisitos deberán entenderse y aplicarse de manera complementaria. La solución deberá permitir a los usuarios debidamente autorizados de la AFD acceder, desde la consola, a la información necesaria sobre las credenciales comprometidas, incluida la contraseña cuando esta forme parte de la evidencia obtenida de data leaks o infostealers y resulte necesaria para las actividades de validación y remediación.
En los reportes generados en formato PDF, las contraseñas deberán presentarse enmascaradas, evitando su exposición innecesaria.
Respecto de la exportación en formato CSV, esta deberá mantener las medidas de protección y privacidad establecidas en el PBC, por lo que las contraseñas deberán exportarse en forma enmascarada y no en texto claro, conforme a lo establecido en el PBC.

Consulta 25 - Experiencia con relación a los ítems ofertados

Consulta	Fecha de Consulta	29-09-2026

En el apartado Experiencia Técnica punto 1 , se solicita demostrar experiencia con relación a los ítems ofertados dentro de los últimos cinco años (2021, 2022, 2023, 2024 y 2025), mediante facturaciones, contratos o actas de recepción final de organizaciones públicas o privadas. Al respecto, se solicita que, para el Lote 8 – Ítems 1 y 2, sea aceptada como experiencia válida la provisión, venta, implementación, suscripción y/o licenciamiento de soluciones de ciberseguridad en general, considerando que este tipo de soluciones forman parte de un mismo ámbito tecnológico y requieren capacidades similares para su provisión, implementación y soporte.

Respuesta	Fecha de Respuesta	05-10-2026

Respecto a la consulta formulada, se aclara que la experiencia requerida será evaluada en relación con la naturaleza y el ámbito tecnológico de los servicios ofertados para cada lote o ítem. En ese sentido, para el Lote 08 podrán ser admitidas experiencias relacionadas con la provisión, venta, implementación, suscripción, licenciamiento y/o soporte de soluciones de ciberseguridad, siempre que las documentaciones presentadas permitan verificar razonablemente la vinculación de la experiencia acreditada con el objeto de contratación solicitado