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 488164 - LPN 09-26 RENOVACIÓN DE LICENCIAS DE ANTIVIRUS Y PROTECCION DE ESTACIONES DE TRABAJO

Consulta 1 - Aclaración sobre ejecución remota de scripts y comandos

Consulta	**Fecha de Consulta**	06-10-2026

En relación con el requisito que establece que la solución deberá permitir la creación de scripts de ejecución en Python, VBScript y/o la ejecución de comandos de sistemas operativos de manera remota, solicitamos confirmar que el requisito podrá considerarse cumplido cuando la solución permita la ejecución remota de comandos del sistema operativo y de scripts mediante lenguajes soportados por la plataforma, tales como PowerShell, Bash u otros equivalentes, manteniendo las capacidades requeridas de investigación, administración y respuesta remota.

Respuesta	**Fecha de Respuesta**	07-11-2026

Se aclara que el requisito se tendrá por cumplido cuando la solución permita la ejecución remota de comandos del sistema operativo y/o la creación y ejecución de scripts mediante lenguajes soportados por la plataforma (tales como Python, VBScript, PowerShell, Bash u otros equivalentes), manteniendo las capacidades de investigación, administración y respuesta remota exigidas. Ello en razón de que el propio requisito admite la ejecución de comandos del sistema operativo ("y/o") y de que las Especificaciones Técnicas deben evitar condiciones que limiten la participación a un fabricante en particular, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 2 - Aclaración sobre colectores personalizados para cacería de amenazas

Consulta	**Fecha de Consulta**	06-10-2026

Respecto al requisito que establece que la solución deberá permitir la creación de colectores de información de manera personalizada para realizar búsquedas en tiempo real y procesos de cacería de amenazas, solicitamos aclarar si podrá considerarse cumplido mediante funcionalidades equivalentes que permitan realizar consultas, búsquedas y recopilación personalizada de telemetría y artefactos de seguridad sobre los endpoints desde la plataforma centralizada, sin requerir necesariamente la utilización de un componente denominado específicamente “colector”.

Respuesta	**Fecha de Respuesta**	07-11-2026

Se aclara que el requisito se tendrá por cumplido mediante funcionalidades equivalentes que permitan, desde la plataforma centralizada, realizar consultas, búsquedas y recopilación personalizada de telemetría y artefactos de seguridad sobre los endpoints, en tiempo real y para la cacería de amenazas, sin que sea necesaria la existencia de un componente denominado específicamente "colector". Ello en razón de que lo exigido es la capacidad funcional y no una denominación comercial, conforme a las Especificaciones Técnicas, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 3 - Aclaración sobre sistemas operativos de los activos a proteger

Consulta	Fecha de Consulta	06-10-2026

A efectos de dimensionar correctamente la solución y validar su compatibilidad, solicitamos indicar los sistemas operativos y versiones actualmente utilizados en las estaciones de trabajo y servidores incluidos en el alcance, detallando en lo posible las cantidades correspondientes a Windows, Linux y macOS, así como la existencia y cantidad de sistemas operativos obsoletos o fuera de soporte del fabricante.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que el Instituto no suministra inventario de sistemas operativos ni de versiones, por resguardo institucional y no constituir un requisito necesario para la preparación de las ofertas. Corresponde al oferente garantizar que la solución ofertada cumpla con lo requerido en las Especificaciones Técnicas del Ítem 1 para 5.000 (cinco mil) estaciones de trabajo y 1.000 (mil) servidores, con los sistemas operativos allí solicitados, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 4 - Aclaración sobre cantidad total de equipos y servidores

Consulta	Fecha de Consulta	06-10-2026

Solicitamos aclarar la composición exacta de las 6.000 licencias requeridas, considerando que en las Especificaciones Técnicas se mencionan 6.000 estaciones de trabajo para las funcionalidades de antimalware, control de dispositivos, control de navegación y HIPS, mientras que para EDR se establecen 5.000 estaciones de trabajo y 1.000 servidores. Favor confirmar si el universo total a proteger corresponde a 6.000 activos, distribuidos en 5.000 estaciones de trabajo y 1.000 servidores, o si los 1.000 servidores son adicionales a las 6.000 estaciones de trabajo.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que el universo total a licenciar en el Ítem 1 es de 6.000 (seis mil) equipos, compuesto por 5.000 (cinco mil) estaciones de trabajo y 1.000 (mil) servidores, y dicha composición aplica a todas las funcionalidades requeridas en el ítem. Los 1.000 (mil) servidores no son adicionales a las estaciones de trabajo. Ello en concordancia con la cantidad de 6.000 licencias establecida para el ítem y con la composición fijada para los agentes de protección EDR (5.000 estaciones de trabajo y 1.000 servidores), por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 5 - Eliminar programas remotamente mediante PowerShell/scripts

Consulta	Fecha de Consulta	06-10-2026

Sírvase confirmar que el requisito de eliminar programas de manera remota podrá ser cumplido mediante la ejecución remota de scripts o comandos desde la consola de administración, incluyendo PowerShell, que permitan realizar la desinstalación del software.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que el requisito de eliminar programas de manera remota se tendrá por cumplido cuando, desde la consola de administración, la solución permita ejecutar remotamente scripts o comandos (incluyendo PowerShell) que realicen la desinstalación del software, atendiendo que lo exigido es la capacidad funcional de remediación remota y no un mecanismo específico, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 6 - Aclaración sobre almacenamiento histórico de registros por un año

Consulta	Fecha de Consulta	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, se establece que: “La solución debe tener la capacidad de permitir búsqueda de información por un periodo mínimo de 90 días, con la opción de exportar o almacenar en frío (cold storage) los registros históricos por hasta 1 año para fines de auditoría y cumplimiento”.

Considerando que el propio requerimiento contempla la exportación de los registros como alternativa para su conservación histórica, solicitamos a la Convocante confirmar que el almacenamiento por hasta un año podrá realizarse mediante la integración de la solución ofertada con un SIEM o repositorio externo institucional.

En consecuencia, entendemos que no será obligatorio mantener durante un año toda la información dentro de la consola EDR, siempre que la solución permita su exportación o integración y se garantice su conservación por el plazo requerido. ¿Es correcta nuestra interpretación?

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que es la correcta su interpretación. Las Especificaciones Técnicas establecen que la solución debe permitir la búsqueda de información por un período mínimo de 90 días, "con la opción de exportar o almacenar en frío (cold storage)" los registros históricos por hasta 1 año. En consecuencia, la conservación por hasta un año podrá realizarse mediante la exportación o integración de la solución con un SIEM o repositorio externo institucional, sin que sea obligatorio mantener la totalidad de la información dentro de la consola EDR, siempre que se garantice su conservación por el plazo requerido, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 7 - Aclaración sobre la cantidad de estaciones de trabajo y servidores

Consulta	Fecha de Consulta	07-10-2026

En las Especificaciones Técnicas del Ítem 1 se requieren agentes de antimalware, control de dispositivos, control de navegación y HIPS "para 6.000 estaciones de trabajo", y agentes de protección EDR "para 5.000 estaciones de trabajo y 1000 servidores".
Al respecto, solicitamos a la Convocante confirmar si es correcto nuestro entendimiento de que el total de equipos a licenciar en el Ítem 1 es de 6.000 (seis mil), compuesto por 5.000 (cinco mil) estaciones de trabajo y 1.000 (mil) servidores, y que dicha composición aplica a todas las funcionalidades requeridas en el ítem.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que es correcto su entendimiento. Se confirma que el universo total a licenciar en el Ítem 1 es de 6.000 (seis mil) equipos, compuesto por 5.000 (cinco mil) estaciones de trabajo y 1.000 (mil) servidores, y dicha composición aplica a todas las funcionalidades requeridas en el ítem. Ello en concordancia con la cantidad de 6.000 licencias establecida para el ítem y con la composición fijada para los agentes de protección EDR, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 8 - Aclaración sobre eliminación y modificación de llaves de registro

Consulta	Fecha de Consulta	07-10-2026

Respecto al requisito "La solución debe tener la capacidad de eliminar y modificar llaves de registro", solicitamos confirmar si es correcto nuestro entendimiento de que el mismo se considera cumplido cuando la solución permite realizar dichas acciones de forma remota desde la consola centralizada, mediante una sesión de respuesta remota sobre el equipo con ejecución de comandos del sistema operativo (por ejemplo, reg.exe o PowerShell), sin requerir necesariamente una acción gráfica específica con esa denominación.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que es correcto su entendimiento. El requisito se considerará cumplido cuando la solución permita eliminar y modificar llaves de registro de forma remota desde la consola centralizada, mediante una sesión de respuesta remota sobre el equipo con ejecución de comandos del sistema operativo (por ejemplo, reg.exe o PowerShell), sin requerir necesariamente una acción gráfica específica con esa denominación, por cuanto lo exigido es la capacidad funcional, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 9 - Aclaración sobre requisitos de riesgo interno, recomendaciones de políticas y security posture

Consulta	Fecha de Consulta	07-10-2026

Respecto a los requisitos (i) "La solución deberá proveer elementos tecnológicos que notifiquen proactivamente respecto al riesgo interno basado en la comparación del panorama global de amenazas con los sistemas de contramedidas locales", (ii) "La solución deberá proveer recomendaciones al analista respecto a políticas enfocadas a fortalecer las capacidades y contramedidas contra campañas y amenazas que puedan afectar a la organización en particular" y (iii) "La herramienta debe tener la capacidad de realizar un security posture para determinar los equipos que estén desprotegidos ante amenazas mundiales", solicitamos confirmar si es correcto nuestro entendimiento de que se consideran cumplidos cuando la solución, desde la misma consola:
evalúa el estado de protección y la configuración de políticas de los equipos frente a las recomendaciones del fabricante, identificando los equipos sin protección, con protección incompleta o con configuraciones débiles;
contrasta dicha información con la inteligencia de amenazas global del fabricante; y
proporciona al analista recomendaciones de ajuste de políticas y contramedidas;
sin que sea necesario que dichas funcionalidades se presenten como un módulo con una denominación específica.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que es correcto su entendimiento. Los requisitos referidos al riesgo interno, a las recomendaciones de políticas y al security posture se tendrán por cumplidos cuando la solución, desde la misma consola: a) evalúe el estado de protección y la configuración de políticas de los equipos frente a las recomendaciones del fabricante, identificando equipos sin protección, con protección incompleta o con configuraciones débiles; b) contraste dicha información con la inteligencia de amenazas global del fabricante; y c) proporcione al analista recomendaciones de ajuste de políticas y contramedidas; sin que sea necesario que tales funcionalidades se presenten como un módulo con una denominación específicas, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 10 - Aclaración sobre la admisión de productos de otro fabricante como oferta principal

Consulta	Fecha de Consulta	07-10-2026

En el Ítem 1 la descripción indica "Licencia Trellix MVISION Standard, cantidad 6.000, upgrade a la versión MVISION Protect Plus EDR", y el llamado se denomina "Renovación de licencias de antivirus y protección de estaciones de trabajo". Por otra parte:
En la sección "Ofertas Alternativas", el PBC establece "No Aplica", y define que una oferta alternativa "se configura necesariamente con la presentación de la oferta principal [...] y, de manera separada e independiente, una propuesta alternativa".
En las Especificaciones Técnicas del mismo ítem figura, como requisito EXIGIDO, la fila "Oferta Alternativa": "El oferente podrá presentar como oferta un producto que cumpla con las especificaciones técnicas requeridas o superiores. La plataforma alternativa ofertada debe estar valorada entre las soluciones líderes del cuadrante Gartner".
El propio PBC (Especificaciones Técnicas "CPS") dispone que "se deberán evitar referencias a marcas, números de catálogos u otros detalles que limiten los materiales o artículos a un fabricante en particular. Cuando sean inevitables dichas descripciones, siempre deberá estar seguida de expresiones tales como 'o sustancialmente equivalente' u 'o por lo menos equivalente'".
Atendiendo a lo expuesto, solicitamos a la Convocante confirmar si es correcto nuestro entendimiento de que:
La mención a la marca y productos Trellix MVISION en la descripción del ítem es referencial de la plataforma actualmente instalada, y debe entenderse seguida de la expresión "o sustancialmente equivalente".
Se admitirá, como oferta principal y única, la provisión de licencias de un producto de otro fabricante que cumpla o supere la totalidad de las Especificaciones Técnicas y que esté valorado como Líder en el cuadrante de Gartner, incluyendo la implementación y migración previstas en el PBC; y que dicha oferta no será considerada "oferta alternativa" en los términos de la sección "Ofertas Alternativas" del PBC, ni requerirá la presentación adicional de una oferta de la marca Trellix.
El cuadrante de Gartner aplicable es el Magic Quadrant for Endpoint Protection Platforms, en su edición más reciente publicada a la fecha de presentación de ofertas.
La presente aclaración se solicita a fin de evitar interpretaciones divergentes en la etapa de evaluación, en resguardo de los principios de igualdad y libre competencia (Art. 4, Ley N° 7021/22), considerando que la aclaración formará parte integrante del pliego conforme a la cláusula "Respuestas y aclaraciones" del PBC.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que es correcto su entendimiento. Se aclara que: a) la mención a "Licencia Trellix MVISION Standard ... upgrade a la versión MVISION Protect Plus EDR" tiene carácter meramente referencial de la plataforma actualmente instalada; b) se admitirá, como oferta principal, la provisión de licencias de un producto de otro fabricante que cumpla o supere la totalidad de las Especificaciones Técnicas y cuya plataforma esté valorada entre las soluciones líderes del cuadrante Gartner, incluyendo la implementación y migración previstas, sin que ello constituya "oferta alternativa" en los términos de la sección "Ofertas Alternativas" del Pliego ni requiera la presentación de una oferta de la marca mencionada; y c) el cuadrante aplicable es el Magic Quadrant for Endpoint Protection Platforms, en su edición más reciente publicada a la fecha de presentación de ofertas. La presente aclaración se realiza en resguardo de los principios de igualdad y libre competencia establecidos en el Art. 4 de la Ley N° 7021/22, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 11 - Solicitud de ajuste del período mínimo de búsqueda de información

Consulta	Fecha de Consulta	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, se establece que: “La solución debe tener la capacidad de permitir búsqueda de información por un periodo mínimo de 90 días, con la opción de exportar o almacenar en frío (cold storage) los registros históricos por hasta 1 año para fines de auditoría y cumplimiento”.

A fin de admitir soluciones que disponen de una retención nativa menor, pero que permiten conservar la información mediante mecanismos de integración y exportación, solicitamos a la Convocante considerar como válido un período mínimo de búsqueda de 30 días dentro de la solución EDR, siempre que esta permita exportar o integrar los eventos con un SIEM o repositorio externo institucional para conservar y consultar la información correspondiente al período restante.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, al respecto, esta Convocante aclara que no corresponde reducir el período mínimo de búsqueda, por cuanto el plazo de 90 días constituye una condición mínima establecida en las Especificaciones Técnicas, definida en función de las necesidades de investigación y respuesta a incidentes de la Institución. La exportación o integración con herramientas externas está prevista únicamente como opción para la conservación de los registros históricos por hasta 1 año y no sustituye la capacidad de búsqueda mínima exigida dentro de la solución, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 12 - Aclaración sobre modelo híbrido de administración y operación EDR

Consulta	Fecha de Consulta	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, dentro del apartado Administración, se requiere una “Solución de Administración centralizada y unificada” y se indica que: “La solución debe ofrecer uno de estos modelos de gestión: On-Premises, IaaS o SaaS”.

Solicitamos a la Convocante confirmar que el requerimiento en cuestión implica que, en cualquiera de los modelos ofertados, siempre sea posible que la administración y gestión de los agentes Endpoint sea posible realizarse desde la consola On-Premises instalada en la infraestructura de la Institución, permitiendo que la telemetría y las capacidades de detección, investigación y respuesta de EDR operen mediante una plataforma en la nube.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, al respecto, esta Convocante aclara que las Especificaciones Técnicas establecen expresamente que "La solución debe ofrecer uno de estos modelos de gestión: On-Premises, IaaS o SaaS". En consecuencia, no corresponde exigir que, en cualquiera de los modelos, la administración se realice desde una consola On-Premises instalada en la infraestructura de la Institución, ya que ello implicaría incorporar una condición no prevista en las bases, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 13 - Aclaración sobre control de dispositivos periféricos multiplataforma

Consulta	Fecha de Consulta	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, dentro del apartado Antivirus Endpoint, se requieren “Agentes de Control de Dispositivos para 6.000 estaciones de trabajo” y agentes de protección para estaciones con sistemas operativos Windows, MAC y Linux.

Solicitamos a la Convocante confirmar que la capacidad de control de dispositivos deberá permitir administrar y aplicar políticas de habilitación, restricción o bloqueo sobre dispositivos USB y otros periféricos en los equipos protegidos, contemplando los sistemas operativos Windows, macOS y Linux incluidos en el alcance.

¿Es correcta nuestra interpretación?

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que es correcta la interpretación en cuanto a la funcionalidad requerida. El control de dispositivos deberá aplicarse sobre las estaciones de trabajo protegidas, debiendo la solución permitir administrar y aplicar, desde la consola centralizada, políticas de habilitación, restricción o bloqueo sobre dispositivos USB y otros periféricos, como mínimo en los equipos con sistemas operativos Windows y macOS, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 14 - Aclaración sobre capacidades forenses nativas

Consulta	Fecha de Consulta	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, se establece que: “La solución deberá brindar la capacidad de realizar búsquedas a largo plazo de objetos particulares para el análisis forense de amenazas”.

Solicitamos a la Convocante confirmar que las capacidades forenses requeridas comprenden la adquisición remota y bajo demanda de evidencia desde los endpoints, incluyendo archivos, información de procesos, memoria, adquisiciones de disco completas o parciales y colecciones de triage, con posibilidad de seleccionar múltiples endpoints y ejecutar las adquisiciones de manera centralizada.

Asimismo, solicitamos confirmar que estas capacidades deberán ser nativas de la solución ofertada y no depender de herramientas forenses externas o de terceros. ¿Es correcta nuestra interpretación?

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, al respecto, esta Convocante aclara que el requisito exige "la capacidad de realizar búsquedas a largo plazo de objetos particulares para el análisis forense de amenazas" y será evaluado en esos términos. Las modalidades específicas de adquisición de evidencia planteadas en la consulta no forman parte del alcance establecido en las Especificaciones Técnicas, y su incorporación implicaría una modificación de las bases que la Convocante no considera necesaria para satisfacer la necesidad de la contratación, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 15 - Aclaración sobre inteligencia de amenazas por industria y país

Consulta	**Fecha de Consulta**	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, se requiere que la solución provea información sobre campañas de amenazas globales en tiempo real, pueda discriminar aquellas específicas para la industria y el país de la organización, anticipe amenazas emergentes y proporcione recomendaciones para fortalecer las capacidades y contramedidas aplicables.

Solicitamos a la Convocante confirmar que estas capacidades deberán estar integradas nativamente en la solución ofertada y permitir relacionar las campañas identificadas con el nivel de exposición de la organización, generando recomendaciones específicas de mitigación o ajuste de las políticas de protección de los endpoints.

¿Es correcta nuestra interpretación?

Respuesta	**Fecha de Respuesta**	07-11-2026

Se aclara que, es correcta su interpretación en cuanto a que dichas capacidades deberán formar parte de la solución ofertada. Las Especificaciones Técnicas exigen que la solución provea información respecto a las campañas de amenazas globales en tiempo real, siendo capaz de discriminar aquellas que son específicas para la industria a la que pertenece la organización, así como el país; que tenga la capacidad de anticipar amenazas emergentes y priorizarlas en función de su impacto potencial en el entorno de la organización; y que provea recomendaciones al analista respecto a políticas enfocadas a fortalecer las capacidades y contramedidas. En consecuencia, los requisitos se tendrán por cumplidos cuando la solución, desde la misma consola: a) provea inteligencia de amenazas global del fabricante, actualizada de forma continua; b) permita discriminar las campañas y amenazas por industria y por país o región; c) relacione dicha inteligencia con el entorno de la organización, a fin de identificar las amenazas que puedan afectarla; y d) proporcione al analista recomendaciones de ajuste de políticas de protección de los endpoints y de contramedidas. No se exige una metodología específica de correlación ni que tales funcionalidades se presenten como un módulo con una denominación específica, por cuanto lo exigido es la capacidad funcional, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 16 - Solicitud de técnicos certificados por el fabricante como requisito de capacidad técnica

Consulta	Fecha de Consulta	07-10-2026

En los requisitos de Capacidad Técnica se exige que el oferente cuente con "al menos 2 técnicos radicados en el país con experiencia en el uso del software para la instalación/configuración y capacitación". Por su parte, las Especificaciones Técnicas (fila "Servicios") exigen que el soporte técnico local y/o remoto sea "realizado por profesionales debidamente certificados por el fabricante de la herramienta, por un periodo de 2 (dos) años", en modalidad 24x7x365 con tiempo máximo de respuesta de 1 hora para incidentes críticos (ej. brotes de ransomware, infecciones masivas o indisponibilidad de la consola de administración).
Sin embargo, los requisitos de capacidad técnica no prevén verificar, en la etapa de evaluación, que el oferente cuente efectivamente con dichos profesionales certificados.
Considerando:
la dimensión del proyecto: 6.000 licencias que abarcan las estaciones de trabajo y los servidores institucionales;
su criticidad: implementación, configuración y migración en un plazo de 90 días sobre la plataforma de seguridad en producción, y aplicación de los controles de seguridad operativa de la sección 2 de las Especificaciones Técnicas (hardening, gestión de vulnerabilidades, de cambios y de incidentes);
el nivel de servicio exigido (24x7x365 con respuesta en 1 hora), que requiere contar con más de un profesional certificado para garantizar la continuidad del soporte ante la ausencia de uno de ellos;
solicitamos a la Convocante evaluar e incorporar mediante adenda que, de los técnicos requeridos, al menos 2 (dos) cuenten con certificación técnica vigente emitida por el fabricante de la solución ofertada, a ser acreditada con copia de los certificados junto con el listado y currículum vitae del plantel técnico.
Lo solicitado guarda coherencia con lo ya exigido en las Especificaciones Técnicas y con la exigencia de solvencia técnica del oferente (Art. 19, Ley N° 7021/22), y se aplica por igual a todos los oferentes, cualquiera sea la marca ofertada.
De no considerarse procedente su incorporación como requisito de la oferta, solicitamos indicar en qué etapa y con qué documentación se verificará el cumplimiento de la exigencia de "profesionales debidamente certificados por el fabricante" prevista en las Especificaciones Técnicas.

Respuesta	Fecha de Respuesta	07-11-2026

El oferente deberá remitirse al Pliego de Bases y Condiciones Ultima versión.

Consulta 17 - Aclaración sobre colectores y scripts personalizados

Consulta	Fecha de Consulta	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, se establece que la solución deberá permitir la creación de colectores de información personalizados para búsquedas en tiempo real y procesos de cacería de amenazas, así como soportar la creación de scripts y la ejecución remota de comandos de sistemas operativos.

Solicitamos a la Convocante confirmar que la solución deberá permitir crear y administrar de manera centralizada colectores o scripts personalizados, mediante los cuales el equipo de seguridad pueda definir la información forense que será recopilada remotamente desde los endpoints, sin depender de herramientas externas.

Asimismo, solicitamos confirmar que estos colectores podrán ejecutarse bajo demanda sobre endpoints Windows, macOS y Linux y que la información obtenida quedará disponible para su posterior análisis. ¿Es correcta nuestra interpretación?

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que es correcta la interpretación. La solución deberá permitir crear y administrar de manera centralizada, desde la consola, consultas, colectores o scripts personalizados mediante los cuales el equipo de seguridad pueda definir la información que será recopilada remotamente desde los endpoints, sin depender de herramientas externas. Dichas consultas o scripts deberán poder ejecutarse bajo demanda sobre endpoints Windows, macOS y Linux, y la información obtenida deberá quedar disponible en la plataforma para su posterior análisis. Lo exigido es la capacidad funcional, por lo que no es necesario que el componente se denomine específicamente "colector", y la creación de scripts podrá realizarse en Python, VBScript u otros lenguajes soportados por la plataforma (tales como PowerShell o Bash), o mediante la ejecución remota de comandos del sistema operativo, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 18 - Incorporación de certificaciones ISO/IEC 27001 e ISO 9001:2015 como requisito de capacidad técnica.

Consulta	**Fecha de Consulta**	07-10-2026

Se observa que, en los requisitos de capacidad técnica del oferente, el PBC solicita autorización del fabricante, antigüedad mínima de 2 años en el rubro de software, acreditación de condiciones de instalación, configuración y soporte, y al menos 2 técnicos radicados en el país, sin exigir al oferente certificación alguna de su sistema de gestión de seguridad de la información ni de su sistema de gestión de calidad.
Se formula la presente solicitud con base en lo siguiente:
Justificación del propio PBC. En "Identificación de la unidad solicitante y justificaciones", la Convocante declara que la contratación responde a una "necesidad técnica impostergable para preservar la estabilidad y seguridad del entorno tecnológico institucional", y que las especificaciones responden a criterios de "necesidad, proporcionalidad y adecuación tecnológica, orientados a preservar la continuidad del servicio, la confidencialidad de la información institucional y la mitigación efectiva de riesgos de ciberseguridad".
Coherencia con las Especificaciones Técnicas. La sección 2 exige controles de seguridad operativa alineados a CIS Controls, NIST CSF, NIST SP 800-40 y MITRE ATT&CK (MFA, RBAC, trazabilidad inalterable, cifrado, hardening documentado, gestión de vulnerabilidades, cambios e incidentes con evidencias), y el ítem exige soporte local y/o remoto 24x7x365 canalizado por mesa de ayuda, e instalación, configuración y migración en 90 días. El oferente adjudicado operará sobre la plataforma de seguridad que protege la totalidad de los equipos de la institución, tanto estaciones de trabajo como servidores.
Norma internacional. La ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información) y la ISO 9001:2015 (Sistema de Gestión de Calidad) son los estándares internacionales que acreditan, mediante auditoría de tercera parte, que el oferente cuenta con procesos de seguridad y de calidad aplicables a los controles y servicios exigidos. El propio PBC (Especificaciones Técnicas "CPS") establece que "siempre que sea posible deberán especificarse normas de calidad internacionales".
No afecta la competencia entre marcas. Se trata de un requisito sobre la capacidad del oferente, no sobre el producto, y se aplica por igual a todos los participantes, en línea con los principios de igualdad y libre competencia, razonabilidad y valor por dinero (Art. 4, Ley N° 7021/22) y con la exigencia de solvencia técnica o profesional del oferente (Art. 19, Ley N° 7021/22).
Solicitud: se solicita a la Convocante evaluar y, de considerarlo procedente, incorporar mediante adenda, como requisito de capacidad técnica del oferente, la presentación de copia de: (a) certificado vigente ISO/IEC 27001; y (b) certificado vigente ISO 9001:2015; emitidos por organismo de certificación, con alcance que comprenda servicios de implementación y/o soporte de soluciones de TI o seguridad, vigentes a la fecha de apertura de ofertas.
De no considerarse procedente, se solicita informar el fundamento técnico por el cual se prescinde de estos estándares en una contratación cuyo objeto es la seguridad de la información institucional.

Respuesta	**Fecha de Respuesta**	07-11-2026

Se aclara que, si bien el objeto de la contratación es la protección de la información institucional, la naturaleza del llamado no se corresponde estrictamente con la exigencia de las certificaciones, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 19 - Aclaración sobre búsquedas históricas y en tiempo real

Consulta	**Fecha de Consulta**	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, se establece que la solución deberá permitir “la ejecución de búsquedas condicionales de archivos o artefactos de manera histórica y en tiempo real en la organización” y generar investigaciones en tiempo real sobre una estación de trabajo o dirección IP.

Solicitamos a la Convocante confirmar que estas capacidades deberán estar disponibles desde una misma plataforma y permitir búsquedas históricas y en tiempo real sobre la totalidad de los endpoints, así como consultas específicas sobre un dispositivo determinado, utilizando indicadores de compromiso como hashes, archivos, procesos, líneas de comando y conexiones de red.

Asimismo, entendemos que deberá ser posible utilizar los resultados de una búsqueda histórica o de un indicador de compromiso para realizar una validación inmediata sobre los endpoints y determinar su presencia actual, alcance y persistencia, sin requerir herramientas o consolas adicionales. ¿Es correcta nuestra interpretación?

Respuesta	**Fecha de Respuesta**	07-11-2026

Se aclara que es correcta su interpretación. Las capacidades de ejecución de búsquedas condicionales de archivos o artefactos de manera histórica y en tiempo real, y de investigación en tiempo real de una estación de trabajo o dirección IP, deberán estar disponibles desde una misma plataforma y permitir búsquedas sobre la totalidad de los endpoints protegidos, así como consultas específicas sobre un dispositivo determinado, utilizando indicadores de compromiso tales como hashes, archivos, procesos, líneas de comando y conexiones de red. Asimismo, la solución deberá permitir utilizar los resultados de una búsqueda histórica o de un indicador de compromiso para consultar en tiempo real los endpoints que se encuentren conectados y determinar su presencia actual, sin requerir herramientas o consolas adicionales, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 20 - Aclaración sobre priorización de amenazas según la postura de seguridad

Consulta	Fecha de Consulta	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, se requiere que la herramienta pueda realizar un security posture para determinar los equipos desprotegidos ante amenazas mundiales, generar recomendaciones específicas basadas en el análisis del entorno y notificar proactivamente el riesgo interno mediante la comparación del panorama global de amenazas con las contramedidas locales.

Solicitamos a la Convocante confirmar que la solución deberá identificar y priorizar dinámicamente las amenazas y campañas con mayor probabilidad de afectar a la organización, considerando su industria, ubicación geográfica, los actores de amenaza involucrados y la postura de seguridad real de sus endpoints.

Asimismo, entendemos que la solución deberá correlacionar la inteligencia de amenazas con la exposición y el nivel de cobertura de los endpoints, identificar brechas específicas y proporcionar recomendaciones accionables para mejorar las políticas y controles de seguridad, en lugar de presentar únicamente inteligencia o rankings globales sin correlación con la exposición específica de la Institución. ¿Es correcta nuestra interpretación?

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, es correcta la interpretación en cuanto a que la solución no podrá limitarse a presentar inteligencia o rankings globales. Las Especificaciones Técnicas exigen que la herramienta realice un security posture para determinar los equipos que estén desprotegidos ante amenazas mundiales; que notifique proactivamente respecto al riesgo interno basado en la comparación del panorama global de amenazas con los sistemas de contramedidas locales; que tenga la capacidad de anticipar amenazas emergentes y priorizarlas en función de su impacto potencial en el entorno de la organización; y que provea recomendaciones al analista respecto a políticas enfocadas a fortalecer las capacidades y contramedidas contra campañas y amenazas que puedan afectar a la organización en particular. En consecuencia, los requisitos se tendrán por cumplidos cuando la solución, desde la misma consola: a) evalúe el estado de protección y la configuración de políticas de los equipos frente a las recomendaciones del fabricante, identificando equipos sin protección, con protección incompleta o con configuraciones débiles; b) contraste dicha información con la inteligencia de amenazas global del fabricante, la cual deberá poder discriminarse por industria y por país o región; c) priorice las amenazas en función de su impacto potencial en el entorno de la organización; y d) proporcione al analista recomendaciones de ajuste de políticas y contramedidas. No se exige una metodología específica de priorización o correlación, ni la consideración de criterios adicionales a los establecidos en las Especificaciones Técnicas, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 21 - Aclaración sobre gestión de incidentes y asignación de personal

Consulta	Fecha de Consulta	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, se establece que: “La solución deberá proveer de una herramienta de gestión de incidentes y ‘case management’ que permita la documentación de los siguientes elementos”, incluyendo “Personal asignado a un caso de investigación”.

Solicitamos a la Convocante confirmar que este requerimiento podrá cumplirse mediante capacidades nativas de la solución ofertada o mediante su integración nativa, por API, con un módulo o plataforma de gestión de casos del mismo fabricante.

En este último supuesto, entendemos que no será obligatorio que el módulo de gestión de casos se encuentre incluido en el licenciamiento inicial ni que opere dentro de la misma consola, siempre que la solución ofertada demuestre compatibilidad e integración para incorporar dicha capacidad, sin necesidad de reemplazar la solución de protección y detección de endpoints. ¿Es correcta nuestra interpretación?

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, al respecto, esta Convocante aclara que las Especificaciones Técnicas establecen que "La solución deberá proveer de una herramienta de gestión de incidentes y case management" que permita documentar los elementos allí detallados. En consecuencia, dicha capacidad deberá formar parte de la solución ofertada, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 22 - Procesamiento y analítica de investigación en la nube

Consulta	Fecha de Consulta	07-10-2026

En relación con el requerimiento que establece que todo el procesamiento de datos y la analítica relacionados con las capacidades de investigación deberán realizarse en la nube, entendemos que el procesamiento de las búsquedas históricas y la analítica de investigación deberán ejecutarse en dicha infraestructura, sin depender de servidores locales de procesamiento para esas funcionalidades.
¿Es correcta nuestra apreciación?

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, al respecto, esta Convocante aclara que el requisito establece que "Todo el procesamiento de datos y analítica relacionadas con las capacidades de investigación de la solución deberá realizarse en la nube". La redacción es suficientemente clara y será evaluada en esos términos, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 23 - Aclaración sobre estados de los procesos de análisis

Consulta	Fecha de Consulta	07-10-2026

En las Especificaciones Técnicas del Ítem 1 - Renovación de Licencias de Antivirus, se establece que: “La herramienta debe permitir asignar distintos estados a los procesos de análisis para determinar la etapa en que se encuentra un incidente”.

Entendemos que el requisito podrá considerarse cumplido cuando la solución permita identificar, registrar y visualizar el estado de las acciones y procesos de investigación o respuesta asociados al incidente.

Asimismo, entendemos que no será obligatorio contar con estados personalizados ni con un flujo de trabajo independiente de gestión de casos, siempre que el analista pueda consultar el tipo de acción realizada, su estado y el avance de las actividades ejecutadas durante la investigación y respuesta al incidente. ¿Es correcta nuestra interpretación?

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, al respecto, esta Convocante aclara que el requisito establece que la herramienta debe permitir asignar distintos estados a los procesos de análisis para determinar la etapa en que se encuentra un incidente, y será evaluado conforme a su redacción, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 24 - Alcance de la retención mínima de 90 días

Consulta	Fecha de Consulta	07-10-2026

En relación con el requerimiento de retención mínima de 90 días y las capacidades de búsqueda histórica e investigación de amenazas, solicitamos aclarar si dicho período corresponde a los datos recolectados necesarios para ejecutar esas investigaciones, además del historial de alertas.
Entendemos que, para los datos comprendidos en este requerimiento, el dimensionamiento y licenciamiento ofertados deberán garantizar su disponibilidad para consulta durante al menos 90 días, considerando los límites de almacenamiento aplicables.
¿Es correcta nuestra apreciación?

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, al respecto, esta Convocante aclara que las Especificaciones Técnicas establecen la capacidad de búsqueda de información por un período mínimo de 90 días. El dimensionamiento y el licenciamiento de la solución son responsabilidad del oferente, quien deberá garantizar el cumplimiento de lo requerido durante toda la vigencia contractual, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 25 - Búsquedas personalizadas para investigación y cacería de amenazas

Consulta	Fecha de Consulta	07-10-2026

En atención a los requerimientos de búsquedas históricas, búsqueda de archivos o artefactos y procesos de cacería de amenazas, entendemos que la solución deberá permitir al analista definir criterios de búsqueda personalizados sobre la información recolectada y conservada correspondiente a dichos requisitos, sin limitar estas capacidades a la consulta de alertas previamente generadas.
¿Es correcta nuestra apreciación?

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, es correcta la apreciación. La solución deberá permitir al analista definir criterios de búsqueda personalizados sobre la información recolectada y conservada por la solución durante el período de búsqueda exigido en las Especificaciones Técnicas, tanto para búsquedas históricas como para la búsqueda de archivos o artefactos y los procesos de cacería de amenazas, sin que estas capacidades se limiten a la consulta de alertas previamente generadas, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 26 - CONSULTA

Consulta	Fecha de Consulta	07-10-2026

Considerando que las Especificaciones Técnicas establecen que el módulo de investigación profunda deberá formar parte de la misma solución y que no se aceptará un análisis realizado por personal humano para dicho análisis, solicitamos confirmar que el cumplimiento deberá acreditarse mediante capacidades automáticas propias de la solución ofertada, no pudiendo sustentarse exclusivamente mediante servicios MDR, SOC, analistas humanos o servicios profesionales adicionales.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, al respecto, esta Convocante aclara que las Especificaciones Técnicas ya establecen que "El módulo de investigación profunda solicitado en el pedido de EDR deberá formar parte de la misma solución" y que "No se aceptará un análisis realizado por personal humano para este análisis". El requisito es claro y será evaluado en esos términos, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.

Consulta 27 - CONSULTA

Consulta	Fecha de Consulta	07-10-2026

Respecto de los requerimientos de búsqueda histórica e investigación de amenazas, solicitamos confirmar que la solución deberá permitir efectuar consultas retrospectivas sobre la telemetría recolectada de los endpoints durante el periodo de retención exigido, incluso respecto de objetos, procesos, conexiones o comportamientos que no hayan generado originalmente una alerta o incidente de seguridad.

Respuesta	Fecha de Respuesta	07-11-2026

Se aclara que, al respecto, esta Convocante aclara que los requisitos de búsqueda histórica, búsqueda de información por un período mínimo de 90 días y análisis forense se encuentran establecidos en las Especificaciones Técnicas y serán evaluados conforme a su redacción, por lo que el oferente deberá ajustarse a la versión 1 del Pliego de Bases y Condiciones publicada en fecha 23 de setiembre de 2026.