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 485291 - SERVICIO DE MONITOREO NOC/SOC

Consulta 1 - Aclaración sobre cantidad de activos a licenciar

Consulta	Fecha de Consulta	29-09-2026
Considerando que las EETT indican como activos a monitorear 75 EndPoints, 25 servidores Windows, 4 servidores Linux y 6 servidores físicos, solicitamos aclarar la cantidad exacta de licencias de la solución EDR/SOC que deberá contemplar la oferta, indicando si los 6 servidores físicos se encuentran incluidos dentro de los 25 servidores Windows y 4 Linux o si deberán considerarse como activos adicionales.		

Respuesta	Fecha de Respuesta	02-10-2026
Se aclara que la solución de EDR/SOC deberá contemplar el licenciamiento para un total de 104 activos/agentes (75 Endpoints + 25 Servidores Windows + 4 Servidores Linux). Los 6 servidores físicos mencionados corresponden a la infraestructura de host/hipervisores que alojan a dichos servidores virtuales, por lo que SÍ requieren licenciamiento adicional de agente EDR.		

Consulta 2 - Cantidad de usuarios para concienciación

Consulta	Fecha de Consulta	29-09-2026
Solicitamos indicar la cantidad total de usuarios o funcionarios que deberán disponer de acceso a la herramienta de concienciación y entrenamiento en ciberseguridad durante los 12 meses de prestación, a efectos de dimensionar correctamente el licenciamiento requerido.		

Respuesta	Fecha de Respuesta	02-10-2026
Se aclara que para el acceso a la herramienta de concienciación y entrenamiento deben ser considerados 75 usuarios.		

Consulta 3 - Frecuencia del Penetration Testing

Consulta	Fecha de Consulta	29-09-2026
Las EETT incluyen servicios de Penetration Testing Interno y Externo dentro del alcance del SOC. Solicitamos aclarar cuántas ejecuciones deberán realizarse durante los 12 meses de contrato, indicando si se requiere una única evaluación, evaluaciones periódicas o ejecución bajo demanda, así como la cantidad aproximada de activos, direcciones IP, aplicaciones web y/o servicios comprendidos en cada evaluación.		

Respuesta	Fecha de Respuesta	02-10-2026
Se aclara respecto a los servicios de Pentesting interno y externo se aclara que el servicio debe contemplar dos (2) pruebas anuales, una por cada semestre.		

Consulta 4 - Aclaración sobre conformación del equipo técnico

Consulta	Fecha de Consulta	29-09-2026

Considerando que las EETT requieren al menos 6 técnicos de Monitoreo y Seguridad, además de personal certificado para las distintas herramientas y especialidades, solicitamos aclarar si un mismo profesional podrá ser computado para el cumplimiento de más de uno de los requisitos técnicos y de certificación, siempre que reúna las certificaciones y experiencia solicitadas.

Respuesta	Fecha de Respuesta	02-10-2026

La Convocante ratifica los requerimientos mínimos de personal y certificaciones establecidos en las Especificaciones Técnicas del Pliego de Bases y Condiciones, los cuales responden a la necesidad operativa de garantizar la disponibilidad permanente, la cobertura continua (24x7x365) y el cumplimiento de los Acuerdos de Nivel de Servicio (SLA) exigidos. En consecuencia, cada perfil solicitado deberá ser acreditado por profesionales distintos, no admitiéndose la duplicación de personas físicas para la cobertura de los requerimientos mínimos independientes.

Consulta 5 - Aclaración sobre tiempos de atención de incidentes

Consulta	Fecha de Consulta	29-09-2026

Las EETT establecen un tiempo de notificación ante incidentes de hasta 15 minutos, mientras que posteriormente el cuadro SLA establece tiempos de respuesta inicial de hasta 2 horas para incidentes críticos. Solicitamos aclarar que el plazo de 15 minutos corresponde exclusivamente a la detección y notificación del incidente, mientras que los tiempos establecidos en el cuadro SLA corresponden al inicio de las acciones de atención y resolución

Respuesta	Fecha de Respuesta	02-10-2026

En relación a los plazos de respuesta, la Convocante aclara que deberá cumplirse con la totalidad de los tiempos establecidos en las Especificaciones Técnicas y en los Acuerdos de Nivel de Servicio (SLA). El tiempo de notificación ante incidentes de hasta quince (15) minutos constituye un requisito independiente y obligatorio asociado a la detección y comunicación oportuna de eventos. Asimismo, deberán cumplirse los tiempos de respuesta inicial y resolución previstos en el cuadro de SLA conforme a la severidad del incidente.

Consulta 6 - Integración con infraestructura SIEM existente

Consulta	Fecha de Consulta	29-09-2026

Considerando que las EETT requieren la exportación e integración de eventos mediante Syslog, CEF y/o API hacia la infraestructura de monitoreo o SIEM de CAJA ANDE, solicitamos indicar fabricante, producto y versión de la plataforma SIEM actualmente utilizada, así como el mecanismo de integración previsto.

Respuesta	Fecha de Respuesta	02-10-2026

En relación la consulta sobre la integración y exportación de eventos, se aclara que los oferentes deberán considerar para su propuesta que la integración deberá realizarse utilizando mecanismos y estándares abiertos expresamente previstos en las Especificaciones Técnicas, incluyendo Syslog, CEF y/o API REST, según corresponda.

Consulta 7 - Alcance de protección de correo electrónico

Consulta	Fecha de Consulta	29-09-2026

En las especificaciones de la herramienta EDR se menciona que la consola deberá contener componentes para la protección del correo electrónico e integrarse a la plataforma SOC central. Solicitamos aclarar si la provisión de protección de correo electrónico forma parte obligatoria del alcance de la contratación y, en caso afirmativo, indicar la cantidad de cuentas, plataforma de correo utilizada y funcionalidades mínimas requeridas.

Respuesta	Fecha de Respuesta	02-10-2026

La Convocante aclara que las funcionalidades requeridas deberán ajustarse a lo establecido en las Especificaciones Técnicas y a las capacidades nativas de la solución ofertada por cada oferente, siempre que permitan el cumplimiento de los objetivos funcionales y operativos previstos para el servicio.
En caso de que la solución propuesta contemple mecanismos de protección, monitoreo o análisis asociados al correo electrónico, los mismos deberán encontrarse debidamente integrados con la plataforma de administración y monitoreo ofertada, conforme a los requerimientos establecidos en el Pliego.
La definición de los componentes específicos, mecanismos de integración y funcionalidades efectivamente implementadas formará parte de la propuesta técnica de cada oferente y será evaluada en función del cumplimiento integral de las Especificaciones Técnicas requeridas.

Consulta 8 - Sobre la duración de la prestación de los Servicios

Consulta	Fecha de Consulta	01-10-2026

Referencia: Sección "Plan de prestación de los servicios", ítem b "Servicio mensual", que estipula una cantidad de "12 MES"; en contraposición a la sección "Indicadores de Cumplimiento de Contrato", que exige la presentación de un informe de conformidad mensual "por el plazo de 24 meses a partir de la fecha del acta de entrega". Solicitamos a la convocante que para la correcta planificación de las obligaciones contractuales, sea aclarada la duración total del servicio requerido. Dado que el plazo de ejecución afecta a la estructura servicios operativos, el período de licenciamiento continuo necesario para las herramientas tecnológicas y la provisión ininterrumpida de los servicios de monitoreo.

Respuesta	Fecha de Respuesta	02-10-2026

En relación a la consulta se aclara que la duración de la prestación de los servicios. La convocante aclara que el plazo de prestación de los servicios es de 24 meses.

Consulta 9 - Sobre el estándar de sanitización y eliminación de datos

Consulta	Fecha de Consulta	01-10-2026

Referencia: La sección de mejora continua, estipula proceder a la destrucción y sanitización de los datos conforme a la norma NIST SP 800-88 R1, emitiendo un certificado de borrado seguro en un plazo no mayor de 15 días hábiles. Solicitamos que para el cumplimiento de las obligaciones mencionadas, pueda ser considerada la aplicación del estándar actualizado NIST SP 800-88 R2. Dado que la versión R1 ha sido reemplazada (decomisada) y que la revisión R2 refuerza que el Borrado Criptográfico es el método más viable y seguro para alcanzar una eliminación irreversible en infraestructuras modernas, solicitamos a la Convocante confirmar si el procedimiento de eliminación de datos y la consecuente emisión del certificado podrán regirse de acuerdo a la versión vigente del estándar.

Respuesta	Fecha de Respuesta	02-10-2026

Se aclara a los interesados que la referencia a la norma NIST SP 800-88 R1 en la sección de Mejora Continua constituye un parámetro de requerimiento mínimo de seguridad y cumplimiento. En consecuencia, la presentación de certificaciones o metodologías basadas en revisiones posteriores o actualizadas (como la NIST SP 800-88 R2) que igualen o superen los niveles de sanitización, seguridad y trazabilidad requeridos, resulta plenamente admisible para el cumplimiento del contrato, no requiriéndose modificación de las bases del llamado.