

Consultas Realizadas

Licitación 468051 - SERVICIO DE MONITOREO DE SISTEMAS CRITICOS DE LA DGIC (NOC)

Consulta 1 - Especificaciones Técnicas

Consulta	Fecha de Consulta	22-09-2025
En relación al Pliego de Bases y Condiciones de la Licitación ID 468051 – “Servicio de Monitoreo de Sistemas Críticos de la DGIC (NOC)”, solicitamos aclaración respecto a la modalidad de prestación del servicio. Considerando que el pliego establece disponibilidad 24x7x365 y soporte técnico in-situ con tiempo de respuesta no mayor a 2 horas, deseamos consultar si sería aceptable la siguiente modalidad: Asignación de un técnico presencial en Asunción, en horario lunes a viernes de 08:00 a 17:00, para el monitoreo diario y atención inmediata de alertas. El resto del monitoreo (fuera del horario mencionado y durante fines de semana) sería realizado de forma remota, desde el centro de monitoreo del proveedor ubicado en territorio nacional (Paraguay), con capacidad de respuesta in-situ en caso de incidentes críticos. Esta modalidad permitiría mantener la cobertura continua requerida, optimizando recursos sin comprometer la calidad del servicio ni los tiempos de respuesta. Agradecemos su orientación sobre si esta propuesta sería considerada válida dentro del marco del pliego.		

Respuesta	Fecha de Respuesta	23-09-2025
En atención a la consulta planteada, corresponde aclarar que el servicio requerido en el Pliego de Bases y Condiciones se enmarca en un modelo de NOC outsourcing remoto, el cual contempla soporte técnico in-situ únicamente en caso de alertas o incidentes críticos. En este sentido, la modalidad de contar con un recurso técnico residente en las instalaciones de la convocante no resulta aplicable, dado que no se dispone de la infraestructura necesaria para albergar a personal técnico en carácter presencial. Por lo tanto, y considerando la criticidad de los servicios solicitados, se ratifica que el oferente deberá ajustar su propuesta a los requerimientos establecidos en el PBC, los cuales garantizan la continuidad 24x7x365 mediante monitoreo remoto y soporte in-situ bajo las condiciones ya definidas en el pliego.		

Consulta 2 - EETT

Consulta	Fecha de Consulta	22-09-2025
Dado que el pliego establece requerimientos específicos en cuanto a la cobertura de servicios críticos, integración con hipervisores, bases de datos, contenedores, y equipos de red, pero no detalla la cantidad estimada de endpoints (servidores físicos/virtuales, dispositivos de red, bases de datos, etc.), solicito muy respetuosamente información técnica complementaria sobre: 1. Cantidad aproximada de endpoints a ser monitoreados (servidores, VMs, equipos de red, bases de datos, etc.). 2. Cantidad de bases de datos (MS-SQL, MySQL) que deben ser integradas. 3. Cantidad de hipervisores (VMware, Nutanix AHV, Hyper-V) en uso actualmente. 4. Cantidad de contenedores Docker/Kubernetes activos en la infraestructura. 5. Cantidad de enlaces de red y VPNs que deben ser monitoreados. Esta información es esencial para prever correctamente las licencias de software así como para garantizar el cumplimiento de los requerimientos técnicos establecidos en el pliego.		

Respuesta	Fecha de Respuesta	23-09-2025
En relación a la consulta planteada, corresponde señalar que la solución ofertada no deberá estar condicionada a la cantidad de licencias, dispositivos, agentes, endpoints o nodos a monitorear. La arquitectura del servicio debe garantizar cobertura integral sobre la totalidad de la infraestructura crítica definida por la convocante, independientemente de la evolución o el crecimiento de los elementos monitoreados durante la vigencia del contrato. Asimismo, el licenciamiento exigido deberá ser de carácter perpetuo y/o ilimitado, sin caducidad ni dependencia de modelos de suscripción que generen costos recurrentes adicionales durante el plazo del contrato. Este enfoque asegura la continuidad operativa, la escalabilidad del servicio y el cumplimiento efectivo de los requerimientos técnicos establecidos en el Pliego de Bases y Condiciones, evitando restricciones que puedan afectar la prestación del servicio o el control de costos por parte de la convocante. El oferente deberá dimensionar su propuesta considerando la capacidad de adaptación ante posibles crecimientos o cambios en la infraestructura monitoreada.		

Consulta 3 - EETT

Consulta	Fecha de Consulta	22-09-2025
En el pliego se menciona como uno de los beneficios esperados del servicio tercerizado de NOC la "gestión proactiva de la seguridad", que contribuiría a la mejora de la seguridad de la infraestructura tecnológica del Ministerio. A fin de comprender con mayor precisión el alcance de este requerimiento, agradecería se pudiera aclarar: 1. ¿Qué se entiende específicamente por "mejora de la seguridad" en el contexto del servicio de monitoreo? 2. ¿Se espera que el proveedor implemente medidas adicionales de seguridad (como escaneo de vulnerabilidades, hardening, correlación de eventos, etc.)? 3. ¿Se requiere integración con soluciones de seguridad existentes (SIEM, antivirus, firewalls, etc.)? 4. ¿Se espera que el proveedor emita recomendaciones o informes de seguridad periódicos? 5. ¿Existe alguna política o estándar de seguridad institucional que deba ser considerado (por ejemplo, ISO 27001, NIST, etc.)?		

Respuesta	Fecha de Respuesta	23-09-2025
La expresión "gestión proactiva de la seguridad", en el marco del servicio tercerizado de NOC, debe entenderse como la capacidad del proveedor de anticipar, detectar y notificar de forma oportuna aquellos eventos, anomalías o patrones de comportamiento que pudieran afectar la disponibilidad y correcto funcionamiento de los servicios de la convocante, este alcance implica que los servicios deberá prevenir interrupciones de servicio mediante el monitoreo continuo y la identificación temprana, y emitir los reportes e informes periódicos junto con las recomendaciones sugeridas orientadas a la mejora continua. Cabe resaltar que no se requiere que el proveedor implemente medidas de seguridad adicionales de carácter intrusivo, como escaneos de vulnerabilidad o hardening, salvo que estas estén expresamente contempladas en el pliego de bases y condiciones. Se espera que la solución se integre con herramientas de seguridad existentes (SIEM, antivirus, firewalls) y que se alinee con las políticas institucionales vigentes, cuando corresponda. El objetivo es fortalecer la capacidad preventiva y reactiva sobre la infraestructura monitoreada, aportando visibilidad y soporte a la gestión de la seguridad institucional de la convocante.		