GOBIERNO DE LA REPÚBLICA DE HONDURAS

COMISIÓN NACIONAL DE BANCOS Y SEGUROS

LPN-CNBS-001-2026

"ADQUISICIÓN Y RENOVACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA COMISIÓN NACIONAL DE BANCOS Y SEGUROS"

CIRCULAR ACLARATORIA No.2

La Comisión Nacional de Bancos y Seguros (CNBS) comunica que, en atención a consultas realizadas por participantes registrados en la Licitación Pública Nacional No. LPN-CNBS-001-2026 denominada "ADQUISICIÓN Y RENOVACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA COMISIÓN NACIONAL DE BANCOS Y SEGUROS" y de conformidad a lo dispuesto en el artículo 105 del Reglamento de la Ley de Contratación del Estado, párrafo segundo, se hacen las siguientes aclaraciones:

#	Referencia y Consultas			Respuestas
1	Lote 1	Endpoint Protection Platform – CrowdStrike Falcon Enterprise	Pregunta: Por favor indicar; ¿Se requiere incluir módulos adicionales de CrowdStrike como Threat Intelligence, Identity Protection o Falcon Complete dentro del alcance o únicamente Falcon Enterprise base?	No. Solo se requieren las licencias indicadas en el documento base.
2	Lote 1	Renovación de solución EPP	Pregunta: Por favor indicar; ¿La renovación contempla continuidad sobre la misma consola existente o se requiere una migración a una nueva instancia?	Se contempla continuidad sobre la misma consola, razón por la cual se indica el Customer ID actual.
3	Lote 1	Endpoint Protection	Pregunta: Por favor indicar; ¿Se dispone de un inventario actualizado de endpoints (tipo, sistema operativo, criticidad) que permita dimensionar correctamente la solución?	La solución se debe dimensionar en base a la cantidad de licencias indicadas en el documento base.
4	Lote 1	Protección de endpoints	Pregunta: Por favor indicar; ¿Se requiere cobertura para servidores críticos o únicamente estaciones de trabajo?	Queda a criterio de la CNBS a que equipo le estará asignando las licencias solicitadas.
5	Lote 1	CrowdStrike Falcon	Pregunta: Por favor indicar; ¿Se requiere integración con herramientas existentes como SIEM, SOAR o plataformas de ticketing?	Si se requiere integración con herramientas de SIEM, SOAR.
6	Lote 1	EDR capabilities	Pregunta: Por favor indicar; ¿Quién será responsable de la respuesta a incidentes detectados por el EDR: CNBS o el proveedor?	La CNBS es responsable de la respuesta a incidentes detectados.
7	Lote 1	Implementación	Pregunta: Por favor indicar; ¿Se requiere despliegue masivo asistido por el proveedor o la CNBS realizará el despliegue?	Se está renovando un producto ya implementado. Cualquier despliegue adicional lo realizará la CNBS.
8	Lote 1	Operación	Pregunta: Por favor indicar; ¿Se espera que el proveedor realice actividades de tuning y reducción de falsos positivos?	No se requiere que el proveedor realice actividades de tuning y reducción de falsos positivos.
9	Lote 1	Integración	Pregunta: Por favor indicar; ¿Se requiere integración con Active Directory para control de identidades?	No se requiere integración con Active Directory.
10	Lote 1	Logs	Pregunta: Por favor indicar; ¿Se requiere retención de logs en la plataforma CrowdStrike o su envío a un SIEM externo?	Se requiere retención de logs estandar para el tipo de licencia indicado en el documento base.
11	Lote 1	Alcance de servicio	Pregunta: Por favor indicar; ¿Se requiere monitoreo activo de eventos generados por la solución o solo administración de la plataforma?	No se requiere ni monitoreo activo de eventos generados por la plataforma, ni se requiere administración de la plataforma.
12	Lote 1	Soporte	Pregunta: Por favor indicar; Cuál es el nivel de soporte esperado (8x5, 24x7, con tiempos de respuesta definidos)?	Se requiere el soporte estandar incluido en las licencias indicadas en el documento base.
13	Lote 1	Seguridad avanzada	Pregunta: Por favor indicar; ¿Se requiere habilitar funcionalidades de contención automática ante amenazas críticas?	No. Solo se requieren las licencias indicadas en el documento base.
14	Lote 1	Arquitectura	Pregunta: Por favor indicar; ¿Existen restricciones de conectividad a internet que puedan afectar el funcionamiento cloud de CrowdStrike?	No.
15	Lote 1	Licenciamiento	Pregunta: Por favor indicar; ¿El licenciamiento debe ser co-terminado con otras soluciones existentes dentro de CNBS?	No.

16	Lote 2	Imperva Data Secure Fabric	Pregunta: Por favor indicar; ¿Se dispone de un inventario detallado de instancias de bases de datos (tipo, versión, ubicación, criticidad) para dimensionar la arquitectura DAM?	La solución se debe dimensionar en base a la cantidad de servidores indicadas en el documento base.
17	Lote 2	Monitoreo de actividad de bases de datos	Pregunta: Por favor indicar; ¿Se requiere implementación en modo agente, proxy o network sniffing, o se espera que el proveedor defina la arquitectura óptima?	Se está renovando un producto ya implementado. No se requiere implementación adicional.
18	Lote 2	Desempeño	Pregunta: Por favor indicar; ¿Existen requerimientos máximos de latencia permitida en transacciones para no afectar sistemas core bancarios?	No.
19	Lote 2	Auditoría	Pregunta: Por favor indicar; ¿Qué normativas regulatorias específicas debe cumplir la solución (ej: PCI-DSS, ISO 27001, regulación local CNBS)?	Se está renovando un producto ya implementado. No se requiere implementar controles de normativas regulatorias adicionales a las ya implementadas.
20	Lote 2	Clasificación de datos	Pregunta: Por favor indicar; ¿Se cuenta con clasificación previa de datos sensibles o se espera que el proveedor implemente mecanismos de discovery y clasificación?	Se está renovando un producto ya implementado. No se requiere que el proveedor implemente mecanismos de discovery y clasificación.
21	Lote 2	Integración	Pregunta: Por favor indicar; ¿Se requiere integración de eventos DAM con el SOC (Lote 6) mediante SIEM o APIs nativas?	Si.
22	Lote 2	Logs	Pregunta: Por favor indicar; ¿Cuál es el volumen estimado de logs de bases de datos (TPS) para dimensionar almacenamiento y procesamiento?	Se está renovando un producto ya implementado. No se requiere dimensionar almacenamiento y procesamiento.
23	Lote 2	Alta disponibilidad	Pregunta: Por favor indicar; ¿Se requiere arquitectura activa-activa o activa-pasiva para los componentes de Imperva DAM?	Se está renovando un producto ya implementado. No se requiere diseñar una arquitectura activa-activa o activa-pasiva por parte del proveedor.
24	Lote 2	Usuarios privilegiados	Pregunta: Por favor indicar; ¿Se requiere monitoreo específico de accesos privilegiados (DBA) con correlación de sesiones?	Se está renovando un producto ya implementado. El producto ya está configurado para el monitoreo específico de accesos privilegiados.
25	Lote 2	Políticas	Pregunta: Por favor indicar; ¿Se espera que el proveedor defina políticas base de monitoreo o CNBS proporcionará lineamientos?	Se está renovando un producto ya implementado. No se requiere que el proveedor defina políticas base de monitoreo.
26	Lote 2	Tuning	Pregunta: Por favor indicar; ¿Se requiere fase formal de tuning para reducción de falsos positivos y durante cuánto tiempo?	Se está renovando un producto ya implementado. No se requiere fase formal de tuning.
27	Lote 2	Integración con IAM/PAM	Pregunta: Por favor indicar; ¿Se requiere correlación de accesos a bases de datos con soluciones de identidad o PAM existentes?	No.
28	Lote 2	Segmentación	Pregunta: Por favor indicar; ¿Las bases de datos se encuentran segmentadas por zonas de seguridad o existe tráfico transversal que deba monitorearse?	No.
29	Lote 2	Continuidad	Pregunta: Por favor indicar; ¿Se requiere plan de contingencia y DRP específico para la solución DAM?	No.
30	Lote 3	Protección de aplicaciones web	Pregunta: Por favor indicar; ¿Se dispone de un inventario completo de aplicaciones web (internas/externas, APIs, microservicios)?	La solución se debe dimensionar en base a la cantidad de aplicaciones y el plan indicado en el documento base.
31	Lote 3	Arquitectura	Pregunta: Por favor indicar; ¿Se espera un modelo WAF en modo reverse proxy, inline, o cloud-based (CDN)?	Reverse proxy.
32	Lote 3	APIs	Pregunta: Por favor indicar; ¿Se requiere protección específica para APIs (REST/GraphQL) con inspección de payload?	Se está renovando una solución ya implementada. Se requiere la protección cubierta en el plan indicado en el documento base.
33	Lote 3	TLS	Pregunta: Por favor indicar; ¿Quién gestionará los certificados SSL/TLS y su ciclo de vida dentro del WAF?	CNBS.
34	Lote 3	DDoS	Pregunta: Por favor indicar; ¿Se requiere protección DDoS L7 integrada o se cuenta con solución externa?	Se está renovando una solución ya implementada. Se requiere la protección cubierta en el plan indicado en el documento base.
35	Lote 3	Bots	Pregunta: Por favor indicar; ¿Se requiere gestión avanzada de bots (good bots vs bad bots)?	Se está renovando una solución ya implementada. Se requiere la protección cubierta en el plan indicado en el documento base.

36	Lote 3	DevOps	Pregunta: Por favor indicar; ¿Se requiere integración del WAF con pipelines CI/CD para validación de cambios?	Se está renovando una solución ya implementada. Se requiere la protección cubierta en el plan indicado en el documento base.
37	Lote 3	Logs	Pregunta: Por favor indicar; ¿Cuál es el volumen estimado de tráfico HTTP/HTTPS para dimensionamiento del WAF?	La solución se debe dimensionar en base a la cantidad de aplicaciones y el plan indicado en el documento base.
38	Lote 3	Falsos positivos	Pregunta: Por favor indicar; ¿Se requiere fase de aprendizaje/monitoring antes de aplicar bloqueo?	Se está renovando un producto ya implementado. No se requiere fase de aprendizaje/monitoring.
39	Lote 3	Integración SOC	Pregunta: Por favor indicar; ¿Se requiere correlación en tiempo real con el SOC para ataques web?	Si.
40	Lote 3	Alta disponibilidad	Pregunta: Por favor indicar; ¿Se requiere arquitectura multi-site o multi-región?	Se está renovando una solución ya implementada. Se requiere la arquitectura cubierta en el plan indicado en el documento base.
41	Lote 3	Compliance	Pregunta: Por favor indicar; ¿Se deben generar reportes específicos para auditoría regulatoria?	No.
42	Lote 3	Seguridad avanzada	Pregunta: Por favor indicar; ¿Se requiere protección contra ataques zero-day mediante ML/behavioral analysis?	Se está renovando una solución ya implementada. Se requiere la protección cubierta en el plan indicado en el documento base.
43	Lote 3	Integración IAM	Pregunta: Por favor indicar; ¿Se requiere integración con sistemas de autenticación (SSO, MFA)?	Se está renovando una solución ya implementada. Ya se integró con un sistema de autenticación.
44	Lote 3	APIs	Pregunta: Por favor indicar; ¿Se requiere descubrimiento automático de APIs expuestas?	Se está renovando una solución ya implementada. Se requiere la protección cubierta en el plan indicado en el documento base.
45	Lote 4	Infoblox DDI	Pregunta: Por favor indicar; ¿Se dispone de un inventario actual de la infraestructura DNS, DHCP e IPAM (on-premise, cloud, híbrido)?	Se está renovando un producto ya implementado. Se debe dimensionar en base a las cantidades indicadas en el documento base.
46	Lote 4	DNS Security	Pregunta: Por favor indicar; ¿Se requiere protección contra DNS tunneling y detección de comunicaciones C2 basadas en DNS?	Se está renovando un producto ya implementado. Se requiere la protección cubierta por las licencias indicadas en el documento base.
47	Lote 4	Arquitectura	Pregunta: Por favor indicar; ¿Se requiere arquitectura distribuida con nodos en múltiples sedes o centralizada?	Se está renovando un producto ya implementado. No se requiere una nueva arquitectura.
48	Lote 4	Alta disponibilidad	Pregunta: Por favor indicar; ¿Cuál es el RTO/RPO esperado para los servicios DNS y DHCP?	Se está renovando un producto ya implementado. No se requiere una nueva arquitectura.
49	Lote 4	Integración	Pregunta: Por favor indicar; ¿Se requiere integración con Active Directory para resolución DNS interna?	Se está renovando un producto ya implementado. El producto ya está integrado con Active Directory.
50	Lote 4	Logs DNS	Pregunta: Por favor indicar; ¿Cuál es el volumen estimado de consultas DNS por segundo (QPS) para dimensionamiento?	Se está renovando un producto ya implementado. Se debe dimensionar en base a las cantidades indicadas en el documento base.
51	Lote 4	Threat Intelligence	Pregunta: Por favor indicar; ¿Se requiere integración con feeds externos o uso exclusivo de feeds Infoblox?	Se está renovando un producto ya implementado. El producto ya está integrado con los feeds requeridos.
52	Lote 4	Segmentación	Pregunta: Por favor indicar; ¿Se requiere segmentación DNS por zonas de seguridad o entornos (producción, pruebas)?	Se está renovando un producto ya implementado. Ya están definidas todas las zonas requeridas.
53	Lote 4	Automatización	Pregunta: Por favor indicar; ¿Se requiere automatización IPAM mediante APIs para integración con otras plataformas?	No.
54	Lote 4	Seguridad	Pregunta: Por favor indicar; ¿Se requiere implementación de DNSSEC?	No.
55	Lote 4	Visibilidad	Pregunta: Por favor indicar; ¿Se requiere visibilidad de tráfico DNS interno vs externo?	Si.
56	Lote 4	Integración NAC	Pregunta: Por favor indicar; ¿Se requiere integración con soluciones NAC o control de acceso a red?	No.
57	Lote 4	Multi-cloud	Pregunta: Por favor indicar; ¿Se deben integrar entornos cloud (AWS, Azure, GCP) con el DDI?	No.
58	Lote 5	Gestión de actualizaciones	Pregunta: Por favor indicar; ¿Se dispone de inventario actualizado de activos a gestionar (OS, aplicaciones, versiones)?	La solución se debe dimensionar en base a las cantidades indicadas en el documento base.
59	Lote 5	Alcance	Pregunta: Por favor indicar; ¿Se deben incluir parches de aplicaciones de terceros o solo sistema operativo?	Como se indica en el documento base, se deben incluir parches de aplicaciones de terceros.
60	Lote 5	Ventanas	Pregunta: Por favor indicar; ¿Cuáles son las ventanas de mantenimiento "protocolo interno" definidas por tipo de activo?	Relacionado a este producto, y los activos que gestionará, no existen ventanas de mantenimiento definidas.

61	Lote 5	Automatización	Pregunta: Por favor indicar; Se espera automatización total del parchado o validación manual previa?	Se espera validación manual previa.
62	Lote 5	Integración	Pregunta: Por favor indicar; ¿Se requiere integración con Tenable (Lote 7) para priorización de vulnerabilidades?	No.
63	Lote 5	Riesgo	Pregunta: Por favor indicar; ¿Se cuenta con metodología de priorización basada en riesgo (CVSS, explotación activa)?	Si.
64	Lote 5	Rollback	Pregunta: Por favor indicar; ¿Se requiere mecanismo de reversión automática de parches?	No.
65	Lote 5	Compliance	Pregunta: Por favor indicar; ¿Qué niveles de cumplimiento mínimo de parchado se requieren (ej: 95%)?	El parchado será realizado por personal de la CNBS, el cual determinará el nivel de cumplimiento mínimo requerido en base al nivel de criticidad de cada parche.
66	Lote 5	Reportes	Pregunta: Por favor indicar; ¿Se requieren dashboards ejecutivos y técnicos diferenciados?	No.
67	Lote 5	SOC	Pregunta: Por favor indicar; ¿Se requiere correlación de activos no parchados con incidentes de seguridad?	No.
68	Lote 5	Herramienta actual	Pregunta: Por favor indicar; ¿Existe una herramienta actual que deba ser migrada o reemplazada?	No.
69	Lote 5	Excepciones	Pregunta: Por favor indicar; ¿Cómo se gestionarán los activos con parches no aplicables o excepciones de negocio?	La gestión de excepciones dependerá del producto a ofertar. Esta gestión será realizada por el personal de la CNBS.
70	Lote 6	Servicio SOC	Pregunta: Por favor indicar; ¿Cuál es el volumen estimado de eventos (EPS/GB por día) a procesar por el SOC?	Un promedio de 510 GB por día, con picos máximos de alrededor de 2.8 TB por día.
71	Lote 6		**Consulta Clasificada "CONFIDENCIAL"**	**CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.2. Este Anexo se compartirá únicamente a los participantes registrados que hayan presentado el Acuerdo de Confidencialidad conforme lo establecido en la cláusula IAO 7.1 de la Sección II. Datos de la Licitación del DB.**
72	Lote 6	Cobertura	Pregunta: Por favor indicar; ¿Se requiere operación 24x7 con cobertura local o remota?	Tal como se establece en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, numeral "1.6: El servicio deberá ser brindado en modalidad 24x7x365, lo cual implica además que el proveedor del servicio debe contar con las capacidades instaladas para garantizar la continuidad de sus operaciones ante cualquier contingencia, asegurando Alta Disponibilidad para proveer servicio completo desde dos países diferentes. Independientemente de la ubicación geográfica desde la cual se preste el servicio, toda la atención, comunicación y soporte deberán ser proporcionados en idioma español."
73	Lote 6	Niveles	Pregunta: Por favor indicar; ¿Cuál es el modelo esperado de niveles (N1, N2, N3) y responsabilidades? Donde desde el proveedor se analicen y se propongan los cambios para que los ejecute CBNS o desde el proveedor se eecuten todas las acciones (ABCG - Altas / Bajas / Cambio / Gestión).	Queda a criterio del Oferente el modelo de niveles a implementar, a fin de dar cumplimiento a lo establecido en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, de los numerales 1 al 6. Note especialmente lo señalado en el numeral "1.3. Respuesta a Incidentes: Brindar respuesta inmediata y/o automática sobre incidentes con patrones de comportamiento citados en el framework de MITRE ATT&CK y que, a criterio del proveedor del servicio, en base a su criterio de experto, convenga configurar una respuesta automática; mientras que, para el resto de los incidentes detectados, brindar acompañamiento y asesoría para dar respuestas a los mismos."
74	Lote 6	SIEM	Pregunta: Por favor indicar; ¿Se cuenta con SIEM existente o el proveedor debe incluirlo?	La CNBS no cuenta con SIEM Existente. Tal como lo establece el documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Requisitos Adicionales, numeral "10. La propuesta debe contemplar todas las licencias, suscripciones, appliance(s) físico y/o servicios requeridos para el correcto funcionamiento del servicio ofertado. En caso de que la propuesta incluya el hospedaje de uno o varios appliances virtuales en la Infraestructura de la CNBS, el oferente deberá indicar claramente en su oferta los recursos técnicos requeridos. La CNBS evaluará y comunicará si cuenta con la capacidad para hospedar el(los) appliance(s) virtual(es) propuesto(s), considerando la compatibilidad con su infraestructura tecnológica y la disponibilidad de recursos."
75	Lote 6	SOAR	Pregunta: Por favor indicar; ¿Se requiere automatización de respuesta mediante playbooks SOAR?	Tal como se establece en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, numeral "1.5.4. Contar con solución SOAR para la orquestación de eventos, automatización y brindar, a nivel de XDR o solución semejante, respuesta inmediata y/o automática sobre incidentes con patrones de comportamiento citados en el framework de MITRE ATT&CK y que, en base al criterio experto del proveedor del servicio, convenga configurar una respuesta automática. Dicha respuesta deberá ser compatible o integrable con la Solución de Protección Perimetral y demás soluciones de Protección de la CNBS."
76	Lote 6	Casos de uso	Pregunta: Por favor indicar; ¿Existe un catálogo de casos de uso o debe ser desarrollado por el proveedor?	Debe ser desarrollado por el Proveedor, a fin de dar cumplimiento al Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, numerales 1 al 6.

77	Lote 6	SLA	Pregunta: Por favor indicar; ¿Cuáles son los tiempos de detección (MTTD) y respuesta (MTTR) esperados?	Tal como lo establece el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, numeral "1.7.1 Reporte con una frecuencia no mayor a media hora después de ocurrido un evento, a través del sistema de Tickets de las alertas que requieren ser conocidas por la CNBS, consignando en el mismo al menos la siguiente información: 1.7.1.1. Detalles del Evento, en donde se indique la URL a la Consola del Proveedor de Servicio donde se visualizan las alertas de la CNBS, fecha y hora de ocurrencia del evento y resumen del evento, origen, destino, usuarios, aplicaciones involucradas, ataque, IOCs, entre otros. 1.7.1.2. Recomendaciones con instrucciones técnicas específicas." Así como el numeral "1.5.4. Contar con solución SOAR para la orquestación de eventos, automatización y brindar, a nivel de XDR o solución semejante, respuesta inmediata y/o automática sobre incidentes con patrones de comportamiento citados en el framework de MITRE ATT&CK y que, en base al criterio experto del proveedor del servicio, convenga configurar una respuesta automática. Dicha respuesta deberá ser compatible o integrable con la Solución de Protección Perimetral y demás soluciones de Protección de la CNBS."
78	Lote 6	Escalamiento	Pregunta: Por favor indicar; ¿Cuál es el flujo de escalamiento esperado hacia CNBS en incidentes críticos?	Queda a criterio del Oferente el flujo de escalamiento en incidentes críticos, a fin de dar cumplimiento a lo establecido en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, de los numerales 1 al 6. Debiendo considerar que el mismo debe consignarse en la Oferta en cumplimiento al Documento de Licitación, pues en la misma sección, Lote y título previamente señalado, se indica en el numeral "14. La propuesta debe contener la descripción del Servicio, que incluya los elementos que satisfacen lo requerido en las Especificaciones Técnicas del presente Documento de Licitación, el acuerdo de nivel de servicio ofertado, escalamiento, procesos y canales de comunicación, así como la Propuesta de Valor Agregado."
79	Lote 6	Threat Intelligence	Pregunta: Por favor indicar; ¿Se requiere integración con feeds de inteligencia externos?	Queda a criterio del Oferente los feeds de inteligencia a incorporar, a fin de dar cumplimiento a lo establecido en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, de los numerales 1 al 6. Sobre este tema en el Documento de Licitación, en la misma sección, Lote y título previamente señalado, se indica en el numeral "1.4. El servicio deberá contar con la tecnología, procedimientos y personal para: 1.4.1. Brindar un servicio con enfoque proactivo de ciberseguridad, que permita identificar y mitigar las amenazas de forma proactiva en una etapa temprana de ataque, antes de que puedan causar daños importantes a los activos y datos digitales de la CNBS. 1.4.2. Tener acceso a insumos básicos de inteligencia de amenazas, que permita mantenerse informados sobre las últimas amenazas cibernéticas, vulnerabilidades y técnicas de ataque."
80	Lote 6	Playbooks	Pregunta: Por favor indicar; ¿Se requiere desarrollo de playbooks específicos por tipo de amenaza?	Tal como se establece en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, numeral "1.5.4. Contar con solución SOAR para la orquestación de eventos, automatización y brindar, a nivel de XDR o solución semejante, respuesta inmediata y/o automática sobre incidentes con patrones de comportamiento citados en el framework de MITRE ATT&CK y que, en base al criterio experto del proveedor del servicio, convenga configurar una respuesta automática. Dicha respuesta deberá ser compatible o integrable con la Solución de Protección Perimetral y demás soluciones de Protección de la CNBS."
81	Lote 6	Reporting	Pregunta: Por favor indicar; ¿Qué tipo de reportes se requieren (operativos, tácticos, estratégicos)?	Tal como se establece en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, numeral "1.7. Proporcionar los siguientes Informes, Boletines y Reportes: 1.7.1. Reporte con una frecuencia no mayor a media hora después de ocurrido un evento, a través del sistema de Tickets de las alertas que requieren ser conocidas por la CNBS, consignando en el mismo al menos la siguiente información: 1.7.1.1. Detalles del Evento, en donde se indique la URL a la Consola del Proveedor de Servicio donde se visualizan las alertas de la CNBS, fecha y hora de ocurrencia del evento y resumen del evento, origen, destino, usuarios, aplicaciones involucradas, ataque, IOCs, entre otros. 1.7.1.2. Recomendaciones con instrucciones técnicas específicas. 1.7.2. Al menos un informe mensual que contenga un resumen ejecutivo, casos atendidos durante el mes por severidad y por tipo, Ajustes realizados y Falsos Positivos depurados, el cumplimiento del Acuerdo de Servicio establecido, así como cualquier información significativa en relación con el servicio. 1.7.3. Reportar a la CNBS en un término no mayor a media hora cuando haya pérdida de conexión de alguna(s) de las Fuentes de datos a su Plataforma de Servicio y/o cuando exista alguna falla o degradación considerable en el funcionamiento del(los) equipos del proveedor instalados en el CPD de la CNBS para proveer el servicio. 1.7.4. Boletines e Informes sobre las últimas amenazas, vulnerabilidades y técnicas de ataque que están teniendo lugar en el entorno global, dichos boletines e informes deberán incluir recomendaciones basadas en buenas prácticas, para asegurar la respectiva prevención, contención y/o erradicación por parte de la CNBS. 1.7.5. Reportes especiales cuando suceda algún incidente de ciberseguridad que impacte la prestación de algún servicio de la CNBS o la seguridad de su información. Cada reporte deberá al menos contener: Estatus del incidente (nuevo, en progreso, remitido a investigación, resuelto, etc.), un resumen del incidente, acciones tomadas para la gestión del incidente, impacto en los activos relacionados, así como los próximos pasos a tomar. El primer reporte deberá de entregarse en un término no mayor a 3 horas después de sucedido el incidente y se emitirán más reportes hasta que concluya la respuesta al incidente, debiendo de entregarlos cuando haya algún avance significativo y/o el período de entrega entre uno y otro no exceda las 12 horas."
82	Lote 6	Gobierno	Pregunta: Por favor indicar; ¿Se requiere participación en comités de seguridad y gobierno?	No. Tal como lo establece el Documento de Licitación, Seccion VI. Lista de Requisitos, Lote 6, Características del Servicio, numeral "5. El servicio debe considerar un proceso de mejora continua, sin perjuicio de las actividades realizadas en la “Etapa de Ajustes", en la “Etapa de Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad", debiendo hacerse los ajustes a las configuraciones y procedimientos que pueden tener los siguientes orígenes: 5.1.A solicitud de la CNBS para dar cobertura a casos concretos que se necesiten, enmarcados en el alcance definido en los requerimientos técnicos de este documento. 5.2.En base a propuestas proactivas del oferente en base a su experiencia. 5.3.Como producto de las siguientes Reuniones Técnicas: 5.3.1.Semanales durante los primeros 2 meses de Servicio. 5.3.2.Quincenales durante los meses 3 y 4 de Servicio. 5.3.3.Mensuales a partir del 5to mes de Servicio."

83	Lote 6	Integración ITSM	Pregunta: Por favor indicar; ¿Se requiere integración con herramientas de gestión de tickets?	Tal como lo establece el Documento de Licitación, Seccion VI. Lista de Requisitos, Lote 6, Características del Servicio, numeral "3. Conceder a la CNBS una herramienta a través de la cual se realice mediante un sistema de Tickets reporte de las alertas que requieren ser conocidas por la misma o en las que se requiere su retroalimentación para ajustes, estableciendo mecanismos para que dentro de la misma se pueda realizar el intercambio de preguntas y respuestas, así como cierres de dichos Tickets. Esta herramienta debe contar con uno o varios Cuadros de Mando (Dashboard) que permitan visualizar todos los Tickets y sus estados."
84	Lote 6	Retención	Pregunta: Por favor indicar; ¿Cuál es el periodo de retención de logs en el SOC?	Tal como lo establece el Documento de Licitación, sección VI. Lista de Requisitos, Lote 6, Características Generales, "Retención de datos en línea (on-line) 1 mes Retención de datos fuera de línea (off-line) 6 meses"
85	Lote 6	MDR	Pregunta: Por favor indicar; ¿Se espera que el proveedor ejecute acciones de contención activa (MDR)?	Tal como se establece en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, numeral "1.5.4. Contar con solución SOAR para la orquestación de eventos, automatización y brindar, a nivel de XDR o solución semejante, respuesta inmediata y/o automática sobre incidentes con patrones de comportamiento citados en el framework de MITRE ATT&CK y que, en base al criterio experto del proveedor del servicio, convenga configurar una respuesta automática. Dicha respuesta deberá ser compatible o integrable con la Solución de Protección Perimetral y demás soluciones de Protección de la CNBS."
86	Lote 6	Compliance	Pregunta: Por favor indicar; ¿Se requieren reportes alineados a regulaciones financieras?	No. Tal como lo establece el Documento de Licitación, Seccion VI. Lista de Requisitos, Lote 6, Características del Servicio, debe dar cumplimiento a los numerales 1 al 6, así como Requisitos Adicionales, numerales 10-19.
87	Lote 6	Integración XDR	Pregunta: Por favor indicar; ¿Se requiere correlación con plataformas EDR/XDR (Lote 1)?	Si.
88	Lote 6	Transición	Pregunta: Por favor indicar; ¿Se requiere fase de transición y conocimiento (shadowing)?	Tal como se establece en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Etapas y Duración del Servicio, "7. Etapa de implementación 7.1. Actividad: En esta etapa el proveedor del servicio realizará el aprovisionamiento y configuraciones iniciales necesarias para brindar los servicios. 7.2. Duración: Máximo 90 días calendario a partir de la fecha de suscripción del contrato. 7.3. Esta etapa quedará finalizada cuando las siguientes actividades sean completadas: 7.3.1. Suministro a la CNBS de las licencias, suscripciones, equipos y/o servicios necesarios para brindar el servicio. 7.3.2. Configuración inicial de la plataforma para asegurar la implementación del servicio. La CNBS emitirá acta de aceptación de la etapa de implementación. 8. Etapa de Ajustes 8.1. Actividad: En esta etapa el proveedor del servicio realizará los ajustes iniciales necesarios para brindar los servicios de forma más afinada. 8.2. Duración: Máximo 45 días calendario a partir de la fecha de aceptación de la etapa de Implementación. 8.3. Esta etapa quedará finalizada cuando las siguientes actividades sean completadas: 8.3.1. Puesta en marcha del servicio, por un período de aprendizaje y ajustes, con una duración máxima de 45 días calendario. 8.3.2. Realización de los ajustes a la configuración de los recursos y los procedimientos asociados al servicio, de conformidad a las oportunidades de mejora identificadas en el período inicial de puesta en marcha del servicio. Los ajustes podrán realizarse de forma paralela a su identificación. 8.3.3. Realización de al menos una reunión semanal, en la que se listen las oportunidades de mejora, así como el avance en la implementación de estas en el transcurso del tiempo. La CNBS emitirá acta de aceptación de la etapa de ajustes. 9. Etapa de Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad Actividad: En esta etapa el servicio ya se encuentra operando de manera más afinada de conformidad a los ajustes hechos en la etapa de Ajustes. 9.2. Duración: Desde de la fecha de aceptación de la etapa de Ajustes hasta el 31 de diciembre de 2026. **IMPORTANTE: Sección VI. Formularios de Oferta** 1.- Para el Lote 6, el oferente debe proponer la cantidad de meses de servicio tomando en consideración los plazos límite para las etapas de implementación y ajustes, así como la fecha estimada para inicio del contrato. En el caso de que el oferente adjudicado finalice antes de los tiempos estimados en dichas etapas y pueda cubrir meses adicionales dentro del presente ejercicio fiscal, se podrá formalizar la ampliación mediante Adendum de conformidad a lo dispuesto en la Ley de Contratación del Estado, su Reglamento y el porcentaje del 24% de ampliación considerado en el presente documento base, específicamente en la IAO 42.1 de la Sección II. Datos de la Licitación. 2.- La CNBS no emitirá pagos por las etapas de implementación y ajustes, únicamente por los meses de servicio prestados por lo que se requiere considerar únicamente los meses de servicio en la Lista de Precios. 3.- Si los meses de servicio no son computados desde el 1 de cada mes, el pago se hará proporcional a los días de servicio prestados ya que la vigencia del contrato debe finalizar el 31 de diciembre de 2026. 4.- La cantidad de servicios del Formulario de Lista de Precios debe ser congruente con los plazos ofertados en el Formulario de Lista de Servicios y Plan de Entregas de la Sección VI. Lista de Requisitos. Datos para que el oferente del Lote 6 proponga la cantidad de meses de servicio: Fecha estimada para inicio del contrato: 15 de mayo de 2026 Plazo Límite para Etapa de Implementación: Noventa (90) días calendarios a partir de la fecha de suscripción del contrato Plazo Límite para Etapa de Ajustes: Cuarenta y Cinco (45) días calendarios a partir de la fecha de finalización expresa de la etapa de implementación.
89	Lote 7	Vulnerability Management (Tenable One)	Pregunta: Por favor indicar; ¿Cuál es el inventario de activos detallado?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 7. Por lo que no se requiere dimensionar el inventario de activos.
90	Lote 7	Vulnerability Management (Tenable One)	Pregunta: Por favor indicar; ¿Cuál es la Frecuencia de escaneo requerida?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 7. Por lo que no se requiere dimensionar la frecuencia de escaneo requerida.
91	Lote 7	Vulnerability Management (Tenable One)	Pregunta: Por favor indicar; ¿Se requiere que el escaneo sea autenticado o no autenticado?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 7. Por lo que no se requiere dimensionar la tipo de autenticación o no para el escaneo.
92	Lote 7	Vulnerability Management (Tenable One)	Pregunta: Por favor indicar; ¿Se requiere que el escaneo autenticado vs no autenticado?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 7. Por lo que no se requiere dimensionar la tipo de autenticación o no para el escaneo.
93	Lote 7	Vulnerability Management (Tenable One)	Pregunta: Por favor indicar; ¿Requiere integración con patch management?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 7. Por lo que no se requiere dimensionar integración con patch management.
94	Lote 7	Vulnerability Management (Tenable One)	Pregunta: Por favor indicar; ¿Rquiere cobertura Cloud?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 7. Por lo que no se requiere dimensionar cobertura Cloud.

95	Lote 8	Awareness	Pregunta: Por favor indicar; ¿Cuál es el inventario o segmentación de usuarios?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 8. Por lo que no se requiere dimensionar inventario o segmentación de usuarios.
96	Lote 8	Awareness	Pregunta: Por favor indicar; ¿Cuál es la frecuencia de campañas phishing?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 8. Por lo que no se requiere dimensionar frecuencia de campañas de phishing.
97	Lote 8	Awareness	Pregunta: Por favor indicar; ¿El contenido para las campañas de phishing deben ser personalizadas en su contenido?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 8. Por lo que no se requiere dimensionar el contenido para las campañas de phishing.
98	Lote 8	Awareness	Pregunta: Por favor indicar; ¿Cuál es el idioma y contexto local con el que se deben tener las campañas de phishing?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 8. Por lo que no se requiere dimensionar el idioma y contexto local para las campañas de phishing.
99	Lote 8	Awareness	Pregunta: Por favor indicar; ¿Cuál es son las métricas de riesgo humano esperadas por CNBS en el presente servicio?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 8. Por lo que no se requiere dimensionar las métricas de riesgo humano.
100	Lote 8	Awareness	Pregunta: Por favor indicar; ¿Se deben crear reportes personalizados para el manejo de pruebas de phishing con los resultados obtenidos de usuarios críticos (privilegiados) o todos deben ser estandar?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 8. Por lo que no se requiere dimensionar los reportes personalizados para el manejo de pruebas de phishing.
101	Lote 8	Awareness	Pregunta: Por favor indicar; ¿Se deben enmarcar las pruebas de phishing para cumplimiento de algun ente regulatorio?	Se está renovando un producto ya implementado, con la información debidamente detallada en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 8. Por lo que no se requiere dimensionar si las pruebas de phishing son en cumplimiento de algún ente regulatorio.
102	Gnal.	Tiempo del servicio	Pregunta: Por favor indicar; ¿Es posible que XXX entregue una oferta no solicitada por mayor cantidad de tiempo, buscando la optimización de costos por la cantidad de tiempo del servicio?	No es posible ofertar por plazos que superen los indicados en el documento base, caso contrario la oferta no será considerada por establecer condiciones que no fueron requeridas.
103	Gnal.	Polizas	Pregunta: Por favor indicar; ¿Cuáles son las polizas que debemos tener en cuenta en el presente proceso para cotizarlas "poliza de seriedad / poliza de participación / poliza de penalización entre otras"?	Entiendáse "pólizas de seriedad/ de participación y de penalización" como las Garantías contempladas en el documento base como son la Garantía de Mantenimiento de Oferta y la Garantía de Cumplimiento de Contrato. Los lineamientos para la presentación de la Garantía de Mantenimiento de Oferta están contemplados en las cláusulas IAO 21.2, 21.3 y 21.8 de la Sección II. Datos de la Licitación (pág.37) y el formato obligatorio para las garantías bancarias y fianzas las ubica en la página 67. En el caso de resultar adjudicados de uno o varios lotes se solicita la presentación de la Garantía de Cumplimiento de Contrato, regulada en la Cláusula CGC 17.3 de la Sección VIII. Condiciones Especiales del Contrato (págs. 121-122) y su formato de uso obligatorio lo ubica en la página 133 del documento base.
104	Lote 6		**Consulta Clasificada "CONFIDENCIAL"**	**CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.2. Este Anexo se compartirá únicamente a los participantes registrados que hayan presentado el Acuerdo de Confidencialidad conforme lo establecido en la cláusula IAO 7.1 de la Sección II. Datos de la Licitación del DB.**
105	Gnal.	IAO 18.3	Agradecemos a la entidad confirmar si actualmente las soluciones que tiene sin licencia activa estan sin soporte y sin actualizacion de firmas?	Se confirma que actualmente la soluciones que se tienen sin licencia activa están sin soporte y sin actualización de firmas.
106	Gnal.	IAO 18.3	Agradecemos a la entidad confirmar si tienen claro que la fecha inicio corre a partir de la fecha de vencimiento que relaciona o necesitan que se realiza una nivelacion en las fechas de terminación.	Como se indica en el documento base, las fecha de inicio debe correr a partir de la fecha de firma del contrato. En este sentido, el oferente deberá estimar junto al fabricante cual será la nueva fecha de vencimiento, de tal forma que cumpla con un mínimo de doce (12) meses a partir de la firma del contrato.
107	Lote 1	Renovación de Solución Corporativa de Protección de Puntos Finales (Endpoint Protection Platform) – CrowdStrike Falcon Enterprise	Agradecemos a la entidad confirmar los features que actualmente tiene activa con la fabrica	Como se indica en el documento base, los features actualmente asociados a la CNBS son los siguientes: - Falcon Endpoint Protection Enterprise Flexible Bundle - Threat Graph Standard - Falcon Firewall Management Bundle Promo - Falcon Prevent - Falcon Insight - Falcon Adversary OverWatch Endpoint - Falcon Device Control Bundle Promo
108	Lote 2	Renovación de Solución para Monitoreo de Actividades de Bases de Datos – Thales Imperva Data Secure Fabric	Agradecemos a la entidad confirmar numero de parte o serial de la solcuion	Como se indica en el documento base, el nombre de los productos/servicios son: - App Protect Professional 50Mbps Base Plan - Edge Load Balancing Add-On Con esa información, y el nombre de cuenta, el oferente puede contactarse con el fabricante y determinar el producto/servicio que actualmente tiene asignado la CNBS.

109	Lote 6	Renovación del Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad en la Infraestructura Tecnológica de la CNBS.	Agradecemos a la entidad confirmar la cantidad de fuentes a monitorear	La cantidad de fuentes a monitorear está debidamente indicada en el Documento de Licitación, sección VI. Lista de Requisitos, Lote 6, Características Generales.
110	Lote 6	Renovación del Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad en la Infraestructura Tecnológica de la CNBS.	Posterior a la firma del Acuerdo de Confidencialidad (NDA), ¿podrá la CNBS proporcionar la lista completa de las fuentes de datos, valores estimados de EPS/FPS, volumen de registros (logs), formatos de logs y periodos de retención requeridos para efectos de dimensionamiento? De no ser posible, ¿podría facilitarse al menos un desglose de los tipos y fabricantes de los nodos (160), endpoints (600) y activos de red (1,500) que serán incorporados al servicio, con el fin de realizar una estimación de precios más precisa para la solución SIEM?	Es correcto, posterior a la Firma del Acuerdo de Confidencialidad (NDA), el oferente tendrá acceso a la lista con información técnica detallada de las fuentes de datos, lo que permitirá determinar los formatos de logs de acuerdo a la Plataforma que oferte. En cuanto a los valores estimados de EPS/FPS, en respuesta a consulta previa se indicó que el volumen promedio de eventos es de 510 GB por día, con picos máximos de alrededor de 2.8 TB por día. En cuanto a los períodos de retención requeridos, los mismos ya están señalados en el Documento de Licitación, sección VI. Lista de Requisitos, Lote 6, Características Generales, "Retención de datos en línea (on-line) 1 mes Retención de datos fuera de línea (off-line) 6 meses"
111	Lote 6	Renovación del Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad en la Infraestructura Tecnológica de la CNBS.	Respecto a los 1,500 activos monitoreados a través de puertos mirror/SPAN, ¿qué proporción de estos ya se encuentra incluida dentro de los 160 nodos y 600 endpoints, y qué clases de activos adicionales conforman el resto? Si bien el cartel indica que los 1,500 activos incluyen nodos y endpoints, se solicita confirmar la composición exacta para un adecuado dimensionamiento de la capa NDR.	Tal como lo establece el Documento de Licitación, sección VI. Lista de Requisitos, Lote 6, Características Generales, dentro de los 1.500 activos se incluyen los 160 nodos a ser monitoreados, así como los 600 Endpoints Gestionados a través de las Soluciones de Protección de Endpoints, el resto de activos corresponden a aquellos usuales cuyo tráfico pasa por un SwitchCore, incluyendo equipos de comunicación, servidores y otros dispositivos finales.
112	Lote 6	Renovación del Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad en la Infraestructura Tecnológica de la CNBS.	¿Existen fuentes en la nube que requieran integración nativa mediante API, tales como Microsoft 365, Azure, Entra ID, AWS, plataformas SaaS o firewalls en la nube, o debe asumirse únicamente la integración de las fuentes que se revelen explícitamente posterior a la firma del NDA?	Detalles técnicos de las fuentes de Datos son consideradas de carácter confidencial, por lo que tal como se establece en el Documento de Licitación, sección II. Datos de la Licitación, IAO 7.1, se compartirán únicamente a las sociedades registradas e interesadas en participar en el presente proceso que hayan presentado el “Acuerdo de Confidencialidad”, firmado y sellado por el Representante Legal de la sociedad registrada, acompañado de la copia del DNI del Representante Legal y el Poder de Representación que lo faculte para tal efecto.
113	Lote 6	Renovación del Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad en la Infraestructura Tecnológica de la CNBS.	En caso de proponerse un sensor virtual, ¿podría la CNBS indicar qué plataforma de hipervisor (por ejemplo, Microsoft Hyper-V, VMware ESXi, u otra), así como los estándares de cómputo, almacenamiento y red disponibles actualmente en la institución, considerando que el cartel establece que la CNBS evaluará la posibilidad de alojar los appliances virtuales propuestos?	La CNBS utiliza como plataforma de hipervisor, Hyper-V y tal como lo señala el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Requisitos Adicionales, numeral 10 "...En caso de que la propuesta incluya el hospedaje de uno o varios appliances virtuales en la Infraestructura de la CNBS, el oferente deberá indicar claramente en su oferta los recursos técnicos requeridos. La CNBS evaluará y comunicará si cuenta con la capacidad para hospedar el(los) appliance(s) virtual(es) propuesto(s), considerando la compatibilidad con su infraestructura tecnológica y la disponibilidad de recursos."
114	Lote 6	Renovación del Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad en la Infraestructura Tecnológica de la CNBS.	¿Cuáles son las soluciones perimetrales y de protección actualmente implementadas con las cuales deberá integrarse la capa de respuesta? El cartel indica la necesidad de compatibilidad o integración con las soluciones de perímetro y protección de la CNBS, sin detallar explícitamente cuáles son.	Detalles técnicos de las fuentes de Datos son consideradas de carácter confidencial, por lo que tal como se establece en el Documento de Licitación, sección II. Datos de la Licitación, IAO 7.1, se compartirán únicamente a las sociedades registradas e interesadas en participar en el presente proceso que hayan presentado el “Acuerdo de Confidencialidad”, firmado y sellado por el Representante Legal de la sociedad registrada, acompañado de la copia del DNI del Representante Legal y el Poder de Representación que lo faculte para tal efecto.
115	Lote 6	Renovación del Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad en la Infraestructura Tecnológica de la CNBS.	¿Cuenta la CNBS con un tenant propio de Microsoft Azure en el cual se alojará la solución Microsoft Sentinel (SIEM), o se espera que dicho tenant sea provisto por el oferente como parte de la propuesta?	La CNBS no dispone de un tenant de Microsoft Azure específicamente habilitado ni configurado para la implementación de soluciones SIEM como Microsoft Sentinel. Tal como lo establece el Documento de Licitación, Seccion VI. Lista de Requisitos, Lote 6, Características del Servicio, numeral "1.5. El servicio deberá contar con una plataforma que integre la(s) solución(es) necesaria(s) para el monitoreo, detección y respuesta de incidentes de ciberseguridad. Dicha plataforma deberá tener las siguientes capacidades: 1.5.1. Realizar ingesta, correlación y almacenamiento de insumos provenientes de diferentes fuentes en un ambiente de trabajo híbrido, tanto en premisa (on-premise): servidores (físicos y virtuales), equipos de comunicación, Next Generation Firewall (NGFW); como soluciones en la nube (cloud-based-systems). Dicha actividad debe realizarse no solamente de la data proveniente de la instalación de agentes en las fuentes, conectores o reenvío de logs mediante protocolo syslog hacia el colector de eventos, sino también de la captura de tráfico de red a través de puerto espejo en el Switch Core de la CNBS, a fin de identificar e investigar diversos tipos de ataques." Asimismo, en los Requisitos Adicionales de dicho Lote, numeral "10. La propuesta debe contemplar todas las licencias, suscripciones, appliance(s) físico y/o servicios requeridos para el correcto funcionamiento del servicio ofertado...". En este sentido, si el servicio ofertado utiliza Microsoft Sentinel como SIEM, queda a criterio del oferente si desea activar una suscripción de Azure para este uso exclusivo bajo el tenant actual de la CNBS.

115	Gnal.	Plazo Apertura de Ofertas	¿existe la posibilidad de otorgar una prórroga al plazo establecido para la presentación de ofertas, con el fin de contar con el tiempo necesario para preparar una propuesta técnica y económica adecuada, en estricto cumplimiento de los requisitos del proceso?	Para la presente Licitación Pública Nacional no es posible brindar ampliación en la fecha indicada para la recepción y apertura de ofertas en virtud que se espera minimizar el desfase en las fechas de expiración de los suministros que componen los ocho (8) lotes del presente proceso conforme a lo indicado en la cláusula IAO 18.3 de la Sección II. Datos de la Licitación del documento base (pág.36).

La presente Circular Aclaratoria No.2 forma parte integral del documento base del referido proceso de licitación, así como su Anexo en el que constan dos (2) consultas y sus respectivas aclaraciones que han sido clasificadas como “CONFIDENCIALES” de conformidad a lo establecido en la cláusula IAO 7.1 de la Sección II. Datos de la Licitación del Documento Base.

Tegucigalpa, M.D.C., 8 de abril de 2026

FERNANDO GONZÁLEZ VILLARS
Gerente Administrativo