



LPN-CNBS-001-2026  
“ADQUISICIÓN Y RENOVACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA COMISIÓN  
NACIONAL DE BANCOS Y SEGUROS”

CIRCULAR ACLARATORIA No.3

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, tomando en consideración que **las primeras veinte (20) consultas y sus respuestas** aplican únicamente para el **Lote 6: Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad en la Infraestructura Tecnológica de la CNBS.**

Consulta No.1

“CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.3. 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.”

Consulta No.2

“CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.3. 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.”

Consulta No.3

“CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.3. 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.”

Consulta No.4

“¿Qué integraciones de seguridad XDR en la nube tienen implementadas actualmente? (Ej.: Microsoft 365, Azure, AWS, Duo, Okta, Google Workspace)”

R/= Microsoft 365

Consulta No.5

“En relación con la seguridad de endpoints, ¿requieren un servicio gestionado o únicamente monitoreo mediante XDR? (Gestionado / Monitorizado)”

R/= Tal como lo establece el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Características del Servicio, numerales “1. El servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad deberá contar con las siguientes funciones y características:

1.1. Monitoreo Continuo: Monitorear los eventos que sucedan en la Infraestructura Tecnológica de la CNBS, a fin de identificar actividades sospechosas o maliciosas en tiempo real (real-time).



1.2. Detección de Incidentes: Detectar incidentes de ciberseguridad que afecten la infraestructura tecnológica de la CNBS, provenientes de amenazas internas y/o externas. El proveedor del servicio deberá estar en la capacidad de identificar y depurar falsos positivos, así como realizar la correspondiente priorización de alertas.

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.

...

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.

1.5.2. Incorporar capacidades UEBA (User and Entity Behavior Analytics), que se enfoque en analizar el comportamiento de usuarios y entidades para detectar actividades potencialmente maliciosas y anómalas.

1.5.3. Utilizar machine learning/inteligencia artificial para detectar actividades anómalas.

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.”

#### Consulta No.6

**“CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.3. 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.”**

#### Consulta No.7

**“¿Cuántos endpoints requieren ser monitoreados?”**

R/= Como lo establece el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Información General:

#### Información General:

Capacidad	Dato
Cantidad de nodos a ser monitoreados mediante Agente, Conectores o reenvío de Logs mediante protocolo syslog: Servidores físicos y/o virtuales, equipos de comunicación, NGFW, Soluciones de Ciberseguridad, tanto on premise como en Nube	160 nodos
Endpoints	600 Endpoints Gestionados a través de Soluciones de Protección de Endpoints
Activos en la Red a ser monitoreados a través de Puerto Espejo	1,500 (incluye los nodos y Endpoints arriba indicados)



#### Consulta No.8

“¿En qué ubicación (on-premise o nube) se encuentra alojado el servidor de gestión de endpoints?”

R/= En Nube.

#### Consulta No.9

“CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.3. 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.”

#### Consulta No.10

“CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.3. 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.”

#### Consulta No.11

“CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.3. 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.”

#### Consulta No.12

“En cuanto a la infraestructura de seguridad de red: ¿Cuántos sitios o ubicaciones poseen?”

R/= Sitio Principal actualmente en producción y Sitio Alterno en Proceso mediante Licitación bajo expediente LP-CNBS-001-2026.

#### Consulta No.13

“CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.3. 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.”

#### Consulta No.14

“CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.3. 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.”



#### Consulta No.15

“En caso de múltiples sitios, ¿existen conexiones entre ellos (VPN, MPLS u otras)?”

R/= VPN, por lo que es transparente para el oferente la ubicación de los equipos en sitio alterno.

#### Consulta No.16

“¿Disponen de algún hipervisor o entorno virtual donde pueda alojarse el agente colector XDR, en caso de no contar con hardware dedicado?”

R/= 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."

#### Consulta No.17

“CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.3. 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.”

#### Consulta No.18

*Sección VI Lista de Requisitos. Numeral 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. ¿Existen restricciones regulatorias, operativas o de seguridad que limiten la implementación de un modelo híbrido, en el cual los componentes de recolección e integración de datos se desplieguen in situ (on-premises), mientras que la operación y monitoreo del SOC se lleven a cabo fuera del territorio de Honduras?”*

R/= No existen restricciones regulatorias ni operativas. En cuanto a seguridad, tal como lo señala el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Requisitos Adicionales, numeral 18 "Certificación vigente ISO/IEC 27001:2022 de su SOC (Centro de Operaciones de Seguridad), que acredite los mecanismos de Seguridad para asegurar la confidencialidad, integridad y disponibilidad de la información involucrada en los servicios prestados.

#### Consulta No.19

“Numeral 18. Certificación vigente ISO/IEC 27001:2022 de su SOC (Centro de Operaciones de Seguridad), que acredite los mecanismos de Seguridad para asegurar la confidencialidad, integridad y disponibilidad de la información involucrada en los



**servicios prestados. ¿Para la certificación del SOC solicitada, es válido presentar certificaciones del personal en ISO/IEC 27001? Asimismo, ¿es posible complementar este requisito con certificaciones adicionales equivalentes o complementarias que respalden la operación del SOC propuesto?”**

R/= Tal como lo señala el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 6, Requisitos Adicionales, numeral 18, se establece explícitamente la certificación vigente del SOC (Centro de Operaciones de Seguridad), lo cual implica una certificación organizacional, emitida por un organismo certificador acreditado, que evidencie que el SOC opera bajo un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022. En ese sentido, las certificaciones del personal no se consideran válidas para el cumplimiento del requisito, ya que no sustituyen ni equivalen a la certificación del servicio o de la organización. Las certificaciones adicionales podrán presentarse únicamente como respaldo complementario; sin embargo, no serán consideradas válidas para dar cumplimiento al requisito exigido, ni como equivalentes o sustitutas de la certificación ISO/IEC 27001:2022 del SOC.

#### **Consulta No.20**

**“Sección VI Lista de Requisitos ¿Es necesario incluir la conectividad como parte del alcance del servicio? En caso afirmativo, ¿existe algún proveedor, tecnología o protocolo de preferencia que deba considerarse?”**

R/= No se está solicitando conectividad, en caso de requerir alguna conexión, se levantará un túnel VPN site-to-site.

#### **Consulta No.21**

**“¿Puede presentarse con firma digital la autorización del fabricante ya que en el proceso anterior de 2024 para estas mismas soluciones presentamos estos documentos de esa manera o necesitan que se presenten apostillados?”**

R/= Ver Enmienda No.1 del 14 de abril de 2026 que contiene los parámetros de firma electrónica aceptados por la Comisión Nacional de Bancos y Seguros.

#### **Consulta No.22**

**“Considerando que son renovaciones, ¿qué información requieren que sea proporcionada en la parte técnica? Podríamos presentar solo un cuadro de cumple / no cumple?”**

R/= Si, presentar cuadro de cumple/no cumple a lo señalado en el Documento de Licitación, Sección VI. Lista de Requisitos, Lote 7: Información General, Numeral 1 y Numeral 2, debiendo consignar el SKU, número de parte, nombre de plan, y/o cualquier identificador de la licencia/suscripción a renovar que corresponda. Así como dar cumplimiento al Requisito General de dicho Lote, Incluyendo constancia de fabricante que indique que el proveedor es un distribuidor autorizado de la solución.

#### **Consulta No.23**

**“¿Requieren sobres separados para la presentación de la información legal, técnica, financiera y económica? ¿Podemos entregar un solo sobre y un solo encuadernado considerando que estaremos participando en varios lotes?”**



R/= Conforme a la Cláusula IAO 23.2 de la Sección II. Datos de la Licitación (página 38 del documento base), la información debe separarse en sobres diferentes indicando “Legal, Técnica, Financiera y Económica” con la aclaración de la información legal, financiera y económica es la misma para la participación de uno, varios o todos los lotes. En el sobre que contiene la documentación técnica debe constar la información técnica requerida para cada lote, dejando clara a qué lote pertenecen los documentos. En el caso que se presente un solo sobre, se debe dejar claro cuál es la documentación técnica que proponen para los lotes ofertados. En ambos casos de presentación, **toda** la información **debe estar foliada** conforme a lo indicado a la cláusula IAO 22.1 de la Sección II. Datos de la Licitación (página 37 del documento base). No es necesario presentar copias.

#### Consulta No.24

##### “Especificaciones Técnicas

Lote No. 05 Renovación de Licencias y Soporte de Solución para la Gestión de Actualizaciones (Patch Manager)  
Características

Lista de Precios y Plan de Entregas

Fecha Límite de Entrega: 15 Días Calendario después de la firma del contrato

Consulta: Respecto al plazo de entrega establecido en los términos de referencia, respetuosamente deseamos plantear una consideración técnica sobre su viabilidad. La solución requerida, basada en nube, implica una implementación integral desde cero, que contempla instalación, configuración, integración con el entorno y validación controlada, por lo que un plazo de 15 días calendario resulta insuficiente para garantizar una ejecución adecuada y alineada a buenas prácticas. En este sentido, sugerimos respetuosamente evaluar una ampliación del plazo, tomando en consideración el tiempo que fue establecido por la Comisión Nacional de Bancos y Seguros en la adquisición original de este lote, el cual respondía de forma más realista a la complejidad de la implementación.

R/= El plazo de 15 días calendario es para la activación y asignación de las licencias a la cuenta de la CNBS. Para la configuración inicial y el enrolamiento de 20 estaciones de trabajo no existe fecha límite, pero tomar en consideración que no se emitirá acta de recepción del producto hasta haberse cumplido esta actividad.

#### Consulta No.25

Lote No. 06 Servicio de Monitoreo, Detección y Respuesta a Incidentes de Ciberseguridad en la Infraestructura Tecnológica de la CNBS

Formulario Lista de Precios

Datos para que el Oferente proponga la cantidad de meses de servicio

Fecha estimada para inicio del contrato: 15 de Mayo de 2026

Consulta: Respecto a la fecha estimada para inicio de contrato, 15 de Mayo de 2026, apreciamos confirmar si esta fecha se encuentra actualizada considerando que la apertura de ofertas es el 22 de Abril y que entre esta fecha y la fecha estimada de inicio de contrato, 15 de Mayo, transcurren un promedio de tres (3) semanas en la que se deberá cumplir el proceso de subsanación, si fuera el caso, adjudicación y oficializar la firma del contrato? Agradecemos su confirmación.”

R/=Ver Enmienda No.1 del 14 de abril de 2026.



#### Consulta No.26

**“Favor aclarar si, para efectos de la presente licitación, la CNBS aceptará documentos suscritos mediante firma electrónica simple, firma electrónica avanzada y/o firma digital, y cuál de dichas modalidades considera válida para cada tipo de documento de la oferta.”**

R/= Ver Enmienda No.1 del 14 de abril de 2026 que contiene los parámetros de firma electrónica aceptados por la Comisión Nacional de Bancos y Seguros.

#### Consulta No.27

**“En caso de aceptar firma electrónica o firma digital, favor indicar si la CNBS exige que la misma provenga de un prestador de servicios de certificación acreditado en Honduras, o si también aceptará certificados emitidos en el extranjero, siempre que permitan verificar autenticidad, integridad y no repudio del documento.”**

R/= Ver Enmienda No.1 del 14 de abril de 2026 que contiene los parámetros de firma electrónica aceptados por la Comisión Nacional de Bancos y Seguros.

#### Consulta No.28

**“¿Cuáles documentos de la oferta deben presentarse necesariamente con firma autógrafa y cuáles pueden presentarse válidamente con firma electrónica o digital?”**

R/= Los únicos documentos que pueden presentarse con firma electrónica son la Autorización del Fabricante, Certificación Accionaria y Constancias de Servicios de Satisfacción, y excepcionalmente el Acuerdo de Consorcio. Ver Enmienda No.1 del 14 de abril de 2026 que contiene los parámetros de firma electrónica aceptados por la Comisión Nacional de Bancos y Seguros.

#### Consulta No.29

**“Favor aclarar si las declaraciones juradas requeridas en el proceso deben presentarse exclusivamente en original físico con firma autenticada ante notario, o si podrán presentarse con firma electrónica avanzada del suscriptor y, en su caso, en qué condiciones.”**

R/= Todas las declaraciones juradas deben presentarse exclusivamente en original físico con firma autenticada ante notario. Ver Enmienda No.1 del 14 de abril de 2026 que contiene los parámetros de firma electrónica aceptados por la Comisión Nacional de Bancos y Seguros.

#### Consulta No.30

**“En el caso de documentos emitidos en el extranjero, tales como cartas del fabricante, autorizaciones del fabricante, certificaciones, constancias corporativas, poderes o documentos equivalentes, favor indicar si serán aceptados cuando estén suscritos electrónicamente o digitalmente por su emisor. Y, en caso de ser firmadas electrónicamente, ¿debe el documento ser apostillado?”**

R/= Los únicos documentos que pueden presentarse con firma electrónica son la Autorización del Fabricante, Certificación Accionaria y Constancias de Servicios de Satisfacción, y excepcionalmente el Acuerdo de Consorcio. Ver Enmienda No.1 del 14 de abril de 2026 que contiene los parámetros de firma electrónica aceptados por la Comisión Nacional de Bancos y Seguros. Si los instrumentos públicos en los que consta la constitución de la empresa,



modificación de denominación social, aumento o disminución de capital, poder de representación, etc., son expedidos en el exterior, deben apostillarse y autenticarse para tener validez en Honduras.

### Consulta No.31

**“Favor aclarar si la sola impresión en papel de un documento originalmente firmado electrónicamente o digitalmente será suficiente para su admisión en este proceso, o si debe acompañarse de evidencia adicional de validación del certificado o de la firma.”**

R/= Ver Enmienda No.1 del 14 de abril de 2026 que contiene los parámetros de firma electrónica aceptados por la Comisión Nacional de Bancos y Seguros. Adicionalmente a la impresión en papel de un documento originalmente firmado electrónicamente, se requiere la remisión del PDF al correo oficial de licitaciones para comprobar su validez. Es opcional acompañar el reporte de veracidad ya que esta será comprobada contra el PDF.

### Consulta No.32

**“En caso de presentarse documentos firmados electrónicamente o digitalmente, la falta de un criterio previamente definido por la administración podrá ser causal de rechazo o descalificación de la oferta.”**

R/=En caso de no cumplir con los parámetros consignados en la Enmienda No.1 del 14 de abril de 2026 o que el PDF no pueda ser validado de manera digital, el requisito está sujeto a subsanación. Si este requisito es presentado en etapa de subsanación y no cumple con lo dispuesto, se incurre en una causal de descalificación por no cumplir sustancialmente con lo requerido.

La presente Circular Aclaratoria No.3 forma parte integral del documento base del referido proceso de licitación, así como su Anexo en el que constan diez (10) 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., 14 de abril de 2026

**FERNANDO GONZÁLEZ VILLARS**

Gerente Administrativo