República de Honduras

COMISIÓN NACIONAL DE BANCOS Y SEGUROS

LPN-CNBS-008-2024
"ADQUISICIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA COMISIÓN NACIONAL DE BANCOS Y SEGUROS"

CIRCULAR ACLARATORIA No.4

La Comisión Nacional de Bancos y Seguros (CNBS) comunica que, en atención a consultas realizadas por participantes registrados en el proceso de Licitación Pública Nacional **No. LPN-CNBS-008-2024** denominada **"ADQUISICIÓN 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 hace la siguiente aclaración:

Consulta No.1
Lote 1: Adquisición de Solución Corporativa de una Plataforma de Protección de Puntos Finales (Endpoint Protection Platform)

1-A. "¿La solución de FortiEDR es nativa en la nube?"
R/= Esa es una respuesta que debe brindar el oferente con la documentación técnica que presente.

1-B. "**Del inciso 9.1 ¿Podrían brindarnos un mayor contexto o indicarnos cuáles son esas amenazas del entorno de la CNBS**?"
R/= En el contexto del numeral 9 de la capacidad de la Solución de contar con Inteligencia de Amenazas para potenciar la protección, se refiere a que la herramienta debe tener la capacidad de comprender el entorno en el que se está ejecutando, tomando en cuenta factores como el sistema operativo de los Endpoints, las aplicaciones que se hospedan en el mismo, entre otros, para determinar las amenazas de dicho entorno de la CNBS.

1-C. "**Del inciso 9.2 ¿Cuál es la expectativa d SLA definido por la CNBS para la recuperación?"**
R/= En ninguna parte de este numeral se está mencionando un SLA. En el contexto del numeral 9 de la capacidad de la Solución de contar con Inteligencia de Amenazas para potenciar la protección, se refiere a la capacidad de priorizar las amenazas a fin de priorizar las respuestas.

1-D. "¿La respuesta ante incidentes, debe ser gestionada por el partner o por la Marca de la Solución?"
R/= La respuesta a un incidente materializado, por ejemplo, la presencia de un malware debe ser gestionada por la propia Solución.

1-E. "**Del inciso 9.4 ¿A qué se refieren con indicadores de compromiso personalizados? La herramienta trae los propios**."
R/= La Solución en efecto debe tener su base de datos de IOCs, sin embargo, en el contexto del numeral 9 de la capacidad de la Solución de contar con Inteligencia de Amenazas para potenciar la protección, debe tener la

Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

capacidad de analizar de forma automatizada las amenazas de los Endpoints para identificar de forma personalizada los IOC que apliquen.

1-F. "Del inciso 10.1 ¿Toda solución necesita configuración previa para la detección de incidentes, a que se refieren puntualmente con ese inciso?"
R/= Se refiere a que, una vez instalado el agente en el Endpoint, la solución tenga la capacidad de realizar análisis de comportamiento en tiempo real, que permita detectar de forma automática si existe algún comportamiento sospechoso.

1-G. "Las capacitaciones solicitadas en los pliegos de términos de referencia ¿Deben tener un mínimo de horas, puede brindarse de manera remoto?"
R/= No hay un mínimo de horas, pero debe alcanzarse lo establecido en el numeral 25, respecto de transmitir los conocimientos para administrar la solución. La capacitación puede realizarse de manera remota.

Consulta No.2:
Lote 3: Adquisición de Suscripciones para Plataforma de Concientización y Entrenamiento Interactivo de Ciberseguridad para 500 Usuarios Final

2-A. "¿Podrían proporcionar ejemplos específicos del tipo de contenido que esperan ver en la biblioteca, como temas de los módulos de entrenamiento o tipos de juegos?"
R/= Ejemplos, pero no limitativos a:

- ✓ Temas de módulos: Uso seguro de correo, internet, WiFi, Dispositivos Móviles, Inteligencia Artificial, Seguridad Física, Ingeniería Social.
- ✓ Tipos de Juego: Trivias, así como escenarios gráficos interactivos que cuente con niveles o secciones e involucre misiones, actividades de resolución de problemas que refuercen las competencias y la información adquirida en los entrenamientos.

2-B. "¿Qué métricas específicas les gustaría obtener de las evaluaciones y simulaciones de phishing?"
R/= Métricas como cuántas personas dieron click, introdujeron datos, abrieron el adjunto, reportaron el correo phishing, entre otros.

2-C. CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.4. 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.

2-D. "¿Qué tipo de escenarios personalizados para las campañas de phishing deben ser capaces de crear?"
R/= La solución debe tener la capacidad de personalizar Plantillas de correo con escenarios basados en información personal, que permita incluir archivos adjuntos para crear las campañas de phishing dirigidas.

Consulta No.3:
Lote 6: Adquisición de Solución en Nube para la Protección de Aplicaciones Web y APIs (Application Programming Interface), WAAP

3-A. <u>CONFIDENCIAL</u>: Ver Anexo de la Circular Aclaratoria No.4. 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.

3-B. <u>CONFIDENCIAL</u>: Ver Anexo de la Circular Aclaratoria No.4. 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.

3-C. "¿Existen políticas específicas o ejemplos de ataques que deban ser tratados particularmente con los modelos de seguridad positivo y negativo?"
R/= No tenemos políticas específicas. Se espera que la Solución pueda ir creando dichas políticas en base a nuevas amenazas que van surgiendo en el entorno mundial.

3-D. "¿Qué parámetros adicionales deben considerarse para las reglas de rate limiting?"
R/= Queda a criterio del Oferente si la Solución propuesta se limitará a los parámetros definidos en el numeral 10,10.1-10.5 o si ofrecerá parámetros adicionales.

3-E. "¿Qué y cuantas aplicaciones o servicios de terceros deben ser monitoreados específicamente?"
R/= No se tiene estimado actualmente.

3-F. "¿Qué sistemas de gestión de identidad federada están en uso actualmente y cómo se integran con la consola centralizada?"
R/= Microsoft Active Directory Federation Services por medio de SAML.

3-G. <u>CONFIDENCIAL</u>: Ver Anexo de la Circular Aclaratoria No.4. 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.

<u>Consulta No.4:</u>

PRODUCTO	LOTE	NÚMERO DE CARACTERÍSTICA	PREGUNTA
Trend Micro	Lote 1		¿Podrían compartir los sistemas operativos en los cuales se instalará el agente? **R**= Windows 10 y 11

<u>Consulta No.5:</u>

PRODUCTO	LOTE	NÚMERO DE CARACTERÍSTICA	PREGUNTA
Imperva WAF	Lote 6	Protección WAF	¿Pueden ampliar más detalles sobre el siguiente requerimiento?

		(Web Application Firewall) y API Punto 21.3	Se detecta una nueva solicitud saliente **R=**Se refiere a que al ejecutarse un script del lado del cliente este se dirige a otro dominio.

Consulta No.6:

CONFIDENCIAL: Ver Anexo de la Circular Aclaratoria No.4. 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:

PRODUCTO	LOTE	NÚMERO DE CARACTERÍSTICA	PREGUNTA
Infoblox	Lote 5	Protección Avanzada de DNS Punto 33.6	• ¿Para hacer un despliegue de los servidores necesarios para el funcionamiento de la solución on-premise, es posible que CNBS pueda asignar esos recursos en los ambientes virtuales que cuentan actualmente? **R**=Si • ¿Existe la posibilidad de actualizar los equipos OSX 10? 10 y 10.12 a una versión mínima OSX 11 ya que estas versiones 10.10 y 10.12 están fuera de soporte por Apple y por lo tanto los fabricantes de terceros no brindan soporte de esta versión? **R=**Si

Consulta No.8:

PRODUCTO	**LOTE**	**NÚMERO DE CARACTERÍSTICA**	**PREGUNTA**
Tenable	Lote 2	Requisitos Adicionales Punto 43 Características Punto 6	• ¿Para hacer un despliegue de los servidores necesarios para el funcionamiento de la solución on-premise, es posible que CNBS pueda asignar esos recursos en los ambientes virtuales que cuentan actualmente? **R**=Si • ¿Con qué solución de terceros quieren hacer la comparación? **R=**No se desea hacer comparación con ninguna solución de terceros.

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

Consulta No.9:

"**Referente al Lote # 1, en los requisitos adicionales,** 15.1. El más reciente Cuadrante Mágico de Gartner para Plataformas de Protección de Endpoints (Gartner Magic Quadrant for Endpoint Protection Platforms), Diciembre 2023. Se sugiere una modificación en el criterio que exige que el fabricante sea líder en tres reportes distintos. Este requisito puede limitar la participación transparente, ya que actualmente solo Crowdstrike cumple con dicha condición, siendo líder en los tres reportes. Para fomentar un proceso más transparente y equitativo, sugiero considerar soluciones de primer nivel que hayan sido evaluadas como Major Player en IDC, Líderes en Gartner y Strong Performer en Forrester. De esta manera, aseguramos que el proceso de selección sea inclusivo y justo, permitiendo la participación de más fabricantes de renombre y brindando una evaluación más completa y diversa de las opciones disponibles en el mercado.

- La cacería de amenazas la debe realizar el fabricante."

R/= En el contexto del numeral 15 del Lote 1, en el que se establece:
15. El fabricante de la solución deberá haber clasificado como líder en "cualquiera" de los siguientes resultados emitidos por fuentes externas de investigación:

15.1. El más reciente Cuadrante Mágico de Gartner para Plataformas de Protección de Endpoints (Gartner Magic Quadrant for Endpoint Protection Platforms), Diciembre 2023.
15.2. El más reciente Forrester Wave para Endpoint Security, Q4 2023.
15.3. El más reciente IDC MarketScape Worldwide Modern Endpoint Security para Empresas (Enterprises), 2024.

Note que "cualquiera" significa que debe ser líder en una "o" dos "o" tres de las evaluaciones, NO exige que se encuentre como líder en las tres evaluaciones.

En cuanto a la cacería de amenazas, en efecto, como se indica en el numeral 13 debe ser gestionada, y se requiere sea por el Fabricante de la solución.

Consulta No.10:

Lote 1: Adquisición de Solución Corporativa de una Plataforma de Protección de Puntos Finales (Endpoint Protection Platform)

"¿Cuál es la cantidad de agentes requeridos (cantidad de servidores, endpoints), sistemas operativos?"
R/= Tal como se indica en el numeral 1 del Lote 1, la solución corporativa debe brindar protección a seiscientos (600) puntos finales (Endpoints) con sistema operativo Windows, correspondientes en Estaciones de Trabajo, por lo que todos los equipos consisten en computadoras de escritorio y computadoras portátiles, no hay servidores.

Consulta No.11:

Lote 2: Adquisición de Solución para la Gestión de Vulnerabilidades de Ciberseguridad

11-A. <u>CONFIDENCIAL</u>: Ver Anexo de la Circular Aclaratoria No.4. 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.

11-B. <u>CONFIDENCIAL</u>: Ver Anexo de la Circular Aclaratoria No.4. 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.

11-C. "El punto 41. ¿La capacitación debe de ser certificada por el fabricante o transferencias de conocimiento?"
R/= Transferencia de conocimientos.

<u>Consulta No.12:</u>
Lote 1. Adquisición de Solución Corporativa de una Plataforma de Protección de Puntos Finales (Endpoint Protection Platform)

12-A. "¿Confirmar si podemos brindar una retención de 1TB o requieren un almacenaje mayor?"
R/= El Oferente deberá determinar el espacio de almacenamiento idóneo de conformidad al uso de espacio de la solución que oferta para proteger 600 puntos finales.

12-B. "Comprender completamente las amenazas en el entorno de la CNBS. ¿A qué se refiere con comprender completamente las amenazas en el entorno de la CNBS? ¿También es red, nube, VPN cliente?"
R/= En el contexto del numeral 9 de la capacidad de la Solución de contar con Inteligencia de Amenazas para potenciar la protección, se refiere a que la herramienta debe tener la capacidad de comprender el entorno en el que se está ejecutando, tomando en cuenta factores como el sistema operativo de los Endpoints, las aplicaciones que se hospedan en el mismo, entre otros, para determinar las amenazas de dicho entorno de la CNBS.

12-C. "Indicar si es requerido brindar servicios de SOC (Security Operations Center) para la resolución de incidentes de la plataforma.
R/= No.

12-D. "Detallar a que se refieren con IOC personalizados ya que actualmente la herramienta cuenta con unos predefinidos."
R/= La Solución en efecto debe tener su base de datos de IOCs, sin embargo, en el contexto del numeral 9 de la capacidad de la Solución de contar con Inteligencia de Amenazas para potenciar la protección, debe tener la capacidad de analizar de forma automatizada las amenazas de los Endpoints para identificar de forma personalizada los IOC que apliquen.

12-E. "Confirmar si se puede ofertar solo el control de dispositivos de USB, pero no el detalle de políticas granulares."
R/= No, la solución debe cumplir lo estipulado en el numeral 11.4.

12-F. "Indicar si es necesario ofertar una solución de DLP."

R/= No es necesario ofertar una solución de DLP.

12-G. "Confirmar si podemos ofertar control de aplicaciones en lugar de solo políticas de firewall."
R/= No, debe de cumplir lo establecido en los numerales 12, 12.1-12.4.
12-H. "Indicar si se debe integrar la solución con el firewall de la institución."
R/= No.

12-I. "Confirmar que podemos ofertar un control de aplicaciones en lugar de un firewall de host."
R/= No, debe de cumplir lo establecido en los numerales 12, 12.1-12.4.

12-J. "Confirmar si podemos ofertar una solución superior en una sola fuente externa como ejemplo MITRE."

R/= No, la Solución ofertada debe cumplir con los numerales 15 y 16.

Consulta No.13:
Lote 3. Adquisición de Suscripciones para Plataforma de Concientización y Entrenamiento Interactivo de Ciberseguridad

13-A. "Confirmar si podemos ofertar elementos interactivos, pero no juegos."
R/= No, la solución deberá cumplir con al menos los requerimientos de contenido enunciados en el numeral 3 y el numeral 5, lo cual incluye juegos.

13-B. "Confirmar si se requiere una certificación global final al completar todos los cursos."
R/= Si, no obstante, note que según lo indicado en el numeral 8, no es solo de manera global, pues la plataforma debe ser capaz de generar certificados de capacitación personalizados, para cuando los usuarios completen el contenido de capacitación asignado, tengan la opción de descargar un certificado de capacitación.

13-C. "Confirmar que podemos ofertar una plataforma con un pensum predefinido."
R/= No, tal como lo establece el numeral 7, la plataforma deberá contar con una herramienta que permita generar de forma automatizada un Programa de concientización adaptado a la CNBS.

13-D. "Confirmar que podemos ofertar un servicio que no utilice machine learning e IA."
R/= No, la Plataforma debe de cumplir los requerimientos indicados en los numerales 11.7, 11.8 y 13.

13-E. "Confirmar que podemos ofertar un servicio sin API para los reportes pero que incluya la exportación de los reportes desde la consola de administración."
R/= No, la plataforma debe de cumplir el requerimiento 15.3, relacionado a APIs.
Consulta No.14:

Lote 6. Adquisición de Solución en Nube para la Protección de Aplicaciones Web y APIs (Application Programming Interface)

14-A. "Confirmar si podemos ofertar una solución sin protección de DDoS."
R/= No, la Solución deberá contar con la capacidad de protección DDoS señalada en los numerales 23, 23.1-23.2.

14-B. "En caso de que requieran una solución de DDoS, indicar si se puede ofertar licenciamiento para una máquina virtual."
R/= No, tal como lo establece el numeral 1, la solución debe ser provista con un despliegue en Nube.

Consulta No.15:
Lote 7: Página 101, inciso 3.2 se solicita "Diagrama de Gantt y estado de los proyectos de despliegue de software automatizado" Y en la página 102, inciso 14.3 se solicita "Poder seguir el progreso a través de gráficos de Gantt."
"Dependiendo de la situación específica, diagramas diferentes a los de Gantt podrían de ser de mayor utilidad. En tal sentido respetuosamente solicitamos cambiar ambos requerimientos para que ahora se lean de la siguiente manera:
"3.2 Diagrama de Gantt o similar y estado de los proyectos de despliegue de software automatizado"
"14.3 Poder seguir el progreso a través de gráficos de Gantt o similar."."
R/= Se acepta solicitud de modificación. **Ver Enmienda No.1**

Consulta No.16:
Lote 6: Página 101, inciso 45.4. Response SLA para el nivel más crítico en 30 minutos.
"Con base en la experiencia de mercado y en búsqueda de una mayor participación de diferentes fabricantes solicitamos ampliar este tiempo de 30 minutos a 1 hora"
R/= No se acepta solicitud, en el caso de una situación de severidad crítica se requiere atención en la menor cantidad de tiempo, por tanto, se mantiene el requerimiento de 30 minutos.

La presente Circular Aclaratoria No.4 forma parte integral del documento base del referido proceso de licitación, así como su Anexo en el que constan **siete (7)** 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., 27 de agosto de 2024

FERNANDO GONZÁLEZ VILLARS

FERNANDO GONZÁLEZ VILLARS
Gerente Administrativo