Oficio No. 091/2024-DE-IHSS

15 DE FEBRERO 2024

Señores
Participantes
Presente

Referencia: LPN-029-2023 "ADQUISICION DE UN SERVICIO PARA GESTION DE INCIDENTES DE SEGURIDAD (SECURITY OPERATION CENTER, SOC) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS)"

Dando cumplimiento a las aclaraciones de la Licitación Pública Nacional, a continuación se detallan las preguntas y respuestas concernientes al proceso de licitación en referencia:

1. **El proveedor del servicio SOC deberá llevar a cabo un máximo de dos (2) análisis de intrusión bajo demanda por cada año de contrato. Estos análisis se realizarán con el objetivo de identificar, evaluar y remediar posibles vulnerabilidades y amenazas en el entorno de seguridad informática del IHSS. Los resultados de estos análisis se presentarán en informes detallados que incluirán recomendaciones de mitigación y acciones correctivas. Esto en referencia a las "NORMAS PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO".**

   Por favor especificar si los dos análisis a los que hacen referencia corresponden a un test y retest o si el cliente espera que por cada uno de estos análisis se realice un retest, osea en total 4 pruebas en el año.
   R./ En relación con esta consulta: Los análisis de intrusión serán solicitados bajo demanda durante la vigencia del contrato, con un máximo de dos (2) evaluaciones de intrusión por año, sin que se realice un **retest** de la evaluación.

2. **Nota: Los tipos de ejercicios de intrusión serán definidos y discutidos en conjunto con el equipo técnico del IHSS, teniendo en consideración alguno de los siguientes temas: Prueba de Penetración Externas, Prueba de Penetración Internas, Prueba de Aplicación Web, Prueba de Red, Prueba Inalámbricas, Prueba de Ingeniería Social, Prueba de Fuerza Bruta y Diccionario, Prueba de Denegación de Servicio (DDoS), Prueba de Análisis de Malware, Prueba de Privacidad de Datos.**
   Por favor especificar si el cliente espera tener la posibilidad de elegir por cada análisis entre una de los tipos mencionados ó si espera que en cada prueba se ejecuten todos los tipos mencionados de pruebas. En cualquier caso, por favor especificar la cantidad de objetivos a analizar (IPs/dominios/subdominios) para poder dimensionar el servicio.

R./ En relación con esta consulta: Por cada ejecución de análisis de intrusión, el IHSS determinara que componentes serán incluidos para la evaluación de seguridad, los proveedores deben contemplar en su oferta la ejecución de todos los análisis detallados en las bases de licitación. En cuanto a la cantidad de IPs/dominios/subdominios a continuación se detallan:

No.	Descripción	Cantidad
1	IP Públicas	20
2	Dominios	1
3	Subdominios	30

3. **La plataforma deberá ser compatible con la amplia gama de dispositivos y productos de diferentes tipologías y fabricantes.**

   Es posible que algunas tecnologías a integrar no estén soportadas nativamente y requieran de un esfuerzo adicional en la fase de implementación por favor especificar el FABRICANTE, VERSION y CANTIDAD de fuentes que desea integrar en el servicio.

   R./ En relación con esta consulta: Las plataformas que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación, para las tecnologías que no estén soportadas nativamente, el proveedor será el responsable de crear los conectores necesarios para la integración de las mismas. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

4. **Una vez notificada la adjudicación del servicio, su implementación será realizada inmediatamente, iniciando con la instalación, configuración e incorporación de los equipos descritos en estas bases de licitación en la solución Centro de Operaciones de Seguridad (SOC) por parte del proveedor. El IHSS proveerá los recursos técnicos de contraparte para ayuda de las integraciones de los equipos y plataformas a monitorear, así mismo validar que el proveedor brinda todo lo que se requiere para el servicio.**

   Para el inicio de la ejecución de los compromisos adquiridos con el cliente es necesario disponer de un contrato u orden de compra por parte del cliente, una notificación de adjudicación del servicio no tiene validez legal. En todo caso, se puede ir adelantando la reunión de kick-off donde se presente a todos los responsables de intervenir en el proyecto las actividades, responsables y fechas en que se deben ejecutar.

   R./ En relación con esta consulta: Se aclara que tal como se detalla en la base de licitación "Una vez notificada la adjudicación del Servicio" y tomando en consideración que el IHSS inicia los proyectos con la firma del contrato y en su efecto la emisión de la con la Orden de Compra.

De igual forma la Gerencia de Tecnología de Información y Comunicaciones con el VoBo del Director Ejecutivo del IHSS, emitirá una orden de inicio para que el proveedor adjudicado inicie la prestación de los servicio requeridos en este proceso de licitación.

5. **El proceso de instalación de los componentes (En caso de ser necesarios) para la operatividad del servicio correrá por parte de proveedor. El IHSS no incurrirá en gastos de instalación en conexiones, accesorios, o lo que derive de la instalación de los componentes.**

   Para poder realizar el proceso de instalación el cliente deberá disponer de una VPN Client-to-site con acceso a las máquinas virtuales que serán aprovisionadas por el cliente para el rol de colectores. Se sugiere que el cliente garantice el canal o ancho de banda para la VPN, de acuerdo a la cantidad de ingesta de datos por día, la cual no es clara en el documento.

   R./ En relación con esta consulta: El IHSS dispondrá de una VPN Client-to-Site mediante la cual el proveedor adjudicado tendrá el acceso a las máquinas virtuales que serán aprovisionadas para el cumplimiento del servicio requerido por el IHSS. Adicionalmente se garantizará el ancho de banda requerido para este servicio, pero es importante que los oferentes incluyan las herramientas de compresión de datos necesaria para evitar la saturación de los enlaces de internet que posee el IHSS.

6. **El proveedor deberá brindar documentación para configuración de nuevas reglas y activos que se requieran para mejorar el monitoreo**

   ¿Favor aclarar si la institución requiere acceso a la plataforma, para crear nuevas reglas de monitoreo? Por favor indicar cuantas personas van a requerir acceso a la consola para considerar temas de formación.

   R./ En relación con esta consulta: El enfoque del presente inciso está orientado a que el proveedor adjudicado indique las necesidades de conectividad y demás accesos que requiera la plataforma del proveedor para mejorar la implementación del servicio.

   Las bases de licitación detallan sobre el personal que necesitará formación para acceder y manejo de la solución y esta se encuentra en la sección de "Especificaciones Generales de los Oferentes", inciso No. 5. Pag.22

7. **El SOC del proveedor deberá contar con el personal necesario para que puedan atender las necesidades de monitoreo del IHSS, durante las 24 horas del día, 7 días a la semana, asimismo, deberá asignar el personal especializado en caso de presentarse algún**

incidente que afecte en gran medida la operatividad del IHSS, sin ningún costo adicional para el IHSS.

Se solicita a la entidad aclarar cuáles serían las tareas a ser llevadas a cabo por el personal especializado, entendiendo que el servicio solicitado es de monitoreo y gestión de incidentes de seguridad, mas no de operación y/o administración de las plataformas de seguridad.

Por favor especificar si el personal especializado que requieren está orientado hacia la respuesta a incidentes y que porcentaje de dedicación debería considerarse.

R./ En relación con esta consulta: El personal especializado que se requiere estará orientado hacia la respuesta a incidentes solo en el caso de existir un incidente que afecte o comprometa la operatividad del IHSS. Se aclara que el proveedor no administrara las plataformas de seguridad que posee el IHSS.

Se deberá considerar lo estipulado en las "ESPECIFICACIONES GENERALES DE LOS OFERENTES" numeral No.9, inciso d) Pag. 24 en las bases de licitación, para brindar el acompañamiento y orientación con medidas de contención para los incidentes de seguridad.

8. **El proveedor deberá incluir dentro del servicio los servidores, software, accesorios (Telecomunicaciones, alimentación eléctrica, entre otros) y cualquier otro componente necesario para la instalación física y lógica de las soluciones que permitan el procesamiento y almacenamiento de los eventos ocurridos en la infraestructura del IHSS.**

Por favor indicar si el cliente está en capacidad de suministrar en cada uno de sus datacenters una máquina virtual con las siguientes características,
CPU 8 Cores 2GHz+
-RAM 16 GB
- HDD 200 GB
- SO Ubuntu Server

R./ En relación con esta consulta: El IHSS está en la capacidad de suministrar y de ser necesario una máquina virtual con las características mencionadas en esta consulta. En caso de que se requiera más de una maquina virtual el proveedor deberá proporcionar los servidores físicos requeridos como parte del servicio.

Observación: La Máquina virtual a implementar debe ser compatible con el Hipervisor Oracle VM.

9. **El sistema de correlación e integración de eventos Security Information and Event Management (SIEM) y otras herramientas que le permitan el cumplimiento del servicio, deberá tener la capacidad para recolectar los eventos generados por los servidores,**

dispositivos de red y de seguridad de red del IHSS, teniendo en cuenta que deberá abarcar todo tipo de amenazas se identifique.

- **se sugiere al cliente que adicionalmente a los eventos de los equipos activos de red a ser monitoreados, la herramienta SIEM tenga la capacidad de obtener las métricas de los mismos, como CPS, Memoria, UpTime entre otros con el mismo agente instalado.**
- **Adicional a la recolección de eventos de seguridad, ¿la institución requiere que sea monitoreada el uso de recursos dentro de los servidores como CPU, memoria, disco e integridad de archivos?**

R./ En relación con esta consulta: Se acepta que los oferentes incorporaré herramientas que permitan la recolección de métricas de uso de los recursos de cómputo de las soluciones a monitorear, esto sin generar algún costo adicional al IHSS.

10. **El oferente deberá suministrar y desplegar el colector utilizando los equipos de cómputo (servidores) proporcionados por el proveedor. Además, se requiere que el oferente incluya el licenciamiento necesario para asegurar el funcionamiento adecuado del colector.**

    Por favor confirmar si el IHSS está en capacidad de suministrar una máquina virtual con las siguientes características:
    - CPU 8 Cores 2GHz+
    - RAM 16 GB
    - HDD 200 GB
    - SO Ubuntu Serve

    R./ En relación con esta consulta: El IHSS está en la capacidad de suministrar y de ser necesario una máquina virtual con las características mencionadas en esta consulta. En caso de que se requiera más de una máquina virtual el proveedor deberá proporcionar los servidores físicos requeridos como parte del servicio.

    Observación: La Máquina virtual a implementar debe ser compatible con el Hipervisor Oracle VM.

11. **Nota: En caso de que el IHSS decida brindar el equipo virtualizado para el montaje del colector, el oferente deberá cooperar y proporcionar los requisitos, configuración y licenciamiento necesario para asegurar la integración eficiente del colector en la infraestructura del IHSS. El proveedor debe estar dispuesto a adaptarse a esta opción si es seleccionada por el IHSS.**

    Por favor confirmar si es válido para el cliente trabajar con un sistema operativo open source como Ubuntu o si se requiere licenciamiento por parte del fabricante.

R./ En relación con esta consulta: La Máquina virtual a implementar debe ser compatible con el Hipervisor Oracle VM. Y en cuanto al Sistema Operativo Open Source UBUNTU SERVER este es compatible con nuestra infraestructura actual.

12. **Deberá soportar la integración de eventos provenientes de Active Directory, DNS, DHCP y concentradores VPN para monitorear la asignación de direcciones IP y asociar eventualmente los usuarios.**

    Por favor suministrar las especificaciones de FABRICANTE, VERSION, CANTIDAD para poder realizar las estimaciones de licenciamiento y servicios profesionales requeridos.

    R./ En relación con esta consulta: Las plataformas que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

13. **Se solicita a la entidad entregar una información más detallada de los activos a ser monitoreados, con respecto a fabricante, modelo, versión de sistema operativo, cantidad de dispositivos, cantidad de usuarios, esto con el fin de validar que si pueden ser monitoreados por las plataformas de SIEM y para el dimensionamiento de los servicios asociados.**

    R./ En relación con esta consulta: Las plataformas que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pag. 30 en las bases de licitación. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

14. **Presentar como mínimo tres (3) constancias originales, emitidas por empresas públicas o privadas en la República de Honduras manifestando que el proveedor ha suministrado el Servicio de Centro de Operaciones de Seguridad (SOC), indicando que cumplió en tiempo, por un valor contractual igual o mayor al 20% del valor ofertado y durante los últimos cinco (5) años. La constancia deberá indicar el cumplimiento en el tiempo, con la calidad y demás obligaciones Contractuales, así como los datos de: Nombre de la persona que se puede contactar, número de teléfono y correo electrónico. ¿Se podrá presentar contratos u órdenes de compra reemplazando la constancia solicitada?**

    R./ En relación con esta consulta: Los oferentes deberán apegarse a lo establecido en los Pliegos de Condiciones.

15. ¿Lo requerido son pruebas de intrusión (ethical hacking) o análisis de vulnerabilidades sin intrusión activa?

1. **Cantidad de Pentest y/o Análisis de Seguridad Externo/Internos por año**

   R./ En relación con esta consulta: Por cada ejecución de análisis de intrusión, el IHSS determinara que componentes serán incluidos para la evaluación de seguridad, los proveedores deben contemplar en su oferta la ejecución de todos los análisis detallados en las bases de licitación, no obstante, el requerimiento será únicamente dos (2) de estos análisis de pruebas, por cada año de contrato. Información adicional a lo indicado será proporcionada al proveedor una vez adjudicado por temas de seguridad y confidencialidad.

2. **Redes perimetrales (infraestructura expuesta a internet)**

   R./ En relación con esta consulta: Los segmentos de red expuestos a internet son tres (3).

3. **Cantidad de direcciones IP en uso / activas**

   R./ En relación con esta consulta: El IHSS cuenta con 20 IP's públicas para estos análisis.

4. **Cantidad de aplicaciones y/o sitios web**

   R./ En relación con esta consulta: Esta información será proporcionada al proveedor una vez que el servicio haya sido adjudicado, en consideración a la seguridad y confidencialidad de los datos.

5. **Cantidad de servidores (virtual/físico) y/o instancias**

   R./ En relación con esta consulta: La cantidad de servidores que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

6. **¿Cuenta con WAF?**

   R./ En relación con esta consulta: NO se incluye dentro del alcance el WAF en este proyecto.

7. **¿Cuenta con IPS?**

   R./ En relación con esta consulta: NO se contempla la inclusión del IPS en este proyecto.

   <u>Redes internas</u>

8. **Cantidad de servidores (virtual/físico) y/o instancias**

   R./ En relación con esta consulta: La cantidad de servidores que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

9. **Cantidad de dispositivos de red CORE (Switches, Routers, etc)**

   R./ En relación con esta consulta: La cantidad de servidores que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

10. **Cantidad de estaciones de trabajo.**

    R./ En relación con esta consulta: La cantidad de servidores que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

11. **¿Se deben incluir pruebas sobre redes inalámbricas? En caso afirmativo, especificar la cantidad de ESSID.**

    R./ En relación con esta consulta: La cantidad de redes inalámbricas que se consideran para este servicio son dos (2).

12. **Cuenta con equipos tipo Mainframe y/o AS/400?**

    R./ En relación con esta consulta: **NO** se contempla la inclusión de equipos tipo Mainframe y/o AS/400 en este proyecto.

13. **Pruebas de Ingeniería Social: No se visualizan en el pliego ¿Se debe incluir alguna prueba de estas?**

    R./ En relación con esta consulta: Las pruebas de Ingeniería Social están contempladas en el Numeral 10, Pág. 25 en las bases de licitación. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

14. **Certificaciones: en el pliego se indica que el/los consultores deben tener una serie de certificaciones, cada consultor debe tener todas las indicadas o puede ser un mix? ¿Cuáles son mandatorios?**

    R./ En relación con esta consulta: Se requiere que todos los oferentes presenten al menos las certificaciones mencionadas las cuales pueden estar repartidas dentro de todo el equipo de operadores del SOC, tal como se especifica en las bases de la licitación.

15. **Presentar 3 constancias originales emitidas en la republica de Honduras manifestando que el proveedor a sumistrado un SOC indicando que cumplió el tiempo contractual mayor al 20 % en los últimos dos años ¿Es posible presentar constancia de clientes a nivel regional como evidencias?**

    R./ En relación con esta consulta: Los oferentes deberán apegarse a lo establecido en los Pliegos de Condiciones.

16. **Para el SIEM, ¿requieren Hardware?, ¿o podemos implementar por medio de Máquina Virtual?**

    R./ En relación con esta consulta: El IHSS está en la capacidad de suministrar de ser necesario una máquina virtual. Con las siguientes características de cómputo máximas:

- **Processor:** 8 Cores 2GHz+
- **Memoria RAM:** 16 GB
- **Almacenamiento:** HDD 200 GB
- **Sistema Operativo:** Windows/Linux (Si el S.O. requiere licenciamiento el proveedor debe proporcionarlo como parte del servicio).

En caso de que se requiera más de una máquina virtual o más recursos de cómputo el proveedor deberá proporcionar los servidores físicos requeridos como parte del servicio.

Observación: La Máquina virtual a implementar debe ser compatible con el Hipervisor Oracle VM.

17. **¿Requieren Alta disponibilidad?**

R./ En relación con esta consulta: Para este proceso el IHSS **NO** se requiere Alta Disponibilidad (HA).

18. **Especificar marca y modelo de los Firewalls**

R./ En relación con esta consulta: Las plataformas que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación, para las tecnologías que no estén soportadas nativamente, el proveedor será el responsable de crear los conectores necesarios para la integración de las mismas. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

19. **¿Qué consola de administración de Firewall utilizan?**

R./ En relación con esta consulta: Las plataformas que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación, para las tecnologías que no estén soportadas nativamente, el proveedor será el responsable de crear los conectores necesarios para la integración de las mismas. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

20. **¿Cuántos Router son? ¿Cuántos switches son? (por separado)**

R./ En relación con esta consulta: En relación con los Router, estos equipos de red **NO** están contemplados para este proyecto. Por lo tanto, los quince (15) dispositivos de red, son Switches de Acceso (Capa 2).

21. **Mencionan 68 servidores Windows IIS/DNS/ AD ¿Favor detallar cuantos servidores para IIS, cuantos para DNS y cuantos para AD?**

R./ En relación con esta consulta: A continuación se detalla:

No.	Tipo de Servidor	Cantidad
1	Internet Information Services (IIS)	12

2	AD/DNS (unificados)	10
	TOTAL	**22**

Nota: En cuanto al resto de servidores (46), se utilizan el despliegue de otros servicios.

22. **¿Qué versiones de Bases de datos tienen?**

R./ En relación con esta consulta: Las plataformas que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación, para las tecnologías que no estén soportadas nativamente, el proveedor será el responsable de crear los conectores necesarios para la integración de las mismas. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

23. **Detallar marca y modelo de solución NAS**

R./ En relación con esta consulta: Las plataformas que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación, para las tecnologías que no estén soportadas nativamente, el proveedor será el responsable de crear los conectores necesarios para la integración de las mismas. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

24. **¿Plan de Microsoft o365 tienen?**

R./ En relación con esta consulta: Las suscripciones de O365 contratadas actualmente son Plan E1 y este está definido en las bases de Licitación en la Pág. 30, en la "TABLA DE PRODUCTOS Y CANTIDADES".

25. **Sobre el numera 10 los análisis de intrusión bajo demanda favor aclarar si requieren un Análisis de Vulnerabilidad o una Prueba de Intrusión. Cantidad de Tipos de Pruebas a realizarse en cada ejercicio por año:**

R./ En relación con esta consulta: Por cada ejecución de análisis de intrusión, el IHSS determinara que componentes serán incluidos para la evaluación de seguridad, los proveedores deben contemplar en su oferta la ejecución de todos los análisis detallados en las bases de licitación, no obstante, el requerimiento será únicamente dos (2) de estos análisis de pruebas, por cada año de contrato. La Información adicional a lo indicado será proporcionada al proveedor una vez adjudicado por temas de seguridad y confidencialidad.

26. **Favor definir el alcance de estas pruebas con la siguiente información:**

- **Prueba de Penetración Externas:** ¿cantidad de IP externas que formaran parte del análisis de intrusión?

  R./ En relación con esta consulta: El IHSS cuenta con veinte (20) IP públicas para estos análisis.
- **Prueba de Penetración Internas:** ¿cantidad de IP internas que formaran parte del análisis de intrusión?

R./ En relación con esta consulta: El IHSS seleccionará una muestra de diez (10) IP interna como objetivo de la Prueba.

- **Prueba de Aplicación Web:** ¿Cantidad de aplicaciones web? ¿Son transaccionales o no?
  R./ En relación con esta consulta: El IHSS seleccionará dos (2) Aplicación Web, NO se incluye dentro del alcance aplicaciones web transaccionales.
- **Prueba de Red:** ¿cantidad de direcciones IP, routers y segmentos por routers?
  R./ En relación con esta consulta: El IHSS seleccionara un segmento de red para dicha prueba, cuyo segmento mas grande tiene un aproximado de 1,000 IP's.
- **Prueba Inalámbricas**: ¿Cantidad de routers y su ubicación?
  R./ En relación con esta consulta: La cantidad de redes inalámbricas que se consideran para este servicio son dos (2).
- **Prueba de Ingeniería Social:** ¿desean Phishing o Vishing? ¿cantidad de usuarios que participarían en las pruebas?
  R./ En relación con esta consulta: Se prefiere Phishing con una muestra del 15% del total de cuentas de correo contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación.
- **Prueba de Fuerza Bruta y Diccionario:** ¿Cuántos sitios o App?
  R./ En relación con esta consulta: El IHSS seleccionará dos (2) sitio como objetivo de la Prueba.
- **Prueba de Denegación de Servicio (DDoS):** ¿Cuántos sitios o App?
  R./ En relación con esta consulta: El IHSS seleccionará un (1) sitio como objetivo de la Prueba.

27. Solamente se requiere experiencia local/regional o también se requiere que el oferente cuente con Security Operation Center (SOC) en el país?

R./ En relación con esta consulta: El IHSS requiere que el Proveedor adjudicado posea experiencia comprobable en el mercado tanto local o regional, en la implementación y/o prestación de servicios de seguridad informática por medio de un Centro de Operaciones de Seguridad (SOC) tal como se establece en el numeral 16, Pág. 27 de las bases de licitación.

28. ¿Por favor confirmar si el IHSS brindara el equipo virtualizado para el montaje del colector?

R./ En relación con esta consulta: El IHSS está en la capacidad de suministrar de ser necesario una máquina virtual. Con las siguientes características de cómputo máximas:

- **Processor:** 8 Cores 2GHz+
- **Memoria RAM:** 16 GB
- **Almacenamiento:** HDD 200 GB

- **Sistema Operativo:** Windows/Linux (Si el S.O. requiere licenciamiento el proveedor debe proporcionarlo como parte del servicio).

En caso de que se requiera más de una máquina virtual o más recursos de cómputo el proveedor deberá proporcionar los servidores físicos requeridos como parte del servicio.

Observación: La Máquina virtual a implementar debe ser compatible con el Hipervisor Oracle VM.

29. Considerando la naturaleza del servicio solicitado en el proceso LPN-029-2023 y tomando en cuenta la aclaración en Item#25. "El centro de operaciones de seguridad NO administrará IPS, Firewall, servidores, estaciones de trabajo, Endpoint, etc., del IHSS"
Por lo anteriormente expuestos consideremos que las certificaciones CCSA (Check Point), CCNA (Cisco), CCNP (Cisco), no son necesarias ya que no se necesita la configuración ni administración, solamente lectura
Les sugerimos puedan considerar certificaciones que garanticen la continuidad operacional del servicio a contratar.

- **Certificación en plataforma SIEM.0**
- **Certificación Ethical Hacking análisis forense, reconocidas a nivel internacional E-council.**

Adicional les sugerimos solicitar Carta del Fabricante en la solución ofertada y nivel de partner.

R./ En relación con esta consulta: En las bases de licitación se están solicitando esas certificaciones debido a que se requieren otras actividades complementarias, y es indispensable que el personal que realizara estas actividades de monitoreo y ejecución posee los conocimientos en cuanto a la operación de las soluciones que posee el IHSS. En su defecto se pueden presentar Certificaciones equivalentes que serán evaluadas por el equipo técnico tal como se menciona en el numeral 25, pág. 29 de las bases de esta Licitación.

30. Por favor su valiosa ayuda detallando los siguientes item:

2	**Fuentes de información / Servidores y Endpoint**	
2.1	Servidores Windows Server / IIS / DNS / AD	68
2.2	Otros servidores / Linux Server	10

Cuantos Servidores Windows Server IIS?
Cuantos Servidores Windows Server DNS?
Cuantos Servidores Windows Server AD?
Cuantos Servidores / Linux Server?

3	**Servicios en Nube (AWS)**	
3.1	Servidores Windows / Linux EC2	10

Cuantos Servidores Linux EC2?

R./ En relación con esta consulta: a continuación se detalla:

No.	Tipo de Servidor	Cantidad
1	Internet Information Services (IIS)	12
2	AD/DNS (unificados)	10
	TOTAL	**22**

Nota: En cuanto al resto de servidores (46), se utilizan el despliegue de otros servicios.

¿Cuántos Servidores Linux EC2?

No.	Tipo de Servidor	Cantidad
1	Servidores Windows	3
2	Linux EC2	7
	TOTAL	**10**

31. **En la Fase III, sub-fase III: Evaluación Técnica en Documentos, solicitan presentar como mínimo tres (3) constancias originales, emitidas por empresas públicas o privadas en la República de Honduras manifestando que el proveedor ha suministrado el servicio de Centro de Operaciones de Seguridad (SOC), indicando que cumplió en tiempo, por un valor contractual igual o mayor al 20% del valor ofertado y durante los últimos cinco (5) años. La constancia deberá indicar el cumplimiento en el tiempo, con la calidad y demás obligaciones Contractuales, así como los datos de: Nombre de la persona que se puede contactar, número de teléfono y correo electrónico.**

¿Podrían ampliar este punto para aceptar también cartas de empresas de otros países de la región de Centro América y Republica Dominicana?

R./ En relación con esta consulta: Los oferentes deberán apegarse a lo establecido en los Pliegos de Condiciones.

32. **En el numeral 3 de las especificaciones generales de los oferentes solicitan brindar un margen mínimo en el dimensionamiento para futuras incorporaciones de fuentes de información. ¿Podrían indicarnos que fuentes, posiblemente, estarían incorporando?**
R./ La adquisición de nuevas tecnologías está sujeta a los procesos de licitación, por lo que no podemos indicar específicamente más allá de lo establecido en las bases de la licitación. La información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad de la información.

33. **En el numeral 5 de las especificaciones técnicas solicitan talleres no certificados de entrenamiento por el represéntate local o fabricante par el uso y manejo de la solución. ¿Podrían ampliarnos que se espera de este taller debido a que el servicio es brindando por nuestro centro de operaciones, quienes son los encargados del uso y manejo de la solución?**

R./ Se espera que los talleres de entrenamiento no certificados garanticen que los empleados del IHSS mencionados en el numeral 5 de las especificaciones técnicas, obtengan la información necesaria para comprender el funcionamiento del servicio y la información que estarán ofreciendo, considerando que el oferente adjudicado será el encargado de monitoreo y manejo de la solución.

34. **En el numeral 7 de las especificaciones técnicas, ¿podrían ampliarnos que se espera cuando dicen Entre otra documentación?**

R./ Se espera que se agregue toda la información necesaria y proporcionada por su solución para respaldar el servicio que se ha brindado, incluyendo documentos técnicos, registros de actividades y cualquier otra documentación relevante que de evidencia del cumplimiento del servicio.

35. **En el numeral 10 de las especificaciones técnicas, solicitan dos (2) análisis de intrusión bajo demanda. Podrían indiciarnos, dependiendo que tipo de prueba, lo siguiente:**

- **¿Cuántas direcciones IP Externas son?**
- **¿Cuántas direcciones IP Internas son?**
- **¿Cuántas aplicaciones Web son?**
- **¿Cuántas redes inalámbricas son?**
- **¿Cuántos usuarios son para la prueba de Ingeniería Social, entendiendo que cuentan con 1700 cuentas de 0365 según la Tabla de Productos y Cantidades?**

R./Por cada ejecución de análisis de intrusión, el IHSS determinara que componentes serán incluidos para la evaluación de seguridad, los proveedores deben contemplar en su oferta la ejecución de todos los análisis detallados en las bases de licitación, no obstante, el requerimiento será únicamente dos (2) de estos análisis de pruebas, por cada año de contrato. Información adicional a lo indicado será proporcionada al proveedor una vez adjudicado por temas de seguridad y confidencialidad.
Los objetivos de las pruebas serán determinados por las necesidades específicas que tenga el IHSS en la ejecución del servicio, con el fin de garantizar su correcto funcionamiento y cumplimiento de los requisitos establecidos.

36. **En el numeral 8 de las especificaciones técnicas mínimas, solicitan que el monitoreo remoto de los eventos correlacionados del Security Information and Event Management (SIEM) y otras herramientas que le permitan el cumplimiento del servicio requerido por el IHSS, se podrá realizar por medio de un enlace de Red Virtual Privado (VPN) en Internet.**

¿Es posible implementar una máquina virtual que funciona como el colector de eventos y hacer la conexión por medio VPN a nuestro centro de operaciones? ¿Esta conexión de VPN será brindado por ustedes?

R./ El IHSS dispondrá de una VPN Client-to-Site/Site-to-site mediante la cual el proveedor adjudicado tendrá el acceso a la máquina virtual que será aprovisionada para el cumplimiento del servicio requerido por el IHSS. Adicionalmente se garantizará el ancho de banda requerido para este servicio, pero es importante que los oferentes incluyan las herramientas de compresión de datos necesaria para evitar la saturación de los enlaces de internet que posee el IHSS.

37. **En el numeral 13 de las especificaciones técnicas mínimas, solicitan que el proveedor deberá brindar documentación para configuración de nuevas reglas y activos que requieran para mejorar el monitoreo. Nuestro Centro de Operaciones de Seguridad es el encargado de realizar las configuraciones necesarias y solo ellos pueden tener acceso a la consola de configuración. Dicho lo anterior, ¿es necesario brindar la documentación solicitada?**

R./ El enfoque del presente inciso está orientado a que el proveedor adjudicado indique las necesidades de conectividad y demás accesos que requiera la plataforma del proveedor para mejorar la implementación del servicio.
Dado que el proveedor necesita acceder a la infraestructura del IHSS para monitorear, es posible que en algún momento requiera modificaciones por parte del IHSS para mejorar la conectividad de la plataforma, especialmente durante el período de adaptación. Por lo tanto, es fundamental que el proveedor detalle cualquier información adicional que pueda necesitar el IHSS para establecer estas nuevas reglas aplicadas en las diferentes capas de seguridad durante la prestación del servicio.

38. **En el numeral 18 de las especificaciones técnicas mínimas, solicitan que el proveedor deberá incluir dentro del servicio los servidores, software, accesorios (Telecomunicaciones, alimentación eléctrica, entre otros) y cualquier otro componente necesario para la instalación física y lógica de las soluciones que permitan el procesamiento y almacenamiento de los eventos ocurridos en la infraestructura del IHSS.**

Para el servicio, podemos proveer el servidor con el software necesario para implementar la máquina virtual del colector. ¿Podrían indicarnos que ustedes cuentan con la alimentación eléctrica y espacio disponible para la implementación del servidor físico?

R./ Las especificaciones establecen que, si el proveedor necesita algún equipo físico para prestar el servicio y este requiere algún accesorio, el proveedor debe proporcionarlo.

39. ¿Podrían indicarnos modelos y versiones de todos los productos/soluciones que se encuentra en la Tabla de Productos y Cantidades?

R./Los modelos y cantidades que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

40. En el pliego de condiciones en Especificaciones Técnicas Mínimas solicitan "El proveedor deberá contar con experiencia comprobable en el mercado local/Regional, en la implementación y/o prestación de servicios de seguridad informática por medio de un Centro de Operaciones de Seguridad (SOC)." sin embargo en los Requisitos Técnicos del mismo pliego indican que el Oferente debe "Presentar como mínimo tres (3) constancias originales, emitidas por empresas públicas o privadas en la República de Honduras manifestando que el proveedor ha suministrado un Centro de Operaciones de Seguridad (SOC)", siendo contradictorio al requerir experiencia regional pero limitando las constancias a nivel nacional.

Solicitamos que sea aceptado por el IHSS presentar mínimo de 3 constancias originales emitidas por empresas públicas o privadas en el mercado local/regional de Latinoamérica para que sean congruentes los requerimientos técnicos tal como lo han realizado otras instituciones públicas de Honduras.

R./ En relación con esta consulta: Los oferentes deberán apegarse a lo establecido en los Pliegos de Condiciones.

41. ¿Se requiere cumplir con alguna normativa (PCI, S0C,27001, u otros)?

R./ En relación con esta consulta: El IHSS este sujeto al cumplimiento de las *"Normas para la Gestión de Tecnologías de Información, Ciberseguridad y Continuidad del Negocio"* por lo cual las empresas proveedores de servicios de TI deben alinearse con esta.

42. ¿Tienen alguna área dedicada de ciberseguridad para cumplir recomendaciones y mejores prácticas?

R./ En relación con esta consulta: Si, tal como lo indica la CNBS en las "NORMAS PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO".

43. ¿Poseen un diagrama de red que puedan compartir para ayudar al diseño de la solución?

R./ En relación con esta consulta: El diagrama de red contiene información confidencial sobre nuestra infraestructura. Esta información se proporcionará al proveedor adjudicado para garantizar la seguridad y confidencialidad de nuestros sistemas.

44. ¿Se puede pasar un detallado de la tabla de productos en el punto 2.1 Servidores Windows Server /IIS / DNS / AD?

R./ En relación con esta consulta: Referente a esta consulta a continuación se detalla:

No.	Tipo de Servidor	Cantidad
1	Internet Information Services (IIS)	12
2	AD/DNS (unificados)	10
	TOTAL	**22**

Nota: En cuanto al resto de servidores (46), se utilizan el despliegue de otros servicios.

45. Favor de compartir la cantidad de Endpoints de Usuarios Finales (Notebooks, PCs de Escritorio) a considerar en la propuesta.

R./ En relación con esta consulta: La cantidad de Usuarios Concurrentes que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

46. Favor de indicar el fabricante y modelos de Firewall que serán cubiertos por el servicio de monitoreo.

RR./ En relación con esta consulta: Las plataformas que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación, para las tecnologías que no estén soportadas nativamente, el proveedor será el responsable de crear los conectores necesarios para la integración de las mismas. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

47. En Especificaciones Técnicas Mínimas solicitan que "El mantenimiento y actualización de las herramientas (monitoreo, prevención, detección y reacción) deberá ser realizado en su totalidad por el personal técnico de la empresa adjudicada". Nuestro entendimiento es que la empresa adjudicada realizara el monitoreo, prevención, detección y reacción de los incidentes que pueden surgir, pero la remediación y corrección será por parte del

personal de IHSS en base a las recomendaciones del SOC. Es correcta esta apreciación, en caso contrario favor de ampliar el detalle del requerimiento.

R./ En relación con esta consulta: El oferente deberá apegarse a lo indicado en el Numeral 9, inciso d) de la pág. 24 de las bases de licitación.

48. **Favor de indicar el espacio en rack, y el voltaje disponible en los mismos, con que dispone el IHSS para la instalación de los servidores requeridos para la aplicación de monitoreo.**

R./ En relación con esta consulta: Ciertos detalles específicos sobre la infraestructura del IHSS son confidenciales por lo cual el oferente debe compartir en su propuesta los requisitos para la conexión de sus equipos.

49. **Confirmar que el IHSS brindara el equipo Endpoint (computadoras) requerido para sus empleados y su centro de monitoreo interno.**

R./ En relación con esta consulta: El oferente deberá apegarse a lo indicado en las bases de licitación.

50. **¿Es requerimiento del IHSS que se cuente con un centro de monitoreo, incluyendo personal de monitoreo, ubicado dentro del territorio de Honduras por parte del oferente?**

R./ En relación con esta consulta: El oferente tiene la libertad de definir la ubicación física de su Centro de Monitoreo, siempre y cuando cumpla con los requisitos establecidos en las Bases de Licitación.

51. **Considerando la complejidad de la solución que se está solicitando, y que las respuestas a las consultas pueden generar consultas adicionales, solicitamos una ampliación en el tiempo de aclaraciones y el tiempo de presentación de ofertas para poder considerar todos los elementos y presentar una oferta de acorde a los requerimientos del IHSS.**

R./ En relación con esta consulta: No se considera necesaria una ampliación del plazo para la presentación de ofertas. El oferente deberá apegarse a lo indicado en las bases de licitación.

.

Sección III, Especificaciones generales		Contenido	Pregunta
52.	1	El centro de operaciones de seguridad **NO** administrará IPS, Firewall, servidores, estaciones de trabajo, Endpoint, etc., del IHSS.	¿Se tiene establecido los casos de uso que serán configurados en la herramienta SIEM para poder generar las alertas de seguridad?

R./ En relación con esta consulta: Para garantizar la integridad y confidencialidad del proceso, ciertos detalles específicos, incluyendo los casos de uso exactos de SIEM, se consideran información confidencial y solo pueden ser discutidos y compartidos con el proveedor adjudicado.

53.	5	La empresa impartirá talleres no certificados de entrenamiento por el representante local o fabricante para el uso y manejo de la solución, donde tendrá una duración mínima dieciséis (16) horas dividas como mínimo en dos (2) jornadas para por lo menos quince (15) participantes,	¿Cliente requiere una gestión compartida de herramienta SIEM? Por la capacitación que requiere en este punto

R./ En relación con esta consulta: La solicitud de talleres de entrenamiento para el uso y manejo de la solución SIEM tiene como objetivo principal asegurar que el equipo del IHSS esté informado y capacitado para comprender la funcionalidad, los informes y las alertas generadas por la herramienta, como una iniciativa para mejorar la colaboración entre el equipo interno y el proveedor del servicio SOC, además de aumentar la capacidad interna de respuesta rápida ante incidentes y amenazas de seguridad identificadas por la solución SIEM.

La gestión operativa diaria, la supervisión y la respuesta a incidentes seguirán siendo responsabilidad primordial del proveedor del servicio SOC, según se detalla en el alcance del servicio, sin embargo, esto no implica una gestión compartida.

54.	9 (d)	El proveedor deberá asignar al personal técnico calificado para brindar el acompañamiento y orientación con medidas de contención para los incidentes de seguridad, y dar indicaciones precisas para que estas sean implementadas por el personal de La Gerencia de Tecnología de Información y Comunicaciones del IHSS, según los protocolos establecidos, así como verificar su eficacia.	¿Es requerido el servicio de gestión a incidentes en el servicio de SOC, esto ya que solicitan en sección III punto 1 que no se tendrá gestión de dispositivos solo alertas de seguridad?

R./ En relación con esta consulta: El IHSS requiere que los servicios de gestión de incidentes estén dentro del servicio de SOC, entendiendo esto como identificar, asesorar y orientar en la respuesta a incidentes, sin que ello implique la gestión directa del proveedor de los dispositivos de nuestra infraestructura. El oferente deberá apegarse a lo indicado en el Numeral 9, inciso d) de la pág. 24 de las bases de licitación.

55. 10	El proveedor del servicio SOC deberá llevar a cabo un máximo de dos (2) análisis de intrusión bajo demanda por cada año de contrato. Estos análisis se realizarán con el objetivo de identificar, evaluar y remediar posibles vulnerabilidades y amenazas en el entorno de seguridad informática del IHSS. Los resultados de estos análisis se presentarán en informes detallados que incluirán recomendaciones de mitigación y acciones correctivas. Esto en referencia a las "NORMAS PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO". Nota: Los tipos de ejercicios de intrusión serán definidos y discutidos en conjunto con el equipo técnico del IHSS, teniendo en consideración alguno de los siguientes temas: Prueba de Penetración Externas, Prueba de Penetración Internas, Prueba de Aplicación Web, Prueba de Red, Prueba Inalámbricas, Prueba de Ingeniería Social, Prueba de Fuerza Bruta y Diccionario, Prueba de Denegación de Servicio (DDoS), Prueba de Análisis de Malware, Prueba de Privacidad de Datos.	¿Pueden proporcionar los activos que serán requeridos para las pruebas de análisis de intrusión solicitadas en este punto?

R./ En relación con esta consulta: Por cada ejecución de análisis de intrusión, el IHSS determinara que componentes serán incluidos para la evaluación de seguridad, los proveedores deben contemplar en su oferta la ejecución de todos los análisis detallados en las bases de licitación, no obstante, el requerimiento será únicamente dos (2) de estos análisis de pruebas, por cada año de contrato. Información adicional a lo indicado será proporcionada al proveedor una vez adjudicado por temas de seguridad y confidencialidad.

56.	22	La solución debe ser capaz de integrar de manera efectiva la consola de administración de ESET Protect Cloud, nuestro sistema actual de antivirus. Esta integración se busca para lograr una identificación eficiente de comportamientos inusuales y para correlacionar eventos generados desde las estaciones de trabajo de los usuarios finales. El propósito principal de esta integración es permitir la rápida detección y mitigación de cualquier amenaza o vulnerabilidad de seguridad informática.	¿Podrían detallar que formato de mensaje de eventos pueden ser exportados desde consola de ESET solicitada?

R./ En relación con esta consulta: El oferente deberá apegarse a los protocolos de mensajería de eventos, mencionados en el numeral 20, Pág. 28 de las bases de Licitación.

57.	24 (a)	Los eventos recolectados por el sistema para administración de Eventos e Información de Seguridad deberán permanecer en el equipo asignado para el propósito. El contratista no podrá hacer copias sin previa autorización del IHSS.	¿el IHSS requiere un equipo SIEM dedicado para otorgar el servicio o puede ser integrado a un servicio multitenant?

R./ En relación con esta consulta: El IHSS está abierto a evaluar soluciones tecnológicas innovadoras y eficientes, cualquier propuesta de servicio multitenant deberá explicar con claridad cómo se garantiza la segregación, seguridad y confidencialidad de nuestros datos, asegurando que estos no serán accesibles o compartidos con otras entidades. En este caso el oferente deberá detallar las medidas de seguridad y aislamiento de datos implementadas, esto sin generar algún costo adicional al IHSS.

58.	24 (c)	Para la implementación del Sistema de Administración de Eventos e Información de Seguridad (SIEM), se requiere de un (1) colector que deberá ser colocado en las instalaciones determinadas por el IHSS. Si el proveedor propone habilitar un colector en su propia infraestructura tecnológica, esta opción será evaluada minuciosamente por el equipo técnico del IHSS. La evaluación se centrará en asegurar que esta implementación no tenga un impacto negativo en la disponibilidad, el rendimiento y el tráfico de nuestra red.	¿Qué requerimientos mínimos son necesarios para la adecuada instalación de collector en centro de datos de proveedor?

R./ En relación con esta consulta: El oferente tiene la libertad de ofrecer soluciones innovadoras o de valor agregado, siempre y cuando estas cumplan con el objetivo principal del contrato, que es proporcionar un servicio efectivo de SOC.

59.	Otra	Estimado de EPS y de MPS	Tiene algún estimado de Eventos por segundo (EPS) o mensajes por segundo (MPS) de la infraestructura que estará integrada al SIEM?

R./ En relación con esta consulta: La información solicitada aún no está disponible por ser la primera contratación de este tipo de servicio. se espera que los oferentes participantes tengan metodologías o experiencias previas que les permitan estimar estos valores basados en infraestructuras de tamaño y complejidad similares a la nuestra, y utilizar esos datos en sus propuestas, especificando claramente las suposiciones hechas.

60.	Otra	Cantidad de empleados	¿Número de empleados que tiene el IHSS? (Que se conecten a su red interna)

R./ En relación con esta consulta: La cantidad de Usuarios Concurrentes que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

61.	Otra	Servicios que desea correlacionar	1) ¿ Puede describir los diferentes servicios en producción que desea correlacionar (ej. Directorio Activo, Aplicaciones Web, Base de Datos, etc.) ?. 2) ¿Requiere alguna funcionalidad avanzada?, explique:.... 3) ¿ Tiene proveedores de nube publica? (Describa)

R./ En relación con esta consulta: Las plataformas que se consideran para este servicio están contempladas en "TABLA DE PRODUCTOS Y CANTIDADES" Pág. 30 en las bases de licitación, para las tecnologías que no estén soportadas nativamente, el proveedor será el responsable de crear los conectores necesarios para la integración de las mismas. Información adicional a lo indicado será proporcionada al proveedor adjudicado por temas de seguridad y confidencialidad.

Nota: Las tablas solicitadas requieren la inserción de información confidencial. Dicha información se proporcionará al proveedor adjudicado, para preservar temas de seguridad y confidencialidad de la información de nuestra infraestructura tecnológica.

Atentamente,

DOCTORA YADIRA XAMILET ALVAREZ
Directora Ejecutiva por Ley
Instituto Hondureño de Seguridad Social

CC: LPN-029-2023
Archivo