INVG. Andino 10:45 AM 9/Enero/2020

CERTIFICACIÓN

El infrascrito Secretario General y Delegado de la Comisión Interventora del INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS), certifica la **RESOLUCIÓN CI IHSS-GAYF No.1504/27-20-2019** aprobada en Sesión Ordinaria No.460 de fecha 27 de diciembre de 2019, que literalmente dice: "**RESOLUCIÓN CI IHSS-GAYF No.1504/27-12-2019**.- La Comisión Interventora del Instituto Hondureño de Seguridad Social (IHSS), **CONSIDERANDO (1):** Que mediante Decretos Ejecutivos PCM-011-2014; PCM-012-2014, PCM-025-2014 y PCM-049-2014 de fechas 15 de enero, 10 de abril, 30 de mayo y 4 de agosto de 2014 respectivamente, publicados en el Diario Oficial la Gaceta, el Presidente de la República en Consejo de Ministros decretó, entre otros: Intervenir al Instituto Hondureño de Seguridad Social (IHSS) por razones de interés público, nombrando para este efecto, una Comisión Interventora con amplios poderes conforme a lo establecido en el Artículo 100 de la Ley General de la Administración Pública. **CONSIDERANDO (2):** Que en el Artículo 100 de la Ley General de la Administración Pública, reformado mediante Decreto No.266-2013 contentivo de la Ley para Optimizar la Administración Pública, Mejorar los Servicios a la Ciudadanía y Fortalecimiento de la Transparencia en el Gobierno, establece que la Comisión Interventora tiene las facultades que les corresponden a los administradores de las mismas, ejerciendo su representación legal. **CONSIDERANDO (3):** Que Ley del Seguro Social en su Artículo 2 establece que el Instituto Hondureño de Seguridad Social cubrirá las contingencias y servicios del Régimen del Seguro de Atención de la Salud, Régimen del Seguro de Previsión Social, Régimen del Seguro de Riesgos Profesionales y Servicios Sociales, las que están sujetas a la reglamentación especial vigente. **CONSIDERANDO (4):** Que la Comisión Interventora mediante Resolución CI IHSS-GAYF No.1025/09-10-2019, aprobó los Términos de Referencia del Concurso Público CP No.001-2019 "CONTRATACIÓN DE SERVICIOS ESPECIALIZADOS DE ETHICAL HACKING, EVALUACIÓN DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA Y CAPACITACIÓN PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS)", mismos que contaron con el Visto Bueno en Certificación B-27-2019 de fecha 9 de octubre de 2019 emitida por el Comprador Público Certificado Número CPC-0062 acreditado por la Oficina Normativa de Contratación y Adquisiciones del Estado (ONCAE) en cumplimiento al Reglamento Operativo de Acreditación y Revocación de Certificación del Comprador Público Certificado. **CONSIDERANDO (5):** Que para este proceso de Concurso Público No.001-2019, retiraron bases, las siguientes empresas: 1.Big Technologic, 2.Intelector Honduras, S.A., 3.Sistemas Aplicativos (SISAP), 4.Inversiones Dinamic Solutions S. de R.L. 5. Deloitte & Touche S. de R.L. **CONSIDERANDO (6):** Que según acta No.1 de RECEPCION Y APERTURA DE OFERTAS DEL CONCURSO PÚBLICO No. CP-001-2019 "CONTRATACIÓN DE SERVICIOS ESPECIALIZADOS DE ETHICAL HACKING, EVALUACIÓN DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA Y CAPACITACIÓN PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL, IHSS" de fecha 26 de noviembre de 2019, presentaron ofertas las siguientes empresas: OFERENTE UNO: DELOITTE & TOUCHE S. DE R.L., quien presentó documentación legal en original y dos copias, conteniendo ciento treinta y un (131) folios, Documentación Técnica en original y dos copias conteniendo ciento treinta y ocho (138) folios. De igual forma presenta Documentación Económica en original y dos copias en sobres debidamente sellados. OFERENTE NUMERO DOS: DINAMIC SOLUTIONS, presentó documentación legal en original y dos copias, conteniendo veintiocho (28) folios, documentación técnica del folio treinta y cinco (35) al folio ciento quince (115) y la documentación de idoneidad técnica del folio ciento dieciséis (116) al folio ciento veintiuno (121) cabe destacar que por manifestación verbal de la representante de Dinamic Solutions

la Documentación Económica consta de los folios veintinueve (29) al folio treinta y cuatro (34), la que fue presentada en original y dos copias en sobres debidamente sellados. OFERENTE NÚMERO TRES: SISTEMAS APLICATIVOS SISAP S.A., presentó documentación legal en original y dos copias conteniendo ciento once (111) folios, documentación técnica conteniendo sesenta y tres (63) folios y la documentación económica en original y dos copias en sobres debidamente sellados. **CONSIDERANDO (7):** Que mediante Acta No.2 DE ANALISIS DE DOCUMENTACION LEGAL DEL PROCESO CONCURSO PÚBLICO NO. CP-001-2019 "CONTRATACION DE SERVICIOS PÚBLICOS ESPECIALIZADOS DE ETHICAL HACKING, EVALUACION DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLOGICA Y CAPACITACION PARA EL IHSS" de fecha 5 de diciembre de 2019, la Comisión de Evaluación procedió a realizar la revisión, análisis y evaluación según términos de referencia numerales 1.1 Documentación Legal, 1.2 Documentación Financiera y 1.3 Documentación Idoneidad Técnica verificando que: LA EMPRESA DELOITTE& TOUCHE S. DE R.L., se le solicitó subsanar 1) Constancia de Solvencia Municipal vigente, extendida por la Alcaldía Municipal del domicilio del representante legal, se le solicita considerando que no la presentó en su oferta. 2) El oferente deberá presentar copia de dos (2) contratos suscritos durante los últimos 3 años de trabajos similares con empresas públicas o privadas indicando persona, contacto, teléfono y dirección que permita verificar que los trabajos se realizaron conforme lo contratado, el valor de los contratos deberá ser de un 20% mínimo, del valor de la oferta presentada. Se le solicita en virtud que no los presentó en su oferta. 3) Autenticar la declaración jurada que en caso de ser adjudicado, en este proceso cumplirá con todas las condiciones solicitadas. Se le solicita debido a que la presentada en su oferta no venía autenticada. LA EMPRESA DINAMIC SOLUTIONS se le solicitó subsanar: 1) La certificación de estar inscrito o solicitud de inscripción en la Oficina Normativa de Contratación y Adquisición del Estado ONCAE. Se le solicita debido a que la presentada en su oferta está incompleta. 2) El oferente deberá presentar copia de dos (2) contratos suscritos durante los últimos 3 años de trabajos similares con empresas públicas o privadas indicando persona, contacto, teléfono y dirección que permita verificar que los trabajos se realizaron conforme lo contratado, el valor de los contratos deberá ser de un 20% mínimo, del valor de la oferta presentada. Se le solicita en virtud que no los presentó en su oferta; 3) Autenticar la declaración jurada que en caso de ser adjudicado, en este proceso cumplirá con todas las condiciones solicitadas. Se le solicita debido a que la presentada en su oferta no venía autenticada. LA EMPRESA SISTEMAS APLICATIVOS SISAP S.A. se le solicitó subsanar: La Autentica de la Certificación de estar inscrito o solicitud de inscripción en la Oficina Normativa de Contratación y Adquisición del Estado ONCAE. Se le solicita debido a que la presentada en su oferta no está autenticada. **CONSIDERANDO (8):** Que en la misma acta en mención se indica que una vez finalizado el plazo de subsanación de la documentación solicitada a estas empresa se verificó lo siguiente: La EMPRESA DELOITTE & TOUCHE S. DE R.L. no subsanó la documentación solicitada mediante Oficio No 001-CE-CP/001/2019 de fecha 27 de noviembre de 2019; La EMPRESA DINAMIC SOLUTIONS, No subsanó toda la documentación solicitada mediante Oficio No 002-CE-CP/001/2019 de fecha 27 de noviembre de 2019; debido a que no presentó copia de (2) dos contratos suscritos durante los últimos 3 años de trabajos similares con empresas públicas o privadas indicando persona, contacto, teléfono y dirección que permita verificar que los trabajos se realizaron conforme lo contratado, el valor de los contratos deberá ser de un 20% mínimo, del valor de la oferta presentada. La EMPRESA SISTEMAS APLICATIVOS SISAP S.A., subsanó en tiempo y forma la documentación solicitada mediante Oficio No. 003-CE-CP/001/2019 de fecha 27 de noviembre de 2019, por lo que Comisión de Evaluación luego del análisis pertinente

concluye que las ofertas presentadas por las EMPRESAS DELOITTE & TOUCHE S. DE R.L. y DINAMIC SOLUTIONS, no serán consideradas para la evaluación técnica, pasando únicamente la empresa Sistemas Aplicativos SISAP S.A. **CONSIDERANDO (9):** Que de acuerdo al Acta No.3 de EVALUACIÓN TÉCNICA DE EVALUACION DE LA DOCUMENTACION, CONDICIONES Y ESPECIFICACIONES TÉCNICAS DEL PROCESO CONCURSO PÚBLICO NO. CP-001-2019 "CONTRATACIÓN DE SERVICIOS ESPECIALIZADOS DE ETHICAL HACKING, EVALUACIÓN DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA Y CAPACITACIÓN PARA EL IHSS", de fecha 11 de diciembre de 2019, la Sub Comisión Técnica inició con la revisión de las especificaciones Técnicas mínimas solicitadas en las bases del CONCURSO PÚBLICO No. CP-001-2019, de la empresa que calificó para ser evaluadas técnicamente siendo esta la Empresa SISTEMAS APLICATIVOS, SISAP, S.A., como se detalla en el siguiente cuadro de revisión:

Descripción	Sistemas Aplicativos SISAP			
	CUMPLE		Folio	Observación
	SI	NO		
1. ANÁLISIS DE SEGURIDAD PARA VULNERABILIDADES EXTERNAS:				
Se requiere realizar un análisis de seguridad, emulando el escenario de un atacante externo, con modalidad de caja negra, de los servicios tecnológicos Institucionales desde redes públicas (Internet) con el objetivo de identificar las vulnerabilidades expuestas de la infraestructura tecnológica que dan soporte a los diferentes servicios públicos que el IHSS presta.	X		12, 13	
Para la realización de este servicio se deberán utilizar procedimientos, herramientas y pruebas de auditoría como las siguientes:	X		5, 10, 11, 13, 14, 15	
a. Descubrimiento				
b. Detección de conexiones externas				
c. Detección de Puertos TCP, UDP				
d. Detección de Servicios				
e. Enumerar y describir las diversas vulnerabilidades que pudieran presentarse en la revisión exhaustiva en la infraestructura tecnológica (Estaciones de trabajo, redes de comunicación, servidores o aplicaciones)				
f. Análisis de la seguridad de las conexiones con proveedores o entidades externas al Instituto				
g. Pruebas de vulnerabilidades				
h. Ejecución de código Exploits y verificación de resultados.				
i. Consolidación				
j. Borrado de rastros y evidencias				
Se deberán utilizar las herramientas especializadas que brinden una mayor calidad de información y resultados para el objetivo descrito para este proceso. Dejando las pruebas fehacientes de si se ha logrado la intrusión con éxito dependerán del tipo de ataque realizado que llevarán a obtener el siguiente tipo de evidencias:				
1. Captura del "trofeo": obtención de algún tipo de archivo de los servidores o redes				
2. Sembrado de pruebas en los servidores				
3. Resultado final comprobado: captura de paquetes, limitación del servicio del recurso (simulada).				
Los componentes objetivos para este análisis externo son:	X		5, 6, 12, 13	
1. Firewall Perimetral				
a. Dirección IP Publica (ISP 1)				
b. Dirección IP Publica (ISP 2)				
2. Los siguientes nombres de dominios y subdominios públicos (estos serán proporcionados al oferente adjudicado):				
a. Nombre dominio o subdominio PÚBLICO 1, 2, n+				
En el caso de encontrar vulnerabilidades críticas, se indicará como proceder para mitigar los riesgos oportunamente, sin necesidad de esperar al Informe Final.				
2. ANÁLISIS DE SEGURIDAD PARA VULNERABILIDAD A LA INFRAESTRUCTURA TECNOLÓGICA Y EQUIPOS INTERNOS:				
Se requiere realizar un análisis de seguridad, emulando el escenario de un atacante interno, con modalidad de caja negra, de los servicios tecnológicos Institucionales desde la red interna (Intranet) con el objetivo de identificar las vulnerabilidades expuestas de la infraestructura tecnológica que dan soporte a los diferentes servicios y equipos internos (servidores, estaciones de trabajo) con que el IHSS cuenta.			6, 16, 17	
Para la realización de este servicio se deberán utilizar procedimientos, herramientas y pruebas de auditoría como las siguientes:				
a. Descubrimiento				
b. Detección de conexiones internas				

c. Detección de Puertos TCP, UDP				
d. Detección de Servicios				
e. Enumerar y describir las diversas vulnerabilidades que pudieran presentarse en la revisión exhaustiva en la infraestructura tecnológica (Estaciones de trabajo, redes de comunicación, servidores o aplicaciones)				
f. Análisis de la seguridad de las conexiones internas, clientes VPN o entidades externas al Instituto.				
g. Pruebas de vulnerabilidades.				
h. Ejecución de código Exploits y verificación de resultados.				
i. Consolidación				
j. Borrado de rastros y evidencias				
Se deberán utilizar las herramientas especializadas que brinden una mayor calidad de información y resultados para el objetivo descrito para este proceso. Dejando las pruebas fehacientes de si se ha logrado la intrusión con éxito dependerán del tipo de ataque realizado que llevarán a obtener el siguiente tipo de evidencias:	X		6, 17, 18, 19	
1. Captura del "trofeo": obtención de algún tipo de archivo de los servidores o redes				
2. Sembrado de pruebas en los servidores				
3. Resultado final comprobado: captura de paquetes, limitación del servicio del recurso (simulada).				
Los componentes objetivos para este análisis externo son:				
1. Firewall interno				
2. Switch CORE Interno	X		6	
3. Estaciones de trabajo (15)				
4. Servidores internos (100)				
3. ANÁLISIS DE SEGURIDAD A LA RED DEL IHSS EN EL CAMPUS DE BARRIO ABAJO:				
Se requiere el desarrollo de un análisis del nivel de seguridad de la infraestructura tecnológica (evaluación de seguridad) en la red de la institución.				
En este análisis se debe verificar los controles de seguridad implementados en la red y las configuraciones de los mismos de acuerdo a mejores prácticas, se analizará lo siguiente:				
• Políticas de firewall interno				
• Procedimientos de Hardening				
• Topología de la Red				
• Configuración segura de Routers (propiedad de los ISPs).				
• Configuración segura de Servidores				
• Control de Acceso a la Red				
• Implementación correcta de Anti Virus	X		6, 20, 21	
• Implementación de Firewall (locales de cada equipo)				
• Configuración Segura de Switches capa 2-3				
• Segmentación de la red				
• Configuración segura red WiFi				
• Configuración recomendable para los PC's				
• Detección de Sniffers colocados en la red				
• Detección de implementación de proxys				
Implementación de un escaneo de vulnerabilidades				
• Distribución de parches de seguridad en la red				
• Configuración Active Directory				
• Acceso remoto a clínicas periféricas y regionales del IHSS.				
4. ATAQUE DE INGENIERÍA SOCIAL				
Se deberá definir y realizar un ataque basado en engaño a un usuario o administrador del IHSS así también de forma presencial, para poder ver, acceder, y conseguir la información que el analista requiere.				
El objetivo a seguir será el siguiente:				
1. Ingresar a las áreas de las oficinas del IHSS.				
2. Identificar los controles que hoy en día están colocados para detectar personal no autorizado.				
3. Analizar la respuesta de los empleados del IHSS en ver una persona no autorizada dentro de sus oficinas.	X		7, 22, 23, 24	
4. Analizar la capacitación de los empleados en temas de ciber seguridad y normas relacionadas a la capacitación de los empleados.				
5. Enviar a los usuarios ataques cibernéticos vía correo electrónico para ver los controles implementados hoy en día, y detectar código malicio en los correos y su eficiencia.				
6. Realizaremos llamadas telefónicas a algunos empleados de IHSS para intentar obtener información del usuario (usuarios y contraseña) y determinar qué tanto los usuarios del IHSS son vulnerables a ataques de tipo de Ingeniería social.				
5. ATAQUE REDES INALÁMBRICAS				
Se debe realizar la evaluación de seguridad de la infraestructura de red inalámbrica Institucional, en el Campus del IHSS en Barrio Abajo de Tegucigalpa.				
El objetivo a seguir será:	X		7, 24, 25	
1. Identificar y verificar los controles de seguridad implementados en la red inalámbrica del IHSS.				
2. Evaluación de la configuración aplicada en las soluciones WiFi.				

3. Detección de las vulnerabilidades que podrían existir en las soluciones WiFi.				
4. Confirmar la seguridad de la red inalámbrica contra ataques cibernéticos.				
6. GENERACIÓN DE INFORME Y ANÁLISIS REALIZADO:				
Como resultado los diferentes análisis y evaluaciones realizadas se deben generar los siguientes documentos y entregables:				
a. Informe de los análisis y evaluaciones realizadas en la totalidad de los componentes indicados en las especificaciones técnicas de manera individualizada, indicando las vulnerabilidades encontradas por cada componente y el procedimiento de corrección.	**X**		**7, 25**	
7. RECOMENDACIONES Y PROPUESTA DE MEJORAS:				
Se deberá generar un informe de recomendaciones y propuesta de mejoras a nivel Institucional, estas mejoras podrían aplicar a diferentes áreas internas del IHSS.	**X**		**7, 25**	
CURSOS DE SEGURIDAD INFORMÁTICA:				
Como parte del proceso se deberán incluir capacitaciones presenciales para el personal designado por el Instituto.				
Las capacitaciones a impartir serán las siguientes:	**X**		**8, 25**	
1. Taller de Seguridad Informática				
2. Taller de Seguridad Hacking				
PERFIL TÉCNICOS REQUERIDO:				
FORMACION ACADEMICA:				
• Profesionales universitarios con título en Ingeniería en Sistemas Computacionales, Informática Administrativa, Ciencias de la Computación o afines.				
• Certificaciones: CEH Certified Ethical Hacker, Licensed Penetration Tester (LPT), Offensive Security Certified Professional (OSCP), Certificación en Seguridad Informática Especializada, CCSA (Check Point), CCNA (Cisco), CCNP (Cisco) y MCSE (Microsoft).	**X**	**31-63**	Cumple de acuerdo con subsanación enviada por SISAP en fecha 11 diciembre de 2019, que cuenta con 47 folios útiles.
EXPERIENCIA: Deberá presentar documentación que acredite lo siguiente:				
• Experiencia comprobada de al menos 5 años en la ejecución de análisis de vulnerabilidad, y seguridad informática (incluir cartas de recomendación de proyectos anteriores).				
• Experiencia comprobada de la realización de transferencias de conocimientos.				

CONSIDERANDO (10): Que así mismo, la Sub-Comisión Técnica detalla el cuadro de evaluación de la Oferta Curricular y Técnica, realizada a la Empresa Sistemas Aplicativos SISAP, S.A.:

No.	Descripción	Puntaje Obtenido
I	**FORMACIÓN ACADÉMICA:**	
	El personal técnico a cargo del proyecto deberá contar al menos con la siguiente formación académica (50 puntos).	
1.1	Profesional universitario con título en Ingeniería en Sistemas Computacionales, Informática Administrativa, Ciencias de la Computación o afines.	10
1.2	Certificaciones:	40
	Certified Ethical Hacker (CEH) – (6)	
	Licensed Penetration Tester (LPT) – (4)	
	Offensive Security Certified Professional (OSCP)– (3)	
	Certificación en Seguridad Informática Especializada – (6)	
	CCSA (Check Point) – (6)	
	CCNA (Cisco) – (5)	
	CCNP (Cisco) – (5)	
	MCSE (Microsoft) – (5)	
II	**EXPERIENCIA ESPECIFICA:**	
	El personal técnico a cargo del proyecto deberá contar al menos con la siguiente experiencia (50 puntos).	
2.1	Experiencia comprobada de al menos 5 años en la ejecución de análisis de vulnerabilidad, y seguridad informática en Instituciones similares en tamaño e instalación al IHSS:	40
	Experiencia de 5 años (40)	
	Experiencia de 4 años (25)	
	Experiencia de 3 años (10)	
2.2	Experiencia comprobada de la realización de transferencias de conocimientos.	10
	PUNTAJE TOTAL	**100**

CONSIDERANDO (11): Que la Sub Comisión Técnica concluyó que la EMPRESA SISTEMAS APLICATIVOS SISAP, S.A., cumple con las especificaciones técnicas solicitadas en las bases de licitación, mismas que están descritas en el cuadro de revisión de esta acta, las que pueden pasar a la siguiente etapa de evaluación. **CONSIDERANDO (12):** Que de acuerdo al Acta No.4 DE APERTURA DEL SOBRE OFERTA ECONOMICA DEL PROCESO CONCURSO PÚBLICO No CP-001-2019 "CONTRATACION DE SERVICIOS PÚBLICOS ESPECIALIZADOS DE ETHICAL

HACKING, EVALUACION DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLOGICA Y CAPACITACION PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS" de fecha 13 de diciembre de 2019, la Comisión de Evaluación del Proceso por Cotización Concurso PÚBLICO No CP-001-2019 procedió al inicio del Acto de Apertura del sobre económico de la siguiente manera: la empresa SISTEMAS APLICATIVOS SISAP, S.A. DE C.V. presentó una oferta económica por un monto de SETECIENTOS VEINTICUATRO MIL NOVECIENTOS CINCUENTA LEMPIRAS EXACTOS (L724,950.00), sin incluir Impuesto Sobre Ventas, en virtud que el Instituto Hondureño de Seguridad Social se encuentra exonerado, según siguiente detalle:

No.	Descripción	SISTEMAS APLICATIVOS (SISAP)
1	Monto de Los Honorarios Profesionales	L634,950.00
2	Monto de Los Gastos Administrativos	L90,000.00
	TOTAL	**L724,950.00**

CONSIDERANDO (13): Que en el Acta en referencia se consigna que la empresa SISTEMAS APLICATIVOS SISAP, S.A. DE C.V., presenta una Garantía de Mantenimiento de Oferta No. 190878 por un monto de VEINTESEIS MIL DOSCIENTOS LEMPIRAS (L26,200.00) extendida por SEGUROS DEL PAIS con una vigencia comprendida del 26 de noviembre de 2019 hasta el día 10 de abril de 2020, dicha oferta económica consta de siete (7) folios. **CONSIDERANDO (14):** Que de acuerdo al Acta de Negociación DEL PROCESO CONCURSO PÚBLICO No CP-001-2019 "CONTRATACION DE SERVICIOS ESPECIALIZADOS DE ETHICAL HACKING, EVALUACION DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLOGICA Y CAPACITACION PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS", de fecha 18 de diciembre de 2019, el ingeniero Francisco Franco Gerente de Tecnología de la Información y Comunicaciones (GTIC), consultó a los representantes de SISAP sí podrían hacer un descuento sin afectar la ejecución de las especificaciones técnica del proyecto en repuesta los representantes de la empresa enviaron nota el día lunes 16 diciembre donde manifestaron que darán un servicio agregado de Evaluación de Eficacia de estrategia de ciberseguridad, según NIST Cybersecurity Framewrok 1.1 con un valor, según la empresa que supera los CINCO MIL DÓLARES ($5,000.00), por lo tanto, se concluyó que la oferta es aceptable y debe continuar con el trámite de recomendación respectivo, por lo que la oferta se ajusta y acepta por estar apegada a los precios de mercado y precios de referencia. **CONSIDERANDO (15):** Que previamente, la Sub Gerencia de Presupuesto en Memorando No.390-SGP/IHSS-2019 consignó disponibilidad presupuestaria para el proceso en referencia en el objeto de gasto 24600 por un monto de DOS MILLONES DOSCIENTOS CINCUENTA MIL LEMPIRAS EXACTOS (L2,250,000.00). **CONSIDERANDO (16):** Que ante lo expuesto la Comisión Evaluadora después de análisis de especificaciones, condiciones técnicas y verificación de precio recomienda a la Comisión Interventora del Instituto Hondureño de Seguridad Social (IHSS) adjudicar el PROCESO CONCURSO PÚBLICO No.CP-001-2019 "CONTRATACION DE SERVICIOS PÚBLICOS ESPECIALIZADOS DE ETHICAL HACKING, EVALUACION DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLOGICA Y CAPACITACION PARA EL IHSS", a la empresa SISTEMAS APLICATIVOS SISAP S.A. de C.V. por un monto de SETECIENTOS VEINTICUATRO MIL NOVECIENTOS CINCUENTA LEMPIRAS EXACTOS (L724,950.00), sin incluir Impuesto Sobre Ventas, en virtud que el Instituto Hondureño de Seguridad Social se encuentra exonerado. **CONSIDERANDO (17):** Que el licenciado Edwin Medina Gerente Administrativo y Financiero del Instituto y actuando como Comprador Público Certificado Número CPC-0062 acreditado por la Oficina Normativa de Contratación y Adquisiciones del Estado (ONCAE), emitió certificación C-47-

2019 de fecha 27 de diciembre de 2019, donde se otorga el Visto Bueno al documento de Actas del Proceso del Concurso PÚBLICO No. CP-001-2019 "CONTRATACION DE SERVICIOS PÚBLICOS ESPECIALIZADOS DE ETHICAL HACKING, EVALUACION DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLOGICA Y CAPACITACION PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS)". **CONSIDERANDO (18):** Que lo anterior se realiza en cumplimiento al Acuerdo Ejecutivo número 028-2018 de fecha 30 de julio de 2018, que reforma el Reglamento de la Ley de Contratación del Estado, adicionando los artículos 44-A, 44-B y 44C, mandando a la Oficina Normativa de Contratación y Adquisiciones del Estado (ONCAE) a reglamentar la acreditación y revocación de la certificación del Comprador Público Certificado (CPC) quienes en mandato a lo indicado, emitieron el Reglamento Operativo de Acreditación y Revocación de Certificación del Comprador Público Certificado (CPC), de fecha 8 de noviembre de 2018 y publicado el 20 de noviembre de 2018 en el Diario Oficial La Gaceta número 37,799, Sección B en sus páginas B.1 a la B.8, aunado a lo antes citado también en acatamiento a la Circular No.ONCAE-009-2019. **CONSIDERANDO (19):** Que este proceso es necesario debido a la necesidad Institucional de realizar un análisis de evaluación de la seguridad de la infraestructura tecnológica instalada y en producción, así mismo al cumplimiento de las recomendaciones para fortalecer la seguridad y la operatividad institucional en el cumplimiento de los diferentes requerimientos internos, externos y de carácter regulatorio a los cuales el instituto se encuentra sujeta. **POR TANTO**; En uso de las atribuciones que la Ley le confiere a la Comisión Interventora y con fundamento en Decreto Ejecutivo No. PCM-011-2014 de fecha 15 de enero de 2014, PCM-012-2014 de fecha 10 de abril de 2014, No. PCM-025-2014 de fecha 30 de mayo de 2014 y No. PCM-049-2014 de fecha 4 de agosto de 2014 publicados en el Diario Oficial La Gaceta en fecha 17 de enero, 3 y 30 de mayo y 9 de agosto de 2014 respectivamente, Artículos 1, 5, 11, 12, 33, 34, 36, 38, 50, 51, de la Ley de Contratación del Estado; Artículos 2, 11, 20, 37,39, 53, 110,125, 127, 132, 136,139 y 141 del Reglamento de la misma Ley, Artículo 100 de la Ley para Optimizar la Administración Pública, Mejorar los Servicios a la Ciudadanía y Fortalecimiento de Transparencia en el Gobierno, en sesión del 27 de diciembre de 2019, **RESUELVE: 1.** Dar por recibida la recomendación de la Comisión Evaluadora de adjudicar el proceso del Concurso Público No. CP-001-2019 "CONTRATACION DE SERVICIOS PÚBLICOS ESPECIALIZADOS DE ETHICAL HACKING, EVALUACION DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLOGICA Y CAPACITACION PARA EL IHSS", a la empresa SISTEMAS APLICATIVOS SISAP S.A. de C.V. por un monto de SETECIENTOS VEINTICUATRO MIL NOVECIENTOS CINCUENTA LEMPIRAS EXACTOS (L724,950.00), sin incluir Impuesto Sobre Ventas, en virtud de cumplir con la documentación legal, técnica financiera, así como las especificaciones y condiciones técnicas contando con el Visto Bueno del según Certificación C-47-2019 de fecha 27 de diciembre de 2019, emitida por el Comprador Público Certificado Número CPC-0062 acreditado por la Oficina Normativa de Contratación y Adquisiciones del Estado (ONCAE) en cumplimiento al Reglamento Operativo de Acreditación y Revocación de Certificación del Comprador Público Certificado. El detalle de acuerdo los precios unitarios y sus totales es el siguiente:

No.	Descripción	SISTEMAS APLICATIVOS (SISAP)
1	Monto de Los Honorarios Profesionales	634,950.00
2	Monto de Los Gastos Administrativos	90,000.00
	TOTAL	**L724,950.00**

2. Adjudicar el proceso del Concurso Público No. CP-001-2019 "CONTRATACION DE SERVICIOS PÚBLICOS ESPECIALIZADOS DE ETHICAL HACKING, EVALUACION DE SEGURIDAD DE LA

INFRAESTRUCTURA TECNOLOGICA Y CAPACITACION PARA EL IHSS" a la empresa SISTEMAS APLICATIVOS SISAP S.A. de C.V. por un monto de SETECIENTOS VEINTICUATRO MIL NOVECIENTOS CINCUENTA LEMPIRAS EXACTOS (L724,950.00) sin incluir Impuesto Sobre Ventas, en virtud de cumplir con la documentación legal, técnica financiera, así como las especificaciones y condiciones técnicas.

NO.	Descripción	SISTEMAS APLICATIVOS (SISAP)
1	Monto de Los Honorarios Profesionales	634,950.00
2	Monto de Los Gastos Administrativos	90,000.00
	TOTAL	**724,950.00**

3. De conformidad al Acta de recomendación de la Comisión Evaluadora del proceso de Concurso Público No. CP-001-2019, dar por aceptada el servicio agregado de Evaluación de Eficacia de Estrategia de Ciberseguridad, según NIST Cybersecurity Framewrok por parte de la empresa SISTEMAS APLICATIVOS SISAP S.A. sin ningún costo para el IHSS. **4.** Autorizar al Director Ejecutivo Interino para que suscriba el contrato con la empresa SISTEMAS APLICATIVOS SISAP S.A. de C.V., de acuerdo a lo indicado en el resolutivo dos (2) y tres (3) de la presente Resolución. **5.** Instruir a la Secretaría General, para que proceda a realizar las siguientes notificaciones: **a.** Notificar el resultado de este proceso a la empresa SISTEMAS APLICATIVOS SISAP S.A. de C.V. conforme lo indicado en el resolutivo dos (2) y tres (3) de la presente Resolución. **b.** Notificar a las demás empresas participantes Big Technologic, Intelector Honduras, S.A., Inversiones Dinamic Solutions,S. de R.L., Deloitte & Touche S. de R.L. del resultado del proceso, según lo indicado en considerando ocho (8) de la presente resolución, para que procedan conforme a Ley a retirar la Garantía de Mantenimiento de oferta presentada. **6.** Instruir a la Unidad de Asesoría Legal, para que en el término de cinco (5) días hábiles, proceda a la elaboración del contrato con la empresa SISTEMAS APLICATIVOS SISAP S.A. de C.V.según lo indicado en el resolutivo dos (2) y tres (3) de la presente Resolución. **7.** Transcribir el resolutivo dos (2) de la presente Resolución a la Gerencia Administrativa y Financiera con el fin de ser remitido a la Oficina Normativa de Contratación y Adquisiciones del Estado (ONCAE). **8.** Autorizar a la Gerencia Administrativa y Financiera para que proceda a remitir a la Oficina Normativa de Contratación y Adquisiciones del Estado (ONCAE) una copia electrónica de la Certificación C-47-2019 de fecha 27 de diciembre de 2019, donde otorga Visto Bueno en su firma y sello, número correlativo y codificado por tipo de documento, a más tardar diez (10) días después de ser otorgada, en cumplimiento al Artículo 5 del Reglamento Operativo de Acreditación y Revocación de Certificación del Comprador Público Certificado. **9.** El costo que se erogue por lo autorizado en la presente Resolución será imputable a la estructura presupuestaria del Régimen del Seguro de Atención de la Salud y distribuido a los demás regímenes de acuerdo a la Metodología de Distribución de los Gastos Administrativos. **10.** Comunicar lo resuelto a la Dirección Ejecutiva Interina, Gerencia Administrativa y Financiera, Gerencia de Tecnología de la Información y Comunicaciones (GTIC), Subgerencia de Presupuesto, Sub Gerencia de Suministros Materiales y Compras, Secretaría General y a la Unidad de Asesoría Legal para los fines legales correspondientes. **11.** La presente Resolución es de ejecución inmediata. **F) VILMA C. MORALES M.,** Presidenta CI IHSS. **F) ROBERTO CARLOS SALINAS,** Miembro CI IHSS. **F) GERMAN EDGARDO LEITZELAR V.,** Miembro CI IHSS. **F) CARLOS ROBERTO ORTEGA,** Secretario General IHSS y Delegado Comisión Interventora en Resolución CI IHSS No.797/24-11-2015".

Y para los fines correspondientes se extiende la presente en la ciudad de Tegucigalpa, Municipio Distrito Central, a los veintisiete días del mes de diciembre del año dos mil diecinueve.

CARLOS ROBERTO ORTEGA
Secretario General IHSS y Delegado Comisión
Interventora en Resolución CI IHSS No.797/24-11-2015