



UNIDAD COORDINADORA DE PROYECTOS

Préstamo No.3541/BL-HO Proyecto "Fortalecimiento Institucional y Operativo de la Administración Tributaria"

**Contrato de Préstamo BID No. 3541/BL-HO
Enmienda No. 2**

No. LPI-SAR-BID-015-2017

"Adquisición de Equipamiento para la Modernización de la Infraestructura Tecnológica del Servicio de Administración de Rentas"

El Servicio de Administración de Rentas (SAR) a través de la Unidad Coordinadora de Proyectos, comunica a las empresas participantes del proceso de Licitación Pública Internacional No. **LPI-SAR-BID-015-2017 "Adquisición de Equipamiento para la Modernización de la Infraestructura Tecnológica del Servicio de Administración de Rentas"**, que con base en la Cláusula 8. Enmienda a los Documentos de Licitación, Sección I. Instrucciones a los Oferentes, se emite la siguiente enmienda:

- 1. Modificar la Parte I. Sección II. Datos de la Licitación, la cual a partir de la presente Enmienda los Lotes e ítems modificados DEBERÁN LEERSE:**

IAO 1.1

MODIFICAR:

A. General			
Número de Lote	Descripción	Items	Cantidad de Bienes
8.	Licencias Varias		
	Herramienta de monitoreo de servicios.	1	2
	Secure CRT.	2	2
	Enterprise Architec.	3	33

"Tributar es Progresar"



AGREGAR NUEVO LOTE NO. 14, EL CUAL SE DERIVA DEL LOTE NO. 8

A. General			
Número de Lote	Descripción	Items	Cantidad de Bienes
14.	Licencias Especializadas		
	FirePower.	1	4
	Licencias de Servidor Virtual Para Autenticación Y Administración de Equipos de Telecomunicaciones.	2	1

Cláusula de la IAO	C. Preparación de las Ofertas
IAO 11.1 (h)	f) Copia de contrato(s) u Orden de Compra con sus actas o comprobantes de recepción a satisfacción del comprador, de productos similares a los ofertados (Ver Sección III). (<i>Se exceptúan los Lotes 8, 10 y 14</i>).

"Tributar es Progresar"



2. Modificar la Parte II. Requisitos de los Bienes y Servicios, Sección VII Lista de Requisitos, la cual a partir de la presente Enmienda los Lotes e ítems modificados DEBERÁN LEERSE:

Lista de Bienes y Plan de Entrega

N° de Artículo	Descripción de los Bienes	Cantidad	Unidad Física	Lugar de Destino Convenido o de acuerdo con los DDL	Fecha Entrega (de acuerdo con los Incoterms)		
					Fecha más Temprana de Entrega	Fecha Límite de Entrega	Fecha de Entrega ofrecida por el Oferente [a ser proporcionada por el Oferente]
[indicar el No.]	[indicar la descripción de los Bienes]	[indicar la cantidad de los artículos a suministrar]	[indicar la unidad física de medida de la cantidad]	[indicar el lugar de entrega destino convenido]	[indicar el número de días después de la fecha de efectividad del Contrato]	[indicar el número de días después de la fecha de efectividad del Contrato]	[indicar el número de días después de la fecha de efectividad del Contrato]
Lote 8	Licencias Varias.	1 Unidades.	Software de Monitoreo de Servicios de Red.	SAR Edificio Gabriel A. Mejía, Col. Palmira.	5 días posteriores a la efectividad del contrato.	45 días posteriores a la efectividad del contrato.	
Ítem 8.1.	Herramienta de monitoreo de servicios.						
Ítem 8.2	Secure CRT.	2 Unidades.	Software de Administración de Equipos de Telecomunicaciones.	SAR Edificio Gabriel A. Mejía, Col. Palmira.	5 días posteriores a la efectividad del contrato.	45 días posteriores a la efectividad del contrato.	

"Tributar es Progresar"



Ítem 8.3	Enterprise Architec.	33 Unidades.	Licencias para desarrollo de Software.	Edificio Gabriel A. Mejía, Col. Palmira.	5 días posteriores a la efectividad del contrato.	45 días posteriores a la efectividad del contrato.
Lote 14 Ítem 14.1	Licencias Especiales FirePower.	4 Unidades.	Licencias de Software de Protección Perimetral.	SAR Edificio Gabriel A. Mejía, Col. Palmira.	5 días posteriores a la efectividad del contrato.	60 días posteriores a la efectividad del contrato.
Ítem 14.2	Licencias de Servidor Virtual Para Autenticación Y Administración de Equipos de Telecomunicaciones.	1 Unidad	Licencias de Software Virtual para autenticación y Administración de Equipos de Telecommunicaion es.	SAR Edificio Gabriel A. Mejía, Col. Palmira.	5 días posteriores a la efectividad del contrato.	60 días posteriores a la efectividad del contrato.

"Tributar es Progresar"



Lista de Servicios Conexos y Cronograma de Cumplimiento

Lote No. 8 Licencias varias

Ítem 8.3 Enterprise Archie.

Servicios conexos de implementación de solución	
Implementación	La compañía que provea los servicios de valor agregado realizará las siguientes actividades: <ul style="list-style-type: none">● Habilitación inicial de suscripción.● Documentos técnicos para la administración y configuración.● Capacitación.
Entrega	El SAR aceptará como entregada la solución cuando esta se encuentre completamente implementada y funcionando de acuerdo a lo establecido en este documento de especificaciones técnicas y a lo que el SAR disponga, y que se haya demostrado su funcionalidad.
Soportaje	
Soportaje vigente	Soportaje por el tiempo de duración de la suscripción 1 año.

“Tributar es Progresar”



Lote No. 14 Licencias Especializadas.

Item 14.1 FirePower

Características	Requerimiento técnico mínimo
Características Generales	
Software requerido	Fire Power L-ASA5525-TAMC-3Y
Tipo de Plan	<ul style="list-style-type: none"> • Producto.
Plan	<ul style="list-style-type: none"> • Licencia.
Cantidad de suscripciones	<ul style="list-style-type: none"> • 4
Beneficiario directo	<p>Servicio de Administración de Rentas – Honduras Centro América:</p> <ul style="list-style-type: none"> • Entrega a la Dirección Nacional de Tecnologías, Edificio Gabriel A. Mejía, Segundo Piso, Tegucigalpa, Honduras.
Características de esta versión:	<ul style="list-style-type: none"> • Servicio de IPS + protección avanzada de Malware + URL Filtering
Plazo de suscripción	<ul style="list-style-type: none"> • 3 años a partir de la fecha de implementación.
Servicios conexos de implementación de solución	
Implementación	<p>La compañía que provea los servicios de valor agregado realizará las siguientes actividades:</p> <ul style="list-style-type: none"> • Habilitación inicial de suscripción. • Documentos técnicos para la administración y configuración.
Entrega	<p>El SAR aceptará como entregada la solución cuando esta se encuentre completamente implementada y funcionando de acuerdo a lo establecido en este documento de especificaciones técnicas y a lo que el SAR disponga, y que se haya demostrado su funcionalidad.</p>
SopORTE	
SopORTE vigente	<p>SopORTE por el tiempo de duración de la suscripción durante 3 años.</p>

“Tributar es Progresar”





ESPECIFICACIONES TÉCNICAS

En el Ítem 1.1: Plataforma de Servidores RISC – Servidores tipo 1

Actualmente se lee como:

Descripción	Original	Modificación
Procesador	>= SPARC T5, 16 núcleos , 3.6 Ghz	>= SPARC M7, 32 núcleos, 4.13 Ghz
Cache de Procesador	>= Shared 8 MB, 8 banked, Level 3 Cache; 128 KB Level 2 unified cache per core	>= 64 MB Level 3 Cache, 8 MB per each core cluster, 256 KB Level 2 per core pair

LOTE 5: Plataforma de Almacenamiento SAN ISCSI

En el Ítem 5.3: Switches 10 Gbps Red de Almacenamiento..

Actualmente se lee como:

Descripción	Original	Modificación
Tasa de reenvío del Switch	1080 Mpps o superior	>= 1050 Mpps
Boot Flash Memory	>= 2 GB	>= 1 GB
Soporte	Soporte en Sitio 8X5X4 NBD.	Soporte 7x24x365

LOTE 6: Telecomunicaciones para Data Center

En el Ítem 6.1: Equipo CORE de Replicación de Data Center.

Actualmente se lee como:

Descripción	Original	Modificación
Características Físicas	El equipo deberá contar con una bandeja de administración de cableado integrada al chasis que permita organizar de forma lateral y equitativa (entre el lado izquierdo y el derecho) todos los cables categoría 6A y las fibras entrantes.	Se elimina esta característica física.

“Tributar es Progresar”





	Con respecto a la altura del equipo, no deberá ser mayor a diez (10) unidades de altura en medida de rack, con el objetivo de maximizar el espacio disponible. Deberá incluir todos los accesorios y herrajes para su debida instalación física.	Se mantiene sin cambio.
	El chasis deberá tener como mínimo seis (7) slots de los cuales 2 slots deben ser dedicados a supervisoras y cuatro (5) a módulos de input/output (linecard).	El chasis deberá tener como mínimo siete (7) slots de los cuales 2 slots deben ser dedicados a supervisoras y cinco (5) a módulos de input/output (linecard).
	El equipo se deberá poder instalar en racks estándar de diecinueve (19) pulgadas EIA.	Se mantiene sin cambio.
	El voltaje requerido por el equipo deberá encontrarse en el rango de 100 a 240 VAC.	Se mantiene sin cambio.
	El equipo deberá operar en las condiciones ambientales típicas del territorio Hondureño; El equipo debe cumplir las siguientes normas: UL 60950-1 Second Edition. CAN/CSA-C22.2 No. 60950-1 Second Edition. EN 60950-1 Second Edition. • IEC 60950-1 Second Edition.	Se mantiene sin cambio.
	El chasis deberá contar con algún mecanismo de seguridad mecánico para evitar el acceso no autorizado al sistema y que impida la manipulación del cableado entrante y la desconexión (intencional o accidental) de los conectores de sus respectivos puertos. Este mecanismo deberá contar con algún tipo de combinación o llave que restrinja el acceso a personal no autorizado.	Se eliminan las características especiales de la bandeja y del chasis.

LOTE 12: Plataforma de Firma Electrónica

En el ítem 12.1 Autoridad Certificadora Raíz.

Actualmente se lee como:

Descripción	Original	Modificación
Algoritmo y Funciones HASH	<ul style="list-style-type: none"> • RSA soportado con longitud de clave de hasta 4.096 bit. • MD5. • SHA-1, SHA-2 hasta SHA-512. 	<ul style="list-style-type: none"> • RSA soportado con longitud de clave de hasta 4.096 bit. • SHA-2 hasta SHA-512.

“Tributar es Progresar”





Cumplimiento de Estandares	<ul style="list-style-type: none"> • RSA PKCS#1_v1.5 • RSA X509 • NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, X.509v3 CRLv2 rfc3280, • http, https. 	<ul style="list-style-type: none"> • RSA PKCS#1_v1.5 • RSA X509 • NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, X.509v3 CRLv2 rfc5280. • http, https.
Generación de Certificados	<ul style="list-style-type: none"> • Generación de petición de certificados ilimitada • El componente RA debe permitir realizar (solicitando al componente CA Subordinada) la generación, revocación, suspensión y rehabilitación de certificados, de acuerdo a la política de certificación definida en el componente AC Subordinada. • El componente RA debe permite revocar, suspender o rehabilitar cualquier certificado que haya sido generado, desde el componente AC Subordinada, solicitando a éste la revocación, suspensión o rehabilitación del certificado. • Capacidad de publicar certificados y CRL en LDAP, Web, SAMBA • Sincronización del reloj del sistema vía NTP • Notificación y registro de errores automático. • Procesado de peticiones de certificación en formato PKCS#10, generadas en navegador web (Microsoft Explorer o Firefox), o bien generación sin petición previa resultando en un fichero PKCS#12. • Descarga o instalación del correspondiente certificado emitido por el componente AC Subordinada, en formato PEM, PKCS#12, o bien, mediante la instalación en navegador web (Microsoft Explorer o Firefox). Notificación mediante correo electrónico, a la finalización de los procedimientos de revocación, suspensión o rehabilitación. 	<ul style="list-style-type: none"> • Generación de petición de certificados ilimitada • El componente Autoridad Certificadora Raíz debe permitir realizar Emisión (generación), revocación, suspensión y rehabilitación de certificados de la Autoridad Certificadora Subordinada, bajo la correspondiente política de certificación configurada. • El componente Autoridad Certificadora Raíz debe permitir la revocación, suspensión y rehabilitación (cancelación de la suspensión) de los certificados emitidos por la Autoridad Certificadora Subordinada. • Capacidad de generar ARL (Lista de certificados revocados de AC Subordinada) y su exportación para su publicación en línea. • Sincronización del reloj del sistema vía NTP. • Notificación y registro de errores automático. • Las partes no modificadas se mantienen inalterables.

“Tributar es Progresar”





	<ul style="list-style-type: none"> • Operación remota de certificados vía webservices seguro y firmado mediante el API Webservice Security (revocación, emisión, consulta, suspensión, rehabilitación). • Integración con repositorio para la obtención de los datos con los que se van a generar los certificados de un repositorio, y deberá permite publicar los certificados en el repositorio. 	<ul style="list-style-type: none"> • Las partes no modificadas se mantienen inalterables.
Interfaces	<ul style="list-style-type: none"> • Sincronización del reloj del sistema vía NTP • Notificación de errores automático • Capacidad de soportar múltiples ACs subordinadas. • Todos los documentos, paneles gráficos, interface de usuario y mensajes de error deberán estar en español. • Capacidad de personalizar los menús de interface gráfica • Todos los elementos de la solución, aplicación, hardware, software y HSMs deben ser del mismo fabricante, para facilitar la responsabilidad sobre el proyecto y la resolución de las posibles incidencias. • Capacidad de entregar los HSMs abiertos y que sean cerrados en presencia de los funcionarios correspondientes, para garantizar que no se introduce ningún elemento externo que pueda ser considerado como inseguro por las autoridades pertinentes 	<ul style="list-style-type: none"> • Sincronización del reloj del sistema vía NTP • Notificación de errores automático • Capacidad de soportar múltiples ACs subordinadas. • Todos los documentos, paneles gráficos, interface de usuario y mensajes de error deberán estar en español. • Capacidad de personalizar los menús de interface gráfica • Todos los elementos de la solución, aplicación, hardware, software y HSMs deben ser compatibles, entre sí. En caso de no ser del mismo fabricante este debe incluir una declaración jurada del fabricante, donde se garantice el soporte y resolución de posibles problemas de compatibilidad. • Capacidad de entregar los HSMs abiertos y que sean cerrados en presencia de los funcionarios correspondientes, para garantizar que no se introduce ningún elemento externo que pueda ser considerado como inseguro por las autoridades pertinentes

“Tributar es Progresar”





En el Ítem 12.2 Autoridad Certificadora Subordinada.

Actualmente se lee como:

Descripción	Original	Modificación
Algoritmo y Funciones HASH	<ul style="list-style-type: none"> • RSA soportado con longitud de clave de hasta 4.096 bit. • MD5. • SHA-1, SHA-2 hasta SHA-512. 	<ul style="list-style-type: none"> • RSA soportado con longitud de clave de hasta 4.096 bit. • SHA-2 hasta SHA-512.
Cumplimiento de Estándares	<ul style="list-style-type: none"> • RSA PKCS#1_v1.5 • RSA X509 • NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, X.509v3 CRLv2 rfc3280, http, https. 	<ul style="list-style-type: none"> • RSA PKCS#1_v1.5 • RSA X509 • NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, X.509v3 CRLv2 rfc5280, http, https.
Interfaces	<ul style="list-style-type: none"> • Sincronización del reloj del sistema vía NTP • Notificación de errores automático • Capacidad de soportar múltiples ACs subordinadas. • Todos los documentos, paneles gráficos, interface de usuario y mensajes de error deberán estar en español. • Capacidad de personalizar los menús de interface gráfica • Todos los elementos de la solución, aplicación, hardware, software y HSMs deben ser del mismo fabricante, para facilitar la responsabilidad sobre el proyecto y la resolución de las posibles incidencias. • Capacidad de entregar los HSMs abiertos y que sean cerrados en presencia de los funcionarios correspondientes, para garantizar que no se introduce ningún elemento externo que pueda ser considerado como inseguro por las autoridades pertinentes • Interfaz de usuario en español que permita: 	<ul style="list-style-type: none"> • Sincronización del reloj del sistema vía NTP • Notificación de errores automático • Todos los documentos, paneles gráficos, interface de usuario y mensajes de error deberán estar en español. • Capacidad de personalizar los menús de interface gráfica • Todos los elementos de la solución, aplicación, hardware, software y HSMs deben ser compatibles, entre sí. En caso de no ser del mismo fabricante este debe incluir una declaración jurada del fabricante, donde se garantice el soporte y resolución de posibles problemas de compatibilidad. • Capacidad de entregar los HSMs abiertos y que sean cerrados en presencia de los funcionarios correspondientes, para garantizar que no se introduce ningún elemento externo que pueda ser considerado como inseguro por las autoridades pertinentes • Interfaz web de operadores con autenticación de cliente (HTTPS), que permite al menos: <ul style="list-style-type: none"> • Configuración de los parámetros que condicionan el

“Tributar es Progresar”





	<ul style="list-style-type: none"> • Realizar peticiones de certificados • Envío de notificaciones por mail al usuario cuando el certificado ha sido generado • Descarga del certificado con contraseña de autenticación enviado en la notificación. 	<p>funcionamiento de los elementos software específicos del componente Autoridad Certificadora Subordinada.</p> <ul style="list-style-type: none"> • Configuración de las políticas de certificación. • Generación manual de una CRL, así como consultas relativas a certificados emitidos, CRLs emitidas, etc.
--	---	---

En el ítem 12.3 Autoridad de Registro.

Actualmente se lee como:

Descripción	Original	Modificación
Algoritmo y Funciones HASH	<ul style="list-style-type: none"> • RSA soportado con longitud de clave de hasta 4.096 bit. • MD5. • SHA-1, SHA-2 hasta SHA-512. 	<ul style="list-style-type: none"> • RSA soportado con longitud de clave de hasta 4.096 bit. • SHA-2 hasta SHA-512.
Cumplimiento de Estándares	<ul style="list-style-type: none"> • RSA PKCS#1_v1.5 • RSA X509 • NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, X.509v3 CRLv2 rfc3280, http, https. 	<ul style="list-style-type: none"> • RSA PKCS#1_v1.5 • RSA X509 • NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, X.509v3 CRLv2 rfc5280, http, https.
Interfaces	<ul style="list-style-type: none"> • Sincronización del reloj del sistema vía NTP • Notificación de errores automático • Capacidad de soportar múltiples ACs subordinadas. • Todos los documentos, paneles gráficos, interface de usuario y mensajes de error deberán estar en español. • Capacidad de personalizar los menús de interface gráfica • Todos los elementos de la solución, aplicación, hardware, software y HSMs deben ser del mismo fabricante, para facilitar la responsabilidad sobre el proyecto y la resolución de las posibles 	<ul style="list-style-type: none"> • Sincronización del reloj del sistema vía NTP • Notificación de errores automático • Capacidad de soportar múltiples ACs subordinadas. • Todos los documentos, paneles gráficos, interface de usuario y mensajes de error deberán estar en español. • Capacidad de personalizar los menús de interface gráfica • Todos los elementos de la solución, aplicación, hardware, software y HSMs deben ser compatibles, entre sí. En caso de no ser del mismo fabricante este debe incluir una declaración jurada del fabricante, donde se

“Tributar es Progresar”





	<p>incidencias.</p> <ul style="list-style-type: none"> • Capacidad de entregar los HSMs abiertos y que sean cerrados en presencia de los funcionarios correspondientes, para garantizar que no se introduce ningún elemento externo que pueda ser considerado como inseguro por las autoridades pertinentes 	<p>garantice el soporte y resolución de posibles problemas de compatibilidad.</p> <ul style="list-style-type: none"> • Capacidad de entregar los HSMs abiertos y que sean cerrados en presencia de los funcionarios correspondientes, para garantizar que no se introduce ningún elemento externo que pueda ser considerado como inseguro por las autoridades pertinentes
--	--	--

En el Ítem 12.4 Autoridad de Validación.

Actualmente se lee como:

Descripción	Original	Modificación
Algoritmo y Funciones HASH	<ul style="list-style-type: none"> • RSA soportado con longitud de clave de hasta 4.096 bit. • MD5. • SHA-1, SHA-2 hasta SHA-512. 	<ul style="list-style-type: none"> • RSA soportado con longitud de clave de hasta 4.096 bit. • SHA-2 hasta SHA-512.
Cumplimiento de Estándares	<ul style="list-style-type: none"> • RSA PKCS#1_v1.5 • RSA X509 • NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, X.509v3 CRLv2 rfc3280, http, https. 	<ul style="list-style-type: none"> • RSA PKCS#1_v1.5 • RSA X509 • NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, X.509v3 CRLv2 rfc5280. http, https.
Interfaces	<ul style="list-style-type: none"> • Sincronización del reloj del sistema vía NTP • Notificación de errores automático • Capacidad de soportar múltiples ACs subordinadas. • Todos los documentos, paneles gráficos, interface de usuario y mensajes de error deberán estar en español. • Capacidad de personalizar los menús de interface gráfica • Todos los elementos de la solución, aplicación, hardware, software y HSMs deben ser del mismo fabricante, para facilitar la responsabilidad sobre el proyecto y la resolución de las posibles incidencias. 	<ul style="list-style-type: none"> • Sincronización del reloj del sistema vía NTP • Notificación de errores automático • Todos los documentos, paneles gráficos, interface de usuario y mensajes de error deberán estar en español. • Capacidad de personalizar los menús de interface gráfica • Todos los elementos de la solución, aplicación, hardware, software y HSMs deben ser compatibles, entre sí. En caso de no ser del mismo fabricante este debe incluir una declaración jurada del fabricante, donde se garantice el soporte y resolución de posibles problemas de compatibilidad. • Capacidad de entregar los HSMs abiertos y que sean cerrados en

“Tributar es Progresar”





	<ul style="list-style-type: none"> • Capacidad de entregar los HSMs abiertos y que sean cerrados en presencia de los funcionarios correspondientes, para garantizar que no se introduce ningún elemento externo que pueda ser considerado como inseguro por las autoridades pertinentes • Interfaz de usuario en español que permita: <ul style="list-style-type: none"> • Realizar peticiones de certificados • Envío de notificaciones por mail al usuario cuando el certificado ha sido generado • Descarga del certificado con contraseña de autenticación enviado en la notificación. 	<p>presencia de los funcionarios correspondientes, para garantizar que no se introduce ningún elemento externo que pueda ser considerado como inseguro por las autoridades pertinentes</p> <ul style="list-style-type: none"> • Interfaz web de operadores en español con autenticación de cliente (HTTPS) que permita: <ul style="list-style-type: none"> • Configuración de parámetros propios de funcionamiento de los elementos de software del componente Autoridad de Validación. • Configuración de los parámetros de autenticación del usuario para acceder a la base de datos del componente Autoridad de Validación para la consulta y descarga de ficheros log de servicio.
<p>Generación de Certificados</p>	<ul style="list-style-type: none"> • El componente AV debe determinar de forma online el estado actual de cualquier certificado emitido por el componente AC subordinada, a través del protocolo OCSP, de acuerdo al estándar RFC2560. • Las respuestas OCSP emitidas están firmadas con la clave privada correspondiente al certificado de firma de respuestas OCSP del componente AV. • Emisión de respuestas OCSP que contienen el estado de revocación de los certificados solicitados, conforme al estándar RFC2560. • Acceso a información de revocación de base de datos de la Autoridad de Certificación y CRL en LDAP, Web, SAMBA • Sin costo de licencias referente al uso de servicio OCSP por número de usuarios • Sincronización del reloj del sistema vía NTP 	<ul style="list-style-type: none"> • El componente AV debe determinar de forma online el estado actual de cualquier certificado emitido por el componente AC subordinada, a través del protocolo OCSP, de acuerdo al estándar RFC6960. • Las respuestas OCSP emitidas están firmadas con la clave privada correspondiente al certificado de firma de respuestas OCSP del componente AV. • Emisión de respuestas OCSP que contienen el estado de revocación de los certificados solicitados, conforme al estándar RFC6960. • Acceso a información de revocación de base de datos de la Autoridad de Certificación y CRL en LDAP, Web, SAMBA • Sin costo de licencias referente al uso de servicio OCSP por número de usuarios • Sincronización del reloj del sistema vía NTP • Administración basada en web seguro (HTTPS) con requerimiento de certificado operador

“Tributar es Progresar”





	<ul style="list-style-type: none"> • Administración basada en web seguro (HTTPS) con requerimiento de certificado operador • Acceso a usuarios finales a través de HTTP-HTTPS Capacidad de publicar certificados y CRL en LDAP, Web, SAMBA 	<ul style="list-style-type: none"> • Las partes no modificadas se mantienen inalterables.
--	--	--

Lote 13: Sistema ERP

Se debe agregar como modificación a la especificación en el lote 13, como un nuevo apartado "Requerimientos del Proveedor."

Requerimientos del Proveedor	
Experiencia	<p>Experiencia en implementación de sistemas mayor o igual a 5 años.</p> <p>La experiencia en implementaciones de magnitud y características similares en instituciones públicas o privadas de la región.</p> <p>Experiencia en la adaptación e implantación de software en proyectos de Sistemas (preferiblemente en sistemas Administrativos o Talento Humano) para lo cual deberá proveer referencia de clientes sobre proyectos concluidos a satisfacción.</p>
Certificado	<p>Experiencia en implementación de sistemas mayor o igual a 3 años.</p> <p>El oferente deberá de acreditar mediante certificado emitido por el fabricante que es partner del software en la región con una antigüedad mayor o igual a 5 años, en el caso de software "in-House" debe acreditar mediante declaración jurada la implantación a satisfacción en 3 instituciones de la región, esta debe incluir teléfonos y nombre del contacto en la empresa para verificar la información.</p> <p>El oferente deberá de aportar un certificado por el fabricante que el software tendrá sostenibilidad por 5 años en el cual tendrá acceso a nuevas versiones, actualizaciones, etc.</p>
Personal	<p>Profesionales con experiencia no menor de 3 años demostrada en proyectos de magnitud y características similares al de esta contratación.</p> <p>El personal asignado para el proyecto de implantación deberá acreditar su experiencia en desarrollo e instalación del software ofertado.</p>

"Tributar es Progresar"





AGREGAR NUEVO LOTE 14

LOTE 14: Licencias especializadas

En el Ítem 14.1 Fire Power.

Actualmente se lee en el Lote 8 ítem 8.3 como:

Descripción	Original	Modificación
Software requerido	Fire Power L-ASA5525-TAM-3Y GPL	Fire Power L-ASA5525-TAMC-3Y
Tipo de Plan	Producto.	Se mantiene sin cambio
Plan	Licencia.	Se mantiene sin cambio
Cantidad de suscripciones	4	Se mantiene sin cambio
Beneficiario directo	Servicio de Administración de Rentas – Honduras Centro América: Entrega a la Dirección Nacional de Tecnologías, Edificio Gabriel A. Mejía, Segundo Piso, Tegucigalpa, Honduras.	Se mantiene sin cambio
Características de esta versión:	Servicio de IPS y protección avanzada de Malware.	Servicio de IPS + protección avanzada de Malware + URL Filtering
Discos SSD		8 unidades, para ser instalados 2 por cada equipo
Compatibilidad		Los SSD deberán ser 100% compatibles con los ASA5525X
Plazo de suscripción	3 años a partir de la fecha de implementación.	

Ítem 14.2. Licencias de Servidor Virtual Para Autenticación Y Administración de Equipos de Telecomunicaciones.

Licencias de Servidor Virtual para autenticación y administración de equipos de telecomunicaciones (ISE)		
Licencia Servidor Virtual	Características	Compatibilidad con VMWare 5.5, 6.0 y 6.5 Compatibilidad con la Infraestructura de Telecomunicaciones del SAR
	Cantidad	Una Licencia de Servidor Virtual.
	Tiempo de Licenciamiento.	Perpetua.
Licencias de	Características	habilitados los protocolos RADIUS, TACACS+, 802.1x Capacidad de Administrar Routers y Switches, WLC

“Tributar es Progresar”



Administración		Habilitada la Autorización, Autenticación y Contabilización
		El licenciamiento deberá incluir: 1. Licenciamiento de máquina virtual, 2. TACACS, 3. Capacidad de Administración de 1000 equipos.
	Tiempo de Licenciamiento.	Perpetua.

3. Modificar la Parte III. Sección IX. Condiciones Especiales del Contrato, la cual a partir de la presente Enmienda los Lotes e ítems modificados DEBERÁN LEERSE:

GCC 16.1	CGC 16.1 - La forma y condiciones de pago al Proveedor en virtud del Contrato serán las siguientes: <u>Pago de bienes importados:</u> El pago de la parte en moneda extranjera se efectuará en US\$ Dólares de los Estados Unidos de América. Se adiciona el Lote No. 14	
	Número de Lote	Forma de Pago (porcentajes del valor del contrato).
	14	Pago único del 100% a la entrega final

Las partes no modificadas mediante esta enmienda se mantienen inalterables, la presente pasa a formar parte integral del Documento de Licitación.

Tegucigalpa, M. D. C., 28 de agosto de 2017.

Lic. Linda Reyes
Coordinadora General

Unidad Coordinadora de Proyectos BID



“Tributar es Progresar”