MINISTERIO DE SALUD PÚBLICA

DIRECCION GENERAL DE SECRETARIA
Departamento de Compras y Suministros
Avda. 18 de Julio 1892 – 3° PISO ANEXO B
Tel. 1934 INTERNO 2011 AL 2016

LICITACION ABREVIADA: 37/2018
APERTURA ELECTRONICA:
Hora: 08/04/2019

EL MINISTERIO DE SALUD PÚBLICA LLAMA A LICITACION ABREVIADA PARA LA COMPRA DE SOLUCIÓN DE SEGURIDAD INFORMÁTICA INTEGRAL

Tabla de contenido

1 OBJETO DEL LLAMADO

Adquisición de una solución de Seguridad Informática Integral para el MSP.
Se prevé adquirir dos lotes con sus respectivos ítems, los cuales se describen a continuación:

Lote	Ítem	Descripción
A	1	Adquisición 2 firewall UTM
	2	Capacitación, instalación y configuración
	3	Paquete de hasta 200 horas para migración de las reglas
B	1	Adquisición de hasta 14 licencias NSX-V advanced
	2	Capacitación, instalación y configuración
	3	Paquete de hasta 200 horas para migración de las reglas

2 DESCRIPCIÓN DETALLADA

2.1 Lote A

2.1.1 Ítem 1 - Adquisición 2 firewall UTM

La solución debe contemplar la existencia de dos Firewalls, uno por cada datacenter (Casco Central y Pando), los mismos deben contar con las siguientes características funcionales:

Debe contar con la función de UTM (Unified threat management) con el fin de controlar los siguientes aspectos del tráfico hacia y desde internet: antivirus, anti-spyware, anti-spam, intrusión, detección y prevención, content filtering.

Debe existir la posibilidad de integrar la solución de Firewall con el Active Directory (Windows Server 2012 r2) con que cuenta el Ministerio de tal manera de poder generar reglas de salida identificando únicamente el usuario del domino que puede realizar la conexión.

La solución deberá incluir un sistema de monitoreo que permita consultar información en tiempo real del comportamiento de los activos de comunicación, debe incluir al menos alertas de CPU, Memoria y cantidad de conexiones.
También debe contar con la capacidad de realizar un monitoreo WAN del estado de las publicaciones, y si corresponde, el envío de alertas.
Es importante que la solución también admita la posibilidad de ser monitoreado en caso de caída.

(Actualmente el MSP cuenta con la solución de monitoreo PRTG)
Los Firewalls deben contar con la posibilidad de ser administrados con una herramienta que permita la gestión centralizada de las tareas.
También debe contar con una solución de logs e informes centralizados para los Firewalls externos. Esta solución deberá poder presentar información rápida al operador para troubleshooting de incidentes e identificación temprana de problemas.
Por último, deberá permitir identificar picos de consumo y conexiones, así como también los respectivos usuarios que las están generando.

Proveer un procedimiento automatizado que respalde periódicamente la configuración del equipamiento involucrado (cortafuego, IPS, etc.) y la almacene en un repositorio, de forma de contar con los respaldos necesarios en caso de una contingencia. Este procedimiento debe ejecutarse sin intervención del usuario administrador, pero debe también poder ejecutarse a demanda mediante un ejecutable, script o similar.

Las características técnicas se encuentran en el Anexo 13.3

2.1.2 Ítem 2: Capacitación, instalación y configuración

Se deberá presentar un plan de capacitación que cubra todos los aspectos de la solución de forma tal que asegure al MSP su correcta administración y operación.
Se debe prever la capacitación como primera tarea del proyecto para un máximo de 8 técnicos.

El nivel de la capacitación será evaluado por personal técnico del Área TIC y de considerarse Insatisfactorio, el mismo deberá ser repetido sin costo parcial o completamente de acuerdo a la evaluación.

La configuración del sistema y su instalación será de responsabilidad del contratista, quien deberá acordar el diseño y plan de acción con el personal técnico del MSP.
Será responsabilidad del contratista la documentación completa de la configuración realizada.

La configuración de Los firewall debe contar con alta disponibilidad a nivel de solución ante la caída de un Firewall. Esto no necesariamente implica tener replicados los Firewall. Si bien replicar los Firewall es una opción válida se valorara una solución/arquitectura que soporte la caída de uno de los Firewalls sin necesidad de poner dos en cada uno de los puntos críticos.
Es importante destacar que la solución de alta disponibilidad debe ejecutarse de manera automática.
La alta disponibilidad debe configurarse en modo activo – activo de forma tal que ambos equipos deben atender los requerimientos (request) de las publicaciones del MSP.

2.1.3 Ítem 3 - Paquete de hasta 200 horas para migración de las reglas de firewall

Es necesario realizar una re-arquitectura de reglas de firewall de la solución actual a la nueva solución. Esto no solo comprende la división natural que surge del cambio de arquitectura que se realiza al pasar de tener un solo Firewall a una nueva solución con dos equipos, sino que también se debe realizar una revisión completa de las reglas actuales a los efectos de verificar su utilidad, dejando únicamente aquellas que correspondan a la nueva situación.

Por lo señalado, esta tarea NO puede ser realizada exclusivamente por una herramienta automática, sino que debe realizarse un análisis de cada caso.

2.2 Lote B

2.2.1 Ítem 1 - Adquisición de hasta 14 licencias NSX-V advanced

Adquisición de hasta 14 licencias NSX-V advanced para complementar nuestro actual ambiente de virtualización.

2.2.2 Ítem 2 - Capacitación, instalación y configuración

Se deberá presentar un plan de capacitación que cubra todos los aspectos de la solución de forma tal que asegure al MSP su correcta administración y operación.
Se debe prever la capacitación como primera tarea del proyecto para un máximo de 8 técnicos.

El nivel de la capacitación será evaluado por personal técnico del Área TIC y de considerarse Insatisfactorio, el mismo deberá ser repetido sin costo parcial o completamente de acuerdo a la evaluación.

La configuración del sistema y su instalación será de responsabilidad del contratista, quien deberá acordar el diseño y plan de acción con el personal técnico del MSP.
Será responsabilidad del contratista la documentación completa de la configuración realizada.

2.2.3 Ítem 3 - Paquete de hasta 200 horas para migración de las reglas

Valen las mismas consideraciones que para el punto 2.1.3, teniendo en cuenta que en este caso se migrarán las reglas que aplican a la red interna.

3 OFERTAS, COMUNICACIONES, PRORROGAS:

3.1 Jurisdicción competente

Por el sólo hecho de presentarse, se entenderá que el oferente hace expreso reconocimiento y manifiesta su voluntad de someterse a las Leyes y Tribunales de la República Oriental del Uruguay.

3.2 Aclaraciones:

Las solicitudes de aclaración podrán ser formuladas por los adquirentes del Pliego Particular mediante comunicación escrita dentro del plazo de 96 horas antes de la apertura, vía mail a: @msp.gub.uy.

Las consultas deberán ser específicas y deberán ser respondidas por la Administración dentro del plazo de 48 hs posteriores a su realización, comunicando las mismas a todos los interesados a través de su publicación en el sitio web de Compras y Contrataciones Estatales (www.comprasestatales.gub.uy)

3.3 Modificación del Pliego Particular

La Administración podrá, antes que venza el plazo para la apertura del llamado, modificar el Pliego Particular ya sea por iniciativa propia o en atención a una consulta u observación formulada por un particular.

Todos los interesados serán notificados de las modificaciones introducidas, en un plazo de 72 hs. antes del término límite para la recepción de las ofertas, vía mail al interesado que formuló la observación y comunicado a los demás interesados a través del sitio web de Compras y Contrataciones Estatales.

3.4 Prorrogas

Cualquier proveedor podrá solicitar prórroga de la Apertura de Ofertas. La misma se presentará personalmente en el Departamento de Compras y Suministros o vía mail a ctejeira@msp.gub.uy Dicha solicitud deberá realizarse hasta 5 días antes del Acto de Apertura fijado para el llamado. Esta

solicitud deberá estar acompañada del recibo de pago del pliego particular de condiciones.

La prórroga será resuelta por la Administración según su exclusivo criterio, comunicando la misma a todos los interesados a través de su publicación en el sitio web de Compras y Contrataciones Estatales.
A efectos de su notificación los oferentes deberán consignar su domicilio actual con todos los datos necesarios para su ubicación.
La comunicación del cambio de domicilio deberá cumplirse mediante escrito presentado en el Departamento de Adquisiciones para ser anexado al expediente de la Licitación y tendrá efecto a partir del día hábil inmediato siguiente a su recepción.

3.5 Presentación de las Ofertas

Las propuestas serán recibidas únicamente en línea. Los oferentes deberán ingresar sus ofertas (económica y técnica completas) en el sitio web www.comprasestatales.gub.uy.
No se recibirán ofertas por otra vía.
La documentación electrónica adjunta de la oferta se ingresará en archivos con formato (.pdf), sin contraseñas ni bloqueos para su impresión o copiado.
Cuando el oferente deba agregar en su oferta un documento o certificado cuyo original solo exista en soporte papel, deberá digitalizar el mismo (escanearlo) y subirlo con el resto de su oferta. En caso de resultar adjudicatario, deberá exhibir el documento o certificado original, conforme a lo establecido en el artículo 48 del TOCAF.

El formulario de identificación del oferente debe estar firmado por el titular, o representante con facultades suficientes para ese acto. En tal caso, la representación debe estar debidamente respaldada en el Registro Único de Proveedores del Estado (RUPE) con los datos de representantes y documentación de poderes ingresados y al menos verificados en el sistema.
Incluir información sobre presentación de garantías o muestras si corresponde.
Las ofertas deberán presentarse redactadas en forma clara y precisa, en idioma español y conforme a lo dispuesto en el Art. 63 del TOCAF.

Las ofertas deberán estar debidamente firmadas por el titular de la empresa y/o representante según contrato o estatuto.

Deberá cotizarse en Moneda Nacional, debiéndose incluir en el precio, el Impuesto al Valor Agregado (IVA). En el caso que esta información no surja de la propuesta, se considerará que el precio cotizado comprende dicho impuesto.

Si en la oferta hubiera discrepancia entre los precios unitarios y los totales, valdrá lo establecido en los precios unitarios.

Cuando exista diferencia entre la cantidad escrita en números y letras, valdrá la escrita en letras.
Las ofertas deberán ser presentadas en el formato establecido en los anexos (I) y (II) de este pliego particular.

3.6 Información confidencial y datos personales

Cuando los oferentes incluyan información considerada confidencial, al amparo de lo dispuesto en el artículo 10 literal I) de la Ley N° 18.381 y artículo 12.2 del Decreto Nº 131/014, la misma deberá ser ingresada en el sistema en tal carácter y en forma separada a la parte pública de la oferta.
La clasificación de la documentación en carácter de confidencial es de exclusiva responsabilidad del proveedor. La Administración podrá descalificar la oferta o tomar las medidas que estime pertinentes, si considera que la información ingresada en carácter confidencial, no reúne los requisitos exigidos por la normativa referida.

El oferente deberá realizar la clasificación en base a los siguientes criterios:

Solo se considera información confidencial:

- La información relativa a sus clientes,
- La que pueda ser objeto de propiedad intelectual
- La que refiera al patrimonio del oferente,
- La que comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos al oferente, que pudiera ser útil para un competidor,
- La que esté amparada en una cláusula contractual de confidencialidad,
- Aquella de naturaleza similar conforme a lo dispuesto en la Ley de Acceso a la Información (Ley Nº 18.381), y demás normas concordantes y complementarias.

En ningún caso se considera información confidencial:

La relativa a los precios, la descripción de bienes y servicios ofertados, y las condiciones generales de la oferta.

Los documentos que entregue un oferente en carácter confidencial, no serán divulgados a los restantes oferentes.

El oferente deberá incluir en la parte pública de la oferta un resumen no confidencial de la información confidencial que ingrese que deberá ser breve y conciso (artículo 30 del Decreto N° 232/010).

En caso que las ofertas contengan datos personales, el oferente, si correspondiere, deberá recabar el consentimiento de los titulares de los mismos, conforme a lo establecido en la Ley Nº 18.331, normas

concordantes y complementarias. Asimismo se deberá informar a quienes se incluyen en el presente llamado, en los términos establecidos en el artículo 13 de la mencionada Ley.

3.7 Apertura de las ofertas

En la fecha y hora indicada se efectuará la apertura de ofertas en forma automática y el acta de apertura será publicada automáticamente en el sitio web www.comprasestatales.gub.uy. Simultáneamente se remitirá a la dirección electrónica previamente registrada por cada oferente en el Registro Único de Proveedores del Estado (RUPE), la comunicación de publicación del acta. Será de responsabilidad de cada oferente asegurarse de que la dirección electrónica constituida sea correcta, válida y apta para la recepción de este tipo de mensajes. La no recepción del mensaje no será obstáculo para el acceso por parte del proveedor a la información de la apertura en el sitio Web: www.comprasestatales.gub.uy.

A partir de ese momento, las ofertas quedarán accesibles para la administración contratante y para el Tribunal de Cuentas, no pudiendo introducirse modificación alguna en las propuestas.

Asimismo, las ofertas quedarán disponibles para todos los oferentes, con excepción de aquella información ingresada con carácter confidencial.
Solo cuando la administración contratante solicite salvar defectos, carencias formales o errores evidentes o de escasa importancia de acuerdo a lo establecido en el artículo 65 del TOCAF, el oferente deberá agregar en línea la documentación solicitada.

Los oferentes podrán hacer observaciones respecto de las ofertas dentro de un plazo de 2 (dos) días hábiles a contar del día siguiente a la fecha de apertura.

Dichas observaciones deberán ser cursadas a través de la dirección de correo detallada par contacto en el presente pliego (ctejeira@msp.gub.uy). Dichas observaciones serán comunicadas por el MSP (vía mail), a todos los oferentes para su conocimiento.

4 CRITERIOS DE EVALUACION DE LAS OFERTAS

Las ofertas serán válidas y obligarán al oferente por el término de 120 (ciento veinte) días, vencido dicho plazo se considerarán prorrogadas, salvo manifestación expresa en contrario.

La admisión inicial de una propuesta no será obstáculo a su rechazo si se constataren luego defectos que violen los requisitos legales o aquellos sustanciales contenidos en el Pliego.

Se considerarán apartamientos sustanciales aquellos que no pueden subsanarse sin alterar

materialmente la igualdad de los oferentes.

Se evaluarán las ofertas desde el punto de vista jurídico-formal, técnico y económico, pudiendo el MSP rechazar aquellas que no se ajusten a los requerimientos y especificaciones sustanciales descritas en el presente Pliego.

El MSP se reserva el derecho de determinar a su exclusivo juicio y en forma definitiva si el oferente posee la capacidad técnica y financiera para realizar el suministro y prestación de productos y servicios requeridos en la presente licitación.
El MSP se reserva el derecho de considerar, a su exclusivo criterio, ofertas que contengan apartamientos menores o no sustanciales con respecto a lo indicado en este Pliego y conforme a lo dispuesto en el TOCAF.

El Organismo se reserva el derecho de realizar por su cuenta las averiguaciones pertinentes a fin de constatar la veracidad de la información presentada en la oferta, así como las consultas pertinentes al oferente.

4.1 Evaluación Técnica y Económica

La evaluación de las ofertas que superen la revisión formal y el juicio de admisibilidad, se realizará en dos etapas:

1. evalución técnica que tendrá un factor de ponderación del 70% de acuerdo a lo especificado en el punto 4.2
2. evaluación económica que tendrá un factor de ponderación del 30% exclusivamente para aquellas ofertas que hayan superado el mínimo requerido en la evalación técnica.

Se describe a continuación la fórmula a utilizar para la evaluación total (E) de las ofertas:

$$E \equiv \frac{C\,\mathbf{bajo}}{C} X \;+\; \frac{T}{T\,\mathbf{alto}}(1-X)$$

Dónde:

C=	Precio evaluado de la oferta.
C bajo =	El precio más bajo de todos los evaluados de ofertas que se ajusten a lo exigido en el presente pliego.
T =	Puntaje técnico total asignado a la oferta.
T alto =	El puntaje técnico más alto otorgado a ofertas que se ajusten a lo exigido en el presente pliego.
X =	Porcentaje de ponderación del precio.

En caso de que el resultado de T y/o C tenga decimales, se aplica el siguiente criterio: si el valor del primer decimal es 5 o más, aumenta el valor del último número en 1.

4.2 Criterios de Evaluación Técnica

Se exponen a continuación los criterios con los que se evaluará técnicamente:

Criterios	Factores	Subfactores	Criterio para mínimo	PUNTAJE	
				Mínimo	**Máximo**
Antecedentes de la empresa	Antigüedad en el ramo objeto de la contratación		3 años de operativa - Se certifica con documentación de estatutos o BPS	1	10
	Experiencia en el objeto de la contratación	Experiencia en Servicios similares en los últimos 5 años en empresas del Sector Público, Sector Salud, Sector Financiero. * No se acumulan factores.	3 Referencias	3	20
		Experiencia en servicios similares en otros sectores de actividad.		0	5
	Certificaciones en Calidad o vinculadas al objeto de la Licitación		Puntaje máximo lo obtendrá empresa con mayor número de certificaciones y el resto se prorrateará en consonancia	1	5
					40
Evaluación Técnica de la Solución	Abordaje y comprensión de la naturaleza y alcance de la solución, aspectos técnicos y funcionales, tomándose asimismo en cuenta el grado de detalle, completitud, pertinencia, justificación y adecuación de cada uno de los aspectos del Servicio propuesto		Solución cuenta con capacidad de Hardware, posibilidades de escalabilidad y disponibilidad.	10	20
	Respuesta a Requerimientos y Plan de Proyecto, Plan de Trabajo		Descripción de tareas, plazos, responsables, plan de	5	10

	General y Planes de Trabajo dependientes, Plan de Capacitación, Plan de Riesgos y Contingencias, Gestión de Proyecto, metodología y herramientas propuestas, plazos contenidos en la propuesta y su adecuación para cumplir con los objetivos del Proyecto.		riesgos.		
Total Solución Técnica					**30**
Equipo propuesto		Jefe de Servicio		5	10
		Personal Asignado a la tarea	2 Técnicos	10	20
Total Equipo					**30**
				70	**100**

Jefe de Servicio

CRITERIOS	Factores	Criterio para mínimo	PUNTAJE	
			Mínimo	**Máximo**
Formación Académica	Titulación Carreras Informáticas de Grado 4 años de duración mínima, valorándose estudios de postgrado y master	Título de 4 años	5	20
	Cursos vinculados al Rol mínimo 20 horas			10
Experiencia	Años de recibido título de Grado	1 año	1	10
	Proyectos en el Rol en proyectos similares últimos 10 años	2 Proyectos		40
	Proyectos en otro Rol en proyectos similares últimos 20 años	1 Proyecto		20
			60	**100**

Técnicos

CRITERIOS	Factores	Criterio para mínimo	PUNTAJE	
			Mínimo	**Máximo**
Formación Académica	Titulación Carreras Informáticas de 3 años de duración mínima, valorándose estudios de grado, y superior.	Título de 3 años	5	10
	Cursos vinculados al Rol mínimo 20 horas			10
	Certificaciones en los productos o servicios ofertados	1		20
Experiencia	Años de experiencia en la implantación de soluciones similares	1 año	1	10
	Proyectos similares en el Rol en los últimos 10 años	2 Proyectos		40
			60	**100**

La evaluación de los puntajes de cada ítem se realizará en base a la documentación suministrada en la oferta y eventualmente la que el MSP obtenga de otras fuentes, en caso que lo entienda conveniente.

El criterio para otorgar el máximo puntaje a un ítem es el siguiente:

El puntaje es de 100 por Perfil y se convertirá a un máximo de 10 puntos al perfil de la tabla general.

La oferta más valorada obtiene el mayor puntaje, las ofertas restantes se ponderan proporcionalmente.

Sólo serán tenidas en cuenta para la evaluación económica aquellas ofertas que superen el mínimo en cada ítem que así lo requiera en la tabla anterior.

5 ADJUDICACION

El MSP podrá desistir del llamado en cualquier etapa de su realización o podrá desestimar todas las ofertas. Ninguna de estas decisiones generará derecho alguno de los oferentes a reclamar por gastos, honorarios o indemnizaciones por daños y perjuicios.

Las ofertas serán estudiadas por una Comisión Asesora de Adjudicaciones, a la que le compete informar fundadamente acerca de la admisibilidad y conveniencia de las ofertas.

A los efectos de producir su informe la Comisión Asesora de Adjudicaciones podrá solicitar a cualquier oferente las aclaraciones necesarias, no pudiendo pedir ni permitir que se modifique el contenido de la oferta.

Si los precios de la o las ofertas recibidas son considerados manifiestamente inconvenientes, el ordenador o en su caso la Comisión Asesora de Adjudicaciones debidamente autorizada por éste, podrá solicitar directamente mejoras en sus condiciones técnicas, de precio, plazo o calidad.

El dictamen de la Comisión Asesora de Adjudicaciones no generará ningún derecho a favor de los oferentes.

En caso de que se presentaran ofertas similares el MSP se reserva el derecho de entablar negociaciones reservadas y/o paralelas con aquellos oferentes que precalifiquen a tal efecto, a fin de obtener mejores condiciones técnicas, de calidad o precio, de acuerdo a lo establecido en el Art. 66 del TOCAF.

Asimismo el MSP podrá realizar negociaciones tendientes a la mejora de oferta en los casos de precios manifiestamente inconvenientes.
El MSP se reserva el derecho de adjudicar la totalidad o parte de los ítems cotizados, según sus intereses.

La adjudicación podrá ser total o parcial por ítem.

El MSP podrá rescindir el contrato por incumplimiento total o parcial del adjudicatario, debiendo notificar al adjudicatario la decisión.

Se verificará en el RUPE la inscripción de los oferentes en dicho Registro, así como la información que sobre el mismo se encuentre registrada, la ausencia de elementos que inhiban su contratación y la existencia de sanciones según corresponda.

A efectos de la adjudicación, el oferente que resulte seleccionado, deberá haber adquirido el estado de “ACTIVO” en el RUPE, tal como surge de la Guía para Proveedores del RUPE, a la cual podrá accederse en www.comprasestatales.gub.uy bajo el menú Proveedores/RUPE/Manuales y videos.

Si al momento de la adjudicación, el proveedor que resulte adjudicatario no hubiese adquirido el estado de “ACTIVO” en RUPE, se le otorgará un plazo de 2 días hábiles contados a partir del día siguiente a la notificación de la adjudicación, a fin de que el mismo adquiera dicho estado, bajo apercibimiento de adjudicar este llamado al siguiente mejor oferente en caso de no cumplirse este requerimiento en el plazo mencionado.-

6 GARANTÍA DE LOS EQUIPOS

Durante el plazo de garantía, el adjudicatario deberá en caso de daños producidos durante la operación y a consecuencia de vicios de fabricación, solucionar la misma en un plazo máximo de 3 (tres) días hábiles a partir de la comunicación (ya sea reparación o reemplazo de equipo).

Para los ítems 1 y 3 la garantía mínima exigida es de 3 años on-site.

El adjudicatario deberá comunicar los datos correspondientes al servicio técnico, el cual deberá recepcionar consultas o reportes de problemas, al menos de 9:00 a 18:00 horas, de lunes a viernes.
El proveedor deberá especificar los mecanismos de contacto para este fin.
Todos los gastos de reparación, transporte, ensayos, etc., son a cargo del oferente.

7 ENTREGA

La entrega deberá realizarse en un plazo máximo de 45 días. Dicho plazo se contará desde el día posterior a la recepción de la orden de compra correspondiente emitida por el Departamento de Compras y Suministros (notificación firme).

La entrega deberá realizarse en la Avda. 18 de Julio 1892 (MSP), 3er. piso Anexo A – Área Gobierno Electrónico, en coordinación con el personal designado a tales efectos.

8 PLAZOS

Los plazos establecidos en el presente pliego, se computan en días hábiles, no se computará el día de la notificación.

9 FORMA DE PAGO

Crédito SIIF, a los 60 (sesenta) días de ingresadas las facturas debidamente conformadas por el Área Gobierno Electrónico.-
No se aceptarán facturas que consignen el cobro de recargos por incumplimiento en el pago de las mismas.-

10 MULTAS

La falta de cumplimiento de cualquiera de las obligaciones asumidas por parte del proveedor dará derecho al MSP a proceder a la aplicación de las siguientes sanciones, pudiendo darse en forma conjunta:

- Eliminación del Registro de Proveedores del MSP.
- Registro del incumplimiento en el Registro Único de Proveedores del Estado.
- Eliminación del Registro Único de Proveedores del Estado.
- Demanda por daños y perjuicios.
- Publicaciones en prensa indicando el incumplimiento.

El adjudicatario incurrirá en mora de pleno derecho sin necesidad de interpelación judicial o extrajudicial alguna por el sólo vencimiento de los términos o por hacer algo contrario a lo estipulado.

El adjudicatario, podrá ser pasible de la siguiente multa:

Para el caso de incumplimiento del plazo acordado para la entrega de los ítems adjudicados, se aplicará al adjudicatario una multa diaria equivalente al 1% (uno por ciento) del monto total, IVA incluido, de cada ítem no entregado en plazo.
Todas las multas serán descontadas del monto de las facturas pendientes hasta un máximo del 30% (treinta por ciento) del monto total adjudicado, IVA incluido, o pudiéndose abonar las mismas con el suministro de insumos cotizados por el proveedor en su oferta, de acuerdo a las necesidades del MSP.

11 NORMAS QUE REGULAN EL PRESENTE LLAMADO

- Apertura electrónica: Decreto Nº275/013 de 3 de setiembre de 2013.
- TOCAF: Decreto Nº 150/012 de 11 de junio de 2012, modificativas y concordantes.
- Acceso a la información pública: Ley N° 18.381 de 17 de octubre de 2008, modificativa Ley Nº 19.178 de 27 de diciembre de 2013.
- Decreto reglamentario de la Ley 18.381: Decreto Nº 232/010 de 2 de agosto de 2010.
- Protección de datos personales y acción de habeas data: Ley Nº 18.331 de 11 de agosto de 2008.
- Decreto reglamentario de la Ley 18.331: Decreto Nº 414/009 de 31 de agosto de 2009.
- Pliego único de bases y condiciones generales para contratos de suministros y servicios no personales: Decreto Nº 131/014 de 19 de mayo de 2014.
- Anexo (I) Costos de insumos del equipamiento ofertado para los ítems 1, 2, 3, 4 y 5.
- Anexo (II) Recomendaciones sobre la oferta en línea.

12 VALOR DEL PLIEGO

El valor del Pliego es de $ 2.000 (pesos uruguayos dos mil).-

Deberá ser abonado en el Departamento de Tesorería del Ministerio de Salud Pública, 18 de Julio 1892, 3er. Piso, oficina 319, en el horario de 9 a 15 horas.-

13 ANEXOS

13.1 Formulario Identificación del Oferente

Llamado Nº - Generación e Implantación de Solución Informática para gestionar cambio de Prestador Integral de Salud

Razón Social de la Empresa: _____

Nombre Comercial de la Empresa: _____

R. U. T.: _____

Fecha de inicio de operaciones en Uruguay _____

Domicilio a los efectos de la presente Consulta:

Correo electrónico: _____

Correo electrónico alternativo: _____

Calle: _____

Localidad: _____

Teléfono: _____ Fax: _____

Socios o Integrantes del Directorio de la Empresa:

Nombre:	**Documento:**	**Cargo:**
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Declaro estar en condiciones legales de contratar con el Estado.

FIRMA/S: _____

Aclaración de firmas: _____

13.2 Formato Resumen Integrante del Equipo

Cargo		Candidato □Principal □Alterno
Información del Candidato	Nombre del Candidato	Fecha de Nacimiento
Calificaciones Profesionales:		
Empleo actual	Nombre del Empleador	
	Dirección del Empleador:	
	Teléfono	Contacto (gerente / funcionario de personal)
	Cargo del candidato	Años con el empleador actual

Resuma la experiencia profesional de los últimos cinco años, en orden cronológico inverso. Indique la experiencia particular pertinente para este proyecto.

Desde	Hasta	Empresa/Proyecto/Cargo/Experiencia pertinente

13.3 Especificaciones Técnicas de los Firewall

Requerimiento/Característica/Funcionalidad

- Soporte para 2000 nuevas sesiones concurrentes por segundo.
- Soportepara800usuariosconcurrentesyconcapacidaddeampliaciónde 25%. Con un factor de 150 sesiones por usuario mínimo.
- Notificación de ataques o bloqueos por correo, consola y snmp.
- Alta disponibilidad - Es aceptable la perdida de sesiones y reconexión automática
- Disponibilidad de fail-over/redundancy. No necesario clúster, la solución debe poder implementar el failover de la manera que se considere
- Configuración activo-activo - NO NECESARIAMENTE CLUSTER
- Se valorara - Fuentes de alimentación redundante, hot swap y con configuración para máxima capacidad de procesamiento.
- La reinstalación de SO/firmware o actualizaciones de SW o HW no deberá generar indisponibilidad en la solución.
- Autenticación de usuarios y perfiles de acceso mediante AD.

Firewall

- Número de políticas permitidas no inferior a 2000
- Protocolos VPN: IPSecySSL; PPTPvalorado. Considerar para la implementación la configuración de: XX IPSec y XX Clientes SSL
- Soporte no menos de 300 sesiones concurrentes en cualquiera de las tecnologías de VPN.
- IPSec compatible con Cisco.
- Soporte a certificados PKI X.509 para construcción de VPNs SSL.
- VPN SSL con soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. Y Soporte para escritorio virtual con acceso a medios extraíbles, recursos compartidos, impresión, restricción de aplicaciones de acceso, etcétera.
- Funcionalidad de DHCP: Cliente DHCP, Servidor DHCP y Relay DHCP.
- Protocolos de ruteo: RIP V1 y V2, OSPF, BGP, etcétera.
- Throughput cortafuegos no inferior a 16Gbps
- Se deben poder operar como mínimo 100 interfaces virtuales (VLAN's).
- Stateful Packet Inspection, para la totalidad de los usuarios
- Monitor en tiempo real de ancho de banda.

IPS para la totalidad de los usuarios

- Protección contra denegación de servicio.
- Análisis por decodificación de protocolos.
- Stateful pattern matching.
- Detección de anomalías de protocolos.
- Análisis basado en heurística y/o firmas.
- Detección de anomalías por estadísticas.
- Desfragmentación IP y reconstrucción de tráfico TCP.
- Bloqueo de paquetes inválidos y mal formados.
- Actualización automática de firmas.
- Protección contra ataques a servicios como ser: smtp, imap, pop,
- telnent, ftp, rlogin, ssh, icmp, dns, rpc, netbios, etcétera.
- Throughput IPS mínimo de 4Gbps.

Antivirus y Antispam para navegación y correo.

- Antivirus modo proxy y en tiempo real.
- Inspeccionar y detectar virus en tráfico IPv6.
- Detección y detención de tráfico spyware, adware, malware/grayware, etcétera.
- Inspección de mensajería instantánea.
- Filtrado de archivos por extensión y tipo
- Actualización de firmas en línea
- Escaneo heurístico

Antispam - Se valorara

- Detección mediante palabras y ausencia/presencia de combinaciones de palabras en cuerpo de correo.
- Definición de listas blancas y negras
- Detección mediante IP de emisor, URL dentro del mensaje, checksum, etcétera.
- Rechazo o etiquetado (con motivo en encabezado mime) de mensajes spam.
- Prevención contra phishing
- Listas negras de DNS
- Reglas heurísticas globales dinámicas
- Filtrado bayesiano
- Funcionamiento modo relay o transparente
- Bloqueo de correos por umbrales de cuentas de usuario o destino

Filtrado de URL y tráfico.

- Capacidad de realizar filtrados por categoría
- Definiciones de distintos perfiles de navegación por categoría de usuarios y grupos de usuarios definidos en LDAP y AD
- Capacidad de filtrado de scripts en páginas web (JAVA/Active X)
- Forzar búsquedas seguras con motores de búsqueda como google, yahoo o bing.
- Capacidad de filtrado de contenido en conexiones IPv6.
- Soporte para protocolos multimedia: SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP) y otros.
- Detección para P2P y programas : Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype, WinNY y otros.
- Inspección de encabezados VoIP

Administración

- Interfaz de administración full web con acceso por HTTPS
- Interfaz web compatible con navegadores Firefox o Chrome. No debe haber limitaciones de funcionalidades por componentes de la interfaz que no se ejecuten con los mencionados navegadores.
- Disponibilidad de línea de comando CLI vía web o ssh.
- Autenticación mediante usuario y password y/o certificados digitales.
- Definición de perfiles de administración.
- Soporte SNMPv2 y SNMPv3.

Reportes y Logging - Se valorara

- Solución centralizada para reportes y Logging con capacidad de ver actividad de aplicaciones, usuarios y amenazas.
- Capacidad de generar consultas mediante SQL o similar.
- Generación de gráficas predefinidas o customizadas.
- Capacidad de customizar reportes y definiciones de plantillas de reportes
- Envío a y captura de syslog de otros dispositivos de red que luego son interpretados mediante consultas customizadas. Aclarar que equipos de red pueden ser integrados sus logs.
- Exportar a CSV y/o otros formatos de texto.

Prevención de fuga de información (DLP)

- Análisis de archivos de ofimática incluyendo formatos planos de texto, MS Office, OpenDocument, pdf y archivos comprimidos.
- Escaneo de protocolos: http, pop3, smtp, imap, nntp, ftp y otros.
- Modalidad de bloqueo de usuario, ip o registro de eventos
- Copia de seguridad de archivo detectado

Control de Aplicaciones

- Identificar aplicaciones por inspección de tráfico e independiente de puertos y protocolo.
- Reconocer de una lista de no menos de 1000 aplicaciones y actualización automática de la lista.
- Para aplicaciones identificadas o desconocidas, modalidad de bloqueo, registro en log o permiso.