MINISTERIO DE HACIENDA SET SUBSECRETARIA DE ESTADO DE TRIBUTACION	INFORME DE EVALUACIÓN N° 30/2014
	LICITACIÓN PÚBLICA NACIONAL N° 09/2014 "ADQUISICIÓN DE EQUIPOS DE SEGURIDAD PARA EL DATACENTER DE LA SUBSECRETARÍA DE ESTADO DE TRIBUTACIÓN DEL MINISTERIO DE HACIENDA" ID N° 271.869.

000577

En la ciudad de Asunción, capital de la República del Paraguay, a los veinte y nueve días del mes de julio del año dos mil catorce, siendo las 16:00 horas se reúnen en la sala de reuniones del Departamento de Contrataciones dependiente de la Dirección de Apoyo y de Administración y Finanzas de la Subsecretaría de Estado de Tributación del Ministerio de Hacienda, los miembros del Comité de Evaluación conformado por Resolución DA N° 162, de fecha 20 de junio de 2014; y modificada por Resolución DA N° 279 de fecha 21 de agosto de 2014, para realizar la evaluación de ofertas correspondientes a la convocatoria de la Licitación Pública Nacional N° 09/2014, **"ADQUISICIÓN DE EQUIPOS DE SEGURIDAD PARA EL DATACENTER DE LA SUBSECRETARÍA DE ESTADO DE TRIBUTACIÓN DEL MINISTERIO DE HACIENDA"**.

Para tal efecto, se hallan presente los siguientes funcionarios:

Alberto Jara, en su carácter de representante del Departamento de Contrataciones.

Martha Riquelme Irún, Representante de la Coordinación Administrativa.

María Liz Caballero, Representante de la Coordinación Financiera.

Pedro R. Velázquez, Representante de la Dirección de TIC`s.

EL Departamento de Contrataciones, entregan los documentos, objeto de análisis, los cuales consisten en las siguientes:

a. Pliego de Bases y Condiciones.
b. Acta de Apertura de Sobres de fecha 25 de julio de 2014.
c. Ofertas de las empresas: TECHNOMA S.A.C.I. y LOGICALIS PARAGUAY S.A.

Antes de iniciar la evaluación de las ofertas todos los miembros del Comité firman la Declaración Jurada que no guardan parentesco cercano con el propietario de la empresa a ser evaluada.

Posteriormente se da lectura al Acta de Apertura de sobres, que en su parte pertinente se observa cuanto sigue:

1- *Se apertura la oferta del Proveedor:* ***TECHNOMA S.A.C.I,*** *el cual cotiza su oferta para el LOTE 1 por un monto total* ***G. 1.633.743.000 (Guaraníes Un mil seiscientos treinta y tres millones setecientos cuarenta y tres mil),***

realizado la verificación cuantitativa de las documentaciones de la oferta, se constata que la firma presenta todas las documentaciones de carácter sustancial, así también las de carácter formal.

2- *Se apertura la oferta del Proveedor:* ***LOGICALIS PARAGUAY S.A.,*** *el cual cotiza su oferta para los LOTES 2, 3 y 4 por un monto total* ***G. 1.560.000.000 (Guaraníes un mil quinientos sesenta millones),*** *realizado la verificación cuantitativa de las documentaciones de la oferta, se constata que la firma presenta todas las documentaciones de carácter sustancial, así también las de carácter formal.*

Seguidamente se verifican las ofertas y el cumplimiento de las documentaciones ***básicas de carácter sustancial***; y para ello hemos elaborado la planilla de comprobación, con la descripción de las documentaciones, el cual forma parte integral del presente Informe de Evaluación y es denominada **ANEXO 1**.

Tras la aplicación de los métodos de evaluación consagrados en el numeral 1 del Artículo 61 del Decreto N° 21909/03, se puede deducir que los Oferentes en concurso **CUMPLEN** con la presentación de las documentaciones básicas de carácter sustancial.

Conforme a las estipulaciones contenidas en el PBC y concordantes con el numeral 2 del Artículo 61 del Decreto N° 21.909/03, se procede a elaborar el **Cuadro Comparativo de Precios (ANEXO 2)**, ordenando de esta forma las mejores ofertas económicas, quedando posicionado con el precio más bajo las propuestas de las siguientes empresas:

Lotes	Descripción	Oferta Económica
Oferente: TECHNOMA S.A.C.I.		
1	Sistema de nueva generación de prevención de intrusos y sistema centralizado de defensa y administración de eventos	1.633.743.000.-
	Total de la oferta	**1.633.743.000-.**
Oferente: LOGICALIS PARAGUAY S.A.		
2	Provisión e implementación de solución de filtrado de contenido, seguridad de publicación Web y Acceso a	642.000.000.-

	Internet	
3	Provisión e implementación de Web Application Firewall	515.000.000.-
4	Provisión e implementación de solución de seguridad de la red anti-ddos	403.000.000.-
	Total de la Oferta	**1.560.000.000**

Continuando con los criterios de evaluación establecidos en el numeral 3 del Artículo 61 del Decreto 21.909/03, se toma en forma provisoria la oferta de las empresas TECHNOMA S.A.C.I. y LOGICALIS PARAGUAY S.A., los cuales serán objeto de análisis pormenorizado con los demás documentos y requisitos exigidos en el Pliego de Bases y Condiciones.

CRITERIOS TÉCNICOS

Además de la presentación de la documentación de carácter formal que avala el cumplimiento de los criterios técnicos, pasamos a efectuar el análisis en cuanto al cumplimiento de los requerimientos correspondiente a las especificaciones técnicas de los bienes ofertados.

A tal efecto, se han verificado los aspectos técnicos de las ofertas; es decir, se tomaron los criterios técnicos plasmados en el PBC, las planillas de especificaciones técnicas y los catálogos de los bienes propuestos por los oferentes. Para tal efecto se ha elaborado la planilla de comprobación denominada **Anexo 3**.

A continuación, se expresan en forma resumida por lotes el cumplimiento de los requerimientos técnicos:

Lotes	Descripción	Especificaciones Técnicas	Catálogos
Oferente: TECHNOMA S.A.C.I.			
1	Sistema de nueva generación de prevención de intrusos y sistema centralizado de defensa y administración de eventos	CUMPLE	CUMPLE
Oferente: LOGICALIS PARAGUAY S.A.			

2	Provisión e implementación de solución de filtrado de contenido, seguridad de publicación Web y Acceso a Internet	CUMPLE	CUMPLE
3	Provisión e implementación de Web application firewall	CUMPLE	CUMPLE
4	Provisión e implementación de solución de seguridad de la red anti-ddos	CUMPLE	CUMPLE

Al aplicar las verificaciones del cumplimiento de los equipos ofertados con las especificaciones técnicas establecidas en la SECCIÓN III del Pliego de Bases y Condiciones surgieron algunas dudas con respecto al alcance de los mismos; por lo cual, de acuerdo a la Cláusula IAO 28.1 de la Sección I – Datos de la Licitación (DDL), fueron requeridas a las firmas participantes las siguientes aclaraciones, las cuales fueron trasladadas a los oferentes a través del Departamento de Contrataciones.

Conforme a la Nota DA/COC Nº 469/2014, fue peticionada a la empresa Technoma S.A.C.I., la presentación de los catálogos correspondiente al Lote 1, y la descripción del modelo ofertado. En tiempo y forma fue presentado los recaudos solicitados por el Oferente Technoma S.A.C.I.

A través de la Nota DA/COC Nº 470/2014, fue solicitada a la empresa Logicalis Paraguay S.A., especifique en el Plan de Capacitación la cantidad de funcionarios, el lugar de realización, e instructor que dictara el curso, para los lotes 2, 3 y 4 respectivamente. En tiempo y forma fue presentado los recaudos solicitados al Oferente Logicalis Paraguay S.A.

Posteriormente y por intermedio de la Nota DA/COC Nº 485/2014, es solicitado a la empresa Technoma S.A.C.I., aclaración respecto al rango de temperatura y humedad de operación, y la combinación de las modalidades de IDS e IPS, correspondiente al ítem 1, del Lote 1, de la oferta presentada. En tiempo y forma fue presentado los recaudos solicitados al Oferente Technoma S.A.C.I.

Conforme consta en la Nota DA/COC Nº 489/2014, fue solicitada a la empresa Technoma S.A.C.I., la presentación de las especificaciones técnicas de los equipos ofertados, en carácter de declaración jurada debidamente completada y firmada. En tiempo y forma fue presentado los recaudos solicitados al Oferente Technoma S.A.C.I.

Por Nota DA/COC Nº 501/2014, fue solicitado a la empresa Technoma S.A.C.I., aclaración respecto al plan de capacitación; y la vigencia del equipo o software y el

soporte del mismo por al menos 3 años. En tiempo y forma fue presentado los recaudos solicitados al Oferente Technoma S.A.C.I.

Luego, a través de la Nota DAAF/DC N° 1/2014, fue solicitada a la empresa Logicalis Paraguay S.A., la presentación de las especificaciones técnicas de los equipos ofertados, en carácter de declaración jurada debidamente completada y firmada. En tiempo y forma fue presentado los recaudos solicitados al Oferente Logicalis Paraguay S.A.

Posteriormente, y por intermedio de la Nota DAAF/DC N° 2/2014, fue solicitada a la empresa Technoma S.A.C.I., la presentación de la documentación que avale la experiencia y el volumen anual de negocios. En tiempo y forma fue presentado los recaudos solicitados al Oferente Technoma S.A.C.I.

Agotadas todas las verificaciones relacionadas a los criterios técnicos de los equipos ofertados, el representante de la Dirección de TIC`s, manifiesta que las empresas Technoma S.A.C.I. y Logicalis Paraguay S.A., **CUMPLEN** con los requerimientos y exigencias técnicas solicitadas en las bases concúrsales.

CAPACIDAD FINANCIERA

Para el análisis y evaluación de la situación financiera de los oferentes propuestos, mencionamos que los datos a ser utilizados fueron proveídos por los mismos oferentes, los cuales consisten en la copias autenticadas de los Balances Impositivos y Estados de Resultados acompañados de la Declaración Jurada del Impuesto a la Renta (Formulario 101), correspondientes a los ejercicios fiscales 2011, 2012 y 2013 respectivamente. Hacemos la salvedad que la empresa Logicalis Paraguay S.A., ha presentado la Constancia del SIPE; por lo cual los Balances Impositivos y Estados de Resultados fueron obtenidos del SIPE.

Asimismo, es importante señalar lo establecido en la Resolución DNCP N° 1766/14 de fecha 30 de junio de 2014, emitida por la Dirección Nacional de Contrataciones Públicas, en cuyo Anexo 2, numeral 3 dice: *"RESPONSABILIDAD DE LA INFORMACIÓN DEL SISTEMA DE INFORMACIÓN DE PROVEEDORES DEL ESTADO.- Los Proveedores registrados son los responsables del contenido, la veracidad, exactitud y oportunidad de la información y documentación que son incorporados al Sistema de Información de Proveedores del Estado (SIPE), por lo que en caso de dudas o discrepancias deberá recurrirse directamente a la persona física o jurídica registrada en el SIPE".*

Hemos analizados los Niveles de Liquidez, Endeudamiento y Rentabilidad de las empresas oferentes, extraída de los Balances Impositivos de los Años 2011, 2012 y 2013 respectivamente. Dejamos constancia que la preparación de los Balances Impositivos constituye exclusiva responsabilidad del oferente. La responsabilidad del Comité de Evaluación consiste en calificar la situación financiera de los oferentes. En este sentido, los oferentes propuestos para la adjudicación Technoma S.A.C.I. y Logicalis Paraguay S.A. **CUMPLEN** con los índices promedios correspondientes a los ratios de Liquidez, Endeudamiento y Rentabilidad.

Asimismo, los cálculos realizados para la obtención de los indicadores financieros, se hallan plasmados en el **ANEXO 4**.

VOLUMEN ANUAL DE NEGOCIOS

Para la verificación del Volumen Anual de Negocios, hemos procedido a elaborar la Planilla de comprobación en la cual se especifican las entidades contratantes, el tipo de documento, la descripción del servicio y el año de ejecución. Para ello, los oferentes han presentado copias de contratos y facturaciones de ventas de bienes y servicios similares a lo licitado, por un monto equivalente al 20% (veinte por ciento) como mínimo del monto total ofertado en la presente licitación en promedio de los 3 (tres) últimos años (2011/2012/2013).

En este sentido, y a efectos de convertir el valor de la operación de moneda extranjera a moneda nacional, hemos observado los mandamientos estipulados en el Decreto Nº 6359/05, Artículo 61 del Anexo; y se ha tomado el tipo de cambio vigente en la fecha de operación, cuya cotización se encuentra publicada en la página Web de la Subsecretaría de Estado de Tributación del Ministerio de Hacienda, Por lo que se concluye, que las empresas propuestas para la adjudicación **CUMPLEN** con el criterio de experiencia. Señalamos que los cálculos se encuentran plasmados en la planilla denominado **ANEXO 5**.

EXPERIENCIA

Conforme a las documentaciones presentadas por los Oferentes analizados, queda acreditado que los mismos, han efectuado instalaciones de equipamientos similares en los últimos 3 años en el mercado local. Por tanto, **CUMPLEN** con la experiencia solicitada.

CAPACIDAD TÉCNICA

En relación a la capacidad técnica, los oferentes Technoma S.A.C.I. y Logicalis Paraguay S.A., han demostrado que **CUMPLEN** con la capacidad técnica; considerando que acreditan estar suficientemente autorizados por los fabricantes

de los equipos ofertados, a representar y comercializar en el Paraguay dichos equipamientos.

Cuentan con el personal técnico certificado por los fabricantes de los equipos ofertados, y prueba de ello es la presentación de los currículum vitae, en la cual constan sus certificaciones y calificaciones otorgadas por los fabricantes.

Asimismo, han presentado el respaldo por escrito del fabricante a las empresas oferentes autorizándolos a prestar el servicio técnico y el cambio de partes por garantía.

En cuanto al suministro de la documentación de carácter formal, y descriptas Sección VII Anexo I del Pliego de Bases y Condiciones, los oferentes en concurso están obligados a presentar toda y cada una de las documentaciones solicitadas.

A tal efecto, hemos elaborado la planilla de comprobación, en la cual se verifica la presentación de las mismas conforme a lo plasmado en el **ANEXO 6**. Por tanto, **CUMPLEN** con el suministro de la documentación de carácter formal.

Prosiguiendo con la evaluación del financiamiento de los bienes a adquirir, se constata que existen los recursos presupuestarios suficientes para la financiación de la adquisición pretendida, según Certificación de Disponibilidad Presupuestaria **(CDP) N° 440/2014** para el presente Ejercicio Fiscal.

Luego de todas las verificaciones practicadas, éste Comité concluye que se han dado y cumplido todos los requerimientos solicitados por la convocante y expresadas en el Pliego de Bases y Condiciones por lo tanto sugiere y recomienda **Adjudicar** a las empresas conforme al siguiente detalle:

Lotes	**Descripción**	**Oferta Económica**
Oferente: TECHNOMA S.A.C.I.		
1	Sistema de nueva generación de prevención de intrusos y sistema centralizado de defensa y administración de eventos	1.633.743.000.-
	Total a Adjudicar	**1.633.743.000.-**
Son Guaraníes: *Un Mil Seiscientos Treinta y Tres Millones Setecientos Cuarenta y Tres Mil, incluyendo el Impuesto al Valor Agregado (I.V.A.).*----------		

Oferente: LOGICALIS PARAGUAY S.A.		
2	Provisión e implementación de solución de filtrado de contenido, seguridad de publicación Web y Acceso a Internet	642.000.000
3	Provisión e implementación de Web Application Firewall	515.000.000
4	Provisión e implementación de solución de seguridad de la red anti-ddos	403.000.000
	Total a Adjudicar	**1.560.000.000**
Son Guaraníes: Un Mil Quinientos Sesenta Millones, incluyendo el Impuesto al Valor Agregado (I.V.A.).----------		

Finalmente, en fecha 19 de setiembre del corriente, manifestamos que los trabajos de evaluación lo hemos realizado conforme a los criterios establecidos en la Ley N° 2051/03 "De Contrataciones Públicas" y sus reglamentaciones y la conclusión a la que llegamos lo hemos efectuados con responsabilidad e independencia de criterios.

Demostrando conformidad, se da fin a la reunión del Comité de Evaluación, firmando el Acta en tres ejemplares de un mismo tenor y a un solo efecto.

María Liz Caballero
Representante de la Coordinación Financiera

Martha Riquelme Irún
Representante de la Coordinación Administrativa

Alberto Jara
Representante del Departamento de Contrataciones

Pedro Velázquez Ferreira
Representante de la Dirección de TIC`s

ANEXO Nº 1

Suministro de la Documentación Básica de Carácter Sustancial

DESCRIPCIÓN	OFERENTES	
	Logicalis Paraguay S.A.	Technoma S.A.C.I.
Formulario de Oferta debidamente completado y firmado. El oferente deberá cotizar todos los ítems indicados en la planilla de precios, no seran admitidas cotizaciones parciales	**CUMPLE**	**CUMPLE**
Garantía de Mantenimiento de Oferta, debidamente extendida	**CUMPLE**	**CUMPLE**
Fotocopia autenticada de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos.	**CUMPLE**	**CUMPLE**
Documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente (no es necesario que esté inscripto en el Registro de Poderes); ó los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas.	**CUMPLE**	**CUMPLE**
Declaración jurada de no hallarse comprendido en las prohibiciones o limitaciones para contratar establecidas en el artículo 40 y de integridad conforme al artículo 20, inc. "w", ambos de la Ley N° 2051/03, de acuerdo con lo dispuesto en la Resolución N° 330/07 de la Dirección General de Contrataciones Públicas.	**CUMPLE**	**CUMPLE**

ANEXO 2

CUADRO COMPARATIVO DE PRECIOS

Lote	DESCRIPCIÓN	LOGICALIS PARAGUAY S.A.						TECHNOMA S.A.C.I.					
		Marca	Procedencia	Unid.de Medida	Cant.	Precio unitario (IVA incluido)	Precio Total (IVA incluido)	Marca	Procedencia	Unid.de Medida	Cant.	Precio unitario (IVA incluido)	Precio Total (IVA incluido)
1	SISTEMA DE NUEVA GENERACION DE PREVENCIÓN DE INTRUSOS Y SISTEMA CENTRALIZADO DE DEFENSA Y ADMINISTRACION DE EVENTOS												
	Ítem 1 – Sistema de nueva generación para la prevención de intrusos (NGIPS) – Tipo A	NO COTIZA						Cisco	EEUU	Unidad	1	585.866.924	585.866.924
	Ítem 2 – Sistema de nueva generación para la prevención de intrusos (NGIPS) – Tipo B	NO COTIZA						Cisco	EEUU	Unidad	1	644.846.816	644.846.816
	Ítem 3 - Sistema centralizado de defensa y administración de eventos de intrusión.	NO COTIZA						Cisco	EEUU	Unidad	1	403.029.260	403.029.260
												TOTAL LOTE 1	1.633.743.000
2	PROVISIÓN E IMPLEMENTACIÓN DE SOLUCIÓN DE FILTRADO DE CONTENIDO, SEGURIDAD DE PUBLICACION WEB Y ACCESO A INTERNET												
	Provisión e implementación de solución de filtrado de contenido, seguridad de publicación web y acceso a Internet	Blue Coat	EEUU	Unidad	1	642.000.000	642.000.000	NO COTIZA					
						TOTAL LOTE 2	642.000.000						
3	PROVISIÓN E IMPLEMENTACIÓN DE WEB APPLICATION FIREWALL												
	Provisión e implementación de Web application firewall	F5 Networks	EEUU	Unidad	2	257.500.000	515.000.000	NO COTIZA					
						TOTAL LOTE 3	515.000.000						
4	PROVISIÓN E IMPLEMENTACIÓN DE SOLUCIÓN DE SEGURIDAD DE LA RED ANTI-DDOS												
	Provisión e implementación de solución de seguridad de la red anti-ddos	Arbor	EEUU	Unidad	1	403.000.000	403.000.000	NO COTIZA					
						TOTAL LOTE 4	403.000.000						
						Total de la Oferta	1.560.000.000					Total de la Oferta	1.633.743.000

María Liz Caballero
Representante de la Coordinación Financiera

Martha Riquelme Irún
Representante de la Coordinación Administrativa

Alberto Jara
Representante del Departamento de Contrataciones

Pedro Velázquez
Representante de la Dirección de TIC´s

ANEXO 3

PLANILLA DE REQUERIMIENTOS TÉCNICOS

LOTE Nº 1 – Sistema de nueva generación de prevención de intrusos y sistema centralizado de defensa y administración de eventos

OFERENTE: TECHNOMA SACI

ESPECIFICACIONES TÉCNICAS			PROPUESTA DEL OFERENTE	
				Observaciones
Sistema de nueva generación para la prevención de intrusos (NGIPS) – Tipo A	Características	Mínimo Exigido	Cumple con las especificaciones requeridas (sí / no)	Oferta adicional a especificaciones técnicas
Cantidad		1(Uno)	SI	
Marca		Especificar	CISCO	
Modelo		Especificar	3D7120-IPS	
Procedencia		Especificar	EEUU	
Rendimiento en la práctica.	Cada dispositivo debe proporcionar como mínimo un throughput de 1 Gbps para el análisis del tráfico que cruza en el segmento de red.	Exigido	SI	
Conexiones Concurrentes	Cada dispositivo debe soportar 2.000.000 de conexiones concurrentes.	Exigido	SI	
Conexiones por segundo	Cada dispositivo debe soportar 35.000 nuevas conexiones por segundo.		SI	
Interfaces	Cada dispositivo debe contar con 1 interface 10/100/1000 Mbps para comunicación con el sistema de administración de correlación de eventos. Deberá contar además con al menos 4 pares de interfaces de 1Gbps cobre para la inspección del tráfico.	Exigido	SI	
Soporte Fail-Open en las interfaces	Cada dispositivo debe permitir el paso del tráfico en el segmento de red sin afectar el funcionamiento de la red (fail-open), en caso de una falla eléctrica, este mecanismo debe ser interno.	Exigido	SI	
Latencia típica	Cada dispositivo debe ofrecer un promedio de latencia típica menor a 150 micro-segundo.	Exigido	SI	
Fuente de poder	Cada dispositivo debe disponer de redundancia de fuentes en configuración (1+1) para prevenir fallas graves en el hardware. Las mismas deben ser mínimamente de 450 watts. Debe trabajar con voltaje de 100VAC a 240VAC.	Exigido	SI	
Temperatura y humedad de operación	El equipo debe operar en una temperatura de entre 5°C a 40°C y una humedad relativa 5% al 85%.	Exigido	SI	
Almacenamiento	El dispositivo deberá estar equipado con disco en estado sólido para almacenamiento.	Exigido	SI	
Memoria RAM	16 Gbps o superior	Exigido	SI	
Software y Hardware	Toda la solución de hardware y software debe ser de un mismo fabricante.	Exigido	SI	
Administración	El dispositivo debe tener la capacidad de ser administrado a través de conexiones SSH, CLI y HTTPS.	Exigido	SI	
Autenticación	El dispositivo debe permitir la autenticación de usuarios y administradores a través de integración con RADIUS.	Exigido	SI	
Modos de operación	El dispositivo podrá operar en los siguientes modos:	Exigido	SI	

	- Modo Inline - Modo Pasivo El monitoreo del dispositivo debe ser transparente para los usuarios y operar en la capa 2 del modelo de OSI, por lo que las interfaces no requieren de una dirección IP ni una dirección MAC.			
Implementación Inline	El dispositivo debe soportar el modo de implementación Inline, en donde se monitorea y protege los segmentos de datos, con tráfico activo de red pasando por él, lo que permite prevenir los ataques de estos segmentos y bloqueado en tiempo real.	Exigido	SI	
Implementación Inline transparente	El dispositivo podrá configurarse en modo transparente; es decir, inline pero sin bloquear tráfico. El sistema sólo alerta que eventos serían bloqueados. El dispositivo debe permitir la configuración de modo transparente para todo el tráfico o apenas para paquetes especificados por dirección IP, protocolo, VLAN ID incluyendo tramas 802.1q.	Exigido	SI	
Implementación Pasivo	El dispositivo debe soportar el modo de implementación Pasivo, permitiendo el monitoreo a través de los HUBs y / o puertos SPAN de switches, siendo el tráfico de red reflejando en él, lo que le permite monitorear el tráfico de ataques.	Exigido	SI	
IDS Pasivo / IPS en línea	El dispositivo deberá soportar la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.	Exigido	SI	
Motor de Detección	El dispositivo debe soportar un motor de detección que inspeccione no solo los detalles de la capa de red, además información residente en cabeceras de los paquetes, a través de una gama amplia de protocolos.	Exigido	SI	
Detección de Trafico o Vulnerabilidades	El dispositivo debe tener la capacidad de detectar tráfico anómalo o vulnerabilidades en las siguientes aplicaciones Instant Messenger y P2P: AOL Instant Messenger; MSN Messenger; Yahoo! Messenger; ICQ; Gnutella; Kazaa; BitTorrent.	Exigido	SI	
Inspección por Segmentos	El dispositivo debe ser capaz de inspeccionar el tráfico asociado a distintos segmentos de redes, es decir, tener políticas específicas por interfaces, ya sean estas pertenecientes a una interface en modo inline o modo pasivo.	Exigido	SI	
Análisis de Trafico	El dispositivo debe contar como mínimo con las siguientes técnicas de análisis de trafico: identificación del protocolo a través del puerto utilizado; identificación de protocolos que utilizan puertos aleatorios; identificación de protocolos en forma independiente del puerto utilizado.	Exigido	SI	
Inspección de Malware	El dispositivo deberá de inspeccionar la presencia de malware a nivel de archivos que utilicen los siguientes protocolos de aplicación: HTTP, SMTP, IMAP, POP3, FTP.	Exigido	SI	
Ataques basado en HTML	El dispositivo debe ser resistente a diversas técnicas de URL ofuscación en ataques basados en HTML.	Exigido	SI	
Creación de reglas propias	El dispositivo debe soportar reglas de detección basada en un leguaje abierto permitiendo a los usuarios crear sus propias reglas.	Exigido	SI	
Tipo de respuestas	El dispositivo debe soportar los siguientes tipos de respuestas: bloquear, ignorar, guardar en un log, enviar correo electrónico, SNMP, respuestas definidas por el usuario, cambios de configuración a equipos de	Exigido	SI	

	seguridad o de red de terceros, sugerencia de cambios a la política en base al análisis de impacto de un evento.			
Protección de ataques sobre VOIP	El dispositivo debe de soportar la identificación y protección de ataques en protocolos de Voice over IP (VoIP) sobre SIP.	Exigido	SI	
Perfil para identificación de dispositivos móviles	El dispositivo debe tener la capacidad de construir un perfil para la identificación de dispositivos móviles, para lo cual debe incluir la siguiente información: track usuarios, vulnerabilidades, aplicaciones. (sin necesidad de hardware o software separado).	Exigido	SI	
Identificación de usuarios	El dispositivo debe mostrar a través de los siguientes protocolos LDAP, POP3, SIP, IMAP, TNS, AIM, que usuario está generando o recibiendo el evento detectado. (sin necesidad de hardware o software separado).	Exigido	SI	
Tunning	El dispositivo deberá ser capaz de hacer recomendación de afinación (tunning) de políticas en base a la información aprendida de la red, mostrando un registro de las reglas recomendadas.	Exigido	SI	
Prevención Ataques de día cero	El dispositivo debe proveer la detección de anomalías de tráfico y análisis de impacto por evento para evitar ataques de día cero, como una funcionalidad dentro del mismo IPS y sin necesidad del uso de aplicaciones adicionales como sistema de detección de anomalías o scanners.	Exigido	SI	
Políticas a nivel de dispositivo, puerto, VLAN y direcciones IP	El dispositivo debe permitir tener la flexibilidad de controlar políticas a nivel de dispositivo, puerto, VLAN y direcciones IP.	Exigido	SI	
Integración con NMAP	El dispositivo deberá ser capaz de agregar a su base de datos de conocimiento los resultados de un escaneo activo utilizando NMAP, este deberá ser incluido como parte del mismo módulo de correlación.	Exigido	SI	
Inspección de Paquetes	El dispositivo debe de proveer monitoreo de segmentos de red en modo promiscuo analizando encabezamiento (header) y el área de datos (payload) de los paquetes que transitan en la red (deep packet inspection), detectando ataques y tráfico no autorizado o sospechoso.	Exigido	SI	
Vulnerabilidades de Host en tiempo real	El dispositivo deberá identificar vulnerabilidades de los host de la red en tiempo real y sin necesidad de correr un análisis de vulnerabilidades.	Exigido	SI	
Capacidad de decodificar e inspeccionar todos los protocolos apoyados en IPv4	El dispositivo debe tener la habilidad de decodificar e inspeccionar todos los protocolos apoyados en IPv4, y cualquier ataque asociado o mal uso incluso si está encapsulado en IPv6.	Exigido	SI	
Capturas de Trafico	El dispositivo debe poder realizar capturas de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y ENC (estándar para el software de análisis de protocolos). El archivo puede ser usado para hacer playback del ataque. Se aceptaran propuestas que consideren la captura de tráfico para el análisis de evidencia en formato compatible con libpcap (compatible a su vez con TCPDUMP), y opcionalmente en formato ENC.	Exigido	SI	
Análisis Dinámico y en Tiempo Real para creación de Mapa de la Red.	El dispositivo debe permitir un análisis dinámico y en tiempo real para crear un mapa de la red monitoreada, incluyendo al menos lo siguiente parámetros: Redes existentes; Host activos; Nuevos Host o servers en la red; Nuevas MAC address en la red; Máquinas virtuales nuevas o existentes; Sistema operativo de cada uno de los host identificados; Servicios activos de cada uno de los host identificados; Aplicaciones activas de cada uno de los host identificados; Vulnerabilidades de cada uno de los host identificados.	Exigido	SI	

Monitoreo de tráfico entre dos Host	El Dispositivo deberá poder crear perfiles de tráfico con reglas específicas para monitorear el tráfico de la red y crear una alarma cuando cierto umbral sea rebasado.	Exigido	SI	
Recopilación de información pasiva de Hosts y sus actividades	El dispositivo debe ser capaz de recopilar información pasiva de los hosts de la red y sus actividades, tales como: sistema operativo; servicios, puertos abiertos; aplicaciones y vulnerabilidades, permitiendo la correlación de datos, eliminación de falsos positivos y políticas de cumplimiento. (sin necesidad de hardware o software separado).	Exigido	SI	
Identificación de Hosts con incumplimiento de Política	El dispositivo debe ser capaz de identificar todos los hosts que presenten un atributo o condición especifica de incumplimiento de la política.	Exigido	SI	
Visibilidad de Consumo de Ancho de Banda	El dispositivo debe ser capaz de proporcionar mayor visibilidad sobre cómo se consume el ancho de banda, ya sea por dirección o puerto, permitiendo ayudar en la solución de problemas de interrupciones o degradaciones de rendimiento de la red. (sin necesidad de hardware o software separado).	Exigido	SI	
Soporte de NTP	El dispositivo debe soportar sincronización de horario a través de NTP (Network Time Protocol).	Exigido	SI	
Respaldo en tiempo real	El dispositivo debe proveer la capacidad de realizar un respaldo de la configuración de la plataforma en tiempo real, o por un horario definido.	Exigido	SI	
Base de Datos propia, lista negras y blancas	El dispositivo debe soportar IP Reputation, además debe permitir la creación de listas negras y listas blancas y debe contar con una base de datos propia, pero además debe permitir el poder configurar cualquier base de datos de terceros.	Exigido	SI	
Soporte de listas de objetos	El dispositivo debe contar con al menos las siguientes listas de objetos de IP Reputation: Bots, CnC, Malware, Attacker, Suspicious.	Exigido	SI	
Capacidad inteligente de correlacionar eventos	El dispositivo debe proporcionar la capacidad inteligente para correlacionar los eventos de intrusión priorizándolo por tipo de bandera de impacto, en donde se categorice según nivel de severidad y relevancia a la infraestructura protegida.	Exigido	SI	
Soporte de directorio activo y/o LDAP	El dispositivo debe soportar integración a través del directorio activo y/o Open LDAP para determinar el comportamiento de la red a través de direcciones IP asociadas a los eventos sospechosos.	Exigido	SI	
Categorías de reglas	El dispositivo debe contar con al menos las siguientes categorías de reglas: File-Executables; DoS; DDoS; Exploit; P2P; Pua-Adware; Scada; Web-IIS; SQL; Indicator-Obfuscation; Sensitive-Data; RPC; Botnet.	Exigido	SI	
Soporte de reglas por plataforma	El dispositivo debe poder soportar reglas por plataforma tal como: Apple; Cisco; Compaq; HP; IBM; Juniper; Microsoft; Nokia; RedHat; Suse; Sun; Juniper.	Exigido	SI	
Soporte de Reglas de Contenido	El dispositivo debe soportar reglas de contenido con al menos los siguientes parámetros: Message; Reference; Action; Protocol; SID; GID; Direction, Source/Destination IP, Source/Destination port; Rule overhead, Metadata.	Exigido	SI	
Soporte de reglas para excepción de inspección	El dispositivo debe contar con la capacidad de crear reglas que permitan enviar tráfico directamente a través del dispositivo sin que sea inspeccionado.	Exigido	SI	
Perfil de Trafico	El dispositivo debe contar con la capacidad de crear un perfil de tráfico, con base al flujo de datos recolectados durante un periodo específico.	Exigido	SI	
Soporte de MDI/MDIX	El dispositivo debe soportar interfaces en modo MDI/MDIX	Exigido	SI	

Protección contra ataques SYN DoS	El dispositivo deberá de proveer protección contra DoS y DDoS (inundación de ataques tipo "SYN DoS").	Exigido	SI	
Soporte de creación de Objetos por nombre	El dispositivo debe soportar la creación de objetos por nombre ya sea por: network, puertos, Vlan, URL, filtros de aplicación y zonas de seguridad.	Exigido	SI	
Control de aplicaciones	El dispositivo debe poder controlar las aplicaciones en cualquier puerto.	Exigido	SI	
Detección de aplicaciones	El dispositivo debe detectar más de 1600 aplicaciones y categorizarlas por riesgo y relevancia.	Exigido	SI	
Detección de ataques a través de firmas	El dispositivo debe detectar ataques basado en firmas de vulnerabilidades, permitiendo la detección de ataques desconocidos o variaciones de ataques conocidos.	Exigido	SI	
Soporte de detección de archivos	El dispositivo debe soportar la detección de tipos de archivos. Además debe soportar acciones cómo permitir o bloquear el tráfico para los tipos de archivos detectados	Exigido	SI	
Soporte de Gestión SNMP	El dispositivo debe permitir la funcionalidad de gestión SNMP e integrarse a productos de red de terceros para proporcionar indicadores clave de estado operacional a grupos de operaciones de red y de operaciones de seguridad.	Exigido	SI	
Consulta de Histórico de Eventos	El dispositivo debe de proveer la opción de consulta, de un histórico de los eventos sucedidos en los equipos ofertados desde la consola principal, con el fin de realizar análisis forense.	Exigido	SI	
Soporte de monitoreo de redes MPLS	El dispositivo debe permitir soportar monitoreo en redes MPLS.	Exigido	SI	
Protección de ataques	El dispositivo debe proteger contra ataques sobre aplicaciones Web como: Shell command injections, Server-site injection, cross-site scripting, directory traversal.	Exigido	SI	
Mecanismo de eliminación de falsos positivos	El dispositivo debe ser capaz de reducir significativamente el esfuerzo del operador y la aceleración de respuesta a las amenazas por dar prioridad a las alertas de forma automática.	Exigido	SI	
Control y protección de trafico de puertos no estándares	El dispositivo debe ser capaz de proporcionar de forma automática los adecuados controles permitiendo la protección el tráfico enviado a través de puertos de comunicación no estándares.	Exigido	SI	
Perfiles de cumplimiento	El dispositivo deberá ser capaz de crear perfiles de cumplimiento con alguna normativa de seguridad para emitir una alerta cuando algunos de los servicios no permitidos por una normativa de seguridad sea utilizado en el segmento de red acotado por la normativa de seguridad.	Exigido	SI	
Escaneo pasivo de la red	El dispositivo debe ser capaz de esperar pasivamente la recopilación de información sobre los flujos de sesión para todos los hosts, incluyendo el tiempo inicio/fin, puertos, servicios y cantidad de datos.	Exigido	SI	
Detección de Anomalías de tráfico de red.	El dispositivo deberá ser capaz de detectar anomalías de tráfico en la red, en base a los patrones de tráfico identificados.	Exigido	SI	
Integración con terceros	El dispositivo deberá permitir una integración para realizar un cambio de configuración o enviar información a módulos de terceros como: Scanners de vulnerabilidades; SEM/SIEM systems; Firewalls; Routers; Switches.	Exigido	SI	
Sistema de Integración con Directorio activo	El dispositivo deberá incluir un sistema de integración con directorio activo, del mismo fabricante, que provea las siguientes características:	Exigido	SI	

	• Deberá permitir la integración con el directorio activo de la red para tener un mapeo de usuario e IP utilizada actualmente.	Exigido	SI	
	• Deberá permitir tener la información de contacto de los usuarios que están siendo atacados.	Exigido	SI	
	• Los eventos de seguridad reportados deberán mostrar el usuario que está generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión.	Exigido	SI	
	• Deberá de poder generar un mapa de eventos de seguridad generados/recibidos por usuario.	Exigido	SI	
	• Deberá de poder generar un mapa de tráfico generado/recibido por usuario.	Exigido	SI	
	• Deberá ser capaz de mantener un mapa de los usuarios, IP actual, tipo de aplicación usada, y un historial de las IP que ese usuario ha usado en el tiempo.	Exigido	SI	
Soporte de syslog	El dispositivo deberá de soportar syslog para eventos de filtrado y errores del sistema.	Exigido	SI	
Generación de Alertas	El dispositivo deberá de soportar la capacidad de generar alertas a través de: syslog, correo electrónico y SNMP.	Exigido	SI	
Análisis Forense	El dispositivo deberá tener una funcionalidad de "packet level" para realizar actividades de análisis forense.	Exigido	SI	
Soporte de búsqueda de firmas	El dispositivo deberá soportar la búsqueda de firmas por nombre a través de la interfaz gráfica.	Exigido	SI	
Soporte de desfragmentación de paquetes	El dispositivo deberá soportar la desfragmentación de paquetes IP fragmentados y/o coincidentes.	Exigido	SI	
Soporte de inspección de tráfico en GRE	El dispositivo debe de soportar inspección de tráfico en GRE.	Exigido	SI	
Puerto de Consola Serial	El dispositivo debe contar con un puerto de consola serial, que permita la configuración mediante línea de comandos.	Exigido	SI	
Soporte para vulnerabilidades de Internet Explorer	El dispositivo deber contar con cobertura de filtros que protejan las vulnerabilidades de internet Explorer.	Exigido	SI	
Soporte de geolocalización	El dispositivo debe soportar geolocalización; permitiendo obtener al menos la siguiente información: país, código postal, longitud, latitud, zona horaria.	Exigido	SI	
Pruebas NSS LABS	El motor de inspección de la solución para el centro de datos debe estar certificada por una metodología de pruebas igual a NSS Labs del 2013 o posterior, en donde avale que la solución cumple satisfactoriamente con las pruebas de anti-evasión dentro de la cuales debe de contemplar: IP Packet Fragmentation; TCP Stream Segmentation; RPC Fragmentation, URL Obfuscation; HTML Evasion; FTP Evasion, para eso se debe de presentar la documentación respectiva. (https://www.nsslabs.com)	Exigido	SI	
	El motor de inspección de la solución debe contar con el reconocimiento del reporte realizado en el 2013 o posterior de NSS Labs, líder en pruebas de productos de seguridad, en donde se demuestre que la solución completo las pruebas satisfactoriamente contando con al menos 99% de efectividad, para lo cual deberá presentar la documentación respectiva. (https://www.nsslabs.com)	Exigido	SI	

	El dispositivo debe soportar 2 Gbps de throughput para paquetes UDP de 1.512 bytes, esto debe estar avalado con la respectiva documentación respectiva de NSS Labs(https://www.nsslabs.com). El documento deberá ser del 2013 en adelante.	Exigido	SI	
Actualización y Mantenimiento	El proceso de actualización de vulnerabilidades y otros aspectos del mantenimiento (como parches y actualizaciones) deberá ser mediante el sitio Web del fabricante del producto y de varias formas: por medio del propio producto, bajando del sitio Web un archivo de actualización o bien automáticamente.	Exigido	SI	
Integración con terceros a través de APIs	La solución de administración debe permitir mecanismos de integración en forma de APIs abiertas, para lo cual deberá de presentar la documentación respectiva con cuales tecnologías se cumple con este modo de integración.	Exigido	SI	
Documentaciones del Fabricante	El fabricante debe contar con un grupo de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.	Exigido	SI	
	El fabricante debe estar referenciado dentro del último cuadrante mágico de Gartner del 2013 en IPS como uno de los líderes, para lo cual deberá de presentar la documentación respectiva.	Exigido	SI	
	El Fabricante deberá proveer el código de sus firmas para demostrar la detección en base a vulnerabilidades y no en comparación de patrones. Este código podrá ser visible en cualquier momento desde la consola de administración para todas las firmas existentes en el IPS.	Exigido	SI	
Garantías	El oferente deberá presentar documentación del fabricante donde autorice a la empresa como representante para el Paraguay.	Exigido	SI	
	La oferta deberá incluir soporte onsite 24x7x365 del proveedor, por todo el periodo de garantía del equipo.	Exigido	SI	
	El oferente deberá presentar respaldo por escrito del fabricante a la empresa oferente autorizándola a prestar el servicio técnico y el cambio de partes por garantía.	Exigido	SI	
	Los técnicos de la empresa oferente deberán estar certificados por el fabricante. Se exigirá la presentación de los certificados de los técnicos pertenecientes a la empresa autorizada por el fabricante.	Exigido	SI	
	Garantía escrita de tres (3) años como mínimo.	Exigido	SI	
	Toda la información generada en este proceso incluyendo, imágenes, información encriptada, redes, configuraciones y cualquier tipo de dato que se genere será de propiedad exclusiva de la SET. Para el efecto la empresa oferente deberá regirse por los términos establecidos en la Política de Seguridad de la SET.	Exigido	SI	
	El oferente deberá entregar por escrito a la SET las licencias si es que las hubiere.	Exigido	SI	
	Queda prohibido al Oferente, bajo toda circunstancia y forma y sin perjuicio de lo dispuesto en estas Bases Administrativas, apoderarse, extraer o retener cualquier información relativa a los servicios licitados y contratados, incluyendo los sistemas de información, la documentación y los datos.	Exigido	SI	

	El oferente deberá, a través de la marca o sus representantes, certificar la vigencia del equipo o software y el soporte del mismo por al menos 3 años, para dicho efecto deberá presentar un escrito en el cual se comprometa que cualquier gasto en que se incurriere por el incumplimiento de esta vigencia, será asumido por el Oferente.	Exigido	SI	
	No se aceptaran equipos REFURBISHED	Exigido	SI	
	Todos estos puntos son requerimientos mínimos y no se aceptarán ofertas que no cumplan con las mismas. Esto a los efectos de garantizar la calidad y compatibilidad de los dispositivos solicitados, así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante, piezas originales, laboratorios autorizados por el fabricante).	Exigido	SI	
Certificación	Certificación de calidad ISO 9000 similares o superior.	Exigido	SI	
Implementación	La oferta deberá incluir instalación, configuración y puesta en funcionamiento de la solución, en un plazo no mayor a 120 días hábiles posterior a la recepción de la orden de compra, además deberá contemplarse la transferencia de conocimiento de la solución al menos a 2 funcionarios técnicos de la Dirección de TIC de la SET. El oferente deberá contar con implementaciones similares en el país, los técnicos que implementen la solución deberán tener una residencia como mínimo de 6 meses en el país.	Exigido	SI	
Capacitación	Deberá estipularse en la Oferta, la capacitación de al menos 2 funcionarios técnicos de la Dirección de TIC de la SET, en toda la solución proveída, para lo cual el Oferente deberá de presentar una Carta Compromiso a través de la cual se compromete que en el plazo no mayor de 8 meses realizara dicha capacitación, la misma podrá ser realizada en la Ciudad de Asunción o el Exterior, en caso de que se estipule la capacitación en el Exterior, el oferente correrá con todos los gastos de al menos 1 funcionario técnico de la Dirección de TIC de la SET.	Exigido	SI	
Lugar de Entrega	Coordinación de Infraestructura de la Dirección de TIC's de la SET	Exigido	SI	
Plazo de Entrega	Hasta 45 días hábiles posterior a la recepción de la Orden de Compra correspondiente	Exigido	SI	

LOTE 1 – ÍTEMS 2

ESPECIFICACIONES TÉCNICAS			PROPUESTA DEL OFERENTE	
			Cumple con las especificaciones requeridas (sí / no)	Observaciones
Sistema de nueva generación para la prevención de intrusos (NGIPS) – Tipo B	Características	Mínimo Exigido		Oferta adicional a especificaciones técnicas
Cantidad		1(Uno)	SI	
Marca		Especificar	CISCO	
Modelo		Especificar	3D8250-IPS	
Procedencia		Especificar	EEUU	

Rendimiento en la práctica.	Cada dispositivo debe proporcionar como mínimo un throughput de 10 Gbps para el análisis del tráfico que cruza en el segmento de red.	Exigido	1Gbps	
Conexiones Concurrentes	Cada dispositivo debe soportar 12.000.000 de conexiones concurrentes.	Exigido	SI	
Conexiones por segundo	Cada dispositivo debe soportar 180.000 nuevas conexiones por segundo.	Exigido	SI	
Interfaces	Cada dispositivo debe contar con 1 interface 10/100/1000 Mbps para comunicación con el sistema de administración de correlación de eventos. Deberá contar además con al menos 2 pares de interfaces de 10Gbps SR para la inspección del tráfico.	Exigido	SI	
Soporte Fail-Open en las interfaces	Cada dispositivo debe permitir el paso del tráfico en el segmento de red sin afectar el funcionamiento de la red (fail-open), en caso de una falla eléctrica, este mecanismo debe ser interno.	Exigido	SI	
Latencia típica	Cada dispositivo debe ofrecer un promedio de latencia típica menor a 150 micro - segundos.	Exigido	SI	
Fuente de poder	Cada dispositivo debe disponer de redundancia de fuentes en configuración para prevenir fallas graves en el hardware. Las mismas deben ser mínimamente de 600 watts. Debe trabajar con voltaje de 100VAC a 240VAC.	Exigido	SI	
Temperatura y humedad de operación	El equipo debe operar en una temperatura de entre 10°C a 35°C y una humedad relativa 5% al 85%.	Exigido	SI	
Almacenamiento	El dispositivo deberá estar equipado con disco en estado sólido para almacenamiento.	Exigido	SI	
Memoria (RAM)	32 Gbps o superior	Exigido	SI	
Software y Hardware	Toda la solución de hardware y software debe ser de un mismo fabricante.	Exigido	SI	
Administración	El dispositivo debe tener la capacidad de ser administrado a través de conexiones SSH, CLI y HTTPS.	Exigido	SI	
Autenticación	El dispositivo debe permitir la autenticación de usuarios y administradores a través de integración con RADIUS.	Exigido	SI	
Modos de operación	El dispositivo podrá operar en los siguientes modos: - Modo Inline - Modo Pasivo El monitoreo del dispositivo debe ser transparente para los usuarios y operar en la capa 2 del modelo de OSI, por lo que las interfaces no requieren de una dirección IP ni una dirección MAC.	Exigido	SI	
Implementación Inline	El dispositivo debe soportar el modo de implementación Inline, en donde se monitorea y protege los segmentos de datos, con tráfico activo de red pasando por él, lo que permite prevenir los ataques de estos segmentos y bloqueado en tiempo real.	Exigido	SI	
Implementación Inline transparente	El dispositivo podrá configurarse en modo transparente; es decir, inline pero sin bloquear tráfico. El sistema sólo alerta que eventos serían bloqueados. El dispositivo debe permitir la configuración de modo transparente para todo el tráfico o apenas para paquetes especificados por dirección IP, protocolo, VLAN ID incluyendo tramas 802.1q.	Exigido	SI	

Implementación Pasivo	El dispositivo debe soportar el modo de implementación Pasivo, permitiendo el monitoreo a través de los HUBs y / o puertos SPAN de switches, siendo el tráfico de red reflejando en él, lo que le permite monitorear el tráfico de ataques.	Exigido	SI	
IDS Pasivo / IPS en línea	El dispositivo deberá soportar la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.	Exigido	SI	
Motor de Detección	El dispositivo debe soportar un motor de detección que inspeccione no solo los detalles de la capa de red, además información residente en cabeceras de los paquetes, a través de una gama amplia de protocolos.	Exigido	SI	
Detección de Trafico o Vulnerabilidades	El dispositivo debe tener la capacidad de detectar tráfico anómalo o vulnerabilidades en las siguientes aplicaciones Instant Messenger y P2P: AOL Instant Messenger; MSN Messenger; Yahoo! Messenger; ICQ; Gnutella; Kazaa; BitTorrent.	Exigido	SI	
Inspección por Segmentos	El dispositivo debe ser capaz de inspeccionar el tráfico asociado a distintos segmentos de redes diferentes (en lugar de tener una sola política por interfaz).	Exigido	SI	
Análisis de Trafico	El dispositivo debe contar como mínimo con las siguientes técnicas de análisis de trafico: identificación del protocolo a través del puerto utilizado; identificación de protocolos que utilizan puertos aleatorios; identificación de protocolos en forma independiente del puerto utilizado.	Exigido	SI	
Inspección de Malware	El dispositivo deberá de inspeccionar la presencia de malware a nivel de archivos que utilicen los siguientes protocolos de aplicación: HTTP, SMTP, IMAP, POP3, FTP.	Exigido	SI	
Ataques basado en HTML	El dispositivo debe ser resistente a diversas técnicas de URL ofuscación en ataques basados en HTML.	Exigido	SI	
Creación de reglas propias	El dispositivo debe soportar reglas de detección basada en un leguaje abierto permitiendo a los usuarios crear sus propias reglas.	Exigido	SI	
Tipo de respuestas	El dispositivo debe soportar los siguientes tipos de respuestas: bloquear, ignorar, guardar en un log, enviar correo electrónico, SNMP, respuestas definidas por el usuario, cambios de configuración a equipos de seguridad o de red de terceros, sugerencia de cambios a la política en base al análisis de impacto de un evento.	Exigido	SI	
Ataques basado en HTML	El dispositivo debe ser resistente a diversas técnicas de URL ofuscación en ataques basados en HTML.	Exigido	SI	
Creación de reglas propias	El dispositivo debe soportar reglas de detección basada en un leguaje abierto permitiendo a los usuarios crear sus propias reglas.	Exigido	SI	
Tipo de respuestas	El dispositivo debe soportar los siguientes tipos de respuestas: bloquear, ignorar, guardar en un log, enviar correo electrónico, SNMP, respuestas definidas por el usuario, cambios de configuración a equipos de seguridad o de red de terceros, sugerencia de cambios a la política en base al análisis de impacto de un evento.	Exigido	SI	
Protección de ataques sobre VOIP	El dispositivo debe de soportar la identificación y protección de ataques en protocolos de Voice over IP (VoIP) sobre SIP.	Exigido	SI	

Perfil para identificación de dispositivos móviles	El dispositivo debe tener la capacidad de construir un perfil para la identificación de dispositivos móviles, para lo cual debe incluir la siguiente información: track usuarios, vulnerabilidades, aplicaciones. (sin necesidad de hardware o software separado).	Exigido	SI	
Identificación de usuarios	El dispositivo debe mostrar a través de los siguientes protocolos LDAP, POP3, SIP, IMAP, TNS, AIM, que usuario está generando o recibiendo el evento detectado. (sin necesidad de hardware o software separado).	Exigido	SI	
Tunning	El dispositivo deberá ser capaz de hacer recomendación de afinación (tunning) de políticas en base a la información aprendida de la red, mostrando un registro de las reglas recomendadas.	Exigido	SI	
Prevención Ataques de día cero	El dispositivo debe proveer la detección de anomalías de tráfico y análisis de impacto por evento para evitar ataques de día cero, como una funcionalidad dentro del mismo IPS y sin necesidad del uso de aplicaciones adicionales como sistema de detección de anomalías o scanners.	Exigido	SI	
Políticas a nivel de dispositivo, puerto, VLAN y direcciones IP	El dispositivo debe permitir tener la flexibilidad de controlar políticas a nivel de dispositivo, puerto, VLAN y direcciones IP.	Exigido	SI	
Integración con NMAP	El dispositivo deberá ser capaz de agregar a su base de datos de conocimiento los resultados de un escaneo activo utilizando NMAP, este deberá ser incluido como parte del mismo módulo de correlación.	Exigido	SI	
Inspección de Paquetes	El dispositivo debe de proveer monitoreo de segmentos de red en modo promiscuo analizando encabezamiento (header) y el área de datos (payload) de los paquetes que transitan en la red (deep packet inspection), detectando ataques y tráfico no autorizado o sospechoso.	Exigido	SI	
Vulnerabilidades de Host en tiempo real	El dispositivo deberá identificar vulnerabilidades de los host de la red en tiempo real y sin necesidad de correr un análisis de vulnerabilidades.	Exigido	SI	
Capacidad de decodificar e inspeccionar todos los protocolos apoyados en IPv4	El dispositivo debe tener la habilidad de decodificar e inspeccionar todos los protocolos apoyados en IPv4, y cualquier ataque asociado o mal uso incluso si está encapsulado en IPv6.	Exigido	SI	
Capturas de Trafico	El dispositivo debe poder realizar capturas de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y .ENC (estándar para el software de análisis de protocolos). El archivo puede ser usado para hacer playback del ataque. Se aceptaran propuestas que consideren la captura de tráfico para el análisis de evidencia en formato compatible con libpcap (compatible a su vez con TCPDUMP), y opcionalmente en formato ENC.	Exigido	SI	
Análisis Dinámico y en Tiempo Real para creación de Mapa de la Red.	El dispositivo debe permitir un análisis dinámico y en tiempo real para crear un mapa de la red monitoreada, incluyendo al menos lo siguiente parámetros: Redes existentes; Host activos; Nuevos Host o servers en la red; Nuevas MAC address en la red; Máquinas virtuales nuevas o existentes; Sistema operativo de cada uno de los host identificados; Servicios activos de cada uno de los host identificados; Aplicaciones activas de cada uno de los host identificados; Vulnerabilidades de cada uno de los host identificados.	Exigido	SI	

Monitoreo de tráfico entre dos Host	El Dispositivo deberá poder crear perfiles de tráfico con reglas específicas para monitorear el tráfico de la red y crear una alarma cuando cierto umbral sea rebasado.	Exigido	SI	
Recopilación de información pasiva de Hosts y sus actividades	El dispositivo debe ser capaz de recopilar información pasiva de los hosts de la red y sus actividades, tales como: sistema operativo; servicios, puertos abiertos; aplicaciones y vulnerabilidades, permitiendo la correlación de datos, eliminación de falsos positivos y políticas de cumplimiento. (sin necesidad de hardware o software separado).	Exigido	SI	
Identificación de Hosts con incumplimiento de Política	El dispositivo debe ser capaz de identificar todos los hosts que presenten un atributo o condición especifica de incumplimiento de la política.	Exigido	SI	
Visibilidad de Consumo de Ancho de Banda	El dispositivo debe ser capaz de proporcionar mayor visibilidad sobre cómo se consume el ancho de banda, ya sea por dirección o puerto, permitiendo ayudar en la solución de problemas de interrupciones o degradaciones de rendimiento de la red. (sin necesidad de hardware o software separado).	Exigido	SI	
Soporte de NTP	El dispositivo debe soportar sincronización de horario a través de NTP (Network Time Protocol).	Exigido	SI	
Respaldo en tiempo real	El dispositivo debe proveer la capacidad de realizar un respaldo de la configuración de la plataforma en tiempo real, o por un horario definido.	Exigido	SI	
Base de Datos propia, lista negras y blancas	El dispositivo debe soportar IP Reputation, además debe permitir la creación de listas negras y listas blancas y debe contar con una base de datos propia, pero además debe permitir el poder configurar cualquier base de datos de terceros.	Exigido	SI	
Soporte de listas de objetos	El dispositivo debe contar con al menos las siguientes listas de objetos de IP Reputation: Bots, CnC, Malware, Attacker, Suspicious.	Exigido	SI	
Capacidad inteligente de correlacionar eventos	El dispositivo debe proporcionar la capacidad inteligente para correlacionar los eventos de intrusión priorizándolo por tipo de bandera de impacto, en donde se categorice según nivel de severidad y relevancia a la infraestructura protegida.	Exigido	SI	
Soporte de directorio activo y/o Open LDAP	El dispositivo debe soportar integración a través del directorio activo y/o Open LDAP para determinar el comportamiento de la red a través de direcciones IP asociadas a los eventos sospechosos.	Exigido	SI	
Categorías de reglas	El dispositivo debe contar con al menos las siguientes categorías de reglas: File-Executables; DoS; DDoS; Exploit; P2P; Pua-Adware; Scada; Web-IIS; SQL; Indicator-Obfuscation; Sensitive-Data; RPC; Botnet.	Exigido	SI	
Soporte de reglas por plataforma	El dispositivo debe poder soportar reglas por plataforma tal como: Apple; Cisco; Compaq; HP; IBM; Juniper; Microsoft; Nokia; RedHat; Suse; Sun; Juniper.	Exigido	SI	
Soporte de Reglas de Contenido	El dispositivo debe soportar reglas de contenido con al menos los siguientes parámetros: Message; Reference; Action; Protocol; SID; GID; Direction, Source/Destination IP, Source/Destination port; Rule overhead, Metadata.	Exigido	SI	

Soporte de reglas para excepción de inspección	El dispositivo debe contar con la capacidad de crear reglas que permitan enviar tráfico directamente a través del dispositivo sin que sea inspeccionado.	Exigido	SI	
Perfil de Trafico	El dispositivo debe contar con la capacidad de crear un perfil de tráfico, con base al flujo de datos recolectados durante un periodo específico.	Exigido	SI	
Soporte de MDI/MDIX	El dispositivo debe soportar interfaces en modo MDI/MDIX	Exigido	SI	
Protección contra ataques SYN DoS	El dispositivo deberá de proveer protección contra DoS y DDoS (inundación de ataques tipo "SYN DoS").	Exigido	SI	
Soporte de creación de Objetos por nombre	El dispositivo debe soportar la creación de objetos por nombre ya sea por: network, puertos, Vlan, URL, filtros de aplicación y zonas de seguridad.	Exigido	SI	
Control de aplicaciones	El dispositivo debe poder controlar las aplicaciones en cualquier puerto.	Exigido	SI	
Detección de aplicaciones	El dispositivo debe detectar más de 1600 aplicaciones y categorizarlas por riesgo y relevancia.	Exigido	SI	
Detección de ataques a través de firmas	El dispositivo debe detectar ataques basado en firmas de vulnerabilidades, permitiendo la detección de ataques desconocidos o variaciones de ataques conocidos.	Exigido	SI	
Soporte de detección de archivos	El dispositivo debe soportar la detección de tipos de archivos. Además debe soportar acciones cómo permitir o bloquear el tráfico para los tipos de archivos detectados	Exigido	SI	
Soporte de Gestión SNMP	El dispositivo debe permitir la funcionalidad de gestión SNMP e integrarse a productos de red de terceros para proporcionar indicadores clave de estado operacional a grupos de operaciones de red y de operaciones de seguridad.	Exigido	SI	
Consulta de Histórico de Eventos	El dispositivo debe de proveer la opción de consulta, de un histórico de los eventos sucedidos en los equipos ofertados desde la consola principal, con el fin de realizar análisis forense.	Exigido	SI	
Soporte de monitoreo de redes MPLS	El dispositivo debe permitir soportar monitoreo en redes MPLS.	Exigido	SI	
Protección de ataques	El dispositivo debe proteger contra ataques sobre aplicaciones Web como: Shell command injections, Server-site injection, cross-site scripting, directory traversal.	Exigido	SI	
Mecanismo de eliminación de falsos positivos	El dispositivo debe ser capaz de reducir significativamente el esfuerzo del operador y la aceleración de respuesta a las amenazas por dar prioridad a las alertas de forma automática.	Exigido	SI	
Control y protección de trafico de puertos no estándares	El dispositivo debe ser capaz de proporcionar de forma automática los adecuados controles permitiendo la protección el tráfico enviado a través de puertos de comunicación no estándares.	Exigido	SI	
Perfiles de cumplimiento	El dispositivo deberá ser capaz de crear perfiles de cumplimiento con alguna normativa de seguridad para emitir una alerta cuando algunos de los servicios no permitidos por una normativa de seguridad sea utilizado en el segmento de red acotado por la normativa de seguridad.	Exigido	SI	
Escaneo pasivo de la red	El dispositivo debe ser capaz de esperar pasivamente la recopilación de información sobre los flujos de sesión para todos los hosts, incluyendo el tiempo inicio/fin, puertos, servicios y cantidad de datos.	Exigido	SI	

Detección de Anomalías de tráfico de red.	El dispositivo deberá ser capaz de detectar anomalías de tráfico en la red, en base a los patrones de tráfico identificados.	Exigido	SI	
Integración con terceros	El dispositivo deberá permitir una integración para realizar un cambio de configuración o enviar información a módulos de terceros como:	Exigido	SI	
	Scanners de vulnerabilidades; SEM/SIEM systems; Firewalls; Routers; Switches.			
	El dispositivo deberá incluir un sistema de integración con directorio activo, del mismo fabricante, que provea las siguientes características:	Exigido	SI	
Sistema de Integración con Directorio activo	• Deberá permitir la integración con el directorio activo de la red para tener un mapeo de usuario e IP utilizada actualmente.	Exigido	SI	
	• Deberá permitir tener la información de contacto de los usuarios que están siendo atacados.	Exigido	SI	
	• Los eventos de seguridad reportados deberán mostrar el usuario que está generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión.	Exigido	SI	
	• Deberá de poder generar un mapa de eventos de seguridad generados/recibidos por usuario.	Exigido	SI	
	• Deberá de poder generar un mapa de tráfico generado/recibido por usuario.	Exigido	SI	
	• Deberá ser capaz de mantener un mapa de los usuarios, IP actual, tipo de aplicación usada, y un historial de las IP que ese usuario ha usado en el tiempo.	Exigido	SI	
Soporte de syslog	El dispositivo deberá de soportar syslog para eventos de filtrado y errores del sistema.	Exigido	SI	
Generación de Alertas	El dispositivo deberá de soportar la capacidad de generar alertas a través de: syslog, correo electrónico y SNMP.	Exigido	SI	
Análisis Forense	El dispositivo deberá tener una funcionalidad de "packet level" para realizar actividades de análisis forense.	Exigido	SI	
Soporte de búsqueda de firmas	El dispositivo deberá soportar la búsqueda de firmas por nombre a través de la interfaz gráfica.	Exigido	SI	
Soporte de desfragmentación de paquetes	El dispositivo deberá soportar la desfragmentación de paquetes IP fragmentados y/o coincidentes.	Exigido	SI	
Soporte de inspección de tráfico en GRE	El dispositivo debe de soportar inspección de tráfico en GRE.	Exigido	SI	
Puerto de Consola Serial	El dispositivo debe contar con un puerto de consola serial, que permita la configuración mediante línea de comandos.	Exigido	SI	
Soporte para vulnerabilidades de Internet Explorer	El dispositivo debe contar con cobertura de filtros que protejan las vulnerabilidades de internet Explorer.	Exigido	SI	
Soporte de geolocalización	El dispositivo debe soportar geolocalización; permitiendo obtener al menos la siguiente información: país, código postal, longitud, latitud, zona horaria.	Exigido	SI	
Pruebas NSS LABS	El motor de inspección de la solución para el centro de datos debe estar certificada por una metodología de pruebas igual a NSS Labs del 2013 o posterior, en donde avale que la solución cumple satisfactoriamente con las pruebas de anti-evasión dentro de la cuales debe de contemplar:	Exigido	SI	

	IP Packet Fragmentation; TCP Stream Segmentation; RPC Fragmentation, URL Obfuscation; HTML Evasion; FTP Evasion, para eso se debe de presentar la documentación respectiva. (https://www.nsslabs.com)			
	El motor de inspección de la solución debe contar con el reconocimiento del reporte realizado en el 2013 o posterior de NSS Labs, líder en pruebas de productos de seguridad, en donde se demuestre que la solución completó las pruebas satisfactoriamente contando con al menos 99% de efectividad, para lo cual deberá presentar la documentación respectiva. (https://www.nsslabs.com)	Exigido	SI	
	El dispositivo debe soportar 2 Gbps de throughput para paquetes UDP de 1.512 bytes, esto debe estar avalado con la respectiva documentación respectiva de NSS Labs (https://www.nsslabs.com). El documento deberá ser del 2013 en adelante.	Exigido	SI	
Actualización y Mantenimiento	El proceso de actualización de vulnerabilidades y otros aspectos del mantenimiento (como parches y actualizaciones) deberá ser mediante el sitio Web del fabricante del producto y de varias formas: por medio del propio producto, bajando del sitio Web un archivo de actualización o bien automáticamente.	Exigido	SI	
Integración con terceros a través de APIs	La solución de administración debe permitir mecanismos de integración en forma de APIs abiertas, para lo cual deberá de presentar la documentación respectiva con cuales tecnologías se cumple con este modo de integración.	Exigido	SI	
Documentaciones del Fabricante	El fabricante debe contar con un grupo de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.	Exigido	SI	
	El fabricante debe estar referenciado dentro del último cuadrante mágico de Gartner del 2013 en IPS como uno de los líderes, para lo cual deberá de presentar la documentación respectiva.	Exigido	SI	
	El Fabricante deberá proveer el código de sus firmas para demostrar la detección en base a vulnerabilidades y no en comparación de patrones. Este código podrá ser visible en cualquier momento desde la consola de administración para todas las firmas existentes en el IPS.	Exigido	SI	
Garantías	El oferente deberá presentar documentación del fabricante donde autorice a la empresa como representante para el Paraguay.	Exigido	SI	
	La oferta deberá incluir soporte onsite 24x7x365 del proveedor, por todo el periodo de garantía del equipo.	Exigido	SI	
	El oferente deberá presentar respaldo por escrito del fabricante a la empresa oferente autorizándola a prestar el servicio técnico y el cambio de partes por garantía.	Exigido	SI	
	Los técnicos de la empresa oferente deberán estar certificados por el fabricante. Se exigirá la presentación de los certificados de los técnicos pertenecientes a la empresa autorizada por el fabricante.	Exigido	SI	
	Garantía escrita de tres (3) años como mínimo.	Exigido	SI	

	Toda la información generada en este proceso incluyendo, imágenes, información encriptada, redes, configuraciones y cualquier tipo de dato que se genere será de propiedad exclusiva de la SET. Para el efecto la empresa oferente deberá regirse por los términos establecidos en la Política de Seguridad de la SET.	Exigido	SI	
	El oferente deberá entregar por escrito a la SET las licencias si es que las hubiere.	Exigido	SI	
	Queda prohibido al Oferente, bajo toda circunstancia y forma y sin perjuicio de lo dispuesto en estas Bases Administrativas, apoderarse, extraer o retener cualquier información relativa a los servicios licitados y contratados, incluyendo los sistemas de información, la documentación y los datos.	Exigido	SI	
	El oferente deberá, a través de la marca o sus representantes, certificar la vigencia del equipo o software y el soporte del mismo por al menos 3 años, para dicho efecto deberá presentar un escrito en el cual se comprometa que cualquier gasto en que se incurriere por el incumplimiento de esta vigencia, será asumido por el Oferente.	Exigido	SI	
	No se aceptaran equipos REFURBISHED	Exigido	SI	
	Todos estos puntos son requerimientos mínimos y no se aceptarán ofertas que no cumplan con las mismas. Esto a los efectos de garantizar la calidad y compatibilidad de los dispositivos solicitados, así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante, piezas originales, laboratorios autorizados por el fabricante).	Exigido	SI	
Certificación	Certificación de calidad ISO 9000 similar o superior	Exigido	SI	
Implementación	La oferta deberá incluir instalación, configuración y puesta en funcionamiento de la solución, en un plazo no mayor a 120 dias hábiles posterior a la recepción de la orden de compra, además deberá contemplarse la transferencia de conocimiento de la solución al menos a 2 funcionarios técnicos de la Dirección de TIC de la SET. El oferente deberá contar con implementaciones similares en el país, los técnicos que implementen la solución deberán tener una residencia como mínimo de 6 meses en el país.	Exigido	SI	
Capacitación	Deberá estipularse en la Oferta, la capacitación de al menos 2 funcionarios técnicos de la Dirección de TIC de la SET, en toda la solución proveída, para lo cual el Oferente deberá de presentar una Carta Compromiso a través de la cual se compromete que en el plazo no mayor de 8 meses realizara dicha capacitación, la misma podrá ser realizada en la Ciudad de Asunción o el Exterior, en caso de que se estipule la capacitación en el Exterior, el oferente correrá con todos los gastos de al menos 1 funcionario técnico de la Dirección de TIC de la SET.	Exigido	SI	
Lugar de Entrega	Coordinación de Infraestructura de la Dirección de TIC's de la SET	Exigido	SI	
Plazo de Entrega	Hasta 45 días hábiles posterior a la recepción de la Orden de Compra correspondiente	Exigido	SI	

LOTE 1 – ÍTEMS 3

ESPECIFICACIONES TÉCNICAS			PROPUESTA DEL OFERENTE	
			Cumple con las especificaciones requeridas (sí / no)	Observaciones: Oferta adicional a especificaciones técnicas
Sistema centralizado de defensa y administración de eventos de intrusión	Características	Mínimo Exigido		
Cantidad		1(Uno)	SI	
Marca		Especificar	cisco	
Modelo		Especificar	DC1500-FS	
Procedencia		Especificar	EEUU	
Análisis automatizado de impactos al correlacionar eventos IDS & IPS	El sistema de administración centralizada debe tener la capacidad de desempeñar el análisis automatizado de impactos al correlacionar eventos IDS & IPS con el estado de la vulnerabilidad según la información del sistema operativo para determinar la posibilidad de éxito contra el objetivo.	Exigido	SI	
Soporte de integración con productos de análisis de vulnerabilidades.	El sistema de administración centralizada debe soportar la integración de productos de análisis de vulnerabilidades.	Exigido	SI	
Soporte de ajustes dinámicos de severidad de ataques	El sistema de administración centralizada debe soportar ajustes dinámicos de severidad en los ataques como resultado de la correlación de eventos.	Exigido	SI	
Soporte de correlación de datos de vulnerabilidades	El sistema de administración centralizada debe soportar la correlación de datos de vulnerabilidades.	Exigido	SI	
Soporte de reportes en formato texto	El sistema de administración centralizada debe soportar reportes en formato texto y gráfico, con exportación en los formatos HTML, PDF e CSV.	Exigido	SI	
Soporte de correlación de patrones de ataques	El sistema de administración centralizada debe soportar la correlación de patrones de ataques (múltiples eventos identificados como un único ataque). Esto se refiere a que el equipo ofertado sea lo suficientemente inteligente para que pueda identificar eventos similares y los pueda relacionar como una sola anomalía, con aplicaciones del mismo fabricante.	Exigido	SI	
Soporte de consola remota con interfaz gráfica	El sistema de administración centralizada debe soportar consola remota con interfaz gráfica, consola remota Web en formato gráfico para el uso en modo de consulta, perfiles diferentes de usuarios.	Exigido	SI	

Capacidad de visualizar las versiones de Software y Hardware	El sistema de administración debe proveer la capacidad de visualizar las versiones de software y hardware de los sensores desde la consola principal y desde cada equipo por separado.	Exigido	SI	
Soporte de auditoría de actividades de usuarios	El sistema de administración centralizada debe soportar auditoria de las actividades de los usuarios.	Exigido	SI	
Soporte de Administración	El sistema de administración centralizada debe soportar la administración de por lo menos 35 sistemas IPS sin necesidad de actualizar el software o licenciamiento.	Exigido	SI	
Perfiles de hosts y usuarios.	El sistema de administración centralizada debe soportar un máximo de 50000 host y usuarios.	Exigido	SI	
Memoria RAM	El sistema de administración centralizada debe contar con al menos 6 GB de memoria RAM, con un almacenamiento de al menos 125 GB.	Exigido	SI	
Administración centralizada de dispositivos.	El sistema de administración centralizada debe soportar actualización remota de los dispositivos tanto a nivel de hardware como de software.	Exigido	SI	
Reportes Detallados	El sistema de administración centralizada deberá permitir reportes detallados sobre lo siguiente: Nuevos host en la red; Vulnerabilidades existentes en la red; Servicios existentes en la red; anomalías de tráfico; Perfiles de tráfico; Sistemas operativos existentes en la red; Vulnerabilidades por cada host; Uso de tráfico por aplicación; Uso de tráfico por usuario; Uso de tráfico por host; Uso de tráfico por servicio; Eventos de seguridad por impacto en la red; Eventos de seguridad por criticidad de la vulnerabilidad.	Exigido	SI	
Reportes Automáticos	El sistema de administración centralizada debe generar reportes en forma automática y enviarlos a una cuenta de correo electrónico para agilizar el proceso de análisis.	Exigido	SI	
Ayuda para Firmas	El sistema de administración centralizada debe contar con información detallada de ayuda para firmas. Cuando aparece una amenaza en la pantalla de la consola, el usuario debe tener la capacidad de visualizar información detallada acerca de la vulnerabilidad hacia la cual está dirigida la amenaza. Ello debe incluir una explicación de la vulnerabilidad, de los sistemas que pueden verse afectados, de información sobre falsos positivos, de información CVE, de explicaciones para parcheo o restauración y de URLs.	Exigido	SI	
Herramientas integradas para visibilidad de estado de los equipos	Es importante que el sistema de administración centralizada cuente con herramientas integradas para tener visibilidad en forma de graficas en tiempo real e historial sobre el estado de salud, como mínimo de:	Exigido	SI	

	CPU, interfaces, memoria, performance, disco, temperatura.			
Análisis de Inteligencia	El sistema de administración centralizada debe tener la posibilidad de realizar análisis de inteligencia con facilidad. Ello incluye análisis basados en el contexto lógico del evento siendo evaluado. Entre los ejemplos se encuentran el retorno de todos los eventos desde la IP fuente elegida, el retorno de todas las vulnerabilidades asociadas con el puerto objetivo elegido, etc. Deben incluirse mecanismos capaces de desempeñar los ejemplos anteriores, y más. El usuario debe poder navegar y analizar, con facilidad, más de un millón de eventos al día.	Exigido	SI	
Personalización de pantalla de consola	El sistema de administración centralizada debe contar con soporte para la personalización de la pantalla de la consola. El usuario debe poder personalizar el contenido de la pantalla y los filtros con base en la dirección IP, rango de red, protocolo, tipo de evento, nombre de evento y servicio, para después guardar dicha configuración bajo nombres personalizados para su uso futuro.	Exigido	SI	
Integración con Tecnologías de Seguridad de Terceros	El sistema de administración centralizada deberá ser capaz de integrarse con tecnologías de seguridad de terceros (Firewall, IPS Wireless, Switches, Routers etc) para generar acciones y/o configuraciones necesarias para remediación de incidentes de seguridad.	Exigido	SI	
Reportes definidos, métrica y disponibilidad de los reportes	El sistema de administración centralizada debe incluir reportes previamente definidos. La consola debe tener la capacidad de producir métricas gráficas y reportes de comparación con base en segmentos de tiempo. La información en los reportes debe estar disponible para un grupo de activos, para todo un sitio o para toda una empresa. Asimismo, el usuario debe poder llegar hasta estos reportes para visualizar los detalles pertinentes.	Exigido	SI	
Actualización de Reglas	El sistema de administración centralizada debe proporcionar la capacidad de activar, desactivar y modificar las reglas individuales, por grupos o categoría de normas.	Exigido	SI	
Reportes pre-definidos y/o personalizados	El sistema de administración centralizada debe proporcionar la capacidad de seleccionar informes pre-definidos y la posibilidad completa de personalización y generación de nuevos reportes.	Exigido	SI	
Capacidad de gestión de ciclo de vida de un evento	El sistema de administración centralizada debe incluir las capacidades de flujo de trabajo para la gestión del ciclo de vida completo de un evento, desde la notificación inicial a través de cualquier respuesta y resolución de las actividades que sean necesarias.	Exigido	SI	

Opciones de respuesta automáticas a amenazas	El sistema de administración centralizada debe ser compatible con múltiples opciones para responder automáticamente a las amenazas detectadas ya sea por alertas automatizados y/o remediación del firewall.	Exigido	SI	
Interfaces	El sistema de administración centralizada debe de tener una interface de red 10/100/1000 para la administración.	Exigido	SI	
Roles Múltiples de Usuarios	El sistema de administración centralizada debe soportar roles múltiples para el usuario dentro de los cuales deben estar: Administrator; Maintenance User; Policy & Response Administrator; Intrusion Event Analyst; Real-Time Network Awareness. Estos roles deben dar lugar o prevenir el uso de ciertos privilegios de parte del usuario. Los privilegios deben incluir una gama de funciones administrativas de reporte o visualización.	Exigido	SI	
Mecanismos de Integración en forma de API's abiertas y/o interfaces abiertas	El sistema de administración centralizada debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para permitir una respuesta automática a las amenazas de los componentes externos y las aplicaciones de recuperación, tales como routers, firewalls, etc.	Exigido	SI	
	El sistema de administración centralizada debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para permitir a los eventos y registro de datos sean compartidos con la red externa y las aplicaciones de gestión de seguridad, tales como sistemas de ticketing, SIEM, plataformas de sistemas de gestión y registro de las herramientas de gestión.	Exigido	SI	
	El sistema de administración centralizada debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para recibir información de fuentes externas, como bases de datos de gestión de configuración, herramientas de administración de vulnerabilidades y sistemas de gestión de parches, de correlación de amenazas y política de TI propósitos de cumplimiento.	Exigido	SI	
	El sistema de administración centralizada debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para exportar información SNMP para sistemas de gestión de la red.	Exigido	SI	
	El sistema de administración centralizada debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para obtener inteligencia de la red (es decir, NetFlow) de routers y switches Cisco.	Exigido	SI	

Integración con escáneres de vulnerabilidades externos	El sistema de administración centralizada debe deberá ser capaz de agregar a su base de datos de conocimiento los resultados de un análisis de vulnerabilidades realizado por un analizador de vulnerabilidades (escaner) incluido en el mismo módulo de correlación.	Exigido	SI	
Tunning de Políticas	El sistema de administración centralizada deberá ser capaz de hacer recomendación de afinación (tunning) de políticas en base a la información aprendida de la red, mostrando un registro de las reglas recomendadas.	Exigido	SI	
Perfil de Trafico de la Red	El sistema de administración centralizada deberá ser capaz de crear un perfil de tráfico de la red para crear líneas base del tráfico existente en la red.	Exigido	SI	
	El sistema de administración centralizada deberá poder crear perfiles de tráfico con reglas específicas para monitorear el tráfico entre dos host de la red y crear una alarma cuando cierto umbral sea rebasado.	Exigido	SI	
Anomalías de Trafico de la Red	El sistema de administración centralizada deberá ser capaz de detectar anomalías de tráfico en la red, en base a los patrones de tráfico identificados.	Exigido	SI	
Soporte de funcionalidades	El sistema de administración debe soportar la funcionalidad de exportar (Export) e importar (Import) políticas, dashboard, búsquedas, workflows.	Exigido	SI	
Perfiles referente a normativa de seguridad	El sistema de administración centralizada deberá ser capaz de crear perfiles de cumplimiento con alguna normativa de seguridad, para emitir una alarma cuando algunos de los servicios no permitidos por una normativa de seguridad sea utilizado en el segmento de red acotado por la normativa de seguridad.	Exigido	SI	
Escaneo de vulnerabilidades de Hosts	El sistema de administración centralizada deberá ser capaz de realizar un escaneo de vulnerabilidades a los host de la red para validar la existencia de las vulnerabilidades o como una respuesta a un incidente, por ejemplo al detectar un nuevo.	Exigido	SI	
Integración con Directorio Activo	El sistema de administración centralizada deberá permitir la integración con el directorio activo de la red para tener un mapeo de usuario e IP utilizada actualmente.	Exigido	SI	
Información de usuarios atacados	El sistema de administración centralizada deberá permitir tener la información de contacto de los usuarios que están siendo atacados.	Exigido	SI	

Generación de alerta en base a perfil de usuario	El sistema de administración centralizada deberá a través de los eventos de seguridad detectados mostrar el usuario que está generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión.	Exigido	SI	
Mapa de eventos de seguridad	El sistema de administración centralizada deberá de poder generar un mapa de eventos de seguridad generados/recibidos por usuario.	Exigido	SI	
Mapa de tráfico de usuario	El sistema de administración centralizada deberá de poder generar un mapa de tráfico generado/recibido por usuario.	Exigido	SI	
Mapa de tráfico de usuario	El sistema de administración centralizada deberá ser capaz de mantener un mapa de los usuarios, tráfico generado/recibido por el usuario, IP actual, tipo de aplicación usada, y un historial de las direcciones IP que ese usuario ha usado en el tiempo.	Exigido	SI	
Soporte de funcionalidad de calendarización de tareas	El sistema de administración centralizada deberá soportar la funcionalidad de calendarizar tareas administrativas tal como: ejecutar respaldos, aplicación de políticas, generación de reportes, ejecutar scaneos, aplicar recomendaciones en la política, importar actualizaciones.	Exigido	SI	
Soporte de creación de un Ciclo de Vida de Incidentes	El sistema de administración centralizada deberá soportar la funcionalidad para la creación de un ciclo de vida de un incidente, permitiendo el cambio del estado del incidente.	Exigido	SI	
Exportación de la política en formato PDF	El sistema de administración centralizada deberá permitir la generación a través de un documento en formato pdf la configuración de la política aplicada.	Exigido	SI	
Capacidad de Implementación	Demostrar capacidad con al menos una implementación finalizada en empresas (públicas o privadas), en el territorio nacional.	Exigido	SI	
Técnicos Certificados	Disponer en su nómina de empleados de técnicos certificados con suficiente experiencia en la solución ofrecida (Como mínimo 2).	Exigido	SI	
	Debido a la complejidad de la infraestructura instalada, en su mayoría equipos (RUTEADORES, SWITCHES, FIREWALS, BALANCEADORES y otros) de la marca Cisco Systems, el oferente deberá poseer en su nómina de empleados, técnicos con suficiente capacidad y certificaciones del nivel Cisco Certified Design Professional (CCDP) (Al Menos 1), Cisco Certified Network Professional Security (CCNP Security) (AL MENOS 2 TECNICOS), Cisco Certified Networking Professional R&S (CCNP Routing & Switching) (AL MENOS 2 TECNICOS)	Exigido	SI	

	El oferente deberá presentar como líder del proyecto a un Ingeniero en Telecomunicaciones o Electrónica con énfasis en Telecomunicaciones.	Exigido	SI	
Prueba de Concepto	La convocante se reserva el derecho de solicitar una Prueba de Concepto in-situ de una solución similar a la ofertada, la misma no podrá extenderse más de 30 días.	Exigido	SI	
Garantías	El oferente deberá presentar documentación del fabricante donde autorice a la empresa como representante para el Paraguay.	Exigido	SI	
	La oferta deberá incluir soporte onsite 24x7x365 del proveedor, por todo el periodo de garantía del equipo.	Exigido	SI	
	El oferente deberá presentar respaldo por escrito del fabricante a la empresa oferente autorizándola a prestar el servicio técnico y el cambio de partes por garantía.	Exigido	SI	
	Los técnicos de la empresa oferente deberán estar certificados por el fabricante. Se exigirá la presentación de los certificados de los técnicos pertenecientes a la empresa autorizada por el fabricante.	Exigido	SI	
	Garantía escrita de tres (3) años como mínimo.	Exigido	SI	
	Toda la información generada en este proceso incluyendo, imágenes, información encriptada, redes, configuraciones y cualquier tipo de dato que se genere será de propiedad exclusiva de la SET. Para el efecto la empresa oferente deberá regirse por los términos establecidos en la Política de Seguridad de la SET.	Exigido	SI	
	El oferente deberá entregar por escrito a la SET las licencias si es que las hubiere.	Exigido	SI	
	Queda prohibido al Oferente, bajo toda circunstancia y forma y sin perjuicio de lo dispuesto en estas Bases Administrativas, apoderarse, extraer o retener cualquier información relativa a los servicios licitados y contratados, incluyendo los sistemas de información, la documentación y los datos.	Exigido	SI	
	El oferente deberá, a través de la marca o sus representantes, certificar la vigencia del equipo o software y el soporte del mismo por al menos 3 años, para dicho efecto deberá presentar un escrito en el cual se comprometa que cualquier gasto en que se incurriere por el incumplimiento de esta vigencia, será asumido por el Oferente.	Exigido	SI	
	No se aceptaran equipos REFURBISHED	Exigido	SI	
	Todos estos puntos son requerimientos mínimos y no se aceptarán ofertas que no cumplan con las mismas. Esto a los efectos de garantizar la calidad y compatibilidad de los dispositivos solicitados, así como los servicios de post-venta (servicio técnico con	Exigido	SI	

	mano de obra certificada por el fabricante, piezas originales, laboratorios autorizados por el fabricante).			
Certificación	Certificación de calidad ISO 9000 similar o superior.	Exigido	SI	
Implementación	La oferta deberá incluir instalación, configuración y puesta en funcionamiento de la solución, en un plazo no mayor a 120 dias hábiles posterior a la recepción de la orden de compra, además deberá contemplarse la transferencia de conocimiento de la solución al menos a 2 funcionarios técnicos de la Dirección de TIC de la SET. El oferente deberá contar con implementaciones similares en el país, los técnicos que implementen la solución deberán tener una residencia como mínimo de 6 meses en el país.	Exigido	SI	
Capacitación	Deberá estipularse en la Oferta, la capacitación de al menos 2 funcionarios técnicos de la Dirección de TIC de la SET, en toda la solución proveída, para lo cual el Oferente deberá de presentar una Carta Compromiso a través de la cual se compromete que en el plazo no mayor de 8 meses realizara dicha capacitación, la misma podrá ser realizada en la Ciudad de Asunción o el Exterior, en caso de que se estipule la capacitación en el Exterior, el oferente correrá con todos los gastos de al menos 1 funcionario técnico de la Dirección de TIC de la SET.	Exigido	SI	
Lugar de Entrega	Coordinación de Infraestructura de la Dirección de TIC's de la SET	Exigido	SI	
Plazo de Entrega	Hasta 45 días hábiles posterior a la recepción de la Orden de Compra correspondiente	Exigido	SI	

LOTE Nº 2 Provisión e implementación de solución de filtrado de contenido, seguridad de publicación Web y Acceso a Internet

OFERENTE: LOGICALIS PARAGUAY S.A.

ESPECIFICACIONES TÉCNICAS			PROPUESTA DEL OFERENTE	
			Cumple con las especificaciones requeridas (sí / no)	Observaciones Oferta adicional a especificaciones técnicas
Solución de Filtrado de Contenido, seguridad de publicación Web y acceso a Internet	Características	Mínimo Exigido		
Cantidad		1(Uno)		
Marca		Especificar	bluecoat	
Modelo		Especificar	SG-900-10b -PR	
Procedencia		Especificar	USA	

Equipo de Filtrado de Contenido que deberá de cumplir con las siguientes características y generalidades	La solución ofertada deberá proporcionar capacidades de administración y reporte centralizado incluyendo control de acceso discrecional, control de versiones, auditoria de usuario y sistema y utilerías de restauración de configuración.	Exigido	SI	
	Para la función de reporte centralizado deberá ofrecer más de 150 reportes pre configurados y la habilidad de construir reportes personalizados.	Exigido	SI	
	Los reportes predefinidos deberán proporcionar información tal como perfiles generales de tráfico, datos de rendimiento específico de aplicaciones, protocolos y usuarios, categorías de filtrado y sesiones.	Exigido	SI	
	La solución deberá proporcionar soporte de administración multisesión (múltiples administradores utilizando el servicio de administración centralizado).	Exigido	SI	
	Para los equipos de filtrado de contenido las cuentas de administrador deberán proporcionar los siguientes derechos de acceso configurables: Denegar, Solo lectura, Lectura/Escritura.	Exigido	SI	
	El sistema de administración centralizado deberá soportar la administración de al menos 400 dispositivos de filtrado de contenido.	Exigido	SI	
	La solución ofertada deberá ofrecer los siguientes mecanismos de autenticación: archivos locales de passwords, NTLM, LDAP (Active Directory, eDirectory, SunOne), Netegrity SiteMinder, Oblix COREid, RADIUS y certificados.	Exigido	SI	
	La solución ofertada deberá ser capaz de evitar la ejecución de códigos maliciosos, notificará al usuario y enviara alertas al administrador.	Exigido	SI	
	La solución deberá estar integrada en una plataforma de hardware de propósito dedicado.	Exigido	SI	
	El sistema operativo deberá ser propietario, seguro y de propósito específico para el dispositivo en cuestión, en lugar de uno de propósito general basado en Unix o Linux, con todas las licencias correspondientes para su uso y administración.	Exigido	SI	
	El equipo deberá contar con la capacidad de correr bases de datos de filtrado propietarias y de terceros de forma simultánea.	Exigido	SI	
	Deberá contar con la posibilidad de catalogar las páginas por Dominio, no por URL o IP.	Exigido	SI	
	Deberá ofrecer función de catalogación en tiempo real de sitios en internet (on-the-fly) que aún no han sido asignados a alguna categoría	Exigido	SI	
	Deberá contar con la posibilidad de incorporar un sitio en varias categorías al mismo tiempo.	Exigido	SI	
	Deberá contar con reconocimiento de sitios en tiempo real en al menos 20 lenguajes.	Exigido	SI	

	Deberá contar con la capacidad de entregar peticiones repetitivas desde el cache del appliance donde corre la base de datos.	Exigido	SI	
	Deberá ofrecer generación de bitácoras (logs) de al menos los siguientes protocolos: http, https, cifs, mapi, ftp, tcp-tunnel, IM, Streaming, DNS, ssl.	Exigido	SI	
	Deberá contar con la capacidad de personalizar el formato de las bitácoras.	Exigido	SI	
	Deberá ofrecer Upload de bitácoras utilizando al menos http con ssl, ftp con ssl.	Exigido	SI	
	Deberá contar con herramienta de análisis y reporte de bitácoras con soporte en Linux o Windows de 64 bits (En caso de que sea Windows, deberá proveerse la Licencia).	Exigido	SI	
	Deberá soportar exportación de la información de los reportes en formatos de texto, HTML y pdf.	Exigido	SI	
	El software de filtrado deberá estar integrado al equipo (appliance), no deberá hacer uso de un equipo externo o independiente para el procesamiento de peticiones o almacenamiento de las bases de datos de filtrado.	Exigido	SI	
	Deberá permitir bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, comparticiòn de archivos punto a punto (P2P file sharing).	Exigido	SI	
	Deberá proporcionar un mecanismo para enviar el contenido malicioso al centro de análisis propio de la solución para su investigación.	Exigido	SI	
	Deberá permitir el bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, etc.	Exigido	SI	
	Deberá detectar y bloquear archivos ejecutables independientemente de la extensión del archivo.	Exigido	SI	
	La actualización de la base de datos para el filtrado de contenido deberá realizarse en tiempo real y de manera automática.	Exigido	SI	
	El motor de análisis de contenido deberá soportar el idioma español, de modo que la base de datos de filtrado de contenido y sus actualizaciones estén debidamente regionalizadas al idioma mencionado.	Exigido	SI	
	Deberá permitir operar en modo de proxy puro y proxy transparente.	Exigido	SI	
	Deberá soportar y controlar los protocolos: HTTP, SSL (como proxy normal y reverso), FTP, CIFS, MAPI, DNS, P2P, SOCKS (v4/v5), Telnet, IM (AOL, MSN, Yahoo Messengers), TCP-Tunnel, MMS, RTSP y QuickTime.	Exigido	SI	
	Deberá ofrecer administración de ancho de banda por aplicación.	Exigido	SI	
	Deberá soportar monitoreo y bloqueo de aplicaciones P2P, BitTorrent, eDonkey, Gnutella, Fasttrack.	Exigido	SI	

	Deberá permitir personalización detallada de políticas de control de acceso de forma visual en el equipo a través de diferentes parámetros como: direcciones IP, grupos de subredes, protocolos, urls, atributos, grupos y usuarios de directorio activo de Microsoft y Open LDAP.	Exigido	SI	
	Deberá permitir el uso de expresiones regulares y tener la capacidad de agregar nuevas expresiones.	Exigido	SI	
	Deberá permitir la creación de categorías de filtrado personalizadas así como la creación de listas blancas y negras de filtrado URL	Exigido	SI	
	La solución propuesta deberá estar certificada por los laboratorios ICSA y haber completado la evaluación NIAP EAL2 (evaluation Assurance Level 2)	Exigido	SI	
	Deberá contar con la capacidad de des-encriptar, inspeccionar y almacenar en cache el contenido web encriptado (SSL) que pase por el equipo, siendo posible aplicar políticas a este tráfico.	Exigido	SI	
	La tecnología SSL que la solución proporcione deberá cumplir con FIPS 140-2.	Exigido	SI	
	Deberá contar con cifrado SSL basado en hardware	Exigido	SI	
	El equipo deberá permitir la recopilación (caching) de páginas web en disco duro y memoria RAM, con el fin de hacer más eficiente el uso de los recursos del equipo.	Exigido	SI	
	El sistema operativo del equipo deberá tener la capacidad de borrar paginas obsoletas o poco visitadas por los usuarios con el fin de optimizar los recursos de almacenamiento interno.	Exigido	SI	
	Deberá tener la capacidad de generar bitácoras de todos los accesos y eventos al sistema operativo, a los eventos de Proxy e historia del caché, generar reportes estadísticos de uso de hardware como CPUs, disco duro, memoria, comportamiento del cache y uso de los protocolos que atiende.	Exigido	SI	
	Deberá ser capaz de monitorear el estado del hardware y sus componentes, generando estadísticas en tiempo real de la temperatura de los CPU's, fuentes de poder, ventiladores, interfaces de red, discos duros, como mínimo.	Exigido	SI	
	Deberá contar con un mecanismo que permita recuperar la configuración del dispositivo en caso de desastre.	Exigido	SI	
	Deberá generar alertas y notificaciones de falla automáticas al menos por medio del correo electrónico.	Exigido	SI	
	La solución ofertada deberá soportar un cliente de aceleración y filtrado de contenido propietario, el cual pueda ser instalado en equipos móviles como laptops para usuarios que se encuentren fuera de la organización.	Exigido	SI	

	La solución deberá soportar optimización de trafico de streaming de video/audio a través de un sistema de caching de objetos (para archivos de audio/video) o realizando un split de la señal de video. Debe ser compatible con Video/audio, MMS, RTSP, QUICK TIME, FLASH.	Exigido	SI	
	La solución propuesta deberá soportar IPv6.	Exigido	SI	

LOTE Nº 3 Provisión e implementación de Web application firewall

ESPECIFICACIONES TÉCNICAS			PROPUESTA DEL OFERENTE	
			Cumple con las especificaciones requeridas (sí / no)	Observaciones Oferta adicional a especificaciones técnicas
Web Application Firewall	Características	Mínimo Exigido		
Cantidad		2(Dos)	SI	
Marca		Especificar	F5	
Modelo		Especificar	F5-BIG-IP-2000S	
Procedencia		Especificar	USA	
Plataforma y Licenciamiento	La solución deberá estar compuesta por todos los componentes de hardware y software necesarios para su completo funcionamiento.	Exigido	SI	
	La solución propuesta deberá soportar un esquema de Alta Disponibilidad en modo activo-pasivo y activo-activo con el fin de obtener un esquema tolerante a fallas.	Exigido	SI	
	La solución deberá estar basada en appliance con un sistema operativo robustecido y específico para su función.	Exigido	SI	
	La solución deberá incluir 8 ports de Gigabit Ethernet cobre.	Exigido	SI	
	La solución deberá soportar al menos 2 módulos Gigabit FO.	Exigido	SI	
	Deberá ofrecer throughput de procesamiento de tráfico L4/L7 de 5 Gbps. La performance deberá considerarse en modalidad proxy reverso e inspeccionando la seguridad de los requerimientos.	Exigido	SI	
	La cantidad de transacciones http por segundo será como mínimo de 500.000 rps.	Exigido	SI	
	Ante la falla de un equipo de la solución (interface, procesador, sistema operativo, software, etc.), otro equipo deberá tomar instantáneamente el tráfico que previamente era procesado por el equipo que falló y no deberá degradarse la performance en ningún aspecto.	Exigido	SI	

	Los appliances componentes de la solución deberán implementarse en clúster.	Exigido	SI	
Funcionalidades	La solución deberá proveer la posibilidad de bloquear las transacciones WEB, FTP y SMTP en forma preventiva, antes de que estas lleguen vía red al servidor.	Exigido	SI	
	Deberá ofrecer compresión de contenido HTTP para optimización de tráfico.	Exigido	SI	
	Deberá ofrecer descompresión de contenido HTTP para inspección en capa 7.	Exigido	SI	
	Deberá ofrecer balanceo de carga en capa 2, 3 y/o 7.	Exigido	SI	
	La solución deberá soportar los tags de prioridad 802.1q.	Exigido	SI	
	La solución deberá funcionar en modo Reverse Proxy Explícito, y Reverse Proxy transparente.	Exigido	SI	
	La solución deberá contar con un modo de aprendizaje que permita definir cuáles son las acciones esperadas y aceptadas para los usuarios.	Exigido	SI	
	La solución deberá acelerar y permitir inspeccionar las conexiones SSL (SSL v3, TLS v1) implementadas en los servidores web. Para ello deberá poder importarse credenciales (llave pública y privada), de manera de abrir el túnel y volver a cerrarlo para que la conexión cifrada termine definitivamente en el servidor de la aplicación.	Exigido	SI	
	Deberá volver a encriptar el contenido hacia el servidor con el mismo o con un certificado diferente.	Exigido	SI	
	Deberá ofrecer protección contra ataques de evasión por ofuscación.	Exigido	SI	
	Deberá ofrecer rearmado del stream TCP.	Exigido	SI	
	Deberá ofrecer protección contra ICMP/UDP flooding.	Exigido	SI	
	La solución deberá validar que el contenido y longitud del protocolo http, incluyendo los encabezados, cuerpo y cookies sea correcto. A su vez, deberá poder restringir los métodos http utilizados en una aplicación Web (GET, POST, PUT, etc.).	Exigido	SI	
	Deberá ofrecer protección de la cookie de SYN contra ataques de SYN flood.	Exigido	SI	
	Deberá ofrecer firmado criptográfico de cookies para verificar su integridad.	Exigido	SI	
	La solución deberá proteger las aplicaciones Web contra ataques comunes como: SQL Injection, LDAP Injection, OS Commanding, SSI Injection, Remote File Inclusion, Mail Command Injection, XML injection, XPath injection y XQuery injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF),	Exigido	SI	

	Web Scrapping, Google hacking. Forced Browsing, Unvalidated redirect and forward, y protección de modificación de campos ocultos.			
	La solución deberá proteger contra ataques de fuerza bruta y DoS.	Exigido	SI	
	La solución deberá soportar la definición de diferentes políticas que podrán asociarse a cada aplicación de forma individual.	Exigido	SI	
	La solución deberá soportar el modelo positivo y negativo en conjunto para detectar y bloquear ataques hacia las aplicaciones protegidas (Web y Web Services).	Exigido	SI	
	La licencia deberá permitir la actualización de firmas. Esta actualización deberá ser soportada por medio de: descarga de firmas desde el WAF o descarga manual de las firmas para posteriormente ser actualizadas en la solución.	Exigido	SI	
	Por cada aplicación protegida, el administrador deberá poder configurar en qué momento se hace solo detección (log) de los ataques recibidos y en qué momento previenen (bloqueo) los ataques.	Exigido	SI	
	Por cada aplicación Web (entendiendo aplicaciones web diferente a diferentes URL's) deberá ser posible deshabilitar la prevención de ataques (bloqueo) y dejar habilitado solo la detección (log) de forma granular con el fin de facilitar el troubleshooting por tipos de ataque.	Exigido	SI	
	Ante un bloqueo, dependiendo del modo de operación, la respuesta (página) que se le envía al usuario deberá tener la opción de personalizarse.	Exigido	SI	
	La solución deberá permitir que hosts o clientes confiables puedan ser excluidos de las medidas de protección.	Exigido	SI	
	La solución deberá poder prevenir fugas de información de datos de información considerada como sensible en las aplicaciones, y debe ser flexible para que el administrador defina el patrón asociado a la información que no se desea exponer.	Exigido	SI	
	En modo aprendizaje, deberá aprender la estructura y elementos de la aplicación y esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad. Como mínimo debe aprender sobre: - URL´s - Parámetros - Tipo de contenidos de los parámetros - Cookies	Exigido	SI	

En modo aprendizaje, deberá aprender además del comportamiento esperado del usuario y esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad. Como mínimo debe aprender sobre: - Longitud del valor esperado - Caracteres aceptados - Si el parámetro es de sólo lectura o editable por el usuario	Exigido	SI	
El modo aprendizaje deberá poder ser activado y desactivado manualmente para extender el tiempo de reconocimiento del patrón de conducta.	Exigido	SI	
Deberá ofrecer herramientas para creación de política automatizada por medio de aprendizaje sobre tráfico productivo y tráfico confiable.	Exigido	SI	
Respecto de algún ataque o alguna otra actividad no autorizada, la solución deberá ser capaz de tomar las acciones adecuadas, como mínimo: - Terminar las solicitudes y respuestas - Bloquear la dirección IP.	Exigido	SI	
La solución deberá contar con un conjunto de patrones correspondientes a los ataques conocidos. Esta base de datos de patrones deberá actualizarse periódicamente en forma automática y no asistida.	Exigido	SI	
Deberá poder leer y proteger los parámetros dinámicos de la página WEB para evitar ataques del tipo parameter tampering.	Exigido	SI	
La solución deberá sincronizar las conexiones entre ambos miembros del cluster.	Exigido	SI	
La solución deberá permitir la creación de reglas lógicas que permitan identificar condiciones definidas por el usuarios, cómo una expresión regular o un valor determinado, en cualquier de los siguientes elementos: - Encabezado y cuerpo del requerimiento HTTP - Encabezado y cuerpo de la respuesta HTTP	Exigido	SI	
Deberá permitir detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque.	Exigido	SI	
La solución deberá cumplir con todos los criterios de evaluación del WAFEC definidos por el Web Application Security Consortium.	Exigido	SI	
La solución deberá proteger las aplicaciones contra las vulnerabilidades definidas en OWASP Top 10 2010.	Exigido	SI	

	La solución deberá soportar el volumen de tráfico requerido y deberá tener una latencia sub-milisegundo, para no impactar el desempeño de la aplicación Web.	Exigido	SI	
	La solución deberá soportar bloqueo de ataques JSON (javascript object notation).	Exigido	SI	
	La solución deberá soportar Interpretación y segurización de código JSON (javascript object notation).	Exigido	SI	
	La solución deberá soportar Interpretación y segurización de código AJAX.	Exigido	SI	
	La solución deberá tener la capacidad de proteger Web Servicies basados en SOAP.	Exigido	SI	
	La solución de monitoreo de aplicaciones Web, deberá: - Inspeccionar y monitorear todos los datos http y la aplicación, incluyendo, los encabezados http, campos de formularios, y el cuerpo http. - Inspeccionar las peticiones y respuestas http. - Tener la habilidad de decodificar datos a su mínima expresión y validarla. - Validar todos los tipos de datos ingresados, incluyendo URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.	Exigido	SI	
	Deberá ofrecer validación del esquema XML.	Exigido	SI	
	Deberá ofrecer prevención contra ataques de denegación de servico XML (XDoS).	Exigido	SI	
	Deberá poder limitar la cantidad de niveles que puede tener un elemento XML.	Exigido	SI	
	Deberá poder limitar el tamaño que puede tener el valor de un elemento XML.	Exigido	SI	
	Deberá ofrecer prevención de ataques de Inyección de código SQL vía XML.	Exigido	SI	
	Deberá permitir importar el WSDL para limitar los métodos SOAP disponibles.	Exigido	SI	
	La solución deberá tener la capacidad de realizar un parche virtual para proteger las vulnerabilidades detectadas.	Exigido	SI	
	La solución deberá poder identificar y mantener un registro de las sesiones Web a nivel aplicativo, por medio del seguimiento de cookies.	Exigido	SI	

	Deberá poder forzar el flujo de navegación que debe seguir un usuario para acceder al contenido protegido, prohibiendo el acceso a todo usuario que intente un acceso directo a ese contenido.	Exigido	SI	
	La solución deberá validar que el contenido y longitud del protocolo http, incluyendo los encabezados, cuerpo y cookies sea correcto.	Exigido	SI	
	Todos los componentes deberán soportar el protocolo de gestión de red SNMP para ser monitoreados por las herramientas propias y para que puedan generar alertas o traps hacia el servidor respectivo.	Exigido	SI	
Administración, Actualización y Reportes	Los logs reportados deberán permitir identificar: la IP origen del atacante, fecha y hora, tipo de ataque al cual se asocia, la aplicación atacada, el recurso solicitado, la acción realizada (detección, bloqueo de la petición) usuario y el detalle de la solicitud donde se visualice la información del request donde se indique el contenido que corresponde al ataque.	Exigido	SI	
	La administración de la solución deberá basarse en roles, donde dependiendo del rol se definen las acciones que el usuario puede hacer sobre la solución.	Exigido	SI	
	La solución de administración deberá permitir, como mínimo, lo siguiente: -Agregar, eliminar o modificar la configuración en un entorno gráfico - Modificar las reglas de la solución -Efectuar la configuración de los componentes de la solución - Visualizar los registros de auditoría, alertas de seguridad y eventos del sistema	Exigido	SI	
	Deberá proveer herramientas de logueo y monitoreo de estadísticas del sistema, las cuales deberán brindar información en tiempo real (del estado actual) como así también reportes históricos de como mínimo las siguientes estadísticas del sistema: - Uso de cpu o de los cpu's para el manager y para los dispositivos gestionados. - Uso de memoria RAM - Paquetes enviados y recibidos por interface física - Errores de transmisión y recepción por interface física - Ancho de banda utilizado por cada dispositivo gestionado. - Ancho de banda utilizado para transmisión por cada interface	Exigido	SI	
	Toda la configuración, administración y monitoreo de la solución deberá efectuarse a través de las "consolas".	Exigido	SI	

	La información reportada en los logs deberá tener la opción de presentarse en forma agregada para simplificar la visualización de los logs. Por ejemplo: Actividades similares por aplicación se agrupan en una misma entrada mostrando la cantidad de veces que estas han ocurrido. Una vez seleccionada la entrada se pueda visualizar el detalle de las entradas que correspondan a estas estadísticas.	Exigido	SI	
	La solución deberá actualizar las firmas de seguridad automáticamente.	Exigido	SI	
	Deberá ofrecer posibilidad de agregar las nuevas firmas en modo simulación a las políticas forzadas.	Exigido	SI	
	La solución deberá poder enviar alertas por email.	Exigido	SI	
	Deberá soportar, como mínimo, protocolo SNMP v2 y v3 para Control y Monitoreo.	Exigido	SI	
	Deberá soportar la consulta mediante protocolo SNMP de la siguiente información: - Uso de CPU o de los CPU's - Estado de cada una de las interfaces de red - Tráfico en cada una de las interfaces de red - Uso de Memoria	Exigido	SI	
	Deberá soportar él envió de alarmas mediante: - Traps SNMP - E-Mails - Syslog	Exigido	SI	
	La solución deberá poder generar alarmas ante los siguientes eventos: - Degradación de la performance - Falla de cualquiera de los componentes de la solución - Problemas de conectividad	Exigido	SI	
	Deberá poseer alarmas automáticas con la información completa (detalle del problema, configuración, log).	Exigido	SI	
	La solución deberá permitir la definición de distintas políticas de seguridad, entendiéndose como tal, al conjunto de reglas bajo el cual estará controlada una determinada aplicación.	Exigido	SI	
	Se deberá permitir elegir la política de seguridad a ser implementada en una aplicación, como así también la aplicación de políticas distintas para aplicaciones distintas.	Exigido	SI	

	El software de administración deberá permitir la visualización en tiempo real de los logs correspondientes a los eventos que hayan violado una política de seguridad determinada, detallando como mínimo: - IP origen. - Nombre de evento. -Severidad del evento. - Fecha y hora de ocurrencia. - Descripción del motivo por el cual fue categorizada.	Exigido	SI	
	La solución de administración deberá permitir la definición de filtros, sobre todos y cada uno de los campos, soportando agrupaciones, permitiendo customizar la información a ser visualizada.	Exigido	SI	
	Se deberá permitir la generación de reportes con toda la actividad registrada en los logs contemplando como mínimo el formato PDF.	Exigido	SI	
	Se deberá permitir automatizar la generación de reportes y su posterior remisión por correo electrónico.	Exigido	SI	
	Deberá contemplar mecanismos que permitan fácilmente la vuelta atrás de una política de seguridad implementada en una aplicación.	Exigido	SI	
	Se deberá permitir el acceso a los logs a través de la base de datos utilizada para el resguardo de los mismos.	Exigido	SI	
	Se deberá permitir que un usuario de la solución defina que transacciones serán logueadas.	Exigido	SI	
Certificación	Certificación de calidad ISO 9000 similar o superior	Exigido	si	
Implementación	La oferta deberá incluir instalación, configuración y puesta en funcionamiento de la solución, en un plazo no mayor a 120 dias hábiles posterior a la recepción de la orden de compra, además deberá contemplarse la transferencia de conocimiento de la solución al menos a 2 funcionarios técnicos de la Dirección de TIC de la SET, en la modalidad On The Job Trainning.	Exigido	SI	
	El oferente deberá presentar documentación del fabricante donde autorice a la empresa como representante para el Paraguay.	Exigido	SI	
	La oferta deberá incluir soporte onsite 24x7x365 del proveedor, por todo el periodo de garantía del equipo.	Exigido	SI	
	El oferente deberá presentar respaldo por escrito del fabricante a la empresa oferente autorizándola a prestar el servicio técnico y el cambio de partes por garantía.	Exigido	SI	

	Los técnicos de la empresa oferente deberán estar certificados por el fabricante. Se exigirá la presentación de los certificados de al menos 1 técnico perteneciente a la empresa, autorizados por el fabricante.	Exigido	SI	
	Garantía escrita de un (1) año como mínimo.	Exigido	SI	
	Toda la información generada en este proceso incluyendo, imágenes, información encriptada, redes, configuraciones y cualquier tipo de dato que se genere será de propiedad exclusiva de la SET. Para el efecto la empresa oferente deberá regirse por los términos establecidos en la Política de Seguridad de la SET	Exigido	SI	
	El oferente deberá entregar por escrito a la SET las licencias si es que las hubiere.	Exigido	SI	
	Queda prohibido al Oferente, bajo toda circunstancia y forma y sin perjuicio de lo dispuesto en estas Bases Administrativas, apoderarse, extraer o retener cualquier información relativa a los servicios licitados y contratados, incluyendo los sistemas de información, la documentación y los datos.	Exigido	SI	
	El oferente deberá, a través de la marca o sus representantes, certificar la vigencia del equipo o software y el soporte del mismo por al menos 3 años, para dicho efecto deberá presentar una escrito en el cual se comprometa que cualquier gasto en que se incurriere por el incumplimiento de esta vigencia, será asumido por el Oferente.	Exigido	SI	
Garantías	No se aceptaran equipos REFURBISHED	Exigido	SI	
	Todos estos puntos son requerimientos mínimos y no se aceptarán ofertas que no cumplan con las mismas. Esto a los efectos de garantizar la calidad y compatibilidad de los dispositivos solicitados, así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante, piezas originales, laboratorios autorizados por el fabricante).	Exigido	SI	
Capacitación	Deberá estipularse en la Oferta, la capacitación de al menos 2 funcionarios técnicos de la Dirección de TIC de la SET, en toda la solución proveída, para lo cual el Oferente deberá de presentar un Carta Compromiso a través de la cual se compromete que en el plazo no mayor de 8 meses realizara dicha capacitación, la misma podrá ser realizada en la Ciudad de Asunción o el Exterior, en caso de que se estipule la capacitación en el Exterior, el oferente correrá con todos los gastos de al menos 1 funcionario técnico de la Dirección de TIC de la SET. Para este efecto se deberá de presentar en la Oferta un Plan de Capacitación de al menos 20 hs.	Exigido	SI	
Lugar de Entrega	Coordinación de Infraestructura de la Dirección de TIC's de la SET	Exigido	SI	
Plazo de Entrega	Hasta 45 días hábiles posterior a la recepción de la Orden de Compra correspondiente	Exigido	SI	

ANEXO 4

LICITACIÓN PÚBLICA NACIONAL Nº 09/2014 "Adquisición de Equipos de Seguridad para el Datacenter de la Subsecretaría de Estado de Tributación del Ministerio de Hacienda"
ID. 271.869

ANALISIS DE LA CAPACIDAD FINANCIERA

Balance cerrado al 31/12/11, 31/12/12 y al 31/12/13

EMPRESA: TECHNOMA S.A.C.I.

Descripción	Cálculos			Total	Promedio	Ponderación: Cumple/No Cumple
	2.013	2.012	2.011			
Índice de liquidez						CUMPLE
Activo corriente	5.923.140.501	2.629.533.589	2.043.781.599			
Pasivo corriente	3.649.506.603	1.813.143.920	935.495.964			
Índice	1,62	1,45	2,18	5,26	**1,75**	
Endeudamiento						CUMPLE
Pasivo total	3.649.506.603	1.813.143.920	1.414.045.608			
Activo total	6.307.590.041	2.869.466.159	2.176.806.270			
Índice	0,58	0,63	0,65	1,86	**0,62**	
Rentabilidad						CUMPLE
Utilidad neta	1.516.379.952	435.564.522	440.676.307			
Capital	1.000.000.000	1.000.000.000	100.000.000			
Índice	1,52	0,44	4,41	6,36	**2,12**	

INTERPRETACIÓN

ÍNDICE DE LIQUIDEZ: El promedio de los últimos 3 años no puede ser menor a 1.-
ENDEUDAMIENTO: El promedio de los últimos 3 años no puede ser mayor a 0,80.-
RENTABILIDAD: El promedio de los últimos 3 años no debe ser negativo.-

María Liz Caballero
Representante de la Coordinación Financiera

Martha Riquelme Irún
Representante de la Coordinación Administrativa

Alberto Jara
Representante del Departamento de Contrataciones

Pedro Velázquez
Representante de la Dirección de TIC´s

LICITACIÓN PÚBLICA NACIONAL Nº 09/2014 "Adquisición de Equipos de Seguridad para el Datacenter de la Subsecretaría de Estado de Tributación del Ministerio de Hacienda" - ID. 271.869

ANALISIS DE LA CAPACIDAD FINANCIERA

Balance cerrado al 31/12/11, 31/12/12 y al 31/12/13

EMPRESA: LOGICALIS PARAGUAY S.A.

Descripción	Cálculos			Total	Promedio	Ponderación: Cumple/No Cumple
	2.013	2.012	2.011			
Índice de liquidez						CUMPLE
Activo corriente	29.248.638.740	21.285.037.194	16.671.167.660			
Pasivo corriente	11.740.223.341	9.794.834.431	9.235.985.719			
Indice	2,49	2,17	1,81	6,47	**2,16**	
Endeudamiento						CUMPLE
Pasivo total	11.740.223.341	9.794.834.431	9.235.985.719			
Activo total	29.767.048.389	21.988.309.049	17.548.121.377			
Indice	0,39	0,45	0,53	1,37	**0,46**	
Rentabilidad						CUMPLE
Utilidad neta	5.805.239.183	3.847.506.511	2.983.160.444			
Capital	110.000.000	110.000.000	110.000.000			
Índice	52,77	34,98	27,12	114,87	**38,29**	

INTERPRETACIÓN

ÍNDICE DE LIQUIDEZ: El promedio de los últimos 3 años no puede ser menor a 1.-

ENDEUDAMIENTO: El promedio de los últimos 3 años no puede ser mayor a 0,80.-

RENTABILIDAD: El promedio de los últimos 3 años no debe ser negativo.-

María Liz Caballero
Representante de la Coordinación Financiera

Martha Riquelme Irún
Representante de la Coordinación Administrativa

Alberto Jara
Representante del Departamento de Contrataciones

Pedro Velázquez
Representante de la Dirección de TIC´s

ANEXO 5

LICITACIÓN PÚBLICA NACIONAL Nº 09/2014 "Adquisición de Equipos de Seguridad para el Datacenter de la Subsecretaría de Estado de Tributación del Ministerio de Hacienda" - ID. 271.869

VOLUMEN ANUAL DE NEGOCIOS

EMPRESA: TECHNOMA S.A.C.I.

Nº	Institución Contratante	Fecha	Documento Nº	Descripción del Servicio	Año 2011	Año 2012	Año 2013
					Monto	Monto	Monto
1	Bepsa del Paraguay SAECA	10/10/2011	Fact. 159	Provisión de Equipos	18.742.674		
2	Telefonía Celular del Paraguay SA	13/12/2013	Fact. 352	Provisión de Equipos			634.041.022
3	Mercopar SACI	01/10/2013	Fact. 135	Provisión de Equipos			6.635.078
4	Vision Banco SAECA	22/08/2013	Fact. 67	Provisión de Equipos			4.867.950
5	Electroban SAECA	27/08/2013	Fact. 69	Provisión de Equipos e implementación			22.543.143
6	Hidrovias del Paraguay SA	10/05/2013	Fact. 977	Provisión de Equipos			52.387.717
7	Procard SA	02/05/2013	Fact. 936	Provisión de Equipos			3.285.184
8	Banco Regional SAECA	02/01/2013	Contrato Technoma Cisco Smartcare Service	Provisión de Equipos conforme al Anexo II y III			1.490.452.689
				TOTALES	**18.742.674**	**0**	**2.214.212.785**
PROMEDIO DE LOS 3 ULTIMOS AÑOS					**744.318.486**		
MONTO REQUERIDO (20% del monto de la oferta presentada)					**326.748.600**		

María Liz Caballero
Representante de la Coordinación Financiera

Martha Riquelme Irún
Representante de la Coordinación Administrativa

Alberto Jara
Representante del Departamento de Contrataciones

Pedro Velázquez
Representante de la Dirección de TIC´s

MINISTERIO DE HACIENDA
SET
SUBSECRETARIA DE ESTADO DE TRIBUTACION

INFORME DE EVALUACIÓN Nº 30/2014

LICITACIÓN PÚBLICA NACIONAL Nº 09/2014 "ADQUISICIÓN DE EQUIPOS DE SEGURIDAD PARA EL DATACENTER DE LA SUBSECRETARÍA DE ESTADO DE TRIBUTACIÓN DEL MINISTERIO DE HACIENDA" ID Nº 271.869.

VOLUMEN ANUAL DE NEGOCIOS

LICITACIÓN PÚBLICA NACIONAL N° 09/2014 "Adquisición de Equipos de Seguridad para el Datacenter de la Subsecretaría de Estado de Tributación del Ministerio de Hacienda" - ID. 271.869

EMPRESA: LOGICALIS PARAGUAY S.A.

N°	Institución Contratante	Fecha	Documento N°	Descripción del Servicio	Año 2011	Año 2012	Año 2013
					Monto	Monto	Monto
1	BBVA Paraguay SA	20/02/2012	Fact. 4125	Provisión de Equipos		256.165.729	
2	Instituto de Previsión Social	26/01/2012	Fact. 4056	Provisión de Equipos		185.800.000	
3	Instituto de Previsión Social	29/02/2012	Fact. 4138	Provisión de Equipos		650.300.000	
4	Netlogic S.R.L.	04/12/2013	Fact. 202	Provisión de Equipos			131.311.618
				TOTALES	**0**	**1.092.265.729**	**131.311.618**
PROMEDIO DE LOS 3 ULTIMOS AÑOS					**407.859.116**		
MONTO REQUERIDO (20% del monto de la oferta presentada)					**312.000.000**		

María Liz Caballero
Representante de la Coordinación Financiera

Martha Riquelme Irún
Representante de la Coordinación Administrativa

Alberto Jara
Representante del Departamento de Contrataciones

Pedro Velázquez
Representante de la Dirección de TIC´s

ANEXO 6

Suministro de la documentación de Carácter Formal

DESCRIPCIÓN DE LA DOCUMENTACION	LOGICALIS PARAGUAY S.A.	TECHNOMA S.A.C.I.
Fotocopia simple de la cédula tributaria (constancia de inscripción en el Registro Único de Contribuyentes RUC) y de los Documentos de Identidad de los representantes o apoderados de la Sociedad.	**CUMPLE**	**CUMPLE**
Declaración Jurada en la que se garantice que el oferente no se encuentra involucrado en prácticas que violen derechos de los menores estipulados en la Constitución Nacional, los Convenios 138 y 182 de la Organización Internacional del Trabajo (OIT), el Código del Trabajo, Código de la Niñez y la Adolescencia, demás leyes y normativas vigentes en la República del Paraguay, conforme al formato aprobado por la Dirección Nacional de Contrataciones Públicas en la Resolución DNCP N° 941/2010.	**CUMPLE**	**CUMPLE**
Fotocopia autenticada de la declaración de IVA del último mes vencido y/o del Impuesto a la Renta o Certificado de Cumplimiento Tributario expedido en el mes anterior a la presentación de la oferta.	**CUMPLE**	**CUMPLE**
Autorización del fabricante conforme al formulario incluido en la Sección VI para importadores y distribuidores de los bienes ofrecidos	**CUMPLE**	**CUMPLE**
Copia de contratos ejecutados de provisión o facturaciones de venta, de bienes similares a lo propuesto, por montos o volúmenes similares del 20% del monto total ofertado en la presente licitación, en promedio de los tres (3) últimos años (2011/2012/2013).Podrán presentarse la cantidad de contratos y recepciones finales que fueren necesarios para acreditar el volumen o monto solicitado, siempre que hayan sido formalizados en el periodo mencionado.	**CUMPLE**	**CUMPLE**
Fotocopia autenticada del Balance General y Estado de Resultados, de los tres (3) ejercicios (2011, 2012 y 2013), conforme a la Resolución N° 173/2.004 del Ministerio de Hacienda acompañados de la Declaración Jurada del Impuesto a la Renta. En caso de firmas unipersonales se deberá presentar fotocopias debidamente autenticadas del Balance de Apertura de la empresa y de la patente comercial correspondiente al año que justifique la antigüedad requerida.	**CUMPLE**	**CUMPLE**
El oferente deberá presentar con su carta oferta las especificaciones técnicas de los bienes ofertados en carácter de **Declaración Jurada** debidamente llenada y firmada con los datos técnicos solicitados.	Presenta, no esta firmada por el Representante	Presenta, no esta firmada por el Representante
Patente Comercial.	**CUMPLE**	**CUMPLE**

Currículo del Personal Técnico, en la cual consten sus calificaciones, acompañados de los respectivos certificados emitidos por el fabricante.	**CUMPLE**	**CUMPLE**
Declaración Jurada, que todos los bienes y/o servicios ofertados son nuevos y es responsable de la calidad conforme a las especificaciones técnicas propuestas.	**CUMPLE**	**CUMPLE**
Declaración Jurada, que cuenta con la disponibilidad de los bienes y/o servicios para su entrega en el tiempo requerido por la Convocante.	**CUMPLE**	**CUMPLE**
Presentar el legajo de documentos foliados y rubricado	**CUMPLE**	**CUMPLE**
Copia de las Documentaciones suplementarias o adendas emitidas; si las hubieres.	**CUMPLE**	**CUMPLE**

GTC/a