CONTRATACIÓN DIRECTA Nº 05/2016
"ADQUSICION DE EQUIPOS DE SEGURIDAD PERIMETRAL DE RED DE LA DMH"
ID. 302.326

ADENDA Nº 03

La DINAC de conformidad al Art. 22, inc, "b" de la Ley Nº 2051/03 y el Art. 40 del Dto. 21909/03, y en uso de sus atribuciones, emite la siguiente Addenda, a fin de **modificar el Anexo B (punto 17 y 18) y el Anexo C Especificaciones Técnicas de los bienes o servicios a ser adquiridos de la Carta de Invitación.**

Anexo B

17 **.Para propósitos de la presentación de las ofertas: La dirección de la Convocante es: *DPTO. DE COMPRAS DIRECTAS/UOC Avda. Mcal. López e/ Vice Pdte. Sánchez y 22 de Setiembre – 3º Piso.***

De no contar con un mínimo de 3 (tres) ofertas vencido el plazo para la presentación de ofertas originalmente establecidas, la Convocante podrá realizar una prórroga de la presentación y apertura según lo estipulado en la Resolución DNCP Nº 805/09 y el artículo 34 de la Ley Nº 2051/03 "De Contrataciones Públicas.

Atención: *Diana Cabrera – Jefa del Dpto. de Compras Directas.*
Dirección: Avenida Mariscal López e/ 22 de Setiembre y Vicepresidente Sánchez.
Número del Piso/Oficina: 3º Piso, Edificio del Ministerio de Defensa Nacional.
Ciudad: Asunción, Paraguay
Código postal: 1752.
La fecha límite para presentar las ofertas es:
Fecha: 29 DE MARZO de 2016.
Hora: hasta las 08:30 a.m.

	FECHA	HORA
Fecha y Hora límite para la recepción de sobres establecida	**29/03/2016**	**08:30**
Fecha y Hora límite para la recepción de sobres modificada	**04/04/2016**	**08:30**

18 **La apertura de las ofertas tendrá lugar en: Dirección: *DPTO. DE COMPRAS DIRECTAS/UOC Avda. Mcal. López e/ Vice Pdte. Sánchez y 22 de Setiembre – 3º Piso.***

Número de Piso/Oficina: 3º Piso, Edificio del Ministerio de Defensa Nacional.
Ciudad: Asunción, Paraguay
Fecha: 29 DE MARZO de 2016
Hora: hasta las 09:00 a.m.

	FECHA	HORA
Fecha y Hora para la Apertura de sobres establecida	**29/03/2016**	**09:00**
Fecha y Hora para la Apertura de sobres modificada	**04/04/2016**	**09:00**

Abg. JULIAN PATIÑO
Coordinador
UOC - DINAC

Anexo C
Especificaciones técnicas de los bienes o servicios a ser adquiridos

ITEM	DESCRIPCION DEL BIEN			CANT.
1.	ROUTER / FIREWALL DE BORDE (SE REQUIERE PARA UN EQUIPO ACTIVO Y EN FUNCIONAMIENTO EN LA INSTITUCION)			1
	Características		MINIMO	
	GENERALIDADES	La función de este equipo será la de proteger le red. Para ello se requiere que cuente con funcionalidades de seguridad, análisis e inspección de contenido a nivel inclusive de las capas superiores. A fin de permitir una mayor participación de oferentes, serán aceptadas soluciones que distribuyan las diferentes funciones seguridad, en equipos separados, siempre y cuando la solución como conjunto cumpla con los requerimientos mínimos exigidos para este ítem.	EXIGIDO	
	RENDIMIENTO Y CAPACIDAD	Performance Firewall Troughput en paquetes de 1518 bytes	2.2 Gbps	
		Sesiones Concurrentes soportadas	2.500.000	
		Nuevas sesiones por segundo	15.000	
		Cantidad de Políticas de Seguridad	8.000	
	CONECTIVIDAD DE RED	Cantidad de puertos 10/100/1000Base-T – Configurables como WAN, LAN o DMZ	18	
		Cantidad de Slots Ópticos que soporten módulos SFP Gigabit	2	
	ROUTING	BGP	EXIGIDO	
		OSPF	EXIGIDO	
		RIP v1/v2	EXIGIDO	
		Soporte a ruteo de multicast	EXIGIDO	
		Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas	EXIGIDO	
		Soporte a políticas de ruteo (policy routing)	EXIGIDO	
		Soporte a ruteo dinámico RIPng, OSPFv3	EXIGIDO	
		Soporte de ECMP (Equal Cost Multi-Path)	EXIGIDO	
	AUTENTICACION DE USUARIOS Y CONTROL DE ACCESO	Capacidad de integrarse con Servidores de Autenticación RADIUS	EXIGIDO	
		Capacidad nativa de integrarse con directorios LDAP	EXIGIDO	
		Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.	EXIGIDO	
	TRADUCCION DE	NAT	EXIGIDO	

Abogado. JULIAN PATIÑO
COORDINADOR
UOC-DINAC

	DIRECCIONES	PAT	EXIGIDO	
		NAT estatico	EXIGIDO	
		NAT con PAT	EXIGIDO	
	ASIGNACION DE DIRECCIONES IP	Cliente DHCP	EXIGIDO	
		Servidor DHCP	EXIGIDO	
		DHCP Relay	EXIGIDO	
	CONMUTACION EN LAYER 2	Soporte de VLAN 802.1Q	512	
		Soporte de Link Aggregation Group (802.3ad) con un mínimo de 4 interfaces por grupo	EXIGIDO	
		Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs	EXIGIDO	
	ADMINISTRACION DE TRAFICO Y CALIDAD DE SERVICIO (QoS)	Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall	EXIGIDO	
		Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo	EXIGIDO	
		Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo	EXIGIDO	
		Capacidad para definir prioridad de tráfico, en al menos tres niveles de importancia	EXIGIDO	
		Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión	EXIGIDO	
		Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.	EXIGIDO	
	ALTA DISPONIBILIDAD	Soporte de Alta Disponibilidad en modo transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.	EXIGIDO	
		Soporte de Alta Disponibilidad en modo Activo-Activo	EXIGIDO	
		Soporte de Alta Disponibilidad en modo Activo-Pasivo	EXIGIDO	
		Posibilidad de definir al menos dos interfaces para sincronía para Alta Disponibilidad de forma a evitar el uso de Multicast en la red	EXIGIDO	
	CONTROL DE APLICACIONES	El equipo deberá poseer prestaciones de Control de Aplicaciones. *Esta funcionalidad deberá estar equipada y activa a la hora de la entrega del equipo. En caso de ser requerido licencias, las mismas deberán ser entregadas con el equipo con una vigencia de 12 meses.*	EXIGIDO	
		Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo	EXIGIDO	
		La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico	EXIGIDO	

Abg. JULIAN PATIÑO
Coordinador
UOC - DINAC

		Las solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante	EXIGIDO	
		El listado de aplicaciones debe actualizarse periódicamente	EXIGIDO	
		Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log	EXIGIDO	
		Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log	EXIGIDO	
		Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping	EXIGIDO	
		Preferentemente deben soportar mayor granularidad en las acciones	EXIGIDO	
	INSPECCION DE CONTENIDO – IDS/IPS	*Debera soportar funcionalidad de IDS/IPS, Esta funcionalidad deberá estar equipada y activa a la hora de la entrega del equipo. En caso de ser requerido licencias, las mismas deberán ser entregadas con el equipo con una vigencia de 12 meses.*	EXIGIDO	
		Performance Inspección IPS	800 Mbps	
		El Detector y preventor de intrusos deberá de estar orientado para la protección de redes	EXIGIDO	
		El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de linea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.	EXIGIDO	
		El detector y preventor de intrusos podrá implementarse en linea y fuera de linea en forma simultánea para distintos segmentos.	EXIGIDO	
		El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos.	EXIGIDO	
		Deberá soportar captar ataques por Anomalía (Anomaly detection).	EXIGIDO	
		Deberá soportar captar ataques basado en análisis de firmas en el flujo de datos en la red (signature based / misuse detection).	EXIGIDO	
		Deberá permitir configurar firmas nuevas para cualquier protocolo.	EXIGIDO	
		Deberá poseer una tecnología de detección tipo Stateful basada en Firmas (signatures).	EXIGIDO	
		Deberá soportar la actualización automática de firmas para el detector de intrusos (por 1 año)	EXIGIDO	
		El Detector de Intrusos deberá mitigar los efectos de	EXIGIDO	

Abg. JULIAN PATIÑO
Coordinador
UOC - DINAC

		los ataques de negación de servicios		
		Deberá contar con mecanismos de detección de ataques basados en Reconocimiento de patrones y Análisis de protocolos.	EXIGIDO	
		Deberá contar con mecanismos de deteccion de ataques basados en Detección de anomalías.	EXIGIDO	
		Deberá contar con mecanismos de deteccion de ataques basados en Detección de ataques de RPC (Remote procedure call)	EXIGIDO	
		Deberá contar con mecanismos de Protección contra ataques de Windows o NetBios	EXIGIDO	
		Deberá contar con mecanismos de Protección contra ataques de SMTP, IMAP o POP.	EXIGIDO	
		Deberá contar con mecanismos de Protección contra ataques DNS.	EXIGIDO	
		Deberá contar con mecanismos de Protección contra ataques a FTP, SSH y Telnet.	EXIGIDO	
		Deberá contar con mecanismos de Protección contra ataques de ICMP.	EXIGIDO	
		Deberá contar con Alarmas mostradas en la consola de administración del equipo.	EXIGIDO	
		Deberá contar con la capacidad de cuarentena. La misma debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto	EXIGIDO	
	INSPECCION DE CONTENIDO – FILTRADO DE URL	El equipo poseer prestaciones de Filtrado de Páginas Web (URL Filtering). *Esta funcionalidad deberá estar equipada y activa a la hora de la entrega del equipo. En caso de ser requerido licencias, las mismas deberán ser entregadas con el equipo con una vigencia de 12 meses.*	EXIGIDO	
		El equipo deberá poseer la capacidad de trabajar como un Proxy Cache	EXIGIDO	
		Capacidad mínima de almacenamiento interno.	30 GB	
		Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 39 millones de sitios web en la base de datos.	EXIGIDO	
		Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.	EXIGIDO	
		Configurable directamente desde la interfaz de administración del dispositivo. Con capacidad para	EXIGIDO	

Abg. JULIAN PATIÑO
Coordinador
UOC - DINAC

		permitir esta protección por política de control de acceso.		
		Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida	EXIGIDO	
		Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.	EXIGIDO	
		Capacidad de filtrado de scripts en páginas web (JAVA/Active X).	EXIGIDO	
	INSPECCION DE CONTENIDO – ANTISPAM	El equipo poseer prestaciones de Antispam. *Esta funcionalidad deberá estar equipada y activa a la hora de la entrega del equipo. En caso de ser requerido licencias, las mismas deberán ser entregadas con el equipo con una vigencia de 12 meses.*	EXIGIDO	
		La capacidad antispam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.	EXIGIDO	
		La capacidad AntiSpam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address)	EXIGIDO	
		La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM	EXIGIDO	
		En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.	EXIGIDO	
	ADMINISTRACION	Soporte de Interfaz CLI	EXIGIDO	
		Soporte de Interfaz WEB (HTTP y HTTPS)	EXIGIDO	
		Puerto serial dedicado para administración.	EXIGIDO	
		Comunicación cifrada y autenticada con username y password, tanto como para la interfase gráfica de usuario como la consola de administración de línea de	EXIGIDO	

Abg. JULIAN PATIÑO
Coordinador

		comandos (SSH o telnet)		
		Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.	EXIGIDO	
		El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS.	EXIGIDO	
		El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.	EXIGIDO	
		Soporte de SNMP versión 2	EXIGIDO	
		Soporte de servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos	EXIGIDO	
	CAPACITACION	La empresa ganadora deberá proveer un curso de capacitación básico con un mínimo de 25 horas de duración sin costo adicional a la entidad a mínimo 4 funcionarios.	EXIGIDO	
	ALIMENTACION ELECTRICA Y DIMENSIONES	Tensión de operación	Alterna, 220VCA	
		Deberá contar con la posibilidad de agregar una fuente de poder secundaria para redundancia.	EXIGIDO	
		MTBF Mínimo Requerido	90.000 Hs.	
		Montaje en rack de 19"	EXIGIDO	
		Garantía y Servicio		
	Garantía de fábrica	1 año de garantía expedida por el fabricante	EXIGIDO	
		El oferente deberá entregar, instalar y configurar el equipo de acuerdo a las indicaciones y a lo definido en las reuniones previas con el personal de la institución	EXIGIDO	
	INSTALACION, CONFIGURACION Y GARANTÍA	La empresa oferente deberá ser Partner autorizado de la marca ofertada, para tal efecto deberá contar con una carta donde el fabricante autorice a proveer, instalar y soportar los equipos adquiridos	EXIGIDO	
		El plazo de garantía será de 12 meses, se entiende por garantía el mantenimiento preventivo y correctivo del equipo en la modalidad 8x5 incluyendo el reemplazo del equipo en caso de fallas. Esta garantía deberá ser expedida por el fabricante del equipo.	EXIGIDO	
		El oferente deberá contar al menos con 5 años de experiencia en el mercado de las Telecomunicaciones	EXIGIDO	
		El oferente deberá contar con un plantel de no menos de 3 técnicos certificados por el fabricante, los mismos deberán pertenecer al plantel estable de la compañía con una antigüedad no menor a 3 años	EXIGIDO	
		El oferente se compromete a efectuar la implementación de la solución llave en mano encargándose de la interoperabilidad de esta solución con los equipos	EXIGIDO	

Abg. JULIAN PATIÑO
Coordinador
UOC-DINAC

		existentes en Meteorología.		
		El oferente deberá dar pleno cumplimiento a lo establecido en el aparado de ***"CONDICIONES GENERALES DE LOS SERVICIOS SOLICITADOS"*** en lo que refiere a cobertura de servicios.	EXIGIDO	

ITEM	DESCRIPCION DEL BIEN	
2	**RENOVACIÓN LICENCIA BUNDLE (ES UNA RENOVACION DE LICENCIA PARA EL EQUIPO FORTINET ACTUALMENTE EN FUNCIONAMIENTO)**	**1**
	MARCA	FORTINET
	MODELO	FORTIGATE 100D
	NRO DE SERIE	FG100D3G13820391
	NIVEL DE SOPORTE CON FABRICA	FORTICARE 8X5
	REEMPLAZO AVANZADO DE PARTES	8X5X365
	NIVEL DE SERVICIO DE FILTRADO DE SEGURIDAD: NGFW, AV, WEB FILTERING AND ANTISPAM SERVICES	UTM BUNDLE
	SKU – LICENCIA REQUERIDA	FC-10-00116-900-02-12
	VIGENCIA DE UN AÑO PARA LA LICENCIA DESDE LA ADJUDICACIÓN DEL CONTRATO	
	REGISTRO Y ACTIVACION DE LICENCIAS	EXIGIDO
	PERIODO DE VIGENCIA	12 MESES

CONDICIONES GENERALES DE LOS SERVICIOS SOLICITADOS

I. SOBRE LOS TÉCNICOS QUE PRESTARÁN SERVICIO:

"EXTENSIÓN DE GARANTIA DEL FIREWALL MTEOROLOGÍA".

1. La Dirección de Meteorología a través del Supervisor del Servicio aprobará los trabajos y/o servicios a ser efectuados; esto habilitará al Oferente a realizar el inicio del servicio.
2. Para el proceso de pago de las facturas se requiere del informe conjunto del Departamento de TI y del Supervisor del Servicio.
3. La contratada debe contar con un mínimo de 4 (Cuatro) técnicos para cubrir los servicios contratados
4. La contratada está obligada al uso de los formularios internos de la Institución para los servicios contratados. Pudiendo esta utilizar además sus propios formularios, en todos los casos los formularios validos son los internos del Ministerio; así como también deberán ceñirse a los procedimientos internos de la Institución.

II. PERIODOS DE EJECUCIÓN DE LOS SERVICIOS

El Servicio de verificación de Sistema Operativo y de Configuraciones será realizado dentro de los siguientes horarios:

1. Ordinario: período normal de actividades de Lunes a Viernes de 07:30 hs. a 17:00 hs.

III. SOBRE EL PERSONAL QUE PRESTARÁ EL SERVICIO

1. Documentación que acredite ser Canal Autorizado y Asistencia Técnica de la marca ofrecida.
2. La firma contratada deberá presentar Currículo Vitae del personal asignado para los servicios contratados.

Abg. JULIAN PATIÑO
Coordinador
DINAC

3. Meteorologia se reserva el derecho de aceptar al personal propuesto por la empresa Contratada; pudiendo solicitar el cambio de los mismos si estos no estuvieren llenando los requisitos de perfil técnico y responsabilidad correspondientes a criterio de la Dirección de Meteorología.

4. La firma contratada es responsable del desempeño, responsabilidad, experiencia e instrucción para el cumplimiento del servicio contratado, así como también del comportamiento, trato con el personal de la institución, etc.

5. El perfil técnico esperado de los técnicos es el siguiente, lo cual deberá ser demostrado con la documentación correspondiente

- La empresa oferente deberá contar con una antigüedad mínima de 3 años en el mercado brindando servicios según lo solicitado en el punto 1 "Experiencia Comprobable".

6. El plantel técnico debe residir del área metropolitana de la ciudad de Asunción.

CONDICIONES ESPECÍFICAS DEL SERVICIO SOLICITADO

I. OBJETIVO

Disponer de infraestructura tecnológica de Equipamiento de Comunicaciones componentes del Sistema de Comunicación de las Redes Locales de la DINAC con garantía vigente para así asegurar el buen funcionamiento de los servicios de conectividad brindados por el dispositivo

II. ACTIVIDADES DE CARÁCTER GENERAL

1) Garantías del Equipamiento y Servicio Técnico Especializado de

2) La Garantía deberá incluir una extensión de garantía por 1 (un) año que permita un remplazo avanzado de partes en 4 horas, a partir de la fecha y hora de la solicitud. Modalidad 8x5x365

3) Soporte web con Acceso registrado (Usuario y Password) para consultas de configuraciones y mejores prácticas.

III. FUNCIONES Y PRODUCTOS ESPERADOS

1) Extensión de garantía de hardware por 1 (un) año de los equipamientos enunciados que contemplará lo siguiente:

a. Soporte de atención de hardware

b. Repuestos y Mano de Obra

c. Traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del oferente.

d. El Proveedor deberá contar en su depósito con un equipo de las mismas prestaciones y características del existente (Para validar el fiel cumplimiento de lo requerido en el punto 2 del ítem anterior (.... Modalidad 8x5x365) el cual podrá ser verificado por la DINAC y cuyos datos deberán ser remitidos en la oferta

2) Servicio de verificación preventivo de hardware cada 6 meses, durante la vigencia de la extensión de la garantía de hardware solicitada.

3) El sistema operativo y demás funcionalidades deberán ser actualizadas en la última versión estable

IV. COORDINACIÓN Y SUPERVISIÓN

- Las tareas serán coordinadas por el TI de DINAC.

Se remite la presente Adenda, que consta de (09) hojas, a todas las empresas invitadas, la cual pasa a formar parte de la misma.

Abg. JULIAN PATIÑO
Coordinador
UOC - DINAC