REPUBLICA DE COLOMBIA

FONDO ROTATORIO DEL MINISTERIO DE RELACIONES EXTERIORES

SELECCIÓN ABREVIADA – SUBASTA INVERSA No. 011 DE 2012.

ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DE DOS (2) APPLIANCE PARA EL FILTRADO DE CONTENIDO PROXY DE LA NAVEGACIÓN A INTERNET, EN ALTA DISPONIBILIDAD CON DETECCIÓN DE AMENAZAS REALES Y PERSISTENTES PARA MÍNIMO 1.000 USUARIOS PARA EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO.

ADENDA No. 2

Fecha: 29 de Agosto de 2012

La Secretaria General del Ministerio de Relaciones Exteriores y representante legal del Fondo Rotatorio, en uso de las facultades legales y de conformidad con la Ley 80 de 1993, el Decreto 734 de 2012, y Ley 1474 de 2011, expide la siguiente Adenda, la cual forma parte integral del Pliego de Condiciones Definitivo de la Selección Abreviada – Subasta Inversa No. 011 de 2012.

1. Se modifica parcialmente el tercer inciso del subnumeral 5 del Anexo No. 2, Anexo Técnico Mínimo, Especificaciones Técnicas Mínimas Excluyentes, del Pliego de Condiciones Definitivo, el cual quedará así:

ANEXO No. 2
ANEXO TECNICO MINIMO
ESPECIFICACIONES TÉCNICAS MÍNIMAS EXCLUYENTES

Las siguientes son las especificaciones minimas técnicas que deben cumplir las propuestas para la ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DE DOS (2) APPLIANCE PARA EL FILTRADO DE CONTENIDO PROXY DE LA NAVEGACIÓN A INTERNET, EN ALTA DISPONIBILIDAD CON DETECCIÓN DE AMENAZAS REALES Y PERSISTENTES PARA MÍNIMO 1.000 USUARIOS PARA EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO, así:

Numeral	Ítem	Descripción
1	Appliance	Entregar 2 Appliance para el filtrado de contenido PROXY de la navegación a internet, en alta disponibilidad con detección de amenazas reales y persistentes para mínimo 1.000 usuarios que cumplan con las siguientes especificaciones:

Numeral	Ítem	Descripción
		1.1 Que Sea un proxy para HTTP, HTTPS, FTP, FTP sobre HTTP, SOCKS y NNTP, STREAMING.
		1.2 Que Posee tecnología de web caching para proveer mejoras adicionales en el desempeño de la red mediante el uso de contenido que sea reusable y de almacenamiento local.
		1.3 Que el modo de operación proxy transparente incluya soporte para usar WCCP (Web Cache Content Protocol) y PBR (Policy Based Routing), teniendo en cuenta que la Entidad ya posee la infraestructura de equipos de comunicación que soporta el protocolo WCCP
		1.4 Que el modo de operación proxy explicito incluye lo siguiente: configuración manual de browser y/o soporte para auto configuración del proxy mediante el uso de PAC, WPAC y políticas de Active Directory.
		1.5 Que soporten configuración de proxy en cadena para poder integrarse con arquitecturas de proxies existentes.
		1.6 Que provean autenticación selectiva utilizando diferentes tipos de autenticación que podrán ser usados de manera simultánea en un mismo ambiente. Los administradores podrán especificar ciertos usuarios para ser autenticados de manera transparente (no login) mientras que otros usuarios deberán autenticarse de manera manual (login required) de forma tal que se puedan usar y aplicar políticas apropiadas en ambientes donde se tengan PC compartidos, PC para uso del público y PC para uso de empleados corporativos.
		1.7 Que incluyen integración con servicios de Active Directory, NTLM, Novell eDirectoty (LDAP), Sun Java System Directory y cualquier otro tipo de directorio basado en LDAP.
		1.8 Que usen tecnología líder que permita desencriptación on-box de trafico HTTPS para inspección profunda de dicho tráfico y aplicación de políticas.
		1.9 Que incluyen aceleración basada en hardware para mejorar el rendimiento del sistema.
		1.10 Que permiten la administración de certificados digitales con el uso de una consola web desde donde también se debe permitir el uso de políticas globales y generación de reportes con el fin de disminuir las tareas administrativas.
		1.11 Que previenen ataques encriptados mediante la capacidad de realizar

Numeral	Ítem	Descripción
		desencriptación de SSL en el Gateway. El malware en un canal encriptado deberá ser identificado mediante diferentes técnicas de detección.
		1.12 Que proveen clasificación por categorías de filtro de contenido (Viajes, deportes, contenido adulto, entre otros) mediante la extracción de elementos (lenguaje natural, palabras clave, colores, fuentes, títulos, fondos) y clasificar este contenido en tiempo real usando máquinas de algoritmos propietarios del Appliance y base de datos de categorías propietaria del fabricante del Appliance.
		1.13 Que proveen análisis de seguridad en tiempo real con el fin de identificar y evitar que amenazas como spyware, phishing, malware, entre otros, lleguen a comprometer los usuarios del servicio de navegación y contar con la capacidad de extraer componentes activos (scripts, exploits, código binario, imágenes, entre otros) que se encuentren dentro del contenido web que pueda activar cualquier actividad malintencionada.
		1.14 Que Proveen alta exactitud en la clasificación de sitios web 2.0
		1.15 Que pueden categorizar dinámicamente sitios web emergentes o sitios web desconocidos con contenido malicioso.
		1.16 Que Detecten archivos embebidos y/o descargas por tipo de archivo o tamaño de archivo.
		1.17 Que cuenten con Capacidad de descomprimir, remover o hacer buffer de archivos de acuerdo con las políticas configuradas. Así mismo de bloquear aplicaciones para Windows maliciosas mediante el uso de Reconocimiento de Aplicaciones, Detección Avanzada de Aplicaciones y Análisis de Seguridad en Tiempo Real.
		1.18 Que la tecnología de Reconocimiento de Aplicaciones use firmas, hashes de aplicaciones y fingerprints para comparar contra una base de datos local antes de descargar archivos ejecutables; este análisis lo debe utilizar en tiempo real y también en sitios con contenido estático.
		1.19 Que cuente con Protección mediante el uso de XLM parsing content scanning
		1.20 Que cuente con al menos 35+ millones de URLs clasificadas dentro de no menos de 100 categorías diferentes dentro de una base de datos propietaria del fabricante.
		1.21 Que cuente al menos con 100 protocolos dentro de la base de datos de

Numeral	Ítem	Descripción
		protocolos.
		1.22 Que Realice actualizaciones diarias, con descargas incrementales con opción de actualizaciones dinámicas y desatendidas.
		1.23 Que cuente con categorías separadas para sitios web que afectan el tiempo de productividad de los empleados y sitios que afecta el ancho de banda del acceso a internet
		1.24 Que cuente con una categoría separada para Seguridad: Allí debe estar contenido sitios web que presentan amenazas como Spyware, MMC (Mobile Malicious Code), Phishing , entre otras amenazas que hayan sido identificadas por un laboratorio de seguridad propiedad del fabricante de las Appliance. Adicionalmente debe tener capacidad de controlar Bot's y protocolos Bot.
		1.25 Que de forma nativa ofrece DLP (Data Leak Prevention) para realizar escaneo sobre contenido saliente con el fin de prevenir pérdidas o fugas de información vitales para la organización.
		1.26 Que Previenen la pérdida de datos sobre los canales de comunicación HTTP, HTTPS (SSL) y FTP.
		1.27 Que cuente con más de 1200 clasificadores de datos que identifiquen números de tarjetas de crédito, números de seguridad social, y cientos de otros tipos de datos relevantes para requerimientos de cumplimientos. Evitando la necesidad de definir y afinar clasificadores usando herramientas de expresiones regulares.
		1.28 Que soporte mínimo dos asistentes para la creación de políticas y reportes predefinidos que automaticen las definiciones de políticas y buenas prácticas así como la creación de reportes de auditoria.
		1.29 Que soporten mínimo dos mecanismos de adquisición de firmas digitales para los documentos y datos confidenciales tales como: • Toma de firmas digitales de diferentes tipos de documentos. • Toma de firmas digitales de datos estructurados (bases de datos) a través de una conexión ODBC.
		1.30 Que soporte para cada incidente generado, almacenen la evidencia forense (archivos, textos, entre otros) y toda la información relevante y necesaria para realizar los seguimientos a que haya a lugar.

Numeral	Ítem	Descripción
		1.31 Que para nuevos sitios web que presenten amenazas de seguridad y que sean identificados por el laboratorio de seguridad, se envie actualizaciones en tiempo real hacia los Appliance de forma tal que se provea protección inmediata. Estas actualizaciones deben ser independientes a las que se realizan sobre la base de datos maestra donde se contienen todas las categorías.
		1.32 Que las actualizaciones de seguridad que se realizan en tiempo real, tengan capacidad de ser entregadas durante las 24 horas del día, a partir de la configuración de los Appliance.
		1.33 Que Provean protección contra amenazas mixtas web mitigando este tipo de amenazas que usan combinación de enlaces web para atacar a las organizaciones y sus empleados.
		1.34 Que Manejen y permitan controlar otros protocolos diferentes a Http, https, ftp, tales como: (IM,P2P, streaming media, entre otros)
		1.35 Que cuenten en su base de datos con al menos 15 protocolos P2P y 15 protocolos IM.
		1.36 Que actualicen su lista de protocolos de manera dinámica.
		1.37 Que tengan la capacidad de aplicar políticas basadas en protocolos.
		1.38 Que tengan la capacidad de asignar umbrales de ancho de banda para varias URL, categorías de URL, protocolos y categorías de protocolos.
		1.39 Que permitan aplicar políticas de ancho de banda para usuarios y grupos.
		1.40 Que Permitan aplicar políticas de ancho de banda por protocolos.
		1.41 Que Permitan aplicar políticas de ancho de banda para usuarios y grupos.
		1.42 Que permitan que se envíen notificaciones a los usuarios cuando sobrepasen los límites de ancho de banda configurados en las políticas.
		1.43 Que Soporten filtrado por tipo de archivo (keyword)
		1.44 Que administren el acceso por categoría del sitio web y por grupo de tipo de archivo (por ejemplo bloquear archivos de audio en sitios de deportes pero permitirlo en sitios de finanzas)

Numeral	Ítem	Descripción
		1.45 Que permitan actualizaciones automáticas para la base de datos que contiene los tipos de archivos.
		1.46 Que tengan la capacidad de bloquear archivos enviados/recibidos por IM.
		1.47 Que permitan aplicar políticas para transferencia de archivos por IM con base en usuarios, direcciones IP, segmentos de red o grupos de directorio.
		1.48 Que la Administración de las políticas para envío/recepción de archivos sea parte integral de los Appliance y sea configurada desde la consola central del producto.
		1.49 Que permita configurar reglas de filtrado por horas del día, días de la semana-horas de estos días.
		1.50 Que permita configurar reglas condicionales donde una vez se le presenta al usuario un mensaje de notificación este pueda seleccionar si desea acceder al sitio web o si desea abandonar el acceso solicitado.
		1.51 Que permita asignar cuotas de tiempo para navegación.
		1.52 Que cuente con "Yes Lists" donde el acceso a los sitios contenidos allí es de acceso libre para todos los usuarios del servicio de navegación.
		1.53 Que permita identificar de manera transparente a los usuarios que hacen uso del servicio y que pertenecen al directorio de autenticación y permita crear listas personalizadas de palabras claves.
		1.54 Que permita personalizar la página de bloqueo que se le presenta al usuario.
		1.55 Que soporte expresiones regulares.
		1.56 Que provea y soporte la aplicación de políticas de uso de internet para usuarios móviles y remotos de forma opcional.
		1.57 Que la administración de las políticas de uso de internet para usuarios móviles y remotos se realice desde la consola central de los Appliance.
		1.58 Que Provea y soporte la opción de un servicio de filtrado en la nube sin la necesidad de la instalación de agentes en los usuarios móviles o remotos.
		1.59 Que la consola de administración de estos servicios sea unificada, es decir, que ofrezca una sola consola desde la cual se pueden generar políticas y monitorear las actividades de los usuarios

Numeral	Ítem	Descripción
		1.60 Que provea la capacidad de distribuir las políticas desde una ubicación central hacia múltiples Appliance distribuidos por toda la entidad.
		1.61 Que tenga una consola Web para gestión, administración y generación de reportes.
		1.62 Que soporte múltiples clases de administradores, como mínimo debe tener los siguientes: Súper Administrador, Administrador Delegado, Administrador Remoto. Adicionalmente debe permitir la administración delegada de políticas y reportes.
		1.63 Que las actividades ejecutadas por los administradores sean auditables y dicha auditoria sea implementada.
		1.64 Que tenga la capacidad de manejar URLs embebidas (Paginas cache de Google, contenido Akamai, etc).
		1.65 Que tenga la capacidad de recategorizar websites de manera automática o por requerimientos de la entidad.
		1.66 Que cuente con una consola unificada basada en web desde la cual se pueda monitorear y controlar tanto las características de control Web y de proxy, usuarios remotos (por agentes y por filtro en la nube) como las características de prevención de pérdida de datos
		1.67 Que Cuente con reportes tipo drill down que se puedan generar y consultar desde la consola web. Estos reportes deben proveer datos históricos y deben tener al menos 80.
		1.68 Que Provea reportes MRTG para análisis detallado del tráfico de red.
		1.69 Que Provea información del desempeño del cache y de los recursos en uso
		1.70 Que cuenta con Capacidad de delegar la generación de reportes y de permitir que el delegatario tenga capacidad de generar los reportes para un grupo específico de usuarios.
		1.71 Que tenga la capacidad para poder generar excepciones tanto permitir o bloquear URLs específicas a usuarios grupos, direcciones IP, rangos de IPs o en forma global
		1.72 Que tenga la capacidad de Integracion a soluciones SIEM: con soporte a formatos Syslog/CEF (Arcsight), Syslog, LEEF [Q radar], Syslog/Key Value pairs (Splunk y otros) o personalizada escribiendo el formato

Numeral	Ítem	Descripción
		1.73 Que tenga la capacidad de bloquear y permitir trafico IPV6
		1.74 Que permita crear URLs personalizadas basadas en IPV6 para excepciones, recategorizar, bloquear o permitir sitios web identificados con direcciones IPV6
		1.75 Que permita agregar y asignar políticas a clientes identificados con una dirección IPv6 o rangos de direcciones IPV6
		1.76 Que soporte proxy transparente y proxy explicito.
2	Instalación	2.1 El proponente adjudicatario Instalará los 2 Appliance en esquema de alta disponibilidad activo-pasivo. Los Appliance serán instalados en el Data Center Principal del Ministerio en un rack existente, el cual cuenta con espacio suficiente para la instalación de los mismos. 2.2 El proponente adjudicatario, suministrará todos los componentes requeridos para la instalación y puesta en correcto funcionamiento de los 2 Appliance, tales como patch cord y cables de poder, entre otros.
3	configuración	3.1 El proponente adjudicatario configurará los Appliance teniendo en cuenta las mejores prácticas que el fabricante ofertado recomiende para garantizar el óptimo funcionamiento de todas las funcionalidades solicitadas en las especificaciones de los mismos, que permitan cumplir con las políticas de seguridad de la entidad. 3.2 El proponente adjudicatario configurará la licencia para mínimo 1000 usuarios 3.3 El proponente adjudicatario realizará el levantamiento de información para la elaboración del diseño de reglas a implementar en los Appliance. Este diseño debe ser avalado por el supervisor del contrato, para la entrega del diseño no pueden pasar más de 8 días calendario contados a partir de la firma de acta de inicio. 3.4 El proponente adjudicatario configurara en los Appliance las reglas aprobadas en el diseño. 3.5 El proponente adjudicatario configurara la consola de administración, en un servidor virtual con Windows 2008 estándar R2, suministrado por la entidad. 3.6 El proponente adjudicatario configurara los Appliance en modo proxy explícito. 3.7 El proponente adjudicatario configurara los Appliance para que se sincronicen con Microsoft Active Directory.

Numeral	Ítem	Descripción
		3.8 El proponente adjudicatario configurara en la consola como mínimo 5 reportes, que permitan verificar el correcto funcionamiento de las reglas implementadas. 3.9 El proponente adjudicatario configurara los Appliance para que se sincronicen con Microsoft Active Directory. 3.10 El proponente adjudicatario configurará los Appliance en esquema de alta disponibilidad y realizará las pruebas que permitan verificar el correcto funcionamiento.
4	puesta en marcha	4.1 El proponente adjudicatario realizará pruebas del correcto funcionamiento de los Appliance en producción con la totalidad de usuarios conectados y realizará los ajustes que se requieran implementar, en caso de presentarse alguna falla o retraso en la conexión a Internet. 4.2 El proponente adjudicatario realizará pruebas de hacking ético a los Appliance, que demuestren que las reglas de seguridad informática están bien configuradas. 4.3 El proponente adjudicatario se compromete a transferir conocimiento que incluya como mínimo los siguientes temas: • Configuración e instalación de los Appliance • Configuración de reglas • Administración de la Consola • Generación de reportes • Afinamiento de los Appliance La anterior transferencia debe ser impartida a 3 personas designadas por el Ministerio de Relaciones Exteriores mínimo de 20 horas que cubrirá todo el contenido, utilizando material o manuales del fabricante y será programada en conjunto con el supervisor del contrato, en una intensidad de 4 horas diarias, durante 5 días. 4.4 El proponente adjudicatario entregará todos los manuales de operación, configuración, y mantenimiento de los Appliance, en medio magnético, en idioma inglés o español. 4.5 El proponente adjudicatario se compromete a que todas las labores de desinstalación, configuración, instalación y puesta en funcionamiento, que impliquen negación de algún servicio informático, se realizarán en horario no hábil programados conjuntamente entre el proponente adjudicatario y la entidad. Estos tiempos podrán ser horas nocturnas, sábados o domingos, sin incurrir en costos adicionales para la Entidad.

Numeral	Ítem	Descripción
5	Garantía y soporte de todos los equipos ofrecidos	5.1 El proponente adjudicatario deberá ofrecer (3) años de garantía (incluido repuestos, mano de obra) a partir de la entrada de los Appliance en el almacén general de la Entidad, en esquema Onsite 7x4x24, con el fabricante, a través de ingenieros y técnicos certificados (mínimo uno) directamente del fabricante en los Appliance ofrecidos. Dichas garantías, deberán ser entregadas al supervisor del contrato que resulte del presente proceso de selección. El proponente adjudicatario deberá realizar 24 visitas durante 3 años de mantenimiento preventivo, las cuales se programarán en conjunto con el supervisor del contrato.

MARIA MARGARITA SALAS MEJÍA
Secretaria General.

Revisó y Aprobó: Diego Fernando Fonnegra. –Jefe Oficina Asesora Jurídica Interna.

Revisó y Aprobó: Ivett Lorena Sanabria Gaitán. – Coordinadora Grupo de Licitaciones y Contratos.

Revisó y aprobó: Martha Lucia Jiménez - Directora de Gestión y Tecnología.

Elaboró: Oscar Fabián Martínez C. – Asesor Grupo Licitaciones y Contratos.

GLC 514-137-112