ANEXO No. 2
ESPECIFICACIONES TECNICAS MINIMAS EXCLUYENTES

Numeral	CARACTERISTICAS	Mínimo Exigido por el F.M.R.E.	BLACK HAT ARCHETYPE
1	**Adquisición y mantenimiento por un (1) año de licencias de Herramienta antivirus para end point y servidores**	El proponente adjudicatario deberá suministrar Protección del antivirus a 1070 clientes, por el término de un (1) año que incluye: 1.1 Se deben brindar 1070 licencias de la última versión del antivirus para estaciones que debe estar disponible y soportada para estaciones XP, Windows 7, Windows Vista, o superior tanto para 32 bits como para 64 bits y para servidores con Windows 2003 o superior tanto en 32 bits como en 64 bits 1.2 Se deben brindar 1070 licencias de la última versión del antivirus La última versión del antivirus debe estar disponible y soportada para plataformas Linux Red Hat , Novell SUSE, EMC Callera y Netapp 1.3 Se deben brindar 1070 licencias de la última versión del antivirus para estaciones que debe estar disponible y soportada para plataformas OS. 1.4 El antivirus debe tener la capacidad de controlar los dispositivos extraíbles por lo menos unidades usb, cd/rw, dvd +- rw, unidades de disco, permitiéndoles ejecutar, leer o escribir. 1.5 Actualizaciones a nuevas versiones liberadas, actualización de motor de escaneo para la versión del antivirus de estaciones y servidores, soporte telefónico en español y por página Web con el fabricante. 1.6 La solución debe manejar actualizaciones incrementales tanto del servidor a la nube, como del servidor a los clientes sin que estás sobrepasen de 100K con el fin mantener un rendimiento óptimo de los canales de comunicación de la entidad. 1.7 El antivirus de las estaciones de trabajo, debe soportar Cisco Network Admisión Control (NAC) 1.8 Las solución antivirus debe tener la capacidad de blindar a través	OK F. 48 Y 49

		de parches virtuales y sin necesidad de modificar las integridad del sistema operativo y/o aplicaciones los problemas de seguridad relacionados con exploits. 1.9 La solución debe tener la Capacidad de detectar y bloquear paquetes "exploit" que atacan vulnerabilidades de aplicaciones como: File Sharing, Instant Messenger, Mail Client, Mapping Applications, Remote Login, SSL Client, Web Browser, Web Media, Winny P2P, backup Server, Database IBM, SQL, Adobe, Internet Explorer y MySQL. 1.10 La solución antivirus deberá examinar por vulnerabilidades los equipos donde esta esté instalada y deberá aplicar de forma automática las correcciones para que estas no puedan ser explotadas por ataques. 1.11 La solución antivirus deberá examinar por puertos abiertos los equipos donde esta esté instalada con el fin de enumerar e identificar posibles fallas de seguridad en el sistema operativo 1.12 El licenciamiento deberá ser por un (1) año contado a partir del 24 de diciembre de 2012. .	
2	**Actualización, configuración y puesta en correcto funcionamiento de la herramienta antivirus.**	El proponente adjudicatario deberá: 2.1 Actualizar la consola existente a la última versión liberada. 2.2 Distribuir actualizaciones de los agentes a los 1070 clientes solicitados incluidos los servidores. 2.3 El proponente deberá instalar en el Ministerio como mínimo un Honypot (software o hardware independiente de las consolas de administración) del mismo fabricante de la solución antivirus para end point, con el fin de detectar ataques por virus de red regionales 2.4 La solución debe ser capaz de bloquear las conexiones web a redes botnets reportar e identificar las mismas. 2.5 La solución debe ser capas e desplegar de forma remota un plug-in anti rootkit sin necesidad de interactuar con las estaciones de trabajo.	OK F. 49 Y 50
3	**Servicio por un (1) año de filtrado de antivirus y antispam en**	El proponente adjudicatario deberá suministrar 1.543 licencias por un año que soporte el servicio de filtrado de antivirus y antispam en la nube para el correo entrante y saliente y garantizar minimo lo	OK F. 50 Y 51

	la nube para el correo entrante y saliente	siguiente: 3.1 Consola de gestión y administración del servicio 3.2 Disponibilidad: 100% disponible 3.3 Gestión de correos en cuarentena 3.4 Cola de mensajes hasta por cinco (5) días para correo entrante 3.5 Reportes en tiempo real de correo entrante y saliente 3.6 SLA Network Uptime: 99.999% 3.7 SLA Entrega de Correo: menos de un (1) minuto (en condiciones normales de la red) 3.8 Bloqueo de virus: 100% de protección contra virus conocidos 3.9 Protección multi-motor Antivirus y AntiSpam (multi-engine) 3.10 Captura de SPAM: 99% del correo entrante 3.11 Reducción de falsos positivos: igual o menor al 0,0003% 3.12 Soporte multidominio para correo entrante 3.13 Soporte de políticas de filtrado por dominio 3.14 Protección contra URL sospechosas embebidas en los mensajes 3.15 Identificar spam en distintos idiomas 3.16 Protección contra phishing embebido en los mensajes 3.17 Permitir crear reglas de control de contenido tanto para la cabecera del correo, asunto, cuerpo y tipos de archivos adjuntos (por ejemplo, PDF y archivos de documento de Microsoft). 3.18 Contar con un módulo de reputación de IP, para realizar un control de Spam de remitentes conocidos. 3.19 La solución de escaneo en la nube, debe ser del mismo fabricante de la solución antivirus de End Point y de correo interno.	
4	**Configuración y puesta en correcto funcionamiento servicio de filtrado de antivirus y antispam en la nube para el correo**	El proponente adjudicatario deberá configurar la solución de filtrado para el correo de antivirus y antispam en la nube en correcto funcionamiento.	OK F. 51

	entrante y saliente		
5	**Adquisición y mantenimiento por un (1) año de licencias para herramienta de filtrado de antivirus, antispam y control de contenido sobre servidores de correo Exchange.**	El proponente adjudicatario deberá suministrar 1070 licencias de filtrado de antivirus, antispam y control de contenido sobre los buzones de los servidores de correo, por el término de un (1) año con las siguientes especificaciones técnicas: 5.1 La solución antivirus debe estar disponible para Microsoft Exchange Versión 2003 - 2010 y no debe ser instalada como un agente sobre el servidor de Exchange sino como una aplicación que se integre con el mismo. 5.2 El software ofertado debe permitir administración centralizada, reportes, actualización y cambios en la configuración en tiempo real. 5.3 La solución Antivirus debe estar disponible para Lotus Domino y no debe ser instalada como un agente sobre el servidor de Exchange sino como una aplicación que se integre con el mismo. 5.4 La solución antivirus debe estar disponible para Microsoft Exchange Versión 2003 - 2010 y no debe ser instalada como un agente sobre el servidor de Exchange sino como una aplicación que se integre con el mismo. 5.5 La solución debe estar soportado para plataformas Clúster de Microsoft. 5.6 La solución de escaneo de correo interno, debe ser del mismo fabricante de las solución antivirus de End Point y de correo en la nube.	OK F. 51 Y 52
6	**Instalación y configuración para herramienta de filtrado de antivirus, antispam y control de contenido sobre servidores de correo Exchange.**	El proponente adjudicatario deberá: 6.1 Instalar sobre los servidores de corro existentes la última versión liberada. 6.2 Configurar y poner a punto la solución según las necesidades del Ministerio de Relaciones Exteriores.	OK. F. 52
7	**Soporte técnico de**	El proponente adjudicatario deberá incluir en el soporte técnico:	

	los productos por el termino de vigencia de las licencias (1 año)	7.1 El proponente adjudicatario garantizará el servicio de soporte por el término de las licencias adquiridas en el presente proceso. El tiempo será contado a partir de la instalación de las licencias 7.2 El proponente adjudicatario deberá garantizar el soporte en las instalaciones de la Entidad, vía E-mail, telefónico ó Web. 7.2 El proponente adjudicatario garantizará que el soporte será 7x24. 7.3 El proponente adjudicatario garantizará los siguientes tiempos de atención y respuesta: 2 horas para responder a la solicitud inicial y máximo 4 horas para atención en sitio. 7.4 El proponente adjudicatario garantizará una (1) visita mensual en sitio, con el fin de realizar diagnósticos, revisiones técnicas, realizar correctivos y ajustes necesarios para el correcto funcionamiento de los productos adquiridos, para lo cual deberá entregar un informe de la labor realizada. 7.5 El proponente adjudicatario deberá informar a la entidad cual es el número del Centro de Recepción de Llamadas y los cambios que del mismo se presenten. 7.6 El proponente adjudicatario deberá realizar las actualizaciones en la consola adquirida cuando salgan nuevas versiones del producto. 7.7 El proponente adjudicatario es el responsable de la creación de reglas de seguridad de acuerdo a las necesidades de la entidad. 7.8 En caso de que se requiera soporte con el fabricante, el proponente adjudicatario garantizará el escalamiento al fabricante, en modalidad 7x24. **7.9** El proponente adjudicatario garantizará el soporte en todos los productos adquiridos, en el presente proceso.	OK F. 52 Y 53
8	**Entrega de licencias**	El proponente adjudicatario deberá hacer entrega del respectivo licenciamiento al supervisor del contrato e informar la dirección URL del fabricante para descargar lo siguiente: 8.1 El software de instalación del producto 8.2 Documentación del producto	OK F. 53
9	**Transferencia de conocimiento**	9.1 El proponente adjudicatario debe realizar la transferencia de conocimiento a cuatro (4) funcionarios del MINISTERIO DE RELACIONES EXTERIORES en la administración del antivirus ofertado mínimo de 16 horas.	OK F. 53 Y 54

		9.2 El proponente adjudicatario debe realizar la transferencia de conocimiento a cuatro (4) funcionarios del MINISTERIO DE RELACIONES EXTERIORES en el manejo del servicio en la nube, mínimo de 8 horas. 9.3 El proponente adjudicatario debe realizar la transferencia de conocimiento a cuatro (4) funcionarios del MINISTERIO DE RELACIONES EXTERIORES en el manejo del producto de filtrado sobre los servidores de correo, mínimo de 4 horas.	
10	**Personal técnico para el servicio de soporte.**	Para el servicio de soporte técnico el proponente adjudicatario deberá contar mínimo con dos (2) técnicos ó ingenieros especializados en productos y soluciones del producto ofertado para llevar a cabo esta labor. A efectos de dar cumplimiento al presente numeral, en el momento de realizar el acta de inicio del contrato, el proponente adjudicatario deberá presentar para cada uno de los ingenieros y/o técnicos la siguiente documentación: a) Hoja de vida del ingeniero y/o técnico presentado. b) Una certificación donde demuestre su experiencia no inferior a un (1) año en instalación, configuración, y soporte de los productos ofertados. c) Una certificación expedida por el fabricante, donde demuestre que el técnico y/o ingeniero es certificado en el producto ofertado.	OK. F. 54

OBSERVACIONES:

La firma Black Hat Archetype, cumple con las especificaciones técnicas requeridas.

VERIFICACION DOCUMENTOS DE CARÁCTER TECNICO

El proponente deberá acreditar que como mínimo ha celebrado en el último año anterior a la fecha del cierre del presente proceso de selección, contratos ejecutados cuyo objeto sea la adquisición y/o venta y/o distribución y/o comercialización y/o suministro de licencias de Antivirus, con su respectiva instalación. (Anexo No.3).

NÚMERO DE CONTRATOS A CERTIFICAR:

Mínimo: Uno (1) Máximo: Tres (3)

CUANTÍA REQUERIDA EN S.M.L.M.V PARA CADA CONTRATO: Cuya sumatoria de los contratos a certificar sea igual o superior al 50% del valor total del presupuesto oficial.

En caso de presentar certificaciones globales deberán desglosar el monto y objeto para el cual aplica dicha certificación. Cuando las certificaciones expresen su valor en dólares, se tendrá en cuenta la TRM a la fecha en que se celebró el contrato certificado.

Cada certificación de experiencia se analizará por separado, en caso de tratarse de contratos adicionales, el valor adicional se convertirá en salarios mínimos mensuales legales vigentes (SMMLV), a la fecha de firma del contrato adicional y se sumará al valor del contrato principal.

	BLACK HAT ARCHETYPE		
	Certificación 1 F. 60 y 61	**Certificación 2 F. 63 Y 64**	**Certificación 3 F. 66**
EMPRESA CONTRATISTA (responsable de la implementación)	**BLACK HAT ARCHETYPE**	**BLACK HAT ARCHETYPE**	**BLACK HAT ARCHETYPE**
FECHA DE EXPEDICIÓN DE LA CERTIFICACIÓN	30 de Julio de 2012	30 de Julio de 2012	28 de Noviembre de 2011
NOMBRE DEL CLIENTE	CONTACT CENTER AMERICAS S.A.	SALUD TOTAL EPS	FUERZA AEREA COLOMBIANA

	BLACK HAT ARCHETYPE		
	Certificación 1 F. 60 y 61	**Certificación 2 F. 63 Y 64**	**Certificación 3 F. 66**
OBJETO DEL CONTRATO Actualización, Adquisición e Instalación de equipos de seguridad, WIFI, Equipos de Red Activa para los centros de cableado y Migración al protocolo IPV6 FASE I.	Suministrar a Contact Center Américas la solución antivirus TREND MICRO para 3750 licencias de end point y servidores. Ubicadas en 4 consolas de administraci´on una en cada sede (sedes: Dorado, San Martin, Fontibón y Cali) integradas a una única consola central en la sede Dorado (Bogotá).	Renovar y suministrar nuevo licenciamiento de la solución antivirus Trend Micro para 4000 licencias referente a la ESS compuesta por las soluciones de filtrado y escaneo web perimetral IWSVA, de filtrado de correo y antispam perimetral IMSVA, de control de correo interno Scan Mail de control antivirus de las estaciones de trabajo OSCE, de control de antivirus de servidores Linux Server Protect y de generación de informes Control Manager para su sede central. De igual forma dar el soporte de la plataforma mediante un servicio 7x24 mediante una mesa de ayuda.	Mantenimiento y actualización de 3693 licencias de antivirus y 1000 licencias de SPAM prevention solution+Network AntiSPAM services de Antivirus para la Fuerza Aérea Colombiana.
NOMBRE DE QUIEN EXPIDE LA CERTIFICACIÓN	RICHARD SANABRIA	ERNESTO FUERTES SALAS	

	BLACK HAT ARCHETYPE		
	Certificación 1 F. 60 y 61	**Certificación 2 F. 63 Y 64**	**Certificación 3 F. 66**
FECHA DE INICIACIÓN DEL CONTRATO (Mes/Año)	28-JUNIO-2010	04-JUNIO-2010	25-ABRIL-2011
FECHA TERMINACIÓN DEL CONTRATO (Mes/Año)	28-JUNIO-2012	04-JUNIO-2012	15-DICIEMBRE-2011
VALOR DEL CONTRATO	$127.013.040	$222.174.600	$203.462.608
SMLMV	215	377	345
SUMATORIA SMLMV : 937			

OBSERVACIONES:

La Firma Black Hat Archetype, cumple con las certificaciones de experiencia solicitadas.

VERIFICACION DOCUMENTOS DE CARÁCTER TECNICO	*BLACK HAT ARCHETYPE*
3.3 CERTIFICACIÓNES DE DISTRIBUIDOR Y/O COMERCIALIZADOR AUTORIZADO DEL SOFTWARE El proponente deberá adjuntar con su propuesta la certificación de distribuidor autorizado del software, expedida por el fabricante Trend Micro, la cual deberá tener fecha de expedición no mayor a treinta (30) días calendario, contados a partir de la fecha del cierre del presente proceso. Dicha certificación deberá estar dirigida al Fondo Rotatorio del Ministerio de Relaciones Exteriores. En el evento que la (s) certificación (es) sea expedida por un distribuidor mayorista, se deberá anexar igualmente la certificación de distribuidor autorizado de este mayorista expedida por el fabricante. Cuando se trate de un consorcio o una unión temporal, cada uno de sus miembros deberá presentar dicha certificación.	*OK F. 58*

OBSERVACIONES:

La Firma Black Hat Archetype, cumple con la verificación de documentos de carácter técnico, por lo tanto está **HABILITADO** TECNICAMENTE.

Bogotá D. C. 09 de Diciembre de 2013

EVALUADOR TECNICO

ORIGINAL FIRMADO
LUCY PABÓN BENÍTEZ