Bogotá D.C., 04/06/2024

Señores
Proveedores interesados

Asunto: Solicitud de Información a Proveedores.

De manera respetuosa se publica la presente solicitud de información a proveedores con el fin de obtener su cotización, la cual servirá de base para la elaboración del estudio de mercado del futuro proceso contractual, que adelantará el Centro Nacional de Memoria Histórica, de acuerdo con la siguiente información:

1. Introducción

El Centro Nacional de Memoria Histórica (en adelante CNMH), del sector de inclusión social y reconciliación, inicia sus labores a partir de la expedición del Ley 1448 de 2011, artículos 146, 147 y 148 y estructurado mediante Decreto 4803 del 20 de diciembre de 2011.

Como establecimiento público de orden nacional con personería jurídica, patrimonio propio y autonomía administrativa y financiera, adscrito al Departamento Administrativo para la Prosperidad Social –DPS-, el CNMH tiene jurisdicción en todo el territorio nacional y tendrá como sede principal la ciudad de Bogotá, D. C. Para su operación el CNMH ha venido dotando las dependencias que lo conforman, de la infraestructura de tecnología, comunicaciones y soluciones informáticas que le apoyen en el desarrollo de sus funciones y actividades que por ley le han sido designadas.

El CNMH requiere adelantar un Estudio de Mercado que le permita establecer el comportamiento de los costos que, por los ítems más adelante detallados, presenta el mercado; para la gestión de los presupuestos que deben amparar las necesidades identificadas.

La presente solicitud de cotización no vincula jurídica ni contractualmente al CNMH. Se constituye como un requisito legal dentro del proceso de planeación contractual.

2. Objeto

Adquisición, puesta en marcha de una solución antivirus para protección de servidores y equipos de usuario final contra malware. Incluye protección de firewall de aplicaciones web (WAF) y correo electrónico integrada con el firewall XGS 3100, equipos activos WLAN y soporte durante la vigencia de la licencia.

Segmento		Familia		Clase		Producto	
Código		Código	Nombre	Código	Nombre	Código	Nombre
43000000	Difusión de Tecnologías de Información y Telecomunicaciones	4323000	Software.	43233200	Software de seguridad y protección.	43233205	Software de seguridad de transacciones y de protección contra virus.
43000000	Difusión de Tecnologías de Información y Telecomunicaciones	43220000	Equipos o plataformas y accesorios de redes multimedia o de voz y datos.	43222600	Equipo de Servicio de red.	43222640	Punto de acceso inalámbrico

3. ESPECIFICACIONES TÉCNICAS Y/O FICHA TÉCNICA DEL BIEN O SERVICIO A ADQUIRIR

La solución debe cumplir los requisitos de la Ficha Técnica, que se presenta en este documento y deben ser entregados en la sede del CNMH, ubicada en la carrera 7 # 32-42 Edificio San Martín - Torre Norte piso 31; implementación, configuración, puesta a punto en operación y capacitación para la gestión, soporte, mantenimiento, recomendaciones, con la documentación respectiva y garantías.

Descripción

El proponente deberá certificar a través de carta, expedida por el fabricante o por un proveedor autorizado por el fabricante, como distribuidor autorizado de la marca.

El proponente deberá indicar en la carta de presentación o en documento que contenga la información descrita en el citado formato, que ha leído, entiende, acepta y cumplirá todos los requerimientos técnicos mínimos establecidos en la “Ficha Técnica” que se presenta en el documento de sondeo de mercado.

Mantenimiento y soporte: mantenimiento preventivo y/o correctivo que se realizará a través de 24 visitas técnicas al año (mensuales), con asistencia en sitio por personal especializado en los productos WAF, protección de correo electrónico, antivirus y access point (AP) adquiridos. Deben corregirse todos los inconvenientes que se presenten en los productos adquiridos y que impidan su normal funcionamiento, trabajando en conjunto con funcionarios del CNMH, ya sea telefónicamente, por acceso remoto, o presencial, realizado por personal certificado. En caso que el CNMH requiera un apoyo en sitio para integración con otras soluciones de la infraestructura interna de la entidad se debe contar con el acompañamiento mínimo de un ingeniero en sitio.

Centro de Servicios y Gestión de Incidentes: el proponente debe contar con un centro de soporte que permita gestionar las peticiones, quejas o reclamos de tipo técnico bajo los estándares ISO 20000 y buenas prácticas

3. ESPECIFICACIONES TÉCNICAS Y/O FICHA TÉCNICA DEL BIEN O SERVICIO A ADQUIRIR

ITIL v.4. Un incidente debe tratarse como uno solo independientemente del canal utilizado para su instauración y seguimiento.

Para efectos de la propuesta, ninguno de los productos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el enlace público del fabricante que verifique que los productos propuestos no están en ese listado.

Los equipos deberán tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.

Se deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad tendrá la potestad de acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante.

Como parte de la propuesta, personal del fabricante y/o partner deberá realizar la implementación, configuración y puesta en operación aplicando las buenas prácticas de implementación. Además, deberá validar el nivel de adopción de buenas prácticas de configuración de los productos implementado en la Entidad; se deberá entregar un informe con las recomendaciones técnicas para mejorar la adopción de las mejores prácticas de seguridad de los productos adquiridos. Esta evaluación se deberá realizar dentro de los seis primeros meses posterior a la finalización de la implementación de los productos y previa coordinación entre la Entidad y el Postor.

Ficha Técnica Firewall de Aplicaciones Web (WAF)

El Centro Nacional de Memoria Histórica, está interesado en adquirir de una solución WAF que permita la protección de sitios web publicados en internet, contra cualquier tipo de software dañino, como malware (virus, troyanos, gusanos, adware, ransomware y spyware. Etc.…), mantenimiento y actualizaciones por parte del fabricante durante el tiempo de la licencia.
Se solicita que el nuevo licenciamiento de WAF entre en servicio desde el 29/11/2024 por uno y/o dos años.

Características Funcionales	Cumple SI/NO
Antivirus: Doble motor antivirus, bloqueo de contenido no escaneable, como archivos cifrados o corruptos.	SI
Threat Filters: motor de escaneo y patrones de ataque para filtrar amenazas comunes y ataques. Protección de ataques de aplicaciones Protección de ataques de inyección SQL Protección de ataques Protección contra scripts entre sitios Detección de escáner Opción de límite de tamaño de escaneo.	SI

3. ESPECIFICACIONES TÉCNICAS Y/O FICHA TÉCNICA DEL BIEN O SERVICIO A ADQUIRIR

Cookie Signing El balanceador de carga integrado distribuye visitantes entre múltiples servidores.	SI
URL Hardening: endurecimiento de URL estático, protege contra la reescritura de URL al firmar todas las URL en la página que está servido.	SI
Form Hardening: endurecimiento de formularios.	SI
Reputaringtion Filte: el filtrado de reputación de IP del remitente es la primera capa de protección contra spam, lo que le permite controlar los mensajes que llegan a través de la puerta de enlace.	SI
Web Server Authentication para autenticación basada en formularios y autenticación básica para acceso al servidor.	SI

Ficha Técnica Protección de Correo Electrónico

El Centro Nacional de Memoria Histórica, está interesado en adquirir una solución de protección de correo electrónico que permita la protección de 590 buzones, contra cualquier tipo de software dañino, como malware (virus, troyanos, gusanos, adware, ransomware y spyware. Etc.…), mantenimiento y actualizaciones por parte del fabricante durante el tiempo de la licencia.
Se solicita que el nuevo licenciamiento de protección de Correo electrónico entre en servicio desde el 29/11/2024 por uno y/o dos años.

Características Funcionales	**Cumple SI/NO**
Protección de Correo Electrónico	SI
Consola cloud	SI
Filtros antispam	SI
Escaneo de malware	SI
Cloud Sandbox	SI
Detección de URL maliciosas	SI
Reescritura de URL en el momento del clic	SI
Análisis de reputación	SI
Detección de anomalías del encabezado	SI
SPF	SI
DKIM	SI
DMARC	SI
Protección de Suplantación de Identidades	SI

3. ESPECIFICACIONES TÉCNICAS Y/O FICHA TÉCNICA DEL BIEN O SERVICIO A ADQUIRIR

Protección contra phishing por suplantación de identidad con procesamiento de lenguaje natural	SI
Análisis de nombres para mostrar (VIP y marcas)	SI
Verificaciones de dominios similares	SI
Prevención de Pérdidas de Datos	SI
Políticas DLP de múltiples reglas para grupos y usuarios individuales	SI
Listas de control de contenido (financieros, contenidos confidenciales, información de salud y PII)	SI
Cifrado TLS aplicado	SI
S/MIME	SI
Autenticación del remitente	SI
Cifrado de mensajes y archivos adjuntos basado en push	SI
Manejo de Mensajes	SI
Escaneo de mensajes entrantes	SI
Escaneo de mensajes salientes	SI
Bandeja de entrada de emergencia	SI
Políticas a nivel de dominio, grupo y usuario	SI
Cuarentena de administrador y usuario	SI
Listas de permisos/bloqueos de administradores y Usuarios	SI
Banners de correo electrónico entrante (remitente confiable, externo, no confiable)	SI
Sincronización de AD o sincronización de Azure AD	SI
redireccionamiento MX	SI

Ficha Técnica Solución Antivirus

El Centro Nacional de Memoria Histórica, está interesado en adquirir de una solución antivirus que permita la protección de servidores y equipo de usuario final contra cualquier tipo de software dañino, como malware (virus, troyanos, gusanos, adware, ransomware y spyware. Etc.…), mantenimiento y actualizaciones del software por parte del fabricante durante el tiempo de la licencia.
El licenciamiento actual rige hasta el 28/11/2024, se solicita que el nuevo licenciamiento de antivirus entre en servicio desde el 29/11/2024 por uno y/o dos años.

Características Funcionales	**Cumple SI/NO**
Prevención contra exploits:	

3. ESPECIFICACIONES TÉCNICAS Y/O FICHA TÉCNICA DEL BIEN O SERVICIO A ADQUIRIR	
Detección y prevención del mecanismo de identificación de propiedades de un sistema por parte de un exploit kit (técnica conocida como exploit kit fingerprinting) sin necesidad de utilizar firmas, patrones o heurísticas.	SI
Mitigación de vulnerabilidades conocidas, desconocidas y día cero.	SI
Identificación de ataques post-explotación:	
Identificación y prevención de intentos de escalar privilegios a nivel de Kernel. Esta protección debe de poder ser utilizada en agentes Windows, Mac y Linux.	SI
Prevención contra malware conocido:	
Capacidad de enviar los archivos clasificados como maliciosos a cuarentena, ya sea que hayan sido identificados al momento de intentar ejecutarse o al momento de ser identificados mediante un escaneo.	SI
Capacidad de enviar los archivos clasificados como maliciosos a cuarentena, ya sea que hayan sido identificados al momento de intentar ejecutarse o al momento de ser identificados mediante un escaneo.	SI
Debe contar con un módulo de prevención de ransomware, el cual debe evitar un proceso de encripción identificando intentos de modificación de archivos.	SI
Prevención de malware desconocido:	
Debe utilizar un modelo matemático generado a partir de aprendizaje de máquina para comparar una gran cantidad de características de un archivo ejecutable, de manera estática, para determinar si es malicioso. Esta protección debe estar disponible para sistemas operativos Windows, Linux y Mac.	SI
Escaneo de archivos ejecutables:	
Permite realizar el escaneo de archivos ejecutables sin la necesidad de firmas.	SI
Permite programar el escaneo de archivos de manera semanal o mensual.	SI
Permite programar el escaneo de archivos de manera semanal o mensual.	SI
Permite definir el día y la hora en la cual se iniciará el escaneo.	SI
Deberá de contar con un dashboard en nube que permite visualizar alertas generadas de distintas fuentes.	SI
Administración y revisión de eventos:	
Administración de políticas centralizado, vía una consola web.	SI
La consola puede clasificar los eventos en tres niveles de acuerdo a su severidad: bajo, medio y alto.	SI
La consola de administración identifica claramente los eventos que han sido reportados y/o bloqueados y aquellos que han sido detectados.	SI
Capacidad para clasificar el estado de los incidentes, alertas en cuatro distintos niveles de severidad: alto, mediano, bajo e informacional.	SI

3. ESPECIFICACIONES TÉCNICAS Y/O FICHA TÉCNICA DEL BIEN O SERVICIO A ADQUIRIR

Permite la actualización y desinstalación del agente a partir de la consola.	SI
Cuenta con integración con Active Directory para la gestión de computadoras y configuración de políticas.	SI
Cuenta con la capacidad de poder crear políticas basadas en los perfiles creados.	SI
Cuenta con la capacidad de poder aplicar políticas a usuarios, grupos, computadoras o unidades organizacionales de Active Directory.	SI
Características del agente:	
Windows 10 Pro (32-bit and 64-bit), Windows 10 Enterprise LTSB, Windows 10 Education, Windows 10 Update 1809, Windows 11 en todas sus versiones, Windows Server 2008 (32-bit, 64-bit; FIPS mode), Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode), Windows Server 2012 (todas las ediciones; FIPS mode), Windows Server 2012 R2 (todas las ediciones; FIPS mode), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016, Windows Server 2016 todas las versiones. Windows Server 2019 todas las versiones, Windows Server 2022 todas las versiones.	SI
OSX 10.10 (Yosemite), OSX 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.14.	SI
CentOS 6, CentOS 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16, Ubuntu Server 22.04.	SI
Soporte para los siguientes ambientes virtuales: VMware ESX, Citrix XenServer, Oracle Virtualbox, Microsoft Hyper-V.	SI
Gestión de usuarios:	
IT Admin. Cuenta con permisos para ver alertas, la gestión e instalación de agentes, las acciones realizadas en la consola, los perfiles, las políticas, el control de dispositivos y las excepciones globales. Puede instalar y gestionar agentes.	SI
Administrador de seguridad. Puede ver las políticas, perfiles, acciones tomadas en la consola, incidentes, alertas, reglas, gestión de agentes, excepciones globales y el control de dispositivos. Puede realizar ciertas acciones de configuración.	SI
Reportes:	
Permite la generación de reportes bajo demanda o programados.	SI
La frecuencia para la generación de los reportes programados podrá ser diaria, semanal o mensual.	SI

ITEM	DESCRIPCIÓN	CANTIDAD	CUMPLE SI/NO
1	Equipo de escritorio y portátil sobre S.O. Windows.	400	SI
2	Equipo de escritorio y portátil Sobre S.O. MAC.	13	SI
3	Servidores Físicos sobre Sistema Operativo Windows	10	SI

3. ESPECIFICACIONES TÉCNICAS Y/O FICHA TÉCNICA DEL BIEN O SERVICIO A ADQUIRIR

4	Servidores Físicos sobre Sistema Operativo Linux	5	SI
5	Servidores Virtualizados mediante Hiper-V con Sistema Operativo Windows	47	SI
6	Servidores Virtualizados mediante Hiper-V con Sistema Operativo Linux	25	SI
Total, Máquinas		500	

El Centro Nacional de Memoria Histórica, actualmente cuenta con una solución de red de área local inalámbrica (WLAN) Sophos, la cual requiere ser ampliada para dar cobertura completa a los pisos 30 y 31, por lo que se requiere adquirir APs que se integren al servicio WLAN actualmente en operación para su administración y gestión centralizada desde la consola Central, a continuación, se describen las características técnicas de rendimiento de los equipos WLAN a adquirir.

Ficha Técnica Access Point (WLAN) piso 30 y 31

Características Funcionales	**Cumple SI/NO**
WLAN Standards: 802.11 a/b/g/n/ac Wave 2	SI
Management: On-premises: Firewall Cloud: Consola Central. We recommend the Wi-Fi 6/6E AP6 Series for cloud management	SI
Radios: 1x 2.4 GHz single-band 1x 5 GHz single-band	SI
Antennas: 4x internal 2.4 GHz antenna for Radio-0 4x internal 5 GHz antenna for Radio-1	SI
Performance: 4 x 4:4 MU-MIMO	SI
Interfaces: 1x RJ45 connector console serial port 1x RJ45 10/100/1000 Ethernet port 1x RJ45 10/100/1000 Ethernet w/PoE	SI
Power (max.): 22.4W	SI
Power-overethernet (min.): PoE+ 802.3at	SI
Certifications and Compliance: CB, UL, CE, FCC, ISED (IC), RCM, Anatel, EN 60601-1-2 (Medical Equipment Directive) Plenum-rated (UL2043)	SI
Deployment: Indoor; desktop, wall, or ceiling mount	SI
Access Point requeridos cinco (5).	SI

Ficha Técnica Access Point Sala de Capacitaciones

Características Funcionales	**Cumple SI/NO**
WLAN Standards: 802.11 a/b/g/n/ac Wave 2	SI

3. ESPECIFICACIONES TÉCNICAS Y/O FICHA TÉCNICA DEL BIEN O SERVICIO A ADQUIRIR	
Management: On-premises: Firewall Cloud: Consola Central. We recommend the Wi-Fi 6/6E AP6 Series for cloud management	SI
Radios: 1x 2.4 GHz/5 GHz dual-band 1x 5 GHz single-band	SI
Antennas: 2x internal dual-band antenna for Radio-0 2x internal 5 GHz antenna for Radio-1	SI
Performance: 2 x 2:2 MU-MIMO	SI
Interfaces: 1x RJ45 connector console serial port 1x RJ45 10/100/1000 Ethernet port 1x RJ45 10/100/1000 Ethernet w/PoE	SI
Power (max.): 11.5W	SI
Power-overethernet (min.): PoE 802.3af	SI
Certifications and Compliance: CB, UL, CE, FCC, ISED (IC), RCM, Anatel, EN 60601-1-2 (Medical Equipment Directive) Plenum-rated (UL2043)	SI
Deployment: Indoor; desktop, wall, or ceiling mount	SI
Access Point requeridos dos (2).	SI

NOTA: DEBE ESPECIFICAR EN LA COTIZACIÓN SI CUMPLE CON TODOS LOS PARÁMETROS ESTABLECIDOS EN LA SOLICITUD DE COTIZACIÓN.

3. Descripción detallada de la oferta: (Para diligenciar por parte del proponente modificar según necesidades)

Ítem	Concepto	Descripción de lo ofrecido (*)
12	Access Point 2x2:2 MU-MIMO	**Sophos, 840E – Se adjunta ficha técnica**
13	Access Point 4x4:4 MU-MIMO	**Sophos, 420E - Se adjunta ficha técnica**

(*) Adjuntar los anexos que estime pertinentes. Detallar: Marca, Modelo y Referencia.

4. Aspectos a incluir en la oferta**:** (Para diligenciar por parte del oferente)

Concepto	Respuesta del Oferente

	Globaltek Security SAS 830.001.516-4 Dana Rodriguez Calle 26 No 69D-91 Oficina 406 3046824425 dana.rodriguez@globalteksecurity.com
Objeto social del oferente	
Forma de Pago	
Plazo de Entrega del contrato	
Régimen Tributario	
Validez de la Oferta (dd-mm-aa)	14/09/2024
Condiciones Comerciales: Garantía Otros	

OBSERVACIONES GENERALES

- Las cantidades adquirir pueden cambiar de acuerdo con la disponibilidad presupuestal, en el momento del estudio de mercado.
- Agradecemos la inclusión de plazo de vigencia de la cotización, la cual se sugiere no sea inferior a tres (03) meses calendario.
- El Valor de la cotización deberá tener en cuenta todos los gastos en los que incurriría por la suscripción, legalización y ejecución del contrato, como impuestos, constitución garantía única, transporte, operarios, etc., en caso de resultar adjudicatario.
- Se requiere que el IVA sea liquidado con dos (02) decimales, en caso de que sea aplicable el impuesto en mención, en el eventual caso de que no haya lugar a la aplicación del IVA, citar la respectiva norma.
- La cotización allegada debe venir debidamente firmada, con el número de identificación de la empresa y membretado.
- Cualquier observación o aclaración a la cotización, realizarla a vía electrónica.
- La cotización debe incluir el transporte hasta las instalaciones

5. Oferta económica: (Para diligenciar por parte del oferente)

Tabla 2. ***Oferta Económica***. ***Por 12 meses***

ITEM	DESCRIPCION	CANTIDAD	VALOR UNITARIO	IVA	VALOR TOTAL
1	Licenciamiento por suscripción. Suscripción – para Firewall de Aplicación Web (WAF), Suscripción por 1 año.	1	$5.200.000	$988.000	$6.188.000
2	Licenciamiento por suscripción para Protección de correo electrónico para 590 buzones de Google workspace por 1 año.	590	$90.000	$ 0	$53.100.000
3	Soporte, mantenimiento preventivo y/o correctivo que se realizará a través de 12 visitas técnicas (mensuales) mediante asistencia remota o en sitio por personal especializado en el producto Antivirus, WAF y equipos activos WLAN.	1	$3.950.000	$750.500	$4.700.500
4	Servicio de Implementación, configuración, puesta a punto en operación, capacitación, soporte y documentación.	1	$4.650.000	$883.500	$5.533.500
5	Antivirus / Antimalware (Software seguridad Servidor físico y virtual), para Sistema Operativo Windows Server.	57	$257.000	$ 0	$14.649.000
6	Antivirus / Antimalware (Software seguridad equipo final), para Sistema Operativo Windows.	300	$135.000	$ 0	$40.500.000
7	Antivirus / Antimalware (Software seguridad Servidores físico y virtual). Linux.	30	$257.000	$ 0	$7.710.000
8	Antivirus / Antimalware (Software seguridad equipo final). MAC	13	$135.000	$ 0	$1.755.000
9	Sesión de Formación o Capacitación para usuario técnico o administrador - hasta 5 Personas.	2	$1.600.000	$ 304.000	$3.808.000
10	Servicio de Soporte técnico durante tiempo de la licencia.	1	$3.500.000	$665.000	$4.165.000
11	Configuración y/o parametrización de la consola de administración Instalación, despliegue de licencia equipos server y cliente.	1	$2.600.000	$ 494.000	$ 3.094.000
12	Access Point 2x2:2 MU-MIMO	2	$ 3.200.000	$608.000	$ 7.616.000

13	Access Point 4x4:4 MU-MIMO	**5**	$ 6.060.000	$ 1.151.400	$36.057.000
				SUB-TOTAL	$177.514.000
				TOTAL, del IVA	$ 11.362.000
				TOTAL	$188.876.000

El suscrito Representante Legal hace constar que los precios cotizados corresponden al comportamiento del mercado actual, son precisos, veraces y reales.

6. Plazo para presentación de la oferta:
Fecha: 14/06/2024
Hora: 5 p.m.

7. Lugar de presentación de la oferta:
Mediante respuesta al correo electrónico de invitación a cotizar jose.torres@cnmh.gov.co y secop II.

8. Contacto en el CNMH:
Dependencia y Servidor Público Responsable del Proceso: Dirección Administrativa y Financiera Gestión - TIC
Nombres: Fabio Arnulfo Velandia Quecán, Ronal Alexis Martínez Cerón, José Miguel Torres Bojaca
Correos electrónicos: fabio.velandia@cnmh.gov.co, ronal.martínez@cnmh.gov.co, jose.torres@cnmh.gov.co
Teléfonos y ext.: (57) 601-7965060 Ext: 159, 103