MINISTERIO DE CULTURA

GOBIERNO DE EL SALVADOR

GOBIERNO DE EL SALVADOR

UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL (UACI)

ORDEN DE COMPRA PARA OBRAS, BIENES Y SERVICIOS

LUGAR Y FECHA:	Alameda Juan Pablo II, Calle Guadalupe Edificio A-5, Plan Maestro, Centro de Gobierno, 19 de noviembre de 2019.	ORDEN No.: OC/GOES144/2019
REFERENCIA	"SUMINISTRO DE LICENCIAS DE ANTIVIRUS PARA EL DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS"	
RAZÓN SOCIAL DEL SUMINISTRANTE		NIT
COMUNICACIONES IBW EL SALVADOR, S.A. DE C.V.		[redacted]

No.	CÓDIGO ONU	CÓDIGO PRESUPUESTARIO	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN TÉCNICA	PRECIO UNITARIO (CON IVA)	VALOR TOTAL (CON IVA)
1	82110000	61403	550	Unidad	ESET Endpoint Protection Advanced (Eset Endpoint Security + File Security), **(Según anexo).**	$ 16.81	$ 9,245.50
					MONTO TOTAL (CON IVA)		**$ 9,245.50**

MONTO TOTAL EN LETRAS: NUEVE MIL DOSCIENTOS CUARENTA Y CINCO 50/100 DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA.

JUSTIFICACIÓN: Para mantener libre de amenazas la infraestructura de red del Ministerio de Cultura, se necesita adquirir un software capaz de identificar, analizar y eliminar las contaminaciones de los archivos que se envían y reciben a través de internet hacia los usuarios finales y revisión de los archivos; así como administrar desde una consola de antivirus, el control, monitoreo de amenazas por usuario.

FINANCIAMIENTO: FONDOS-GOES

GARANTIA: El suministrante se compromete a presentar por escrito **UNA GARANTÍA DE BUEN SERVICIO, FUNCIONAMIENTO Y CALIDAD DE BIENES** a favor del **MINISTERIO DE CULTURA,** con una vigencia de un año, a ser entregada en UACI un día despues de firmada el acta de recepción.	**TIEMPO DE ENTREGA:** 15 días calendario, los cuales iniciarán el día hábil posterior a la fecha que El Suministrante reciba copia de la Orden de Compra autorizada.	**FORMA DE PAGO:** Un sólo pago con crédito a 60 días calendario.

LUGAR DE ENTREGA: Los suministros objeto de esta contratación serán entregados en el Departamento de Informática y Sistemas, Ubicado en Plan Maestro del Centro de Gobierno, Alameda Juan Pablo II, Calle Guadalupe, Edificio A-5, Tercera Planta, San Salvador.

DOCUMENTOS DE COBRO: El Suministrante para la emisión del quedan, deberá presentar en los 5 días hábiles siguientes a la recepción del suministro, Factura de Consumidor Final (duplicado-cliente), a nombre del **MINISTERIO DE CULTURA. NIT 0614-170118-113-6,** junto con la respectiva Acta de recibido de conformidad y copia de la nota de garantía.

ADMINISTRADOR DE ORDEN DE COMPRA: Con base a las facultades que otorga el Acuerdo Nº 0037/2019, emitido por El Ministerio de Cultura, en fecha veintiuno del mes de junio de dos mil diecinueve, se nombra como administrador de esta Orden de Compra al: **Ing. Giovanni Vladimir Cartagena Cruz-Técnico de Informática-Departamento de Informática y Sistemas del Ministerio de Cultura.**

DOCUMENTOS. Forman parte de esta Orden: a)Solicitud de Obra, Bien y Servicio, b)Solicitud de Disponibilidad, c)Términos de Referencia, d)Ofertas de las empresas, e)Cuadro Comparativo (si aplica), f)Opinión Técnica de la Unidad Solicitante (si aplica), g)Resolución de Adjudicación, Resolución Razonada (si aplica), h) Garantía (si aplica), i)Anexos (si aplica).

MODIFICACIÓN UNILATERAL. Queda convenido por ambas partes que cuando el interés público lo hiciera necesario, sea por necesidades nuevas, causas imprevistas u otras circunstancias, El Ministerio de Cultura podrá modificar de forma unilateral la presente Orden, emitiendo al efecto la Resolución correspondiente, la cual formará parte integral de esta Orden.

TOMAR EN CUENTA LAS SIGUIENTES INDICACIONES:

1º Antes de enviar los suministros al lugar de entrega favor comunicarse con el Administrador de la Orden, al teléfono: **2501-4414** con el objeto de coordinar la entrega.

2º El Ministerio de Cultura no se hace responsable por documentos que no se presenten a cobro transcurridos dos semanas después de haberse recibido los suministros de conformidad.

3º Si el suministrante incumpliere en cualquiera de las condiciones de esta orden, se aplicara el artículo 85 de la LACAP.

DESIGNADO

Vo. Bo. JEFE - UACI

SUMINISTRANTE

ELABORADO POR: DINORAH ORELLANA

FORMULARIO AUTORIZADO PARA LA LIBRE GESTIÓN POR UACI

22/11/2019

Luis Pacheco

COMUNICACIONES IBW, EL SALVADOR, S.A. DE C.V.
Antiguo Cuscatlán
EL SALVADOR, C.A.

ANEXO A LA ORDEN No. OC/GOES144/2019

1° **OBJETO.** El Suministrante **COMUNICACIONES IBW EL SALVADOR, S.A. DE C.V.,** se compromete a realizar el **"SUMINISTRO DE LICENCIAS DE ANTIVIRUS PARA EL DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS"; S/251/2019,** de acuerdo a los Términos de Referencia y la oferta del Suministrante, según detalle:

2° **PLAN DE OFERTA ECONÓMICA:**

CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN TÉCNICA	PRECIO UNITARIO (CON IVA)	VALOR TOTAL (CON IVA)
550	Unidad	ESET Endpoint Protection Advanced (Eset Endpoint Security + File Security)	$ 16.81	$ 9,245.50
				$ 9,245.50

3° **DETALLE:**

La empresa se compromete por su cuenta y riesgo a realizar el servicio según el siguiente detalle:

No.	PLAN DE OFERTA TÉCNICA
1	Que la misma versión del Producto, pueda instalarse y configurarse tanto en Computadoras Personales (PC's), portátiles y servidores.
2	Que sea compatible con las diferentes versiones de Sistemas Operativos Microsoft Windows con soporte para plataformas 32 bits y 64 bits.
3	Incluya protección de correo para servidores Linux, Zimbra 8.7, Ubuntu 16, análisis de correo entrante y saliente.
4	Que tenga protección en tiempo real contra cualquier tipo de código malicioso y habilite protección a nivel Kernel.
5	Que incorpore control de acceso a dispositivos USB y unidades ópticas CD/DVD.
6	Que incorpore capacidad para generar CDs y/o USB Booteables, los cuales posean capacidad de análisis con el producto para la inspección de malware en máquinas que no cuenten con la protección del mismo o requieran del uso de los mismos, así mismo dichos medios deben poder ser actualizados una vez se encuentren compilados o en uso (memoria residente).
7	Incorpore chequeo y control de Hotfix de Microsoft Windows, dicho control debe ser capaz de ser configurado para reportar diferentes niveles de actualización o desactivar el informe de las mismas.
8	Que pueda detectar, bloquear y eliminar cualquier tipo de Malware; incluyendo virus, gusanos, troyanos, spyware, phishing, rootkit, adware, riskware, keyloggers y otros códigos maliciosos nuevos y desconocidos. Principalmente, que lo anterior NO dependa de que el Sistema Operativo cliente tenga las actualizaciones y Service Pack al día.
9	Funcionalmente utilice un único motor que no requiera la instalación de ningún plugin adicional o agente para su operación, tanto para computadoras personales como para servidores.
10	Que integre posibilidad de explorar tráfico cifrado vía SSL en POP3 y HTTP.
11	Que pueda proteger contra virus boot, virus macros, virus residentes en RAM, virus de acción directa, virus encriptados, virus polimórficos, virus de FAT, etc.
12	Que pueda realizar búsquedas, detección y eliminación de virus en memorias de almacenamiento USB; así como búsquedas y detección en unidades de CD's y DVD's (aunque en éstos, lógicamente, no pueda eliminarlos).
13	Que incorpore motor heurístico proactivo y preciso de tecnología avanzada.
14	Que pueda detectar, prevenir y eliminar el ingreso de código potencialmente malicioso tipo JAVA, Activex y VBScript.

15	Que pueda detectar virus en archivos compactados, sin importar el número de niveles de compresión, en los siguientes formatos: zip, rar, arj,cab,lhz,tar,ace,izh,upx y otros
16	Que pueda soportar el escaneo y limpieza de paquetes en tráfico HTTP, FTP, SMTP y POP3; tanto en los servidores como en las computadoras personales.
17	Firewall personal a nivel de cliente, administrable de manera local o desde la consola de administración remota.
18	Que permita importar o exportar configuraciones de clientes de manera fácil, vía archivos xml livianos y transportables.
19	Que pueda tener la capacidad de poder enviar a los centros de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad de que puedan ser analizados y clasificados para su contingencia inmediata.
20	Que pueda tener la capacidad de generar un caso de soporte, vía interfaz gráfica sin necesidad de módulos adicionales para su operación.
21	Que cuente con Consola de Administración que pueda instalarse como servidor antivirus en las diferentes versiones de sistemas operativos windows, tanto clientes como server, la cual permita administrar centralizadamente los clientes antivirus y soporte el protocolo snmp.
22	Que el servidor antivirus no requiera IIS, Apache o similar para el correcto funcionamiento de la consola antivirus.
23	Que el servidor central de administración (consola/servidor) no requiera Microsoft Message Queue como requisito para instalación.
24	Que servidor central de administración (consola/servidor) sea compatible a nivel de almacenamiento de registros (logs) en base de datos con MySql.
25	Que permita la instalación de múltiples servidores, consolas; de tal forma que facilite la administración centralizada.
26	Que permita la instalación remota desatendida desde su consola de administración, no importando si esta se realiza en dominio o en grupos de trabajo.
27	Que permita la instalación del producto de manera local, con una configuración previamente definida y sin que se requiera configuración manual; tanto para computadoras personales en red o fuera de ella.
28	Que permita la ejecución de tareas de configuración, actualización y/o exploración "Bajo Demanda", desde su consola de administración.
29	Que permita que las actualizaciones diarias de los componentes del producto se realicen en tiempo real desde internet o vía LAN Server, en forma automática y sin necesidad de intervención del usuario.
30	Que las actualizaciones sean pequeñas e incrementales tanto para las estaciones como para los repositorios de firmas.
31	Que un cliente instalado pueda convertirse en repositorio de actualizaciones, para poder actualizar otros clientes desde él o poder extraer los archivos de actualización y trasladarlos manualmente a otros clientes "stand-alone"; no debería requerir la instalación de módulos adicionales para tales fines.
32	Que permita actualizar de forma manual todos sus componentes y definiciones de virus, en computadoras sin ningún tipo de conectividad a red: es decir, en status "stand-alone".
33	Que permita que su Consola de Administración posea su propio gestor de base de datos y requiera licencias adicionales en el servidor de administración o cualquier computadora personal dentro o fuera de la red LAN.
34	Que permita que su Consola de administración tenga la opción de ver automáticamente los resultados de los procesos realizados, por medio del escaneos "bajo demanda" de cada uno de los clientes en los que se realizaron dichos procesos.
35	Que permita que su Consola de Administración visualice automáticamente las amenazas que se han presentado en cada uno de los clientes, el nombre del archivo donde fue detectado y la acción que el producto tomó para anular la amenaza. Que pemita generar un reporte al respecto.
36	Que permita desde la Consola de Administración el bloqueo, a través de contraseña, de las opciones de configuración de los clientes.
37	Administración del bloqueo, a través de contraseña, de las opciones de configuración en los clientes, las mismas quedaron disponibles al momento de ingresar dicha contraseña localmente en los clientes.

38	Que la configuración establecida para un determinado cliente pueda ser exportada, tanto desde la consola de administración, como desde el mismo cliente, para poder ser importada en otros clientes necesarios.
39	Que su Consola de Administración no requiera la existencia de un Dominio de Red para su buen funcionamiento, pero que si permita administrar clientes antivirus en distinos grupos de trabajo o multidominios ya existentes.
40	Que su Consola de Administración pueda manejar múltiples tipos de Licencias de Software, en diferentes cantidades de equipo y fechas de expiración de las mismas.
41	Que su Consola de administración permita la generación de informes detallados tales como: clientes con mayor porcentaje de alertas, comparativas de alertas(diarias, mensuales y anuales), porcentaje de alertas de las respectivas amenazas, amenazas con mayor intento de incidencia y otros.
42	Que la consola de administración no requiera el uso de MMC (Microsoft management console) para el funcionamiento de la misma.
43	Que el Producto, una vez instalado y configurado en los clientes, no requiera agentes adicionales para integrarse a la consola de administración; de tal forma que se administre de forma transparente.
44	Que el producto posea certificaciones CheckMark e ICSA Labs (incluir certificaciones)
45	Que cuente con soporte local del fabricante y este pueda prestar el servicio de soporte técnico en formato 24X7X365; ya sea que se realice por medio de teléfono, correo, chat en línea o soporte remoto.

4º CAPACITACIÓN Y ACTIVACIÓN DE LAS LICENCIAS

El suministrante se compromete hacer la activación de licencias en 5 días posteriores a la entrega de la orden de compra; y la capacitación será 3 jornadas para el uso de las licencias de antivirus.

CONFORME.

LIC. JOSÉ NAPOLÉON ZEPEDA CARÍAS
DIRECTOR ADMINISTRATIVO

COMUNICACIONES IBW EL SALVADOR, S.A. DE C.V.
SUMINISTRANTE