INSTITUTO NACIONAL DE LA VIVIENDA

Ficha Técnica / Relación de Artículos Requeridos

ITEM	DESCRIPCION	CANTIDAD
1	Licencias Anti Ransomware subscription for 1 year	251
2	Enterprise Software Subscription & Standard Sup soporte empresarial directo del fabricante por 1 año	1
3	Management predefined 1000 endpoints	1
4	Servicios Soluciones, servicio de implementación solución y transferencia de conocimiento con un entrenamiento para 2 personas de la solución.	1

REQUISITOS:

#	COMPONENTE	ESPECIFICACIONES SOLICITADAS
1	Cantidad de software para Dispositivo Terminal (EndPoint) con soporte para sistema operativo Windows 7,8 y 10	Total Doscientos Cincuenta (251)
2	Marca	Especificar
3	Modelo	Especificar
		El módulo de seguridad para dispositivos de usuarios finales debe incluir. - Firewall - Compliance - Control de Aplicaciones - VPN - Encriptación de Disco - Protección de puertos y cifrado de Medio extraíbles

#	COMPONENTE	ESPECIFICACIONES SOLICITADAS
		- Antivirus - Antibot - Emulación de Archivos - Limpieza de documentos - Antiphishing - AntiRansomware - Análisis Forence Solución de antimalware debe proteger las tres fases de un ataque: explotación, mitigación, remediación
4	Firewall Personal	- Solución debe proporcionar la capacidad de implementar políticas de firewall sobre el EndPoint y gestionar de centralizadas controlando trafico entrante y saliente - Solución debe permitir la creación de zonas de seguridad, (Internet y redes confiables), con diferentes permisos controlado accesos no autorizados.
5	Control de Aplicaciones	- Debe permitir el control de aplicaciones por-política o de forma global,

		- La solución debe controlar que procesos y aplicaciones tienen acceso a los recurso: de red, para el tráfico entrante y saliente, Internet y zonas de confianza. Dicho contro no debe depender de la decisión del usuario final;
		- La solución debe permitir configurar reglas de acceso detalladas para programas individuales.

#	COMPONENTE	ESPECIFICACIONES SOLICITADAS
		- Los usuarios administradores deben tener la opción de terminar un proceso potencialmente peligroso.
		-La solución debe permitir personalizar listas negras y blancas de aplicaciones.
6	VPN	- La VPN IPSec debe estar disponible dentro del módulo de EndPoint. -Debe permitir la reconexión automática en caso de pérdida de conexión y / o el cambio de interfaz (por ejemplo .de LAN a Wireless a 3G). -Debe ser compatible con la detección automática de la configuración, tales como NAT Transversal y Modo Oficina. -Debe ofrecer una interfaz para el registro hotspot sin la necesidad de abrir una ventan del navegador. -Debe soportar Autenticación de multiple factor
8	Protección de Puertos y Cifrado de medios externos de almacenamiento	- La solución debe controlar y prevenir el acceso no autorizado de archivos / cambios de privilegios o permisos tanto en medios extraíbles y discos duros, con administración y reportes centralizados.
		- La solución debe controlar la entrada y salida en todos los puertos de conexión, específicamente: o USB, unidades DVD/CD-ROM; Modems; Printers, USB Controllers; o Bluetoot, Bluetooth USB, Still Image Devices (e.g.: Digital Cameras), Infrared Devices; Smart Card Readers; PCMCIA Memory; o Adaptadores de red, tanto cableados como inalámbricos. - Debe permitir integración de forma transparente con Windows Active Directory;
		- Permitir el uso de medios cifrados en cualquier ordenador, independientemente de tener la solución instalada o no, después de una autenticación mediante contraseña. - Solución debe proveer de capacidad de cifrar ciertos archivos y / o carpetas dentro de medios extraíbles

#	COMPONENTE	ESPECIFICACIONES SOLICITADAS
		- La solución debe ser compatible con listas blancas y listas negras para control de medio: extraíbles y / o dispositivos de E / S en cualquier puerto (USB, Firewire, IDE Bluetooth, etc). - La solución debe poder controlar medios extraíbles por su número de serie, lo que permite la creación de políticas para dispositivos únicos, específicos.
9	Antivirus. Antispyware	- La solución debe trabajar con base de firmas de archivos, bloqueo por comportamiento y análisis heurístico. - Solución debe proporcionar actualizaciones de firmas en tiempo real.
		- Anti-spyware debe manejar rootkits, ataques "día cero" y bloquear la instalación de malware a través de sitios web.
		- La solución debe proporcionar una manera de informar a los usuarios finale: con alertas o informes de análisis locales relacionados con la actividad del Ant malware.
		La solución debe permitir las siguientes opciones de tratamiento de sobre antivirus o antispyware; remediación, reparación, cuarentena y borrado.

INSTITUTO NACIONAL DE LA VIVIENDA
DIVISIÓN DE COMPRAS Y CONTRATACIONES
INVI
Techo digno para la gente
Santo Domingo, R. D.

10	Antibot	- Debe identificar y contener hosts infectados para limitar los daños y propagación de malware - Descubrir infecciones por reputación de direcciones IPs, URLs, y DNS. La solución debe permitir uso de indicadores de inteligencia en tiempo real de bases de datos de amenaza en la Nube que contengan (hash de archivo, firmas direcciones IP, DNS, certificados digitales y otros servicios de reputación) para detectar o bloquear la actividad maliciosa en el host. - Una vez detectado el bot debe poder bloquear comunicaciones remotas de comando y control entre la maquina infectada y Servidor de C&C
11	Sandboxing	- Debe Proteger contra el ataques de múltiples vectores de amenazas que llegan a través de descargas de la web, contenido copiado de medios de almacenamiento extraíbles, enlaces o archivos adjuntos en mensajes de correo electrónico, e movimiento lateral de datos y malware entre segmentos de red e infecciones a través de contenido cifrado. Debe permitir combinación de capacidades avanzadas de machine learning, análisis de comportamiento dinámico de Sistema Operativo, identificación de comportamientos maliciosos y sospechosos, tácticas de hacking y técnicas de ingeniería social, análisis de comunicaciones de C & C durante el análisis de sandboxing. - Archivos soportados para Sandboxing deben ser: Al menos 50 tipos de archivos incluyendo: Adobe PDF, Microsoft Word, Excel, PowerPoint, Ejecutables (EXE COM, SCR, Flash SWF, RTF, Zip) - Entrega archivos desinfectados a los usuarios, soportando dos modos de saneamiento o limpieza de documentos: o Mantener tipo de archivo: entrega el archivo en su formato original, eliminando cualquier contenido activo como macros. o Convertir a PDF - los archivos entregados a los usuarios se convierten a formato PDF, una transformación prácticamente imposible para cualquier malware para sobrevivir. Los usuarios pueden obtener un acceso libre al archivo original, si es necesario. El acceso está garantizado sólo si el archivo se encuentra limpio por el motor de detección de emulación de amenazas por sandboxing. - - Archivos soportados para Limpieza del Documentos: Adobe PDF,Microsoft Word Excel, y PowerPoint

#	COMPONENTE	ESPECIFICACIONES SOLICITADAS
		-
12	Limpieza de documentos	- Entregar archivos desinfectados a los usuarios, soportando dos modos de saneamiento o limpieza de documentos: o Mantener tipo de archivo: entrega el archivo en su formato original, eliminando cualquier contenido activo como macros. o Convertir a PDF - los archivos entregados a los usuarios se convierten a formato PDF, una transformación prácticamente imposible para cualquier malware para sobrevivir. - Los usuarios pueden obtener un acceso libre al archivo original, si es necesario. E acceso está garantizado sólo si el archivo se encuentra limpio por el motor de detección de emulación de amenazas por sandboxing. - Archivos soportados para Limpieza del Documentos: Adobe PDF,Microsoft Word Excel, y PowerPoint
13	Antiphising	- Debe utilizar análisis y heurística dinámica para bloquear sitios de phishing engañosos - Debe mantener las credenciales seguras alertando cuando los usuarios intentan utilizar sus contraseñas corporativas en sitios externos

#	COMPONENTE	ESPECIFICACIONES SOLICITADAS
14	AntiRansonware.	- La capacidad de anti- Ransomware mediante la detección automática, bloqueo y l eliminación de las infecciones más sofisticadas ransomware y la restauración d los datos cifrados como parte de su capacidad de remediación automatizada. - Integración con soluciones de Endpoint de otros fabricantes para complementa (Ej. McAfee, Symantec, Kaspersky, etc)
15	Análisis Forence	- Debe construir automáticamente informes forenses, entregando visibilida completa del alcance, daño y vectores del, ataque, incluyendo o Actividades sospechosas o Actividades de Remediación o Impacto al negocio del incidente, como archivo exfiltrados o cifrados por ransomware. o Detalle de la línea de tiempo del Incidente para determinar si es un infección - Elementos maliciosos que fueron remediados (quarentena) - El análisis forense para revelar el ataque completo y sus comportamiento maliciosos o sospechosos. El análisis se debe realizar de forma automátic abarcando arranques del sistema y rastreando los mecanismos de persistencia de malware (por ejemplo, a través del registro, los archivos eliminados, las tarea programadas, Procesos de puestos en marcha, etc.).

#	PARÁMETRO	ESPECIFICACIONES SOLICITADAS
1	Cantidad de equipos	Uno (1)
2	Marca	El software de gestión de puntos finales debe ser de la misma marca que el software de administración central
3	Modelo	Especificar

#	PARÁMETRO	ESPECIFICACIONES SOLICITADAS
4	Administración de políticas para puntos finales	Permitir la administración de seguridad unificada para puntos finales con el fin de poder realizar, la incorporación de la seguridad de equipos de usuarios finales cuando sea necesario. - Debe permitir la gestión de al menos 1000 puntos finales, con al menos las siguientes plataformas Windows: • Windows 10 Enterprise 64-bit • Windows 8 Enterprise, Professional editions 32/64-bit • Windows 7 Enterprise, Professional editions 32/64-bit - Debe permitir gestionar los siguientes módulos sobre el dispositivo terminal. - Firewall - Acceso Remoto por VPN

		- Compliance
		- Protección de puertos y cifrado de Medio extraíbles
		- Control de Aplicaciones
		- Antivirus/Anti Malware
		- Antibot
		- Emulación de Archivos

#	PARÁMETRO	ESPECIFICACIONES SOLICITADAS
		- Limpieza de documentos.
		- Anti-phishing
		- Anti ransomware
		- Análisis Forence

Presentación de Ofertas

El proponente deberá entregar su propuesta en sobre cerrado, debidamente sellada y firmada, conteniendo las siguientes informaciones.

1-Portada del sobre:

- Nombre del proponente
- Dirección
- RNC
- Referencia del procedimiento
- Nombre de la entidad contratante

2-Contenido del sobre:

- Cotización con especificaciones técnicas detalladas de los artículos ofertados, firmada y sellada
- Certificación actualizada de Industria y Comercio que las acredita como Mí pyme

- ITBIS Transparentado
- Condiciones de pago
- Términos de entrega
- Certificación de pago de impuestos actualizados (TSS, ANTICIPO E ITBIS)
- Constancia inscripción (RPE) actualizada
- Documentación que soporte las condiciones requeridas.

3-Condiciones de Pago:

El pago del 100% se hará con crédito a 120 días a partir de la fecha de depósito de la factura firmada y sellada por la unidad de compras y contrataciones, si ha sido recibido el bien.

4-Términos de Entrega

La entrega se hará a los 4 días después de notificada la adjudicación, debiendo ser anterior al pago. Al recibir el servicio se verificará que cumple con las características requeridas por la Institución, ya que al no cumplimiento de estas, el INVI lo rechazará y se dejara cuenta del proveedor, quedando la entidad contratante exenta de la obligación de pago y de cualquier otra obligación.

INSTITUTO NACIONAL DE LA VIVIENDA
DIVISIÓN DE COMPRAS Y CONTRATACIONES
INVI
Techo digno para la gente
Santo Domingo, R. D.