PODER JUDICIAL
DEL ESTADO DE YUCATÁN
CONSEJO DE LA JUDICATURA

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO
PODJUDCJ 14/2021

SERVICIO DE RENOVACIÓN DE LICENCIAMIENTO DEL EQUIPO DE SEGURIDAD DE INFORMÁTICA POR EL PERIODO DE UN AÑO, UBICADO EN EL CENTRO DE JUSTICIA ORAL DE MÉRIDA DEL CONSEJO DE LA JUDICATURA DEL PODER JUDICIAL DEL ESTADO.

PARTIDA ÚNICA.

RENOVACIÓN DE EQUIPO DE SEGURIDAD CHECKPOINT

Cantidad: (1) solución.

Que cumplan y/o excedan las siguientes características técnicas.

Generales	**Se requiere la renovación por 1 año del Licenciamiento, Soporte y Servicios (funcionalidades de Seguridad) para la solución de Ciberseguridad (Firewall Perimetral) propiedad de la dependencia, el cual consiste en:** **Un equipo de seguridad perimetral con funcionalidades de Ciberseguridad de Firewall, VPN, IPS, Anti-Virus, Filtrado de URL, Control de Aplicaciones, Anti-bot, Anti-Spam y SandBox.** **El proveedor licitante deberá de considerar la extensión de garantía que debe contemplar todo el Software y Hardware incluyendo los accesorios (memorias).** **La dependencia cuenta actualmente con una solución de Seguridad Perimetral con las siguientes especificaciones y funcionalidades:** **La solución tiene la capacidad de analizar el tráfico en tiempo real. Soporta aplicaciones de seguridad en una plataforma unificada con los siguientes módulos en el mismo equipo o dispositivo: Stateful Inspection Firewall, Sistema de Prevención de Intrusos, Reconocimiento de Identidad de Usuario, Control de Aplicación y Filtrado de URL, Anti-Bot y Anti-Virus, Emulación de Amenazas (SandBoxing), Extracción de Amenazas (depuración), Anti-Spam y Seguridad de Correo Electrónico, VPN IPSec, gestión de políticas de seguridad, registro y estado. Capacidad de control de acceso para al menos 150 servicios o protocolos predefinidos, soportando al menos los siguientes protocolos: TCP, UDP, ARP, ICMP, IPv4, IPv6, OSPF, IPSEC, RIP.** **Integra en el mismo Equipo o dispositivo de Seguridad el Licenciamiento de Software para la creación de redes virtuales privadas (Virtual Private Network – VPN) IPSEC. Permite como mínimo las siguientes funcionalidades: Cifrado 3DES y AES-256 para IKE Phase I y II IKEv2 más "Suite-B-GCM-128" y "Suite-B-GCM-256" para Fase II; Tiene la capacidad de admitir al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 y Grupo 20. Es compatible con la integridad de los datos con md5, sha1 SHA-256, SHA-384 y AES-XCBC. Soporta VPN´s de sitio a sitio en las siguientes topologías: Full Mesh (todo para todos), Estrella (oficinas remotas al sitio central), Hub and Spoke (sitio remoto a través del sitio central a otro sitio remoto). Permite que el administrador aplique reglas de seguridad para controlar el tráfico dentro de la(s) VPN(´s). Permite la creación y configuración de Redes Privadas Virtuales (VPN´s) basadas en dominio y VPN´s basadas en rutas que utilicen VTI y protocolos de enrutamiento dinámico. Tiene la capacidad de establecer VPN´s con puertas de enlace**

	con IP públicas dinámicas, e incluir compresión de IP para VPNs de cliente a sitio y de sitio a sitio. **En cuanto a la identificación de usuarios, provee múltiples métodos de identificación de usuarios, tales como: Consulta de Active Directory, basada en navegador o en agentes de identidad, Autenticación transparente de Kerberos, Portal Cautivo, RADIUS y LDAP. Tiene la capacidad para adquirir la identidad del usuario al consultar Microsoft Active Directory en función de los eventos de seguridad. Garantiza la autenticación de la identidad del usuario basado en el navegador, para usuarios o activos que no sean de dominio. Tiene la capacidad de compartir o propagar identidades de usuario entre múltiples firewalls de seguridad. Tiene la capacidad de crear roles de identidad para usar en todas las aplicaciones de seguridad. Cuenta con la capacidad de integrarse con los módulos de seguridad para establecer las reglas de control de accesos y prevención de amenazas.** **Integra un Sistema de Prevención de Intrusiones (INTRUSION PREVENTION SYSTEM - IPS), que permite suministrar protección de ataques orientados a conexiones internas y externas. El IPS integrado se basa en los siguientes mecanismos de detección: firmas de explotación, anomalías de protocolo, controles de aplicaciones y detección basada en el comportamiento. Tiene un mecanismo de Fail-Open basado en software, configurable basado en umbrales de CPU de cada uno de los firewalls de seguridad y de su uso de la memoria. Proporciona un mecanismo automático para activar o administrar nuevas firmas a partir de actualizaciones. Permite excepciones de Red basadas en la fuente, el destino, el servicio o una combinación de los tres elementos. Tiene la capacidad para poder activar automáticamente nuevas protecciones mediante la asistencia del administrador, en función de parámetros configurables, tales como: impacto en el rendimiento, gravedad de la amenaza, nivel de confianza, protecciones del cliente, protecciones del servidor. Tiene la capacidad para detectar y prevenir las siguientes amenazas: Uso indebido de protocolos, comunicaciones de malware, intentos de creación de túneles y tipos de ataques genéricos sin firmas predefinidas. Tiene la capacidad de recopilar paquetes de captura para protecciones específicas. Deberá tener la capacidad de detectar y bloquear los ataques a la RED y a la capa de aplicaciones, con protección al menos en los siguientes servicios: SMTP, IMAP, POP, DNS, FTP, Servicios de Windows (redes de Microsoft), Remote Procedure Call (RPC), SSH, Telnet, RLogin. Tiene la capacidad para detectar y bloquear aplicaciones P2P y anonimizadores (anonymizers). Tiene la capacidad de proteger contra el envenenamiento de caché de DNS. Impide que los usuarios accedan a las direcciones de dominio bloqueadas. Protege los protocolos VOIP. Detecta y bloquea las aplicaciones de controles remotos, incluidas aquellas que son capaces de crear túneles a través del tráfico HTTP y HTTPS. Permite al administrador bloquear fácilmente el tráfico entrante y/o saliente en función del país de donde se origina/destina el tráfico, sin necesidad de administrar manualmente los rangos de IP correspondientes al país. Cuenta con la funcionalidad de protección basada en firmas contra ataques de inyección de SQL. La solución inspecciona todo el tráfico de red con respecto a la búsqueda de vulnerabilidades hacia servidores, sin limitarse a solo inspeccionar una parte de la trama o a solo buscar vulnerabilidades en las peticiones hacia los servidores. La solución inspecciona el 100% del tráfico de red haciendo referencia a la comunicación cliente a servidor o servidor a cliente y sus respectivas respuestas.** **Tiene la capacidad de control de aplicaciones y filtrado de URLs, con al menos las siguientes funcionalidades: contener al menos 8,000 aplicaciones conocidas para el Control de Aplicaciones. Tiene clasificación de URL que supere los 190 millones de URL y cubra más del 85% de los principales sitios de "1M" del ranking de Alexa. Capacidad de crear una regla de filtrado con múltiples categorías. Capacidad de crear un filtro para un solo sitio que sea compatible con múltiples categorías. Tiene una interfaz de búsqueda fácil de usar para aplicaciones y URL. Capacidad de clasificar**

	las aplicaciones y las URL por Factor de riesgo. Tiene un control de aplicación unificado y reglas de seguridad URLF. Proporciona un mecanismo en tiempo real, para que le notifique o solicite al usuario acciones basadas en la política de seguridad. Proporciona un mecanismo para limitar el uso de la aplicación en función del consumo de ancho de banda. Permite excepciones de inspección de HTTPS basadas en objetos de red definidos por IP y Máscara de Red o por rango de IPs. Proporciona un mecanismo de modificación en la categorización de la base de datos de URL. Tiene la capacidad de crear políticas para usuarios, IPs, Redes, VPNs y Zonas de seguridad. Capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo. Capacidad de liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos. **Integra las funcionales Anti-Bot y Anti-Virus con las siguientes capacidades: Detecta y detiene el comportamiento anormal sospechoso de la red, debe usar un motor de detección de niveles múltiples, que incluye la reputación de direcciones IP, URL y DNS y detecta patrones de comunicaciones de bots. Es compatible con la detección y prevención de virus y variantes de "cryptors" y ransomware (por ejemplo, Wannacry, Cryptlocker, CryptoWall) mediante el uso de análisis estáticos y/o dinámicos. Tiene mecanismos para proteger contra los ataques de "spear phishing". Tiene la capacidad de detección y prevención para los escondites DNS de Control y Comando (C&C). Tiene la capacidad de buscar patrones de tráfico C&C, no solo en su destino DNS. Cuenta con la aplicación de ingeniería inversa al malware para descubrir su DGA (Generación de nombres de dominio). Tiene la capacidad de captura de DNS como parte de la prevención de amenazas, ayudando a descubrir hosts infectados que generen comunicación C&C. Tiene la capacidad de detección y prevención para los ataques de túnel DNS. Tiene la capacidad de inspeccionar el tráfico cifrado SSL; Actualizar Anti-Bot y Anti-Virus en tiempo real desde servicios de reputación basados en la nube. La funcionalidad de Anti-Virus es compatible con el escaneo de enlaces dentro de los correos electrónicos. Tiene la capacidad de escanear archivos que están pasando por el protocolo CIFS.** **Tiene la capacidad para crear un ambiente de Emulación de Amenazas (Sand-Boxing / SandBox) y la función de Extracción de código malicioso (malware) con la capacidad para detectar y detener de forma inmediata "Ataques de Día Cero" (Zero Day Attacks) y malware desconocido antes de que una firma de protección estática sea creada. Las amenazas detectadas por la solución de SandBox que ni siquiera debe permitir el acceso de la primera muestra, evitando así la existencia del "paciente cero". Es parte de una arquitectura de protección contra amenazas multicapa con capacidad de emular archivos de hasta 90 MB. Tienen la capacidad de implementarse de manera local e híbrida, permitiendo al usuario seleccionar la localización más adecuada para el análisis en la nube dependiendo de la naturaleza del archivo. Soportan la recepción de correo electrónico actuando como un MTA (Mail Transfer Agent). Están integradas en el Equipo o Dispositivo físico de Seguridad y ser autónomas de tal manera que NO se deberá requerir de equipos separados para proteger WEB (HTTP & HTTPs) y para correo electrónico (SMTP & SMTPS). Tienen la capacidad de bloquear llamadas a servidores remotos (Callbacks). En el caso de "Ataques de Día Cero", el Sistema de Protección de malware bloquea la habilidad del malware para realizar llamadas C&C (comando & control). La funcionalidad deberá tener la capacidad de emular archivos ejecutables, documentos, java y flash, en específico: 7z, Cab, Csv, Doc, Docm, Docx, Dot, Dotm, Dotx, Exe, Jar, Pdf, Potx, Pps, Psm, Ppsx, Ppt, Pptm, Pptx, Rar, Rtf, Scr, Swf, Tar, Tgz, Xla, Xls, Xlsb, Xlsm, Xlsx, Xlt, Xltm, Xltx, Xlw, Zip. Tiene la capacidad de virtualizar en al menos los siguientes ambientes: Windows 8.1 64 bits y Windows 10 64 bits, estos ambientes cuentan con diferentes versiones de Office y Adobe. Tienen la capacidad para implementar la solución de SandBoxing y no debe requieren la compra de licenciamiento extra para las instancias de Windows y Office que corren en los ambientes de emulación, la capacidad de inspeccionar, emular, prevenir y compartir los resultados**

	de los eventos de Sand-Boxing con la infraestructura anti malware; tiene la capacidad de realizar una pre-emulación o validación a través de un filtrado estático, en donde se valide si es necesario enviar el archivo a emulación. Tiene la capacidad para detectar el ataque en la fase de exploit, antes de que se ejecute el Shell code y antes de que el malware se descargue/ejecute. Tiene la capacidad de detectar la técnica de explotación "ROP" a través del monitoreo y análisis del flujo en el CPU real, y no en un CPU emulado. Tiene la capacidad de soportar el análisis de ligas dentro de los correos electrónicos, detectando de esta manera intentos de "Phishing" a los usuarios. Tiene la capacidad de generar reportes al detectar archivos maliciosos; el reporte incluye: Captura de pantallas que muestre la ejecución del malware, detalle de los procesos ejecutados, archivos y/o registros del sistema modificados o creados, actividad a nivel de RED. Tiene la capacidad de remover contenido activo o dinámico en documentos Office y PDF con el objetivo de eliminar la ejecución de código malicioso de forma automática al ser recibidos por correo electrónico en sitio. Tiene la capacidad de reconstruir los documentos de ofimática y PDF usando sus elementos seguros, entregando al usuario final un documento libre de riesgos en el mismo formato. Tiene la capacidad de convertir documentos a un formato PDF de forma automática al ser recibidos por correo electrónico. La solución dentro de su motor puede limpiar en tiempo cero cualquier amenaza incrustada en archivos, generando una copia de éstos removiendo contenido dinámico como javascript, VB Script, Powershell esta solución no deberá trabajar en modo proxy si no analizando los flujos de tráfico en capa 3. **Las comunicaciones entre la consola de administración y los dispositivos administrados son cifradas (Encriptadas) por medio de una GUI que no está basada en HTML, por razones de seguridad y en base a las ultimas vulnerabilidades reportadas en el protocolo SSL. La administración es basada en roles para permitir a los administradores delegar los derechos de acceso a dispositivos específicos con los privilegios adecuados de lectura/escritura esto debe aplicar a que se puedan definir administradores por conjuntos de reglas y estos administradores solo puedan modificar su porción de configuración dentro de la política de seguridad. Soporta múltiples administradores trabajando al mismo tiempo, manteniendo un registro de los objetos que están siendo modificados para no ser re escritos. La solución identifica malas prácticas en configuraciones alertando al cliente, sobre reglas que se encuentren mal configuradas. La herramienta cuenta con permisos administrativos, haciendo posible que se generen administradores que solo puedan modificar cierto número de reglas. Cuenta con una herramienta de búsqueda que permita fácilmente filtrar objetos de red, donde permita incluir la opción de buscar objetos duplicados (con la misma IP) y objetos no usados (en una regla o política) y una lista de reglas en que un objeto especifico es usado para una simplificación de las operaciones.** **La solución provee la opción de generar versiones de las políticas para poder regresar a un estado anterior en caso de necesitarlo.**
Consola de Administración	**Se requiere suministro de consola de administración de equipos de seguridad perimetral, basada en software con Licenciamiento, Soporte y Servicios (Reportes, cumplimiento, gestión de amenazas) por 1 año para la solución de Ciberseguridad (Firewall Perimetral) actual de la dependencia.** **La solución de gestión, basada en software deberá ser 100% compatible para integrarse con firewall de seguridad perimetral actual de la dependencia. Deberá ser capaz de gestionar de uno a cinco dispositivos de seguridad perimetral de forma unificada.** **De igual forma la solución deberá integrar funciones de reporteo y cumplimiento en tiempo real, que permita la generación de informes**

	detallados, gestión de amenazas para un análisis forense completo con visibilidad y control de la red. **La solución deberá poder integrarse en el ambiente de virtualización actual de la dependencia según las capacidades requeridas para su implementación.** **Las comunicaciones entre la consola de administración y los dispositivos administrados son cifradas (Encriptadas) por medio de una GUI que no está basada en HTML, por razones de seguridad y en base a las ultimas vulnerabilidades reportadas en el protocolo SSL. La administración es basada en roles para permitir a los administradores delegar los derechos de acceso a dispositivos específicos con los privilegios adecuados de lectura/escritura esto debe aplicar a que se puedan definir administradores por conjuntos de reglas y estos administradores solo puedan modificar su porción de configuración dentro de la política de seguridad. Soporta múltiples administradores trabajando al mismo tiempo, manteniendo un registro de los objetos que están siendo modificados para no ser re escritos. La solución identifica malas prácticas en configuraciones alertando al cliente, sobre reglas que se encuentren mal configuradas. La herramienta cuenta con permisos administrativos, haciendo posible que se generen administradores que solo puedan modificar cierto número de reglas. Cuenta con una herramienta de búsqueda que permita fácilmente filtrar objetos de red, donde permita incluir la opción de buscar objetos duplicados (con la misma IP) y objetos no usados (en una regla o política) y una lista de reglas en que un objeto especifico es usado para una simplificación de las operaciones.** **La solución provee la opción de generar versiones de las políticas para poder regresar a un estado anterior en caso de necesitarlo.** **La solución deberá integrar soporte 7x24 directamente con el TAC del fabricante durante la vigencia del contrato de licenciamiento.** **El proveedor licitante deberá ser un Socio autorizado de la marca ofertada, para lo cual deberá demostrarlo integrando en su propuesta una carta expedida por el fabricante indicando que el proveedor licitante está autorizado para la comercialización de la solución ofertada.**
Cartas y evidencias del fabricante	**El proveedor licitante deberá ser un Socio autorizado de la marca ofertada, para lo cual deberá demostrarlo integrando en su propuesta una carta expedida por el fabricante indicando que el proveedor licitante está autorizado para la comercialización de la solución ofertada.**