Comité de Adquisiciones, Arrendamientos, Servicios y Obra Pública del Consejo de la Judicatura del Poder Judicial del Estado de Yucatán

LICITACIÓN PÚBLICA NÚMERO "PODJUDCJ 10/2023"

"ANEXO TÉCNICO"

PARTIDA ÚNICA
"Contratación del servicio de renovación de licenciamiento del equipo de seguridad de informática por el periodo de un año".

Ubicación: Edificio sede del Centro de Justicia Oral de Mérida (CJOM), sito en la calle 145, número 299 por 54 y 64, colonia San José Tecoh C.P. 97299, de esta ciudad.

SUBPARTIDA	CANT	DESCRIPCIÓN
1	1	**RENOVACIÓN (EXTENSIÓN Y SOPORTE) DE EQUIPO SEGURIDAD FIREWALL** Como parte integral del proyecto, el Licitante deberá considerar la extensión de soporte y licenciamiento para el Gateway de Seguridad instalado en el edificio CJOM, propiedad de la Convocante. Así mismo el licitante, deberá considerar la integración de este Gateway a una Consola de Gestión propiedad de la Convocante. **VIGENCIA** Deberá considerar una vigencia de Licenciamiento y Soporte directo por parte del fabricante de al menos 12 meses, iniciando del 01 de enero de 2024 al 31 de diciembre de 2024. La solución de seguridad deberá contar con un soporte de fabricante con al menos los siguientes alcances: • Soporte de fabricante 24x7, con opción de que la Convocante puede solicitar soporte de manera directa. • Soporte telefónico y por correo electrónico • Solicitudes de soporte ilimitado • Acceso a la base de datos de conocimientos • Acceso a actualizaciones mayores y mejoras • Acceso a Hot Fixes y paquetes de servicio • Solicitud de refacciones bajo proceso (RMA) La solución de seguridad perimetral deberá contar con al menos los siguientes servicios de seguridad para descarga de firmas y actualizaciones: • Control de aplicaciones • IPS • Filtrado de contenido • Antibot • Antivirus • Anti-spam • Anti Phising • Sandbox **SERVICIO DE ACTUALIZACIÓN Y OPTIMIZACIÓN** Se deberá incluir todo lo necesario para la actualización del equipo de seguridad. • Previo al inicio de los servicios, el Licitante deberá realizar mesas de trabajo en conjunto con la Convocante para realizar la identificación

		de requerimientos, arquitecturas de comunicación existentes, redes y recursos que son necesarios proteger con el fin de definir las políticas de seguridad que serán necesarias establecer en la solución de seguridad. • Respaldo de configuraciones. • Actualización del equipo a la última versión de software estable liberada por el fabricante. • Instalación de parches o fixes requeridos para la correcta operación del equipo. • Revisión de las configuraciones existentes para determinar si el equipo de encuentra correctamente configurado con base en los requerimientos de seguridad de la Convocante. • En caso de detectarse que existen configuraciones deficientes, servicios mal configurados o servicios no configurados, será responsabilidad del Licitante subsanar dichas omisiones con el fin de garantizar la correcta protección de los activos informáticos de la Convocante. • Es de importancia mencionar que actualmente este equipo de seguridad funciona de manera standalone. • El licitante deberá dar de alta el firewall de seguridad en una Consola de Gestión existente, así como configurar todos los módulos de servicios para proporcionar a la Convocante información en tiempo real y generar reportes. • El Licitante deberá realizar las pruebas de funcionamiento necesarias para asegurar correctamente la operación del equipo de seguridad. • El Licitante deberá incluir como parte de los servicios la entrega de una memoria técnica al finalizar los servicios. • El Licitante deberá entregar el licenciamiento y las garantías/pólizas de soporte técnico del fabricante. Con el fin de garantizar la correcta ejecución de los servicios, el Licitante deberá incluir como parte de su propuesta técnica el certificado que avale a la persona que realizará funciones de Administrador de Proyectos con las capacidades de Project Management Professional (PMP). El Licitante deberá integrar dentro de su propuesta técnica los certificados de al menos 1 ingeniero con un nivel de certificación a nivel asociado, 1 ingeniero con un nivel de certificación a nivel experto o su equivalente, 1 ingeniero con un nivel de certificación a nivel experto en resolución de problemas, a fin de demostrar que cuenta con las capacidades técnicas de implementación, configuración y puesta en servicio de los equipos para el proyecto. **SOPORTE TÉCNICO PARA EQUIPOS DE SEGURIDAD** El servicio deberá ser al menos por 12 meses. • Los equipos deberán contar con soporte técnico durante la vigencia del servicio con atención las 24 horas del día los 7 días de la semana, en caso de requerirse el reemplazo de partes, el Licitante deberá considerar un nivel de servicio de 8x5xNBD siguiente día hábil y gestionar las refacciones con el fabricante para el

		restablecimiento del servicio. • El licitante deberá mantener actualizada la solución de seguridad durante la vigencia del servicio. • El licitante deberá proporcionar soporte técnico a través de un centro SOC (Security Operation Center) propietario. • Deberá alinear todos sus procesos a las mejores prácticas ITIL, ISO27001:2013, 20000-1:2018, ISO 37001:2016 y 9001:2015. El Licitante deberá proporcionar como parte de su propuesta técnica los certificados que demuestran el cumplimiento de dichos estándares. • El SOC deberá pertenecer al grupo de respuesta de incidencias FIRST. • Atención del SOC en un esquema 24x7x365 • Deberá alinear todos sus procesos a las mejores prácticas ITIL, deberá incluir como parte de su propuesta los certificados de al menos 3 personas que cuenten con certificación ITIL Foundation e ITIL OSA. • El servicio deberá contar mesa de ayuda para la recepción y canalización de tickets de soporte técnico o para reportar incidencias. • Deberá incluir soporte técnico por medio telefónico, remoto y email. • Deberá considerar soporte técnico en sitio para la atención de fallas y el restablecimiento del servicio. **Cartas por parte del fabricante.** • El Licitante deberá demostrar ser un socio autorizado (al menos socio nivel 4 o su equivalente) en la marca ofertada, mediante carta expedida directamente por el fabricante, dicha carta deberá ser firmada por el representante legal del fabricante en México.
2	930	**SUMINISTRO DE LICENCIAS ENDPOINT** Se requiere que el Licitante proporcione una solución de protección de punto final que cumpla con las siguientes características técnicas mínimas: **ADMINISTRACIÓN** **Operacional** • La política deberá poder definir listas blancas para implementar excepciones a la política base. • La solución deberá ser compatible con clientes locales y remotos independientemente de la red. • La solución deberá tener una API profundamente funcional y documentada para admitir la integración y la automatización en toda la plataforma y con otras plataformas. • La solución deberá tener una consola central para definir políticas, crear grupos de sistemas/usuarios, iniciar sesión, implementar actualizaciones, generar informes. • La solución deberá tener soporte. • Deberá proporcionar acceso basado en roles a la consola. • Capacidad para excluir archivos y carpetas de los análisis. (Ejemplo:

		Exenciones para carpetas de bases de datos específicas). • Capacidad para detener completamente el antivirus/EPP durante la instalación de la aplicación. • Control granular de la funcionalidad. • La solución deberá ser capaz de realizar operaciones de inserción en los clientes finales. • La solución debería poder proporcionar una recopilación remota de registros de resolución de problemas. • La solución debería permitir ejecutar un script de PowerShell remoto en el cliente. • La solución deberá ser "Network Aware" y tener la capacidad de cambiar la política del cliente según su ubicación de red. • La solución deberá tener soporte para importar y prevenir IOC personalizados. • El acceso a la consola deberá ser compatible con el uso de autenticación de sistemas de terceros. **Despliegue** • La solución deberá proporcionar métodos modernos y sencillos de implementación/instalación/desinstalación remota (incluida la compatibilidad con secuencias de comandos). • La solución deberá tener la capacidad para la instalación remota nativa y la implementación del cliente sin el uso de herramientas de terceros. • La solución deberá utilizar un "token de autenticación" para registrar de forma segura una nueva instalación de cliente en el servidor de gestión. • La solución deberá permitir gestionar la versión del agente y los componentes desde la interfaz de gestión. **Nube** • La solución deberá proporcionar gestión como un servicio. • La solución permite la selección de la región de la nube. • La solución deberá tener copias de seguridad proporcionadas como parte del servicio. • La solución deberá cumplir con el RGPD. • La solución deberá tener una separación total de datos entre clientes. • La solución de gestión deberá ser compatible con un cliente completo o un cliente ligero basado en web. • La solución deberá tener autenticación de dos factores para el inicio de sesión del administrador. • La autenticación web deberá admitir la autenticación SAML. • La Convocante deberá contar con una sola consola de gestión en la nube, por lo que el Licitante deberá realizar las actividades necesarias para crear, unificar, transferir o eliminar consolas de gestión, con fin que el licenciamiento sea administrado en una sola Consola a nombre de la Convocante.

		Registro e informes • La solución deberá poder proporcionar alertas de correo electrónico en tiempo real. **CLIENTE** **Soporte de SO y VDI** • SO compatibles: Clientes Windows a partir del Windows 7 SP1 Pro +; Servidores Windows a partir del Windows 2008 R2 + Mac OS: 10.15 + (compatible con M1 completamente nativo) Linux: Debian v10, Ubuntu 18.04, CentOS 8, Red Hat Enterprise Linux 8.1 • La solución admite entornos VDI, tanto persistentes (flotantes) como no persistentes (dedicados). Los proveedores de Microsoft Terminal Server, Vmware Horizon y Citrix PVS/MCS son totalmente compatibles. • La solución deberá estar alineada y ser compatible con las últimas versiones del sistema operativo. • Esta solución permitirá implementar el cliente y proteger las máquinas que se ejecutan en servidores de terminales y cajeros automáticos. • Esta solución permite ejecutar funciones de protección de dispositivos habilitadas: HVCI, Credentials Guard y Windows Defender App Control. **Características del cliente** • El agente deberá ser liviano. • La solución es configurable para una utilización mínima de los recursos del sistema. • La solución deberá proporcionar la capacidad de ejecutarse en un hipervisor. • La solución deberá proporcionar métodos modernos y sencillos de implementación/instalación/desinstalación remota (incluida la compatibilidad con secuencias de comandos). • La solución permite actualizar a versiones más nuevas sin realizar un reinicio. • El tamaño del paquete de la solución incluirá solo los componentes relevantes para implementar en un solo instalador. • La solución deberá proporcionar capacidades de proxy para clientes que están fuera de línea y para limitar el uso del ancho de banda. • La solución debería poder recuperar actualizaciones de firmas para Internet mediante un proxy NTLM autenticado con las credenciales de un usuario conectado. • Al realizar actualizaciones, la solución descargará solo los cambios acumulados de la versión instalada. **Detección** • La solución deberá recopilar continuamente los eventos del sistema necesarios para la detección y el análisis. El proveedor deberá enumerar elementos específicos que se recopilan en tiempo real. (Los datos recopilados a través de secuencias de comandos posteriores al evento o la interacción en vivo con el host se tratan en

		un requisito separado). Los ejemplos deberán incluir, entre otros, eventos de proceso, modificaciones de archivos y registros, conexiones de red, actividad entre procesos, argumentos de línea de comando, eventos de Windows, consultas y respuestas de DNS. • La solución deberá monitorear continuamente e informar los hallazgos lo más rápido posible. Si un endpoint no puede informar inmediatamente sobre los resultados, los resultados deberán almacenarse localmente hasta que puedan cargarse en el sistema de gestión central de la solución. • La solución deberá permitir alertas en tiempo real o registro de eventos notables basados en contenido personalizado (comportamientos) o indicadores atómicos de compromiso basados en tipos de datos identificados por la solución. • La solución deberá proporcionar una forma de garantizar que la información del proceso, los metadatos, las solicitudes de dns, las conexiones de red, los archivos binarios o cualquier otra información recopilada no se comparta con el proveedor o un tercero (por ejemplo, VirusTotal) sin una suscripción explícita. • La solución deberá poder demostrar gráficamente la actividad del sistema (árboles de procesos u otro tipo de interfaz de mapeo) para ayudar en las investigaciones. • La solución deberá capturar metadatos detallados sobre archivos binarios y procesos que se ejecutan en puntos finales. Los detalles deberán incluir, entre otros, el hash del binario (MD5, SHA-256), la información del editor, los detalles de la firma del código, la frecuencia observada en nuestro entorno, la información de la versión y el propietario del sistema de archivos. • La solución deberá tener la capacidad de cambiar la marca de las notificaciones de los usuarios. • La solución deberá tener la capacidad de controlar el nivel de mensajes para mostrar a los usuarios. **Respuesta** • La solución deberá proporcionar una forma de aislar un sistema que asegure que los controles preventivos se mantengan durante los reinicios. La configuración de aislamiento deberá estar preestablecida para permitir que el punto final se aísle de las amenazas, pero pueda conectarse a los sistemas de investigación/remediación. • La solución deberá ser capaz de aplicar inmediatamente controles preventivos (bloquear actividad específica o maliciosa conocida, etc.). • La solución deberá tener una capacidad de respuesta en vivo que permita la capacidad de interactuar de forma remota con el sistema. • La solución deberá proporcionar la capacidad de escribir una respuesta en vivo de forma condicional (es decir, si sucede X, entonces sucede Y). • La solución deberá tener una sólida comunidad de intercambio de

		socios. • La solución deberá permitir a los analistas la capacidad de alternar rápidamente entre diferentes actividades observadas en un punto final y proporcionar información contextual si está disponible. • La solución deberá tener la capacidad de buscar en todos los puntos finales los IOC u otros atributos del sistema que no se capturan en los datos de telemetría en tiempo real. **Informes** • La solución no deberá exponer la actividad de un usuario a otro usuario que esté usando la misma máquina. **PROTECCIÓN DE DATOS Y DISPOSITIVOS** **Protección de puertos** • La solución deberá brindar administración de todos los puertos de punto final, con registro centralizado de la actividad del puerto para auditoría y cumplimiento. • La solución permitirá notificaciones de mensajes de usuario personalizados al conectar un dispositivo según el escenario. **Cumplimiento** • La solución obligará a los terminales a cumplir con las reglas de seguridad definidas para la organización. Los equipos que no cumplan se mostrarán como no conformes y se les pueden aplicar políticas restrictivas. • La solución hará cumplir las aplicaciones y los archivos requeridos en función de la configuración de cumplimiento al monitorear la presencia de archivos específicos, valores de registro y procesos que deberán estar ejecutándose o presentes en las computadoras finales. • La solución hará cumplir las aplicaciones y los archivos prohibidos en función de la configuración de cumplimiento mediante la supervisión de la presencia de archivos específicos, valores de registro y procesos cuya ejecución o presencia está prohibida en los equipos terminales. • La solución aplicará una verificación Anti-Malware para verificar que las computadoras tengan un programa anti-malware instalado y actualizado. • La solución deberá admitir la integración con Windows Server Update Services (WSUS). **Cortafuegos** • La solución hará cumplir las reglas del cortafuegos para permitir o bloquear el tráfico de red a las computadoras finales en función de la información de conexión, como direcciones IP, puertos y protocolos. • La solución se utilizará para determinar si los usuarios pueden conectarse a redes inalámbricas mientras se encuentran en la LAN de su organización para proteger la red de las amenazas asociadas con las redes inalámbricas.

		• La solución definirá si los usuarios pueden conectarse a la red de la organización desde puntos de acceso en lugares públicos, como hoteles o aeropuertos. • La solución se utilizará para restringir o permitir el tráfico de red IPV6. • El Firewall del cliente de la solución deberá permanecer activo durante la actualización del cliente. • La solución deberá incluir una opción para que Aislamiento de host aísle o permita un host específico (acceso a la red) que está bajo ataque de malware y presenta un riesgo de propagación. **Control de aplicaciones** • La solución se utilizará para restringir el acceso a la red para aplicaciones específicas. El administrador de Endpoint Security define políticas y reglas que permiten, bloquean o cancelan aplicaciones y procesos. • La solución podrá incluir aplicaciones en la lista blanca o en la lista negra. • La solución deberá admitir la habilitación/deshabilitación del tráfico originado por los procesos WSL ("Subsistema de Windows para Linux"). • La solución se utilizará para restringir el acceso a la red para aplicaciones específicas. El administrador de Endpoint Security define políticas y reglas que permiten, bloquean o cancelan aplicaciones y procesos. • La solución podrá incluir aplicaciones en la lista blanca o en la lista negra. • La solución deberá admitir la habilitación/deshabilitación del tráfico originado por los procesos WSL ("Subsistema de Windows para Linux"). **AntiMalware** • La solución deberá ser capaz de identificar la similitud de un archivo malicioso con una familia de malware conocida. • La solución permitirá el escaneo programado de unidades locales, mensajes de correo. Unidades ópticas y dispositivos extraíbles. • En caso de detección de malware, la solución aislará los archivos del sistema operativo, pero no se eliminarán de forma permanente. El usuario puede restaurar archivos en cuarentena, si no son maliciosos. • La solución deberá proporcionar una interfaz de línea de comandos para iniciar el análisis de malware. • La solución deberá proporcionar una interfaz de línea de comandos para actualizar la base de datos de firmas antimalware. • La solución deberá ser compatible con un Anti-malware compatible con DHS. • La solución AV deberá ser capaz de proporcionar pruebas de que el escaneo se ha realizado en la mayoría de los archivos .DAT actuales

		o proporcionar un método de prueba igualmente eficaz que satisfaga los requisitos de auditoría para las soluciones AV sin DAT. • La solución protegerá la computadora de todo tipo de amenazas de malware, desde gusanos y troyanos hasta adware y registradores de pulsaciones de teclas. La solución gestionará de forma centralizada la detección y el tratamiento de malware en los equipos finales. • La solución permitirá el escaneo programado de unidades locales, mensajes de correo. Unidades ópticas y dispositivos extraíbles. • Las soluciones deberán descargar firmas de un proxy NTLM autenticado con las credenciales de un usuario conectado. • La solución debería poder usar un cliente dedicado como proxy para actualizaciones de firmas antimalware para clientes que están fuera de línea y no tienen una conexión directa a Internet o para limitar el uso de ancho de banda. • En caso de detección de malware, la solución aislará los archivos del sistema operativo, pero no se eliminarán de forma permanente. El usuario puede restaurar archivos en cuarentena, si no son maliciosos. **Protección contra ransomware** • La solución protegerá contra ransomware existente y de día cero sin requerir actualizaciones de firmas. • La solución reparará y restaurará los archivos que se cifraron durante un ataque de ransomware. • La solución anti-ransomware tiene validación de terceros. **Protección conductual** • La solución aprovechará múltiples sensores para identificar de manera efectiva y única los comportamientos de malware genérico, así como los comportamientos específicos de la familia de malware. • La solución prevendrá o detectará inmediatamente comportamientos maliciosos sin importar si la máquina está en línea o fuera de línea. • La solución detectará y evitará ataques sin archivos utilizando únicamente procesos de Windows. • La solución detectará y evitará ataques sin archivos basados en secuencias de comandos. • La solución deberá proteger contra la técnica "Pass The Hash" para el robo de credenciales. • La solución debería detectar archivos LNK (acceso directo de Windows) maliciosos. • La solución deberá detectar la escalada de privilegios locales (LPE) de día cero. • La solución se integrará con la interfaz de análisis antimalware (AMSI) de Microsoft para recibir y analizar scripts decodificados. **Modelos ML para análisis estático** • La solución deberá ser capaz de identificar archivos de día cero incluso si no están familiarizados con ningún servicio de reputación. • Cualquier modelo de ML utilizado por el endpoint deberá actualizarse

		con frecuencia para protegerlo contra nuevos ataques de día cero. • La solución deberá impedir que el usuario use archivos hasta que se verifiquen y se determine que son benignos. • El Motor de Detección Estática de la solución deberá monitorear el acceso a los archivos. • La solución deberá comprobar la reputación de los archivos en función del hash ssdeep/Fuzzy. **Anti-robot** • La solución identificará y bloqueará la comunicación saliente a sitios C&C maliciosos. • Los recursos de inteligencia de amenazas en la nube se utilizarán para actualizaciones e identificación de ataques C&C de día cero. • Tras un ataque de bot identificado, la solución remediará completamente el ataque dejando el punto final limpio e ileso. **Protección de navegación web** • Navegadores compatibles, al menos, Windows: Chrome, Edge (cromo), FireFox. Sistema operativo Mac: Safari, Chrome, FireFox. • La solución deberá tener capacidades de limpieza sin hardware adicional. Los archivos entrantes se extraerán de todo el contenido malicioso potencial, como secuencias de comandos, macros y contenido activo. • Al realizar la limpieza, el usuario final deberá poder acceder al archivo original si el sandbox lo considera benigno. • Los archivos entrantes se emularán mediante sandboxing para contenido potencialmente malicioso. • La solución detectará sitios de phishing de día cero que solicitan credenciales de usuario, incluso si los motores de reputación no los conocen. • La solución deberá impedir que el usuario explore direcciones URL o dominios maliciosos conocidos. • La solución deberá impedir que el usuario utilice sus credenciales corporativas en un sitio que no pertenezca al dominio corporativo. • La solución deberá proporcionar filtrado de URL basado en categorías con una lista adicional en blanco y negro. • La solución deberá aplicar la función "Búsqueda segura" cuando emplean los motores de búsqueda de Google, Bing y Yahoo. • El usuario no deberá poder eliminar la protección de navegación de ninguna manera. **Sandboxing** • Todos los archivos escritos en el sistema de archivos serán monitoreados y analizados estáticamente. Si se encuentran como potencialmente maliciosos, los archivos serán emulados por sandboxing y puestos en cuarentena si se encuentran como maliciosos. • La solución deberá ser capaz de limpiar completamente el endpoint de cualquier resto del ataque en caso de que el sandbox encontrara

		que el archivo es malicioso. **Prevención de exploits** • La solución detectará y evitará técnicas de explotación de software confiable. • La solución tiene la capacidad de bloquear los nuevos ataques RDP RCE como BlueKeep en sistemas sin parches. **EDR** **Análisis forense** • La solución creará automáticamente un análisis de incidentes para cada detección/prevención que ocurra. Este análisis deberá incluir árboles de ejecución de procesos incluso entre arranques si es relevante. • El informe forense identificará automáticamente el punto de entrada de la actividad maliciosa y resaltará el daño potencial, la acción de remediación y toda la cadena de ataque. • La solución mejorará las detecciones de seguridad o antimalware de terceros mediante la creación y visualización automáticas de un informe de incidentes. • El informe forense registrará, presentará y quitará la ofuscación de los scripts de PowerShell utilizados durante un ataque. • La solución enumerará el análisis de reputación de los archivos, las URL y las IP utilizadas durante un ataque. La solución mostrará la geolocalización de IP como parte de la información de reputación. • La solución podrá seguir métodos indirectos de ejecución utilizados por malware como llamadas WMI e inyecciones para poder rastrear la actividad de malware más avanzado. • La solución deberá incluir los siguientes sensores: Servicio de ejecución remota Descubrimiento del proceso de creación Descubrimiento de la ventana de la aplicación Tarea programada Captura de pantalla Captura de entrada DDE (intercambio dinámico de datos). • La solución creará un informe de incidentes que mostrará el incidente en términos de Mitre ATT&CK Matrix. • La solución permitirá la búsqueda de múltiples tipos de datos de sensores no detectados, incluidos datos de archivo, proceso, red, registro, inyección y usuario. • La solución permitirá la remediación de cualquier archivo o proceso que se encuentre a través de la plataforma EDR. • La solución permitirá el análisis forense y el informe de cualquier indicador encontrado a través de la plataforma EDR. • La solución proporcionará múltiples opciones de remediación manual, como Cuarentena, Proceso de eliminación y Análisis forense con remediación. • La solución proporcionará una capacidad de gestión central para aislar las máquinas de forma remota. • La solución permitirá la búsqueda de incidencias mediante técnicas de Mitre Att&ck.

		• La solución deberá tener la capacidad de ver las direcciones MAC de cada computadora que envíe datos. • La solución EDR deberá proporcionar datos relacionados con periféricos y dispositivos de almacenamiento externo. • La solución enriquecerá automáticamente los resultados de búsqueda con reputación. **REGISTRO E INFORMES** **Informes** • La solución debería generar informes periódicos sobre tipos de malware, tipos de vulnerabilidades explotadas, etc. • La solución deberá tener la capacidad de generar informes visuales. • La solución deberá proporcionar el estado de salud del agente. **Registros** • La solución deberá mostrar el proceso afectado, las claves de registro afectadas y los archivos afectados en el entorno del sistema operativo. • La solución mostrará capturas de pantalla y videos de emulación de archivos maliciosos en el entorno Sandbox. • La solución debería poder registrar la comunicación de C&C desde el archivo BOT emulado. **CUMPLIMIENTO DE LA NORMATIVA** La solución deberá cumplir con al menos: • Reglamento Internacional de Tráfico de Armas (ITAR). • Ley Federal de Gestión de la Seguridad de la Información (FISMA). • Marco de gestión de riesgos del Departamento de Defensa (RMF). • Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA). • Normas de seguridad de la industria de tarjetas de pago (PCI). • Directiva de la comunidad de inteligencia (ICD) 503. • La solución deberá cumplir con las regulaciones de GDPR. **Inteligencia de amenazas** **Nube** • La solución deberá actualizarse dinámicamente en función de una red global de sensores de amenazas mediante el intercambio de datos de amenazas. **VIGENCIA** Deberá considerar una vigencia de Licenciamiento y Soporte directo por parte del fabricante de al menos 24 meses. La solución de seguridad deberá contar con un soporte de fabricante con al menos los siguientes alcances: • Soporte de fabricante 24x7, con opción de que la Convocante puede solicitar soporte de manera directa. • Soporte telefónico y por correo electrónico • Solicitudes de soporte ilimitado • Acceso a la base de datos de conocimientos • Acceso a actualizaciones mayores y mejoras

		• Acceso a Hot Fixes y paquetes de servicio **Carta por parte del fabricante.** • El Licitante deberá demostrar ser un socio autorizado (al menos socio nivel 4 o su equivalente) en la marca ofertada, mediante carta expedida directamente por el fabricante, dicha carta deberá ser firmada por el representante legal del fabricante en México. **CURSOS** El licitante deberá considerar un curso oficial en un centro autorizado de entrenamiento autorizado por el Fabricante, deberá ser un curso básico para la administración de la solución de protección de punto final para 1 asistente. **SERVICIO DE INSTALACIÓN** Se deberá incluir todo lo necesario para la correcta instalación y operación de la solución de protección de punto final. • Se deberá incluir suministro, configuración, puesta a punto del licenciamiento solicitado. • El Licitante deberá de considerar los servicios profesionales para la instalación, configuración y puesta en funcionamiento de la solución de protección de punto final • Activación y configuración de las funciones de seguridad. • La Convocante proporcionará al Licitante ganador el inventario de equipos de cómputo y servidores sobre los cuales se deberá desplegar la solución de protección. • El Licitante deberá crear los paquetes de instalación adecuados para realizar la instalación de todos los equipos de cómputo o servidores. • El Licitante deberá realizar la validación de los sistemas operativos y versiones al fin de asegurar el 100% de la compatibilidad de la solución antes de realizar la instalación del agente. • El licitante deberá crear una estrategia de despliegue masivo, en caso de no poder realizarse, el Licitante deberá realizar la instalación manual de al menos 50 agentes. • El licitante deberá realizar la configuración de la Consola de Administración en la nube del fabricante. • El Licitante deberá proporcionar la documentación con el proceso para ejecutar la instalación manual para que la Convocante finalice el despliegue de la solución de seguridad • Deberá considerar al menos: o Configuración de hasta 10 políticas. (Web & Files Protection) o Configuración de Behavioral Protection. (Best Practice) o Configuración de Análisis y Remediciones. (Best Practice) • El servicio deberá considerar una sesión remota para las pruebas de comunicación entre los componentes, agentes de la consola y aplicación de políticas. • El licitante deberá realizar la configuración de todos los módulos o

		funcionalidades de seguridad incluidos en el licenciamiento. • El Licitante previo al inicio de los trabajos deberá realizar un plan de trabajo en conjunto con la Convocante a fin de garantizar la correcta ejecución de los trabajos y la mínima afectación de los equipos de cómputo o servidores. • El Licitante deberá realizar las pruebas de funcionamiento necesarias para asegurar correctamente la operación de los equipos de seguridad. • El Licitante deberá incluir como parte de los servicios la entrega de una memoria técnica al finalizar los servicios profesionales. • El Licitante deberá entregar el licenciamiento y las garantías/pólizas de soporte técnico del fabricante. Con el fin de garantizar la correcta ejecución de los servicios, el Licitante deberá incluir como parte de su propuesta técnica el certificado que avale a la persona que realizará funciones de Administrador de Proyectos con las capacidades de Project Management Professional (PMP). **SOPORTE TÉCNICO PARA LICENCIAS ENDPOINTS** El Licitante deberá brindar soporte técnico a solución de protección de puntos finales por al menos 2 años, los alcances del soporte técnico cumplir con: • Deberá contar con una mesa de ayuda para la recepción de solicitudes de atención con un esquema de atención 24x7. • Deberá contar con soporte técnico durante la vigencia del servicio con atención en un esquema de tipo 5x8. • Deberá incluir soporte técnico por medio telefónico, remoto y email. • Deberá incluir soporte técnico en las configuraciones y resolución de dudas sobre la administración de la solución de seguridad. • Deberá incluir acciones correctivas y resolución de problemas para incidencias. • Apertura de casos y seguimiento puntual con fabricante para incidencias. • El licitante deberá mantener actualizada la solución de seguridad durante la vigencia del servicio. • El licitante deberá proporcionar soporte técnico a través de un centro SOC (Security Operation Center) propietario. • Deberá alinear todos sus procesos a las mejores prácticas ITIL, ISO27001:2013, 20000-1:2018, ISO 37001:2016 y 9001:2015. El Licitante deberá proporcionar como parte de su propuesta técnica los certificados que demuestran el cumplimiento de dichos estándares. • El SOC deberá pertenecer al grupo de respuesta de incidencias FIRST. • Deberá alinear todos sus procesos a las mejores prácticas ITIL, deberá incluir como parte de su propuesta los certificados de al menos 3 personas que cuenten con certificación ITIL Foundation e ITIL OSA.