ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

Partida "A"

Software de Seguridad Perimetral

CANT	DESCRIPCIÓN MINIMAS REQUERIDAS
1	**RENOVACIÓN DEL LICENCIAMIENTO PARA LA SEGURIDAD PERIMETRAL DE ALTA DISPONIBILIDAD** El Licitante deberá ofertar renovación de Seguridad Perimetral, los cuales deberán cumplir con las siguientes especificaciones mínimas: **CARACTERÍSTICAS GENERALES** • El fabricante del sistema de seguridad perimetral deberá tener al menos 20 años de experiencia en el Mercado de seguridad informática. • El fabricante deberá proporcionar exclusivamente soluciones de seguridad de Internet. • El fabricante deberá proporcionar evidencia de las posiciones de liderazgo año tras año en firewall empresarial, firewalls UTM y prevención de intrusiones basadas en datos independientes de la industria de la seguridad. • El Fabricante deberá proporcionar evidencia de la posición de liderazgo año tras año del Cuadrante Mágico de Gartner para las soluciones de Prevención de Intrusión y / o el Cuadrante Mágico Gartner del firewall de la red empresarial. • Deberá ser capaz de soportar estas aplicaciones de seguridad de próxima generación en una plataforma unificada: Stateful Inspection Firewall, Sistema de Prevención de Intrusos, Adquisición 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, VPN IPSec y acceso móvil. • Para la protección de la red perimetral, se requieren un clúster (2 appliances) de ciberseguridad, los cuales deberán contar con las siguientes capacidades: • El cluster deberá gestionarse de manera centralizada por un Servidor de Administración Centralizada de Seguridad. • La solución del fabricante deberá proveer un mecanismo para constantemente educar al usuario final de la política de seguridad en tiempo real. • El fabricante deberá otorgar todas las certificaciones de la solución.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• El fabricante deberá tener la capacidad para proveer una solución para mitigar ataques de tipo denegación de servicio. • Los Gateways de seguridad deberán usar Stateful Inspection basada en el análisis granular de la comunicación y el estado de la aplicación para rastrear y controlar el flujo de la red. • La solución deberá admitir el control de acceso para al menos 150 servicios o protocolos predefinidos. • La solución deberá soportar control de acceso usando objetos de tipo data center genéricos. • La solución deberá soportar un ilimitado número de lenguajes en los objetos de tipo Check de Usuarios. • La solución deberá soportar la instalación de políticas aceleradas. • La solución deberá soportar la instalación de políticas de seguridad de manera concurrente. • La solución deberá soportar el recuento de aciertos en las reglas de NAT. • La solución deberá soportar objetos de dominio, actualizables, zonas de seguridad, roles de acceso y centro de datos. • Deberá proporcionar estadísticas de recuento de aciertos de reglas de seguridad a la Consola de administración. • Deberá permitir que las reglas de seguridad se apliquen en intervalos de tiempo que se configurarán con una fecha / hora de caducidad. • La comunicación entre las consolas de administración y los Gateways de seguridad deberá estar encriptada y autenticada con Certificados PKI. • Los Gateways de seguridad deberán soportar métodos de autenticación usuario, cliente y sesión. • Los Gateways de seguridad deberán soportar el siguiente esquema de autenticación de usuario a nivel Gateway y a nivel módulo de VPN: tokens, TACACS, RADIUS y certificados digitales. • La solución deberá incluir una base de datos local para aceptar la autenticación y autorización por usuario sin la necesidad de un dispositivo externo. • La solución deberá soportar DHCP en modo server y relay. • La solución deberá soportar HTTP y HTTPS Proxy. • La solución deberá incluir la facilidad para trabajar en modo transparente y modo puente. • La solución deberá admitir Alta disponibilidad de Gateways e intercambio de carga con sincronización de estado. • La solución deberá ser compatible con la integración de terceros (API pública).

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• Motor de comparación de firmas que permita contrastar el contenido del tráfico de una sesión contra patrones de firmas de virus, ataques de intrusión, reconocimiento de aplicaciones u otros patrones sin comprometer el rendimiento de la red. • Soporte de protocolos: TCP, UDP, ARP, ICMP, IPv4, IPv6, OSPF, IPSec, RIP. • La solución deberá soportar 6 a 4 NAT o 6 a 4 Tunnel. • La solución deberá soportar integración al Directorio activo utilizando tráfico IPV6. • La solución deberá soportar ver el log del tráfico de IPV6. • La plataforma deberá soportar la habilidad para desplegar la tabla de enrutamiento de IPV6 • Para el presente esquema se requiere una arquitectura de un clúster, es decir, dos gateways. • Los componentes de la Solución de Seguridad Perimetral deberán tener la capacidad individual de: o Brindar soporte de al menos 7 millones de sesiones o conexiones concurrentes. o Brindar soporte de al menos 160,000 sesiones o conexiones por segundo. o Brindar soporte de al menos 35 Gbps de throughput ideal de Firewall y 4 Gbps de VPN AES-128. o Brindar soporte de al menos 18 Gbps de Inspección y prevención de tráfico malicioso (IPS) y 5 Gbps para Amenazas Avanzadas. o Contar con al menos una interfaz de 1G dedicado para administración remota, adicional a una de sincronía. o Contar con al menos 8 interfaces de 1G de cobre o Contar con al menos 4 interfaces de 10G SFP+ y 4 transceivers SR o Contar con memoria RAM de 32GB o Fuente de poder redundante AC o 1 Unidad de Rack **VPN** • La solución deberá admitir 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. • La solución deberá 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

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• La solución deberá ser compatible con la integridad de los datos con md5, sha1 SHA-256, SHA-384 y AES-XCBC.
	• Se deberá admitir CA interna y CA externa de terceros.
	• La solución deberá incluir soporte para VPN de sitio a sitio en las siguientes topologías:
	  o Full Mesh (todo para todos),
	  o Estrella (oficinas remotas al sitio central)
	  o Hub and Spoke (sitio remoto a través del sitio central a otro sitio remoto).
	• La solución deberá soportar encripción SHA/512
	• La solución deberá ser compatible con la configuración de VPN con una GUI mediante la adición de objetos de arrastrar y soltar a las comunidades de VPN
	• La solución deberá admitir VPN SSL sin cliente para el acceso remoto.
	• La solución deberá soportar autenticación de máquina.
	
	IDENTIFICACIÓN DE USUARIOS
	
	• Deberá poder adquirir la identidad del usuario al consultar Microsoft Active Directory en función de los eventos de seguridad.
	• Deberá tener un método de autenticación de identidad de usuario basado en el navegador para usuarios o activos que no sean de dominio
	• Deberá proveer múltiples métodos de identificación de usuarios: Consulta de AD, basada en navegador o agentes de identidad, Autenticación transparente de Kerberos, portal captivo.
	• Deberá soportar entornos de servidor de terminal.
	• La solución deberá integrarse perfectamente con los servicios de directorio, IF-MAP y Radius.
	• El impacto en los controladores de dominio deberá ser inferior al 3%.
	• La solución de identidad deberá admitir servidores de terminal y Citrix.
	• Deberá poder adquirir la identidad del usuario de Microsoft Active Directory sin ningún tipo de agente instalado en los controladores de dominio.
	• Deberá tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios;
	• Deberá tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• La solución deberá soportar integración de portal cautivo con SAML 2.0 y proveedores de identidad de terceros. **IPS** • El fabricante deberá proveer evidencia de que año tras año aparece como líder en el cuadrante mágico de Gartner para Sistemas de prevención de intrusos o en la categoría de Firewall de Red Empresarial. • Se deberá suministrar el servicio de IPS pudiendo brindarse con el mismo Appliance, en una configuración de alta disponibilidad, para la protección de ataques orientados a conexiones internas y externas. • IPS deberá basarse en los siguientes mecanismos de detección: firmas de explotación, anomalías de protocolo, controles de aplicaciones y detección basada en el comportamiento. • IPS y el módulo de firewall deberán integrarse en una plataforma. • IPS deberá tener un mecanismo de fail-open basado en software, configurable basado en umbrales de CPU de Gateways de seguridad y uso de memoria. • IPS deberá proporcionar un mecanismo automático para activar o administrar nuevas firmas a partir de actualizaciones. • IPS deberá admitir excepciones de red basadas en la fuente, el destino, el servicio o una combinación de los tres. • IPS deberá incluir un modo de solución de problemas que establece el perfil en uso para detectar solo, con un clic sin modificar las protecciones individuales. • IPS deberá ser capaz de detectar y prevenir las siguientes amenazas: uso indebido de protocolos, comunicaciones de malware, intentos de tunelización y tipos de ataques genéricos sin firmas predefinidas. • Para cada protección, la solución deberá incluir el tipo de protección (relacionada con el servidor o con el cliente), la gravedad de la amenaza, el impacto en el rendimiento, el nivel de confianza y la referencia de la industria. • IPS deberá poder detectar y bloquear los ataques a la red y a la capa de aplicaciones, protegiendo al menos los siguientes servicios: servicios de correo electrónico, DNS, FTP, servicios de Windows (redes de Microsoft). • El Licitante deberá proporcionar evidencia de liderazgo para proteger las vulnerabilidades de Microsoft. • IPS y/ o Application Control deberán incluir la capacidad de detectar y bloquear aplicaciones P2P y evasivas.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• La solución deberá proteger contra el envenenamiento de caché de DNS e impide que los usuarios accedan a las direcciones de dominio bloqueadas. • La solución deberá proporcionar protecciones de protocolos VOIP • IPS deberá detectar y bloquear las aplicaciones de controles remotos, incluidas aquellas que son capaces de crear túneles a través del tráfico HTTP. • La solución deberá permitir al administrador bloquear fácilmente el tráfico entrante y / o saliente en función de los países, sin la necesidad de administrar manualmente los rangos de IP correspondientes al país. • Actualizaciones periódicas durante la vigencia del contrato de nuevas definiciones, las actualizaciones deberán realizarse de forma automática, programada por fecha y hora. • Deberá integrarse protección basada en firmas contra ataques de inyección de SQL. • Deberá sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad; **CONTROL DE APLICACIONES Y FILTRADO DE URLS** • La base de datos de control de aplicaciones deberá contener al menos 10,000 aplicaciones conocidas. • La solución deberá tener una clasificación de URL que supere los 200 millones de URL y cubra más del 85% de los principales sitios de 1M de Alexa. • La solución deberá ser capaz de crear una regla de filtrado con múltiples categorías. • La solución deberá ser capaz de crear un filtro para un solo sitio que sea compatible con múltiples categorías. • La solución deberá tener granularidad de usuarios y grupos con reglas de seguridad. • El caché local del Gateway de seguridad deberá dar respuesta al 99% de las solicitudes de categorización de URL dentro de las 4 semanas de producción. • La solución deberá tener una interfaz de búsqueda fácil de usar para aplicaciones y URL. • La solución deberá clasificar las aplicaciones y las URL y las aplicaciones por Factor de riesgo. • El control de la aplicación y la política de seguridad URLF deberán poder definirse por las identidades del usuario.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• El control de la aplicación y la base de datos URLF deberán ser actualizados por un servicio basado en la nube. • La solución deberá tener un control de aplicación unificado y reglas de seguridad URLF. • La solución deberá proporcionar un mecanismo para informar o solicitar a los usuarios en tiempo real que los eduquen o confirmen acciones basadas en la política de seguridad. • Deberá permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora); • Deberá ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad • Deberá tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory, y la base de datos local. • Permitir página de bloqueo personalizada. • Permitir el bloqueo y continuación (que permite al usuario acceder a un sitio bloqueado potencialmente informándole en la pantalla de bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio). • Deberá tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo • Deberá ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos. • La solución deberá admitir el control de acceso para al menos 150 servicios o protocolos predefinidos. **ANTI-BOT y ANTIVIRUS** • El Licitante deberá tener una aplicación integrada Anti-Bot y Anti-Virus en el firewall de próxima generación. • La aplicación Anti-Bot deberá ser capaz de detectar y detener el comportamiento anormal sospechoso de la red. • La aplicación Anti-Bot deberá usar un motor de detección de niveles múltiples, que incluye la reputación de direcciones IP, URL y DNS, y detectar patrones de comunicaciones de bots. • Las protecciones anti-Bot deberán poder escanear en busca de acciones de bots. • La solución deberá ser compatible con la detección y prevención de virus y variantes de Cryptors y ransomware (por ejemplo, Wannacry,

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	Cryptlocker, CryptoWall) mediante el uso de análisis estáticos y / o dinámicos. • La solución deberá tener mecanismos para proteger contra los ataques de spear phishing. • Ataques basados en DNS • La solución deberá tener capacidades de detección y prevención para los escondites DNS de C&C. • La solución deberá buscar patrones de tráfico C&C, no solo en su destino DNS. • Invertir malware de ingeniería para descubrir su DGA (Generación de nombres de dominio). • Característica de captura de DNS como parte de nuestra prevención de amenazas, ayudando a descubrir hosts infectados generando comunicación C&C. • La solución deberá tener capacidades de detección y prevención para los ataques de túnel DNS. • La política Anti-Bot y Anti-Virus deberá administrarse desde una consola central. • La aplicación Anti-Bot y Anti-Virus deberá tener un mecanismo centralizado de correlación e informe de eventos. • La aplicación de antivirus deberá poder evitar el acceso a sitios web maliciosos. • La aplicación antivirus deberá poder inspeccionar el tráfico cifrado SSL. • Anti-Bot y Anti-Virus deberán tener actualizaciones en tiempo real de servicios de reputación basados en la nube. • Anti-Virus deberá ser capaz de detener los archivos maliciosos entrantes. • Anti-Virus deberá poder escanear archivos archivados. • Las políticas de antivirus y anti-Bot se deberán administrar de forma centralizada con la configuración de políticas granulares y su aplicación. • El Anti-Virus debería admitir más de 50 motores AV basados en la nube. • El Anti-Virus debería ser compatible con el escaneo de enlaces dentro de los correos electrónicos. • El Anti-Virus deberá Escanear archivos que están pasando el protocolo CIFS. **INSPECCIÓN SSL (INBOUND / OUTBOUND)**

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• La solución deberá ofrecer soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de mitigación de amenazas. • La solución deberá ser compatible con Perfect Forward Secrecy (PFS, ECDHE Cipher Suites). • La solución deberá aprovechar la base de datos de filtrado de URL para permitir al administrador crear una política de inspección https granular. • La solución puede inspeccionar el filtrado de URL basado en HTTPS sin necesidad de descifrado SSL. • Soporte TLS 1.3 **PROTECCIÓN CONTRA AMENAZAS DESCONOCIDAS (DIA CERO)** • La solución deberá ofrecer soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de mitigación de amenazas. • La solución deberá ser compatible con Perfect Forward Secrecy (PFS, ECDHE Cipher Suites). • La solución deberá ser compatible con AES-NI, AES-GCM para mejorar el rendimiento. • La emulación de amenazas / sandboxing deberá integrarse con SSL Inspection. • La solución deberá aprovechar la base de datos de filtrado de URL para permitir al administrador crear una política de inspección https granular. • La solución deberá poder inspeccionar el filtrado de URL basado en HTTPS sin necesidad de descifrado SSL. • La solución deberá proporcionar la capacidad de proteger contra ataques de malware desconocidos y de día cero antes de que se hayan creado protecciones de firma estática. • Prevención en tiempo real: malware desconocido paciente-0 en la navegación web. • Prevención de malware desconocido en tiempo real paciente-0 en el correo electrónico. • La solución deberá ser capaz de emular al menos 53 tipos de archivos como ejecutables, documentos, JAVA y flashear específicamente: 7z, cab, csv, doc, docm, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, pif, com, gz, bz2, tgz, apk (android), ipa (iphone), ISO, js, cpl, vbs, jse, vba, vbe, wsf, wsh.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• La solución deberá ser capaz de emular ejecutable, documentos, JAVA y flash específicamente dentro de varios protocolos: HTTP, HTTPS, FTP, SMTP, CIFS (SMB), SMTP, TLS. • El motor de emulación deberá ser compatible con varios sistemas operativos, como XP y Windows7, 8,10 32 / 64bit, incluidas las imágenes personalizadas. • La solución deberá soportar el análisis estático para Windows, Mac OS-X, Linux o cualquier plataforma x86. • El motor de emulación debería poder inspeccionar, emular, prevenir y compartir los resultados del evento de sandboxing en la infraestructura antimalware. • La solución deberá permitir la emulación de archivos con un tamaño superior a 80 Mb en todos los tipos que admita. • Las soluciones deberán ser compatibles con los motores de detección basados en el aprendizaje automático de máquinas. • El motor de emulación deberá superar el 90% de tasa de captura en las pruebas de Virus Total donde los archivos .PDF y .exe maliciosos conocidos se modifican con encabezados "no utilizados" para demostrar la capacidad de las soluciones para detectar malware nuevo y desconocido. • La solución deberá detectar el tráfico de C&C de acuerdo con la reputación dinámica de ip / url. • La solución deberá ser capaz de emular y extraer archivos incrustados en documentos. • La solución deberá poder escanear documentos que contienen URL. • La solución deberá tener capacidades anti-evasión que detecten la ejecución de sandbox. • La solución deberá entregar reportes basados en el framework de MITRE. • La solución deberá soportar administración autónoma de la prevención de amenazas. • La solución deberá soportar la actualización automática de los perfiles de la política de prevención de amenazas. **GESTIÓN DE SEGURIDAD**

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• El Licitante deberá considerar la extensión del licenciamiento y soporte de la solución de gestión de seguridad actual, propiedad de la Convocante. • El licenciamiento a renovar deberá incluir las funcionalidades de vistas de eventos de seguridad y generación de reportes personalizados, de los hallazgos más relevantes. • El licitante deberá realizar todas las gestiones con el fabricante para unificar todos las productos, licencias y servicios bajo un único identificador de cuenta a nombre de la Convocante. Las funciones que la solución de gestión de seguridad deberá realizar son: • Tras la detección de archivos maliciosos, se deberá generar un informe detallado para cada uno de los archivos maliciosos. • El informe detallado deberá incluir: capturas de pantalla, líneas de tiempo, creación / modificaciones de clave de registro, creación de archivos y procesos, actividad de red detectada. • La aplicación de administración de seguridad deberá poder coexistir en la puerta de enlace de seguridad como una opción. • La solución deberá incluir la capacidad de distribuir de forma centralizada y aplicar nuevas versiones de software de puerta de enlace • La solución deberá incluir una herramienta para administrar centralmente las licencias de todas las puertas de enlace controladas por la estación de administración • La GUI de administración deberá tener la capacidad de excluir fácilmente la dirección IP de la definición de firma IPS. • El Visor de registro deberá tener la capacidad de excluir fácilmente la dirección IP de los registros de IPS cuando se detecta como falso positivo • La GUI de administración deberá tener la capacidad de acceder fácilmente a la definición de firmas IPS a partir de los registros de IPS • La solución deberá combinar la configuración de políticas y el análisis de registros en un solo panel, para evitar errores y lograr la confianza del cambio. • La solución de administración de políticas deberá proporcionar registros de reglas similares para el usuario a medida que crea o modifica reglas (registros de contenido) • La GUI de la solución deberá proporcionar una navegación fácil entre cientos de políticas, cada una con hasta 1 millón de reglas. Se deberán

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	proporcionar saltos entre sub políticas y títulos de sección, así como una búsqueda exhaustiva. **REGISTRO Y MONITOREO** • El registro central deberá ser parte del sistema de gestión. • La solución deberá proporcionar la opción de ejecutarse en el servidor de administración o en un servidor dedicado. • El visor de registro deberá tener la capacidad de realizar búsquedas indexadas. • La solución deberá tener la capacidad de registrar todas las aplicaciones de seguridad integradas en la puerta de enlace e incluir IPS, Control de aplicaciones, Filtrado de URL, Antivirus, Anti-Bot, Antispam, Identidad del usuario, Acceso móvil. • La solución deberá incluir un mecanismo automático de captura de paquetes para que los eventos IPS proporcionen un mejor análisis forense. • La solución deberá proporcionar diferentes registros para la actividad regular del usuario y registros relacionados con la administración. • La solución deberá proporcionar la siguiente información del sistema para cada puerta de enlace: Sistema Operativo, uso de CPU, uso de memoria, todas las particiones de disco y porcentaje de espacio libre en el disco duro. • La solución deberá incluir el estado de todos los túneles VPN, sitio a sitio y cliente a sitio. • La solución deberá incluir una configuración de umbral personalizable para realizar acciones cuando se alcanza un determinado umbral en una puerta de enlace. Las acciones deberán incluir: Iniciar sesión, alerta, enviar una captura SNMP, enviar un correo electrónico y ejecutar una alerta definida por el usuario. • La solución deberá incluir gráficos pre-configurados para monitorear la evolución en el tiempo del tráfico y los contadores del sistema: las principales reglas de seguridad, los principales usuarios de P2P, los túneles VPNs, el tráfico de red y otra información útil. La solución deberá proporcionar la opción de generar nuevos gráficos personalizados con diferentes tipos de gráficos. • La solución deberá incluir la opción de registrar el tráfico y las vistas del sistema en un archivo para su posterior visualización en cualquier momento.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	VIGENCIA La solución completa, deberá considerar una vigencia de Licenciamiento y Soporte directo por parte del fabricante de 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 La solución de gestión deberá contar con al menos los siguientes servicios: • Cumplimiento • Correlacionador de eventos • Reportes **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 los equipos de seguridad Firewall y Solución de Gestión para 2 asistentes.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	SERVICIO DE INSTALACIÓN PARA EQUIPOS DE SEGURIDAD Se deberá incluir todo lo necesario para la correcta instalación y operación de los equipos de seguridad. • Previo al inicio de los servicios de instalación, 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. • Se deberá incluir suministro, colocación, puesta a punto de la infraestructura solicitada. • El licitante deberá considerar que la Convocante cuenta con una infraestructura de seguridad la cual el Licitante deberá retirar de los racks de comunicaciones para poder realizar correctamente la instalación de los nuevos equipos. • Configuración de los equipos Firewall en alta disponibilidad. • Configuración de políticas de ruteo, seguridad y acceso a los recursos DMZ. • Configuración de funcionalidades de balanceo de enlaces WAN para permitir la navegación de usuarios a través de una red privada de enlaces inalámbricos y/o internet, y en caso de pérdida de la comunicación primaria se cambie a la ruta de salida alterna de manera automática sin afectar la disponibilidad de los servicios. • Establecimiento de una red de comunicaciones VPN site-to-site o client-to-site según requiera la Convocante. • Configuración de acceso por medio de restricción origen/destino de puertos TCP/UDP/ICMP y direcciones IP. • Configuración de NAT/PAT • Configuración de funcionalidad de firewall con validación de estados de conexión • Activación y configuración de las funciones de seguridad. • El licitante deberá realizar la configuración de todos los módulos o funcionalidades de seguridad incluidos en el licenciamiento del equipo. • El licitante deberá realizar una instalación nueva de la Consola de Gestión solicitada a renovar. La Consola deberá ser puesta en operación sobre una infraestructura de servidor virtual que será proporcionada por la Convocante. El licitante deberá proporcionar la

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	lista de requerimientos que son necesarios y validar la infraestructura proporcionada para el correcto funcionamiento de la solución. • El licitante deberá dar de alta todos los firewalls de seguridad solicitados en este Anexo Técnico en la Consola de Gestión, 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 de los equipos 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. • El Licitante deberá considerar que los equipos serán instalados en edificio dentro de la ciudad de Mérida, y como parte de su propuesta deberá considerar todos los gastos necesarios para la correcta implementación en sitio. La información y ubicación de dicho edificio será acordado con el Licitante ganador. 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 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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

Partida "B"

Software de Antivirus Endpoint

CANT	DESCRIPCIÓN MINIMAS REQUERIDAS
295	**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: Con el fin de contar con una estrategia de seguridad integrada en los firewalls perimetrales y la protección final de equipos, ambas soluciones deberán ser del mismo fabricante. **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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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**

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	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

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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).

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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 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 **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.

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	• 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).

ANEXO TÉCNICO
LICITACIÓN PÚBLICA NÚMERO "PODJUDTSJ-CA 18/2023"

	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.