Bogotá D.C.,

Asunto: SOLICITUD DE INFORMACIÓN PARA ESTUDIO DE MERCADO

Respetados señores:

Atentamente solicito su colaboración, a efectos de obtener información para consolidar estudios de mercado sobre los bienes, obras y/o servicios que se citan a continuación:

OBJETO	Adquirir la suscripción de un software de protección autónoma en la nube y en la red para los endpoint, servidores y correo electrónico (XDR – Detección y respuestas extendidas) – TREND MICRO- modulo VISION ONE.	
UNSPSC	**DESCRIPCION**	**CODIGO UNSPSC**
	Mantenimiento y soporte de software	81112200
	Software de seguridad y protección	43233200
	Nota: Por favor indicar el código en el cual está clasificado el bien o servicio a contratar.	
DESCRIPCIÓN Y/O ALCANCE	**ESPECIFICACIONES TECNICAS MINIMAS**	**COTIZACION ALTERNATIVA**
	Ver anexo.	En caso de que aplique o se requieran
PLAZO PARA EJECUCIÓN-	El plazo para la ejecución del contrato que se suscriba será hasta el 22 de diciembre del 2022, aprobación de las garantías que constituirá el contratista. previa expedición del registro presupuestal	
LUGAR DE EJECUCION	Para todos los efectos, el lugar de ejecución del contrato será en las sedes del Ministerio de Hacienda y Crédito Público, en la sede del contratista y de manera virtual en el evento de requerirse, previa autorización del Supervisor del contrato, bajo herramientas tecnológicas autorizadas por el Ministerio de Hacienda y Crédito Público.	
FORMA DE PAGO	EL MINISTERIO pagará al CONTRATISTA, **una vez se encuentre aprobado el P.A.C. (Programa anual mensualizado de caja),** el valor del contrato en **un solo pago**, previa entrega del documento que acredite la suscripción del licenciamiento solicitado y firma del acta de recibo a satisfacción por parte del contratista y el supervisor del contrato. Dicho pago se efectuará **con sujeción a la disponibilidad del PAC**, dentro de los diez (10) días hábiles siguientes a la radicación en la Subdirección Financiera y la debida presentación de la factura y del cumplido expedido por el supervisor designado, la certificación de pago de aportes parafiscales y de seguridad social por parte del contratista y registro de carga de dichos soportes en SECOP II.	
VALIDEZ DE LA COTIZACION	La Entidad requiere que la cotización tenga validez como mínimo de noventa (90) días Calendario. En la cotización debe relacionar su período de validez	

COTIZACIÓN ALTERNATIVA *	
Detallar: CUANDO COMPRENDA VARIOS ÍTEMS, SE DEBE COTIZAR INDIVIDUALMENTE CADA UNO	**VALOR UNITARIO**
VALOR TOTAL (incluido IVA)	

NOTA: Si el cotizante encuentra que algo falta, no es procedente o es diferente a lo consignado en la descripción técnica de la necesidad, es importante que lo manifieste, justificando la razón que sustenta el cambio, para que el ministerio, previo análisis, determine la procedencia de la sugerencia. Para tal fin deberá determinar los costos de la cotización alternativa.

Agradecemos se sirva remitir la información respectiva a más tardar el día 22 de octubre 2021 a través de correo electrónico invtecnologia@minhacienda.gov.co o a la siguiente dirección: Calle 7 B Nro. 6B-80 Edificio Casas de Santa Bárbara.

Cordialmente,

(FIRMADO DIGITALMENTE)
RICARDO FERNELIX RIOS ROSALES
Director de Tecnología

* Si el cotizante desea presentar una cotización alternativa a la solicitada por el Ministerio, debe cumplir con las condiciones técnicas mínimas de la cotización básica.

ANEXO No. 1

REQUERIMIENTOS TÉCNICOS MÍNIMOS

1.	**CONDICIONES TECNCAS**: Las licencias a suscribir deberán permitir:
1.1	Contar con la capacidad de integrarse con la infraestructura que actualmente tiene el Ministerio para la protección de las estaciones de trabajo, servidores y correo electrónico contra código malicioso.
1.2	Permitir mediante el uso de motores de Inteligencia Artificial obtener, visibilidad completa de todas las actividades, bloqueos y eliminación de las amenazas de código malicioso presentes en la red
1.3	Contar con todas las actualizaciones del software a la última versión liberada por el fabricante, así como parches o "fixes" liberados en el mercado de acuerdo con las recomendaciones del fabricante, para lo cual el contratista debe planear y aplicar dichas actualizaciones a todos los equipos que hacen parte de la herramienta ofertada sin costo adicional para el Ministerio de Hacienda y Crédito Público, durante el tiempo de vigencia de la suscripción.
1.4	Monitorear, registrar y realizar investigaciones de seguridad actuales e históricas en sus diferentes puntos finales. Por medio de un panel debe permitir la investigación preliminar y de causa raíz de un incidente, permitiendo ubicar los puntos finales en riesgo antes de ejecutar el Análisis de causa raíz en profundidad para identificar los vectores de ataque
1.5	Investigar las amenazas y permitir localizar los objetos sospechosos en la red. Si la red es el objetivo de un ataque en curso o un APT, una investigación de amenazas puede: • Evaluar el alcance del daño causado por el ataque dirigido • Proporcionar información sobre la llegada y progresión del ataque. • Ayuda en la planificación de una respuesta efectiva a incidentes de seguridad.
1.6	Generar investigaciones detalladas que permitan realizar una investigación sobre el estado actual del sistema. Las investigaciones detalladas deben permitir configurarse para que se ejecuten en períodos específicos y también admitir un conjunto más amplio de criterios mediante el uso de reglas de OpenIOC y YARA
1.7	Permitir generar investigaciones preliminares para identificar rápidamente los puntos finales que son posibles candidatos para un análisis adicional. Una investigación preliminar debe utilizar metadatos del servidor para obtener resultados rápidamente
1.8	Permitir graficar toda la cronología de los eventos generados en una investigación por medio de un gráfico de anillos que muestra el número total de puntos finales clasificados ya sea estén relacionados, o no relacionados a otros procesos, en cola o cancelados. La información debe estar siendo actualizada en tiempo real y de forma automática mientras avanza una investigación
1.9	Permitir la búsqueda de Indicadores de Compromiso (IoC) en búsqueda de comunicaciones específicas, actividad de registro, actividad de la cuenta autenticada en el sistema y procesos en curso.
1.10	Permitir por medio de la consola el análisis y visualización de la siguiente información: - Comunicación: IP, Puerto, Dominio, DNS - Malware o cualquier archivo: SHA1 hash, nombre de archivo, ruta del archivo, tipo del archivo - Registro de actividad - Procesos corriendo - Actividad de cuenta de usuario
1.11	Permitir la integración con información externa de IoC (Indicators Of Compromises) como reglas YARA, OpenIoC, STIX, TAXII
1.12	Permitir el análisis de comportamiento de un malware, actividades específicas de IoC y conexiones de comando a control
1.13	Contar con la capacidad de tener una interfaz la cual debe estar integrada con la consola de administración de las soluciones de seguridad como FortiSIEM, imperva, varonis, change auditor y open vas con las que cuenta el Ministerio para tener desde un solo punto el análisis, el contexto completo de los eventos y la línea de tiempo de los

	sucesos
1.14	Contra con la capacidad de convivir con cualquier solución de malware en el caso que el equipo a proteger tenga otro tipo de protección.
1.15	Controlar los programas que demuestran un comportamiento anormal asociado con ataques de exploits.
1.16	Escanear documentos en busca de códigos de exploits integrados y vulnerabilidades conocidas
1.17	Permitir la detección de amenazas tipo Fileless a través de la exploración de memoria mejorada para detectar comportamientos de procesos sospechosos. El agente debe tener la capacidad de terminar los procesos sospechosos antes de que se pueda hacer cualquier daño
1.18	Analizar los archivos desconocidos de baja prevalencia utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso.
1.19	Contar con la capacidad de recopilar datos del sensor en los endpoints(IOC) y almacenarlos de forma centralizada para su posterior análisis
1.20	Solucionar en línea datos volátiles como: manejo de archivos, claves de registro, procesos, hilos, controladores cargados, , tareas, servicios, DNS, ARP, socket, etc
1.21	Contar con la capacidad de registrar eventos críticos basados en criterios establecidos por el administrador.
1.22	Contar con la capacidad de realizar barrido de IOC en todos los dispositivos con sensor
1.23	Contar con la capacidad de asociar los datos de registro y logs de los procesos con otros artefactos de disco y/o memoria
1.24	Utilizar solo un agente para realizar la protección antimalware, virtual patching, DLP, control de aplicaciones y EDR
1.25	Contar con la capacidad de buscar reglas de Yara en: memoria, memoria de proceso, registros, archivos individuales, carpetas, disco entero y eventos
1.26	Permitir realizar consultas y posteriormente crear, configurar y generar alertas personalizadas con base en ellas
1.27	Permitir la exportación de inteligencia de amenazas a través de STIX/TAXII
1.28	Contar con la capacidad de mostrar todos los dispositivos en los que un proceso principal (padre) inicia otros procesos (hijos) especialmente de tipo powershell y cmd.
1.29	Contar con la capacidad de identificar amenazas aun cuando usen powershell codificado
1.30	Detectar y reportar tareas programadas maliciosas
1.31	Revelar la cadena completa de procesos afectados por el malware/comportamiento malicioso
1.32	Contar con la capacidad de mostrar la línea de tiempo de incidentes detectados por la herramienta
1.33	Contar con la capacidad de mostrar en una sola vista todo el ciclo de vida del ataque de la amenaza
1.34	Permitir que el trabajo de investigación continúe en el dispositivo aislado sin permitir que se extienda la actividad maliciosa por medio de cuarentena y/o aislamiento de los sistemas infectados
1.35	Contar con la funcionalidad de EDR, la cual no debe requerir un agente adicional a los agentes de Endpoint Protection instalados en las maquinas del Ministerio de Hacienda
1.36	Permitir la detección y respuesta de correlación entre los agentes de seguridad de los endpoints, servidores y el correo del Ministerio de Hacienda
1.37	Contar con la funcionalidad XDR, la cual debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques
1.38	Contar con la capacidad de tener modelos de correlación, los cuales deben combinar múltiples reglas y filtros utilizando una variedad de técnicas de análisis pero no limitándose a Data Stacking y Machine Learning
1.39	Contar con la capacidad de detección y respuesta, así como de proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad
1.40	Contar con la capacidad de tener gráficas de representación visual de los objetos que levantaron la alerta y la relación entre ellos

1.41	Contar con la funcionalidad XDR, la cual debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos
1.42	Contar con la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las accionas que una amenaza llevó a cabo en un servidor, endpoint, o carga de trabajo en la nube.
1.43	Permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para reproducir las comunicaciones y ver el detalle de acciones de un atacante como comunicaciones de comando y control o movimientos laterales.
1.44	Permitir la búsqueda proactiva a través de endpoint, red, email, y servidores (como telemetría, NetFlow, meta data, etc.) usando un simple constructor de consultas
1.45	Contar con la capacidad de hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda.
1.46	Contar con la capacidad que desde el resultado de una búsqueda poder ejecutar acciones de respuesta y generar un análisis de causa raíz
1.47	Contar con la capacidad de poder construir, guardar y reutilizar búsquedas para Threat Hunting básico
1.48	Detectar proactivamente búsquedas automáticas de IoC publicados por el vendor
1.49	Contar con la funcionalidad Threat Intelligence embebida, la cual debe ser capaz de identificar la campana asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.
1.50	Contar con la capacidad de tener enlaces desde la consola centralizada de visibilidad de eventos a la documentación del framework de MITRE ATT&CK
1.51	Contar con la capacidad que desde una sola ubicación poder iniciar y ver el estado de respuesta del endpoint, email, servidores y red.
1.52	Permitir tener opciones de respuesta “context aware” para acciones rápida desde la plataforma
1.53	Permitir ejecutar acciones de respuesta rápidamente haciendo click derecho en el workbench o desde los resultados de búsqueda de Threat Intelligence
1.54	Contar con la funcionalidad de un API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR
1.55	Proveer un conector para Splunk nativo
1.56	Contar con una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud
2.	**CONDICIONES DE GARANTIA:** La garantía consiste en mantener en perfecto estado de funcionamiento todas las licencias instaladas en la plataforma adquirida a través de la suscripción del contrato.
2.1	El tiempo de garantía será hasta el 22 de diciembre del 2022 contado a partir de la activación del licenciamiento objeto del presente proceso de contratación.
2.2	La aplicación de la garantía no puede generar costos adicionales a los especificados en la PROPUESTA. Para tal efecto, el PROPONENTE debe considerar todos los costos de configuración y los que juzgue necesarios para cumplir efectivamente con el tiempo de garantía ofrecido en la propuesta.
2.3	Durante el período de la garantía realizar visitas en sitio para verificar la configuración, comportamiento y estabilización de la plataforma cuyo distanciamiento no podrá ser mayor de 40 días. En los casos de actualizaciones críticas la visita deberá implementarse de forma inmediata.
2.4	Durante todo el periodo de garantía prestar el servicio de atención y solución a los incidentes que se presenten en cada uno de los elementos y componentes de la plataforma que hacen parte del presente proceso de selección, por llamado del Ministerio de Hacienda y Crédito Público y sin costo adicional para el mismo, el cual comprende como mínimo la realización de las siguientes actividades por parte del contratista:

	a. Atender y solucionar las fallas que se presenten, así como la aplicación de los correctivos necesarios para restablecer y preservar el buen funcionamiento de los endpoint, servidores y correo electrónico. b. Prestar asistencia técnica ilimitada mediante la atención presencial, vía telefónica, por correo electrónico o remoto a solicitud del Ministerio de Hacienda y Crédito Público en un esquema de atención 5x8. c. Evaluar e informar al Supervisor del contrato los riesgos derivados de la instalación de actualizaciones. Previo a la ejecución de un cambio o actualización, debe presentar al Supervisor del contrato, un informe en donde se advierta los riesgos y el impacto de los mismos. d. En la planeación contemplada para realizar cualquier cambio se debe tener en cuenta, acciones de retorno, en el evento que se presente algún inconveniente técnico con las funcionalidades implementadas con el fin de garantizar las correctas condiciones de funcionamiento. e. Previa la implementación de una actualización, cambio o configuración el contratista debe presentar al Supervisor del Contrato un informe que contenga la descripción de los recursos requeridos y actividades necesarias para la ejecución de los mismos; así como, los tiempos de no disponibilidad del servicio y las pruebas de correcto funcionamiento posteriores al cambio. f. Previo a la ejecución de los cambios requeridos, se contará con la aprobación y coordinación del supervisor del contrato. g. Posterior a la realización de una actualización, cambio o configuración en la solución, si se presenta un fallo, y mientras se identifica y corrige la falla, se debe desinstalar y dejar instalada la versión que venía funcionando antes de la actualización, sin que esto implique en costo adicional alguno para el Ministerio. h. Todo cambio de actualización, así como desinstalación de versiones de software deberá ser documentado y entregado al supervisor del contrato en un informe, dentro de los cinco (5) días hábiles siguientes a la actualización o desinstalación realizada. i. Cuando se presenten ciberataques a nivel mundial el proveedor deberá enviar al Ministerio informe mediante correo electrónico y deberá realizar de manera proactiva las actualizaciones y/o configuraciones para mitigar los riesgos que estos ataques generen. j. Reinstalar consolas en caso de que se requiera sin costo adicional.
2.5	**TIEMPOS DE RESPUESTA**
	a. Prestar un servicio de atención técnica, a través del cual se recibirán los incidentes reportados por el Ministerio de Hacienda y Crédito Público, en el que se deberá hacer un registro que incluya mínimo los datos de fecha, hora y descripción, el cual se utilizará para identificar y hacer seguimiento al caso reportado.

	b. Responder al incidente reportado por el Ministerio dentro de un plazo no mayor de dos (2) horas contadas a partir del reporte del mismo. Por incidente se entenderá todos los casos de fallas, mal funcionamiento o anomalías que se presente en los bienes y servicios adquiridos objeto del proceso de selección.
2.6	**HORARIO PARA LA PRESTACIÓN DEL SERVICIO**
2.7	Los servicios de soporte y mantenimiento técnico se prestarán de lunes a viernes, en horario de 8 am a 5 pm**.** Los plazos en horas se contarán dentro del horario establecido de tal forma que un plazo estipulado de cuatro horas que empiece a contar a las 4:00 p.m. se suspenderá a las 5:00 p.m. para continuar al día siguiente a partir de las 8:00 a.m., terminando el plazo para este caso, a las 11:00 a.m. del día hábil siguiente. Sin embargo, previo acuerdo con el supervisor del contrato, se pueden realizar las actividades que se consideren en un horario diferente al antes señalado.
3.	**TRANSFERENCIA DE CONOCIMIENTO**
3.1	Realizar transferencia de conocimiento a 5 funcionarios que administren la herramienta del Ministerio de Hacienda y Crédito Público, en la transferencia de conocimiento se proveerá información específica referente a la administración, operación, configuración y manejo para cada uno de los elementos y componentes de la plataforma objeto del presente proceso de selección, así como de las ventajas y mejoras, de los cambios de parámetros o de las configuraciones que se recomienden o se implementen. El contratista acordará con el supervisor del contrato la fecha, el lugar y/o manera como se llevará a cabo la transferencia de conocimiento.
4.	**RECURSO HUMANO:** El contratista deberá dentro de los 5 días hábiles siguientes al inicio del Contrato, presentar ante el Supervisor del Contrato, para su aprobación las hojas de vida del personal que prestará el servicio de soporte, actualización y mantenimiento con mínimo el recurso humano que se relaciona a continuación: Un profesional con**:** ➢ Experiencia mínima certificada de 2 años en la implementación de soluciones de TREND MICRO. Para acreditar la experiencia del profesional se deberá aportar certificaciones que deberán contener como mínimo la siguiente información: • Nombre o razón social de la firma o entidad que emite la certificación • Nombre e identificación de la persona a la que se está certificando • Actividades y/u obligaciones específicas realizadas. • Período de ejecución indicando fechas de inicio y terminación (día, mes y año). ➢ Copia del título académico o acta de grado ➢ Matrícula o Tarjeta Profesional, certificación de vigencia de la misma, expedida por la Entidad que regule el ejercicio de su profesión. ➢ Hoja de vida ➢ Copia de la cédula de ciudadanía

	Para la verificación de experiencia que se acredite por parte de ingenieros, se tendrá en cuenta la experiencia adquirida conforme a lo establecido en la Ley 842 de 2003, es decir la experiencia profesional solo se computará a partir de la fecha de expedición de la matrícula profesional o del certificado de inscripción profesional, respectivamente. Durante la ejecución del proyecto es posible realizar el cambio del recurso humano, siempre y cuando se mantengan las competencias anteriores y no se genere afectación en el desarrollo del contrato, no obstante, en caso de requerirse reemplazo, el mismo deberá ser aprobado por la Entidad, a través de la supervisión contractual, que en todo caso deberá cumplir con los requisitos mínimos habilitantes señalados en los términos de referencia.
5.	**CERTIFICADOS DE FABRICANTE** El proponente deberá aportar con su propuesta, una certificación con fecha de expedición no mayor a 90 días a la fecha máxima de presentación de ofertas, emitida por el fabricante de la solución TREND MICRO, en la que conste que el proponente está autorizado para prestar servicios de soporte y mantenimiento técnico o la prestación de servicios postventa, a dicha solución, Adicionalmente, en la certificación debe constar: • El nivel de membresía del proponente, el cual debe ser el nivel más alto. • En caso de proponentes plurales, la certificación puede ser aportada por alguno de los integrantes
6.	**CONFIDENCIALIDAD**
6.1	El levantamiento de información que realicen los ingenieros o la información que sea entregada por el Ministerio de Hacienda y Crédito Público dentro de las actividades objeto del contrato serán tratados por el Contratista en forma confidencial, adhiriéndose a las políticas de seguridad y de terceros del Ministerio de Hacienda y Crédito Público

ANEXO No. 2

COTIZACION ECONOMICA

COMPONENTES	CANTIDAD	VALOR UNITARIO OFRECIDO INCLUIDO IVA	VALOR TOTAL OFRECIDO INCLUIDO IVA
Suscripción de licencias de XDR TREND MICRO – MODULO VISION ONE	2100		

NOTA 1: La oferta económica deberá realizarse en la plataforma SECOP II

NOTA 2: El valor de la oferta económica deberá incluir la totalidad de los costos directos e indirectos que genere la prestación de los servicios y demás costos inherentes a la ejecución de los requerimientos técnicos mínimos solicitados.

ANEXO No. 3
INFORMACION ADICIONAL

Relacione los 3 contratos más representativos y con objeto similar celebrados en los dos últimos años con otras Entidades Estatales y/o Privadas (número y fecha del contrato, nombre entidad contratante).

No. del Contrato	Fecha del Contrato	Nombre Entidad Contratante

PROVEEDOR

Nombre o Razón Social del Cotizante _____
Nombre del Representante _____
Nit o Cédula de Ciudadanía No. _____ de_____
Dirección _____
Ciudad _____
Teléfono _____
Fax _____
Correo electrónico _____