

	UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA
	Anexo 1. Ficha Técnica

ANEXO 1 FICHA TÉCNICA - RENOVACIÓN Y SOPORTE TÉCNICO DEL LICENCIAMIENTO ANTIVIRUS DE LA ENTIDAD.

SITUACION ACTUAL:

La Unidad Administrativa Especial Migración Colombia dispone de una infraestructura tecnológica distribuida a nivel nacional destinada al procesamiento de la información misional. Para el desarrollo de sus funciones, el personal requiere conectividad a Internet y herramientas de intercambio y colaboración de información corporativa a través de estaciones de trabajo, servidores, buzones de correo electrónico y dispositivos móviles corporativos.

Actualmente, estos activos tecnológicos se encuentran protegidos mediante la suite de seguridad **Trend Micro Vision One**, la cual proporciona capacidades de protección, detección y respuesta EDR/XDR para los diferentes componentes tecnológicos cubiertos por el licenciamiento vigente.

En consecuencia, se requiere adelantar oportunamente la renovación del licenciamiento y su respectivo soporte técnico, con el propósito de garantizar la continuidad de las capacidades de seguridad y protección actualmente dispuestas por la Entidad, evitando interrupciones derivadas del vencimiento del licenciamiento.

Códigos UNSPSC

UNSPSC – Decreto 1082 de 2015 (o norma vigente)			
ÍTEM	GRUPO	CÓDIGO	DENOMINACIÓN (Clase o producto)
1	Productos de Uso Final	43232800	Software de administración de redes
2	Productos de Uso Final	43232900	Software para trabajo en redes
3	Productos de Uso Final	43233200	Software de seguridad y protección
4	Productos de Uso Final	43233700	Software de administración de sistemas
5	Servicios	81112200	Mantenimiento y soporte de software

ESPECIFICACIONES TÉCNICAS DEL OBJETO DEL PROCESO DE CONTRATACIÓN

CUADRO DE CANTIDADES:

A continuación, se relacionará el cuadro de cantidades y denominación técnica de las licencias de antivirus que se pretenden renovar, así como las licencias nuevas que se pretenden adquirir y el correspondiente soporte que este servicio requiere.

	UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA
	Anexo 1. Ficha Técnica

ÍTEM	DESCRIPCIÓN	CANTIDAD
1	RENOVACIÓN/SUMINISTRO -Protección para Endpoint – Estaciones de trabajo (1900) y servidores (50), un (1) año de actualizaciones y soporte, a partir de la firma del acta de inicio.	1900/50
2	RENOVACIÓN/SUMINISTRO - TrendAI Flex (credits) Academic 1+ Renew - CREM Core	2400
3	RENOVACIÓN/SUMINISTRO: Protección de la Plataforma de Microsoft Office 365 - Email and Collaboration Security Core y XDR for Email (EmDR)	2400
4	RENOVACIÓN/SUMINISTRO: Protección de dispositivos móviles y Tablet	150
5	Soporte especializado, por un (1) año, para todos los componentes de la Plataforma de seguridad Trend Micro, que comprende la atención en modalidad 5X8X4 de los siguientes servicios: • Actualizaciones, las que se requieran en el año, • Atención y solución incidentes en sitio los que se requieran en el año. • Monitoreo, Despliegue y transferencia de conocimiento de las soluciones contratadas.	1

ESPECIFICACIONES Y CARACTERISTICAS TÉCNICAS MÍNIMAS REQUERIDAS

A. PROTECCIÓN EDR XDR PARA ESTACIONES DE TRABAJO Y SERVIDORES:

Renovación/suministro de licenciamiento de protección para 1.900 estaciones de trabajo y 50 servidores, incluyendo capacidades de gestión de exposición al riesgo, un (1) año de actualizaciones y soporte.

Ítem	Característica técnica requerida	Cant.	Unidad
1.1	Arquitectura, administración y compatibilidad Plataforma de protección de endpoints y servidores de nueva generación, con capacidades EPP/NGAV y EDR o funcionalidades equivalentes. • Consola de administración centralizada, en modalidad nube, local o híbrida, indicando el modelo ofertado.	1900 / 50	Licencias

Ítem	Característica técnica requerida	Cant.	Unidad
	- Compatible con estaciones de trabajo y servidores Windows, Linux y macOS soportados por el fabricante. - Administración centralizada de políticas de seguridad por grupos, sedes, áreas, criticidad o tipo de activo. - Administración basada en roles, perfiles o privilegios diferenciados para usuarios administradores. - Registro de auditoría de acciones administrativas realizadas en la consola. - Actualización automática de agentes, motores, firmas, reglas, sensores o componentes de protección. - Comunicación segura entre los agentes y la consola mediante protocolos cifrados. - Capacidad de despliegue, actualización y administración remota de agentes		
1.2	Prevención y protección contra amenazas - Protección contra virus, malware, spyware, ransomware, troyanos, amenazas persistentes y amenazas de día cero. - Motor de detección basado en firmas, reputación, comportamiento, machine learning, inteligencia artificial o tecnología equivalente. - Protección contra ransomware, incluyendo bloqueo, contención, recuperación o mecanismo equivalente para reducir el impacto sobre archivos afectados. - Protección contra explotación de vulnerabilidades, ataques fileless, scripts maliciosos, macros, PowerShell, WMI o técnicas similares. - Control de aplicaciones permitidas, no permitidas o de comportamiento riesgoso. - Control de dispositivos externos, incluyendo USB y medios removibles. - Firewall de host, prevención de intrusiones a nivel de host o funcionalidad equivalente. - Protección contra manipulación, desactivación o desinstalación no autorizada del agente de seguridad.	1900 / 50	Licencias

	UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA
	Anexo 1. Ficha Técnica

Ítem	Característica técnica requerida	Cant.	Unidad
	Capacidad de aplicar políticas diferenciadas para estaciones de trabajo y servidores.		
1.3	Detección, respuesta e investigación - Capacidades de detección y respuesta ante amenazas en endpoints y servidores. - Aislamiento remoto de equipos comprometidos o sospechosos. - Cuarentena, bloqueo, eliminación o contención de archivos maliciosos o sospechosos. - Terminación remota de procesos maliciosos o no autorizados. - Visualización de eventos de seguridad asociados al endpoint o servidor afectado. - Línea de tiempo, trazabilidad o reconstrucción de eventos relacionados con una amenaza. - Identificación de indicadores de compromiso asociados a archivos, procesos, conexiones, usuarios, dominios, direcciones IP o hashes. - Clasificación de alertas por severidad, criticidad o nivel de riesgo. - Asociación de eventos con tácticas, técnicas y procedimientos de ataque, preferiblemente bajo MITRE ATT&CK o marco equivalente. - Recomendaciones de contención, investigación y remediación.	1900 / 50	Licencias
1.4	Gestión de exposición, inventario, reportes e integraciones - Inventario de activos protegidos, incluyendo nombre del equipo, sistema operativo, dirección IP, usuario asociado, versión del agente y estado de protección. - Identificación de vulnerabilidades, configuraciones inseguras, exposición al riesgo o postura de seguridad del activo, según capacidades de la solución ofertada. - Priorización de riesgos considerando criticidad, severidad, exposición, amenaza activa o impacto potencial. - Recomendaciones de remediación, mitigación o mejora de postura de seguridad.	1900/50	Licencias

	UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA
	Anexo 1. Ficha Técnica

Ítem	Característica técnica requerida	Cant.	Unidad
	• Tableros ejecutivos y técnicos sobre estado de protección, amenazas detectadas, activos vulnerables, eventos críticos y cumplimiento de políticas. • Reportes exportables en formatos comunes como PDF, CSV, XLSX o equivalentes. • Generación de alertas ante eventos críticos o fallas de protección. • Integración mediante API, syslog, conectores o mecanismos equivalentes con SIEM, SOAR, XDR u otras herramientas de seguridad existentes. • Conservación o consulta histórica de eventos de seguridad, según las capacidades y condiciones de la solución ofertada. • Vigencia de licenciamiento por un (1) año, a partir del vencimiento del licenciamiento actual o desde la activación del servicio, según aplique.		

B. TrendAI CREM Core:

Renovación - TrendAI CREM Core para 2400 usuarios.

Ítem	Característica técnica requerida	Cant.	Unidad
2.1	Cumplimiento, reportes y cuantificación de riesgo: mapeo automatizado frente a marcos de cumplimiento, generación de reportes listos para auditoría y visualización del riesgo técnico traducido a impacto de negocio para la toma de decisiones.	2.400	Licencias
2.2	Automatización de remediación: recomendaciones guiadas por IA, playbooks automatizados y acciones de mitigación —incluido parcheo virtual cuando aplique— para reducir el tiempo de respuesta y la exposición.		
2.3	Descubrimiento continuo de superficie de ataque: identificación en tiempo real de activos conocidos, desconocidos, no administrados y de terceros, incluyendo identidades, dispositivos, activos cloud, redes y aplicaciones.		

	UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA
	Anexo 1. Ficha Técnica

Ítem	Característica técnica requerida	Cant.	Unidad
2.4	Gestión y priorización de vulnerabilidades basada en riesgo: evaluación contextual que prioriza las exposiciones según criticidad del activo, actividad de amenazas, probabilidad de explotación e impacto para el negocio; no solo por la severidad CVSS.		

C. PROTECCIÓN PARA LA PLATAFORMA MICROSOFT 365:

Renovación/suministro de licenciamiento de protección para 2.400 usuarios/buzones sobre la plataforma Microsoft Office 365 (Exchange Online, Teams, SharePoint, OneDrive).

Ítem	Característica técnica requerida	Cant.	Unidad
2.1	Arquitectura, integración y administración - Integración con Microsoft 365 (Exchange Online, Teams, SharePoint y OneDrive) mediante API, conectores o mecanismos soportados por el fabricante. - Consola centralizada para la administración de políticas de seguridad del correo electrónico y plataformas de colaboración. - Administración de políticas por usuarios, grupos, dominios o unidades organizacionales. - Compatibilidad con autenticación mediante Microsoft Entra ID o mecanismos equivalentes. - Actualización automática de motores, reglas, indicadores y componentes de protección. - Registro de auditoría de eventos y acciones administrativas.	2.400	Licencias
2.2	Protección frente a amenazas - Protección contra phishing, spear phishing, compromiso de correo empresarial (BEC), suplantación de dominio, remitente o identidad. - Protección contra malware, ransomware y amenazas de día cero. - Análisis de archivos adjuntos mediante sandboxing o tecnología funcionalmente equivalente.	2.400	Licencias

	UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA
	Anexo 1. Ficha Técnica

Ítem	Característica técnica requerida	Cant.	Unidad
	- Protección contra enlaces maliciosos mediante análisis en tiempo de clic (time-of-click) o mecanismo equivalente. - Detección de archivos maliciosos compartidos en Exchange Online, SharePoint, OneDrive y Teams. - Detección basada en firmas, reputación, comportamiento, inteligencia artificial, machine learning o tecnologías equivalentes.		
2.3	Detección, respuesta, reportes e integración - Capacidad de búsqueda, investigación y remediación de correos electrónicos ya entregados. - Capacidad de poner en cuarentena, eliminar o retirar mensajes maliciosos de los buzones cuando la solución lo permita. - Generación de alertas y notificaciones sobre amenazas detectadas. - Reportes ejecutivos y técnicos sobre amenazas, tendencias, usuarios afectados y eventos de seguridad. - Exportación de reportes en formatos estándar (PDF, CSV, XLSX o equivalentes). - Integración mediante API, Syslog o mecanismos equivalentes con plataformas SIEM, SOAR o herramientas de monitoreo existentes. - Vigencia del licenciamiento por un (1) año a partir del vencimiento del licenciamiento actual o desde la activación del servicio, según aplique.	2.400	Licencias

D. PROTECCIÓN PARA DISPOSITIVOS MÓVILES Y TABLETS:

Renovación/suministro de licenciamiento de protección para 150 dispositivos móviles y tabletas corporativas.

	UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA
	Anexo 1. Ficha Técnica

Ítem	Característica técnica requerida	Cant.	Unidad
3.1	Arquitectura, administración y compatibilidad - Solución de defensa contra amenazas móviles (Mobile Threat Defense – MTD) o tecnología funcionalmente equivalente para dispositivos Android e iOS. - Compatible con las versiones de Android e iOS soportadas por el fabricante. - Integrable con plataformas de gestión de dispositivos móviles (MDM/UEM) mediante conectores, API o mecanismos equivalentes. - Consola centralizada para la administración y monitoreo de dispositivos protegidos. - Administración de políticas de seguridad por grupos, usuarios o dispositivos. - Actualización automática de motores, reglas y componentes de protección.	150	Licencias
3.2	Protección frente a amenazas y evaluación de seguridad - Detección de aplicaciones maliciosas, potencialmente no deseadas o con comportamiento riesgoso. - Detección de dispositivos con jailbreak, root o mecanismos equivalentes que comprometan la integridad del sistema operativo. - Protección contra phishing, enlaces maliciosos y sitios web fraudulentos durante la navegación o el uso de aplicaciones compatibles. - Evaluación de la postura de seguridad del dispositivo, considerando versión del sistema operativo, configuraciones inseguras, vulnerabilidades conocidas y estado general del dispositivo. - Identificación de redes Wi-Fi inseguras o potencialmente maliciosas, cuando la solución lo soporte. - Generación de alertas frente a eventos de seguridad detectados en los dispositivos protegidos.	150	Licencias

	UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA
	Anexo 1. Ficha Técnica

Ítem	Característica técnica requerida	Cant.	Unidad
3.3	Monitoreo, reportes e integración • Inventario de dispositivos protegidos con información del sistema operativo, versión, usuario asociado y estado de protección. • Reportes ejecutivos y técnicos sobre amenazas detectadas, cumplimiento de políticas y estado de seguridad de los dispositivos. • Exportación de reportes en formatos estándar (PDF, CSV, XLSX o equivalentes). • Integración mediante API, Syslog o mecanismos equivalentes con plataformas SIEM, SOAR u otras herramientas de monitoreo cuando la solución lo permita. • Registro de eventos y trazabilidad de incidentes de seguridad asociados a los dispositivos móviles. • Vigencia del licenciamiento por un (1) año a partir del vencimiento del licenciamiento actual o desde la activación del servicio, según aplique.		

E. SOPORTE ESPECIALIZADO:

El contratista deberá prestar soporte técnico especializado para los componentes de la plataforma Trend Micro Vision One objeto del contrato, durante la vigencia del licenciamiento, bajo modalidad 5x8x4.

Cuando una incidencia no pueda ser solucionada mediante atención telefónica o remota y se determine la necesidad de atención presencial, el contratista deberá disponer del personal técnico especializado para la atención en sitio.

La metodología de escalamiento del soporte será la siguiente:

1. Primer nivel: Soporte técnico del contratista.
2. Segundo nivel: Soporte técnico especializado del contratista.
3. Tercer nivel: Soporte técnico del fabricante.

El alcance a la renovación del licenciamiento y soporte técnico especializado que debe brindarse de la siguiente manera:

Las actividades asociadas a la **renovación del licenciamiento Trend Micro Vision One** y sus servicios de soporte técnico especializado deberán prestarse de manera proactiva y

	UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA
	Anexo 1. Ficha Técnica

preventiva, con el fin de minimizar la ocurrencia de incidentes que afecten la disponibilidad, operación y desempeño de la plataforma, garantizando su correcto funcionamiento durante toda la vigencia contractual.

El contratista deberá asegurar que la Entidad disponga de licencias vigentes, suscripciones activas, acceso a actualizaciones, parches, mejoras funcionales, bases de conocimiento, firmas de seguridad, inteligencia de amenazas y demás beneficios ofrecidos por el fabricante para la solución Trend Micro Vision One, sin costo adicional para Migración Colombia durante la vigencia del contrato.

El contratista deberá gestionar ante el fabricante todos los trámites necesarios relacionados con la renovación del licenciamiento, soporte técnico, actualizaciones, incidentes y requerimientos que se presenten sobre la plataforma, garantizando el restablecimiento oportuno del servicio cuando sea requerido.

Durante la vigencia del contrato, el contratista deberá atender todos los requerimientos técnicos que presente la Entidad, incluyendo consultas sobre funcionamiento de la plataforma, configuración, parametrización, optimización, acompañamiento técnico, diagnóstico de incidentes, actividades de soporte especializado y recomendaciones de buenas prácticas de seguridad.

Monitoreo y seguimiento de la plataforma

El contratista deberá realizar actividades de monitoreo y seguimiento continuo sobre la plataforma Trend Micro Vision One, con el fin de verificar su correcto funcionamiento, disponibilidad, estado de los servicios, generación de alertas, recepción de eventos de seguridad y operatividad de los mecanismos de protección implementados. Como resultado de estas actividades, deberá informar oportunamente a la Entidad sobre cualquier anomalía, riesgo identificado o hallazgo relevante que pueda afectar la seguridad o el desempeño de la plataforma, presentando las recomendaciones técnicas correspondientes para su mitigación y mejora continua.

Los requerimientos, incidentes, monitoreo y seguimiento de la plataforma deberán ser atendidos bajo una modalidad de soporte 5X8X4, garantizando disponibilidad permanente para la recepción, escalamiento y seguimiento de casos. Para incidentes críticos que afecten la operación de la plataforma o la visibilidad de eventos de seguridad, el tiempo máximo de respuesta inicial deberá ser de cuatro (4) horas.

Transferencia de conocimiento

	UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA
	Anexo 1. Ficha Técnica

Durante la ejecución del contrato, el contratista deberá realizar actividades de transferencia de conocimiento dirigidas al personal designado por Migración Colombia, orientadas al fortalecimiento de las capacidades técnicas y operativas para la administración, monitoreo, configuración y aprovechamiento de las funcionalidades de Trend Micro Vision One. Estas actividades deberán incluir sesiones de capacitación, acompañamiento técnico, recomendaciones de mejores prácticas, atención de inquietudes y socialización de nuevas funcionalidades o actualizaciones relevantes de la solución, sin generar costos adicionales para la Entidad.

F. ADMINISTRACIÓN DE LA PLATAFORMA DE SEGURIDAD.

El contratista deberá entregar un plan de trabajo acorde con las actividades relacionadas con el objeto del contrato, incluyendo las actividades de administración técnica especializada, monitoreo, soporte, revisión, optimización, actualización y transferencia de conocimiento previstas durante la vigencia contractual.

Adicionalmente, deberá revisar y evaluar el estado de configuración y operación de los componentes de la plataforma Trend Micro Vision One objeto de renovación, incluyendo, según aplique, agentes, sensores, políticas, integraciones, versiones, cobertura y funcionalidades habilitadas, identificando las oportunidades de ajuste y optimización requeridas para su adecuado funcionamiento.