ANEXO N°1

FICHA TÉCNICA

OBJETO: Adquirir y renovar el licenciamiento, soporte y servicios de la plataforma de ciberseguridad Trend Micro Vision One para fortalecer la protección y respuesta ante amenazas que afecten los activos de información de la Superintendencia Nacional de Salud.

Con base en el clasificador de bienes y servicios de las Naciones Unidas, a continuación, se establece el sector económico al que pertenece el servicio a contratar:

UNSPSC	SEGMENTO	FAMILIA	CLASE	PRODUCTO
43222634	43 Difusión de Tecnologías de Información y Comunicaciones	22 Equipos o plataformas y accesorios de redes multimedia o de voz y datos	26 Equipo de servicio de red	34 Dispositivo de monitoreo o manejo de redes
43222503	43 Difusión de Tecnologías de Información y Comunicaciones	22 Equipos o plataformas y accesorios de redes multimedia o de voz y datos	25 Equipo de seguridad en la red	03 Equipos de seguridad de evaluación de vulnerabilidad
43233205	43 Difusión de Tecnologías de Información y Comunicaciones	23 Software	32 Software de seguridad y protección	00 Software de Seguridad y protección
43233200	43 Difusión de Tecnologías de Información y Comunicaciones	23 Software	32 Software de seguridad y protección	05 Software de seguridad de transacciones y de protección contra virus
81112202	81 Servicios Basados en Ingeniería, Investigación y Tecnología	11 Servicios informáticos	22 Mantenimiento y soporte de software	02 Actualizaciones o parches de software

BIENES Y SERVICIOS A CONTRATAR

CATEGORÍA	PRODUCTO	CANTIDAD	SKU
SOPORTE DE FABRICANTE Y LICENCIAMIENTO			
Renovación	Trend Vision One - Endpoint Security (Essentials)	1300	VORA0036
Adquisición	Trend Vision One - Endpoint Security (Pro)	300	VORA0043
Renovación	Trend Vision One Email and Collaboration Security – Essentials	1250	VORA0126

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

ISO 14001:2015 BUREAU VERITAS Certification
Estamos certificados

CATEGORÍA	PRODUCTO	CANTIDAD	SKU
Renovación	Service Add-on to Apex One a través de Trend Vision One Credits	1600	ADRA0012
Adquisición	Trend Vision One (CREM) - Cyber Risk Exposure Management - Essentials	2850	VORA0204
Renovación	Deep Discovery Inspector Series 1000 - 1Gbps - Software only	1	DDRI0003
SERVICIOS			
Adquisición	Instalación, configuración y puesta en funcionamiento **y transferencia de conocimiento de la solución integral Trend Micro Vision One**	1	SVRADMIN
Adquisición	Bolsa de horas de servicios profesionales especializados (**soporte, mantenimiento, afinamiento y atención de incidentes cibernéticos**, etc.)	1500	SVRSUPP
CAPACITACIÓN			
Adquisición	Vouchers de certificación	4	SVRSUPP

DESCRIPCIÓN DETALLADA DE LOS BIENES Y SERVICIOS A CONTRATAR

LÍNEA	PRODUCTO	CANTIDAD	DESCRIPCIÓN
Renovación	**Trend Micro Vision One Endpoint Security Essential**	**1.300 licencias**	Renovación de licenciamiento hasta el 30 de diciembre de 2028, de Trend Vision One Endpoint Security Essential, incluyendo los siguientes módulos o funciones: 1. Protección para sistemas operativos Windows, Linux y Mac OS. 2. Antimalware y análisis de comportamiento. 3. Aprendizaje de máquina y reputación web. 4. Control de dispositivos. 5. Prevención de pérdida de datos (DLP). 6. Firewall local. 7. Control de aplicaciones. 8. Prevención de intrusos (IPS). 9. Virtualización de protección.
Adquisición	**Trend Micro Vision One Endpoint Security Pro**	**300 licencias**	Renovación de licenciamiento hasta el 30 de diciembre de 2028, de Trend Micro Vision One Endpoint Security Pro que incluye los siguientes módulos o funciones: 1. Cloud One Workload Security. 2. Antimalware Protection.

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

ISO 14001:2015 BUREAU VERITAS Certification

Estamos certificados

LÍNEA	PRODUCTO	CANTIDAD	DESCRIPCIÓN
			3. File Integrity Monitoring. 4. Intrusion Prevention con parchado virtual. 5. Firewall de host. 6. Control de aplicaciones. 7. XDR (Extended Detection and Response).
Renovación	**Trend Micro Vision One Email and Collaboration Essentials**	**1.250 licencias**	Renovación de licenciamiento hasta el 30 de diciembre de 2028, de Trend Micro Vision One Email and Collaboration Essentials, incluyendo los siguientes módulos o funciones: 1. Protección en la nube para correo y plataformas de colaboración. 2. Protección desde la puerta de enlace de correo. XDR para correo electrónico. 3. Gestión del riesgo de exposición cibernética (CREM). 4. Visibilidad y análisis centralizados.
Renovación	**Trend Micro Apex One Sandbox as a Service Add-on**	**1.600 licencias**	Renovación de licenciamiento hasta el 30 de diciembre de 2028, de Trend Micro Apex One Sandbox as a Service Add-on Antimalware, incluyendo los siguientes módulos o funciones: 1. Add-on de Sandbox para la solución de protección de endpoints, que funcione sobre el mismo agente de manera automática; toda la solución debe ser monomarca. 2. Funcionalidad para la inspección de archivos sospechosos en ambientes controlados en la nube. Por cada producto de la suite del antivirus y para la solución de detección de amenazas avanzadas, el proveedor deberá ofrecer la última versión disponible en el mercado o la que la Superintendencia requiera y esté soportada por la casa matriz.
Adquisición	**Trend Micro Vision One – Cyber Risk Exposure Management (CREM) Essential**	**2.850 créditos**	Adquisición de créditos hasta el 30 de diciembre de 2028, correspondientes al módulo Cyber Risk Exposure Management (CREM) de Trend Vision One, que permite la gestión integral del riesgo cibernético de la Entidad. **Incluye los siguientes módulos o funciones:** 1. Descubrimiento automático de activos locales y en la nube. 2. Evaluación y priorización de vulnerabilidades.

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

ISO 14001:2015 BUREAU VERITAS Certification
icontec Carbono Neutro Certificado
Estamos certificados

LÍNEA	PRODUCTO	CANTIDAD	DESCRIPCIÓN
			3. Gestión de la superficie de ataque (*Attack Surface Management*). 4. Cumplimiento normativo y auditoría continua. 5. Cuantificación de riesgo y exposición cibernética. 6. Automatización de acciones de mitigación. Visibilidad integral mediante paneles ejecutivos (*Dashboards*) y reportes analíticos. **Nota técnica:** Este producto se rige bajo el esquema de licenciamiento por créditos (Credit-Based Licensing) de Trend Micro. Los créditos se asignan dinámicamente desde la consola Vision One, en función del número de activos evaluados y del alcance de las funciones activas. Este modelo permite redistribuir los créditos durante la vigencia del soporte, garantizando flexibilidad operativa y optimización de recursos.
Renovación	**Trend Micro Deep Discovery Inspector (DDI) – 1 Gbps (Software Only)**	**1 (renovación de licencia)**	Renovación del licenciamiento del Deep Discovery Inspector (DDI) 1 Gbps hasta el 30 de diciembre de 2028, correspondiente al analizador de tráfico de red que permite la detección temprana de amenazas avanzadas y malware en movimiento lateral dentro de la infraestructura de la Entidad. **Incluye las siguientes funcionalidades:** 1. Análisis de tráfico en red para detección de amenazas persistentes avanzadas (*APT*). Identificación de malware y comportamientos anómalos en tiempo real. 2. Inspección profunda de paquetes (*Deep Packet Inspection*). 3. Detección de comunicaciones con servidores de comando y control (*C&C*). 4. Integración nativa con la consola Trend Vision One XDR, para correlación de eventos entre red, endpoint y correo. 5. Capacidad de inspección de hasta 1 Gbps de tráfico con soporte de actualizaciones continuas de firmas y motores.

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

ISO 14001:2015 BUREAU VERITAS Certification
icontec Carbono Neutro Certificado
Estamos certificados

LÍNEA	PRODUCTO	CANTIDAD	DESCRIPCIÓN
Adquisición	**Instalación, configuración, puesta en funcionamiento y transferencia de conocimiento de la solución integral Trend Micro Vision One**	**1**	Implementación, configuración, puesta en marcha y transferencia de conocimiento de todas las soluciones Trend Micro incluidas en el presente proceso (Trend Vision One Endpoint Security Essentials, Endpoint Security Pro, Email and Collaboration Essentials, Apex One Sandbox as a Service Add-on, Cyber Risk Exposure Management (CREM) Essential, y Deep Discovery Inspector 1Gbps), garantizando su correcta integración, interoperabilidad y funcionamiento dentro de la infraestructura tecnológica de la Superintendencia Nacional de Salud. **Incluye:** 1. Instalación y configuración inicial de la consola Trend Vision One y de todos los módulos contratados y renovados con el fabricante. 2. Activación de conectores de telemetría y correlación entre endpoints, red, correo y nube. 3. Integración del licenciamiento, sincronización con los servicios de Trend Micro y validación de compatibilidad con la infraestructura institucional. 4. Ejecución de pruebas funcionales, verificación de comunicación, detección y generación de reportes de seguridad. 5. Elaboración y entrega de documentación técnica del despliegue, parámetros de configuración y manual operativo básico. 6. Transferencia de conocimiento a mínimo dos (2) funcionarios designados por el supervisor del contrato, con una duración mínima de 15 horas, sobre la administración, operación y monitoreo de la solución integral implementada. **Objetivo:** asegurar la correcta operación y alineación de la plataforma de ciberseguridad con las políticas institucionales, permitiendo la administración centralizada, la visibilidad integral y el monitoreo unificado de amenazas desde la consola Trend Vision One.

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

ISO 14001:2015 BUREAU VERITAS Certification
icontec Carbono Neutro Certificado
Estamos certificados

LÍNEA	PRODUCTO	CANTIDAD	DESCRIPCIÓN
Adquisición	**Bolsa de horas de servicios profesionales especializados para soporte, mantenimiento, afinamiento y atención de incidentes cibernéticos**	**1.500 horas**	Prestación Servicios profesionales especializados bajo modalidad de bolsa de horas, orientada a garantizar la operación continua, el mantenimiento, la actualización y la atención de incidentes durante la vigencia del soporte contratado de la solución integral Trend Micro Vision One implementada en la Superintendencia Nacional de Salud que comprende los productos Endpoint Security Essentials, Endpoint Security Pro, Email & Collaboration Essentials, Apex One Sandbox as a Service Add-on, Cyber Risk Exposure Management (CREM) Essential y Deep Discovery Inspector 1Gbps. **Alcance de las actividades cubiertas por la bolsa:** 1. Soporte técnico especializado 7x24 en modalidad presencial o remota, para atender incidentes, anomalías o fallas de la plataforma que afecten su disponibilidad o desempeño. 2. Atención reactiva ante incidentes cibernéticos, garantizando respuesta inmediata y sin restricción de tiempo ante ataques, infecciones o cualquier evento de seguridad que afecte la infraestructura tecnológica. El contratista deberá disponer de los recursos humanos y tecnológicos necesarios hasta el restablecimiento total del servicio en un 100 %. 3. Mantenimiento preventivo mensual, con revisión de estado de la plataforma, políticas, motores, parches, registros y módulos habilitados, asegurando su correcta operación conforme a las directrices del fabricante. 4. Mantenimiento correctivo, con diagnóstico y solución de fallas detectadas en componentes, conectores o integraciones de Vision One. 5. Afinamiento y optimización de políticas de seguridad, ajuste de reglas de detección, correlación de eventos, umbrales de alerta, integraciones con correo, endpoints y red, así como evaluación de desempeño. 6. Gestión y aplicación de actualizaciones, asegurando que todos los componentes cuenten con las últimas versiones y definiciones publicadas por Trend Micro.

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

ISO 14001:2015 BUREAU VERITAS Certification

Estamos certificados

LÍNEA	PRODUCTO	CANTIDAD	DESCRIPCIÓN
			7. Análisis forense y respuesta avanzada a incidentes, coordinando con el fabricante para la investigación de eventos de seguridad de alto impacto. 8. Documentación técnica, trazabilidad y reportes: el contratista deberá generar reportes de cada actividad ejecutada y mantener una matriz de control de uso de horas con detalle de fechas, personal asignado, actividad desarrollada y estado de cierre. Recurso humano mínimo exigido: **Perfil 1:** Ingeniero líder técnico • Formación académica: Ingeniero en Sistemas, Telecomunicaciones, Electrónica o áreas afines. • Especialización en Seguridad de la Información o Informática. • Certificaciones requeridas: – CISM (Certified Information Security Manager) – CEH (Certified Ethical Hacker) v10 o superior – CISSP (Certified Information Systems Security Professional) – IPv6 Certified Security Engineer (Gold) – Certificado o constancia de entrenamiento emitido por Trend Micro en Trend Vision One Endpoint Security Advance. • **Experiencia:** mínimo dos (2) años en administración, soporte y resolución de problemas de soluciones Trend Micro. • **Obligación:** anexar documento mediante el cual se compromete a prestar sus servicios en caso de adjudicación. **Funciones principales:** • Dirigir y ejecutar la implementación, configuración, administración y soporte especializado de las soluciones Trend Micro durante la ejecución del contrato. • Garantizar el desempeño óptimo y alineación con las políticas de seguridad institucional. Diseñar y aplicar políticas de protección en endpoints.

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

ISO 14001:2015 BUREAU VERITAS Certification
icontec Carbono Neutro Certificado
Estamos certificados

LÍNEA	PRODUCTO	CANTIDAD	DESCRIPCIÓN
			• Gestionar incidentes. • Coordinar con el fabricante. • Generar reportes técnicos y ejecutivos. • Proponer mejoras continuas y realizar transferencia de conocimiento al personal de la Entidad. **Perfil 2: Técnico especializado:** • Formación académica: Técnico o tecnólogo en sistemas, telecomunicaciones, electrónica o afines. • Certificaciones requeridas: – Trend Vision One Endpoint Security Advance – Vision One XDR (bajo la denominación anterior del fabricante), o “Trend Vision One™ Security Operations Professional (Training y/o Exam)” (bajo la denominación actual del fabricante). • Experiencia: mínimo dos (2) años en administración, soporte y resolución de problemas de soluciones Trend Micro. • Obligación: anexar documento mediante el cual se compromete a prestar sus servicios en caso de adjudicación. **Actividades asignadas:** atención de casos de soporte, ejecución de mantenimientos, levantamiento de evidencias y comunicación continua con la supervisión de la Entidad. **Acuerdos de Nivel de Servicio (ANS):** • **Nivel 5 – Crítico:** afecta la operación del negocio (ej. servidor de base de datos caído). Atención inmediata. Respuesta telefónica: 30 min. Asistencia en sitio: máximo 2 horas. • **Nivel 4 – Urgente:** puede afectar la operación si no se resuelve oportunamente (ej. falla en la recepción de correos). Respuesta telefónica: 2 horas. Asistencia en sitio: máximo 4 horas. • **Nivel 3 – Importante:** no afecta la operación del negocio, pero requiere solución. Respuesta telefónica: 4 horas. Asistencia en sitio: dentro de la misma semana.

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

ISO 14001:2015 BUREAU VERITAS Certification
icontec Carbono Neutro Certificado
Estamos certificados

LÍNEA	PRODUCTO	CANTIDAD	DESCRIPCIÓN
			• **Nivel 2 – Monitoreo:** sin afectación operativa. Atención durante la semana siguiente al evento. • **Nivel 1 – Información:** consultas o verificaciones. Atención durante el mes siguiente. **Objetivo:** Garantizar la continuidad, estabilidad, seguridad y disponibilidad de las plataformas Trend Micro de la Superintendencia Nacional de Salud, mediante la provisión de soporte especializado, respuesta oportuna ante incidentes y mantenimiento integral, asegurando el cumplimiento de los niveles de servicio y la preservación de la postura de ciberseguridad institucional.
Adquisición	**Capacitación y entrenamientos certificados oficiales Trend Micro (vouchers de certificación)**	**4 vouchers**	Adquisición de cuatro (4) entrenamientos certificados oficiales del fabricante Trend Micro, orientados al fortalecimiento de las competencias técnicas del personal de la Subdirección de Tecnologías de la Información (STI) de la Superintendencia Nacional de Salud, en la administración, operación y respuesta ante incidentes de las soluciones implementadas bajo la plataforma Trend Micro Vision One. **Alcance del servicio de capacitación:** 1. Acceso a cursos oficiales dictados por Trend Micro Education Services o centros de entrenamiento autorizados por el fabricante. 2. Entrenamientos con certificación internacional válida y material de estudio oficial del fabricante, que incluyen laboratorios prácticos, evaluaciones y voucher de examen. 3. Modalidad virtual o presencial, en idioma español o inglés (según disponibilidad del fabricante). 4. La capacitación debe cubrir los siguientes cursos oficiales o equivalentes: • **Trend Vision One XDR Administrator** (gestión y correlación de eventos). • **Trend Vision One Endpoint Security Advanced** (configuración y administración de endpoints). • **Apex One Advanced Protection** (detección avanzada y control de amenazas). • **Deep Discovery Inspector Administrator** (detección de amenazas en red).

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

ISO 14001:2015 BUREAU VERITAS Certification
icontec Carbono Neutro Certificado
Estamos certificados

LÍNEA	PRODUCTO	CANTIDAD	DESCRIPCIÓN
			Requisitos adicionales: • Cada participante deberá contar con acceso completo a los entornos de laboratorio oficiales del fabricante. • Los certificados deberán emitirse a nombre de los funcionarios designados por la Entidad. • El contratista deberá gestionar la inscripción, seguimiento y entrega formal de los certificados al supervisor del contrato.

Para cumplir el objeto del contrato, el contratista deberá en cumplir y satisfacer las especificaciones técnicas en cada licencia, las especificaciones mínimas de aceptación de estas son:

Trend Vision One – Endpoint Security Essentials
Protección de Endpoints
La solución debe permitir despliegue y administración centralizada en nube (consola SaaS del fabricante) y operación en entornos híbridos, garantizando alta disponibilidad de la consola y acceso seguro mediante roles y MFA.
La solución debe contar con un agente unificado por endpoint, capaz de ejecutar protección antimalware, antiransomware, control de aplicaciones, control de dispositivos (USB/medios extraíbles) y protección web en tiempo real.
La solución debe incorporar detección basada en comportamiento y machine learning (online/offline) para prevenir malware desconocido, con capacidades de rollback cuando aplique y cuarentena local administrada.
La solución debe incluir protección contra exploits y mitigación de vulnerabilidades a nivel de endpoint (end-point exploit protection / virtual patching cuando aplique), reduciendo la superficie de ataque sin depender de parches del SO.
La solución debe integrarse nativamente con la plataforma Trend Vision One (XDR) para correlación de telemetría, investigación y respuesta, sin requerir la compra de consolas adicionales ajenas al portafolio contratado.
La solución debe soportar los sistemas operativos de endpoint vigentes según matriz del fabricante (p. ej., Windows 10/11 y versiones soportadas de macOS), con actualización transparente del agente.
La solución debe permitir políticas por grupos (usuarios, unidades, OU/sitios), herencia y excepciones finas (hash, ruta, certificado, URL/categoría) y modo de protección por perfiles (altamente restrictivo/estándar/flexible).
La solución debe ofrecer Actualizaciones automáticas y continuas de motores, firmas y reputación (web/file) durante toda la vigencia de las licencias sin costos adicionales, con ventanas de mantenimiento configurables.
La solución debe proveer reportes y tableros (infecciones, amenazas bloqueadas, cumplimiento de políticas, endpoints desactualizados), con exportación a CSV/PDF y envío programado por correo.
La solución debe integrarse con Apex One Sandbox as a Service (adquirido en este proceso) para detonación de archivos sospechosos y enriquecimiento de veredictos en el endpoint.

ISO 14001:2015 BUREAU VERITAS Certification

Estamos certificados

La solución debe permitir instalación masiva (paquetes MSI/DMG, GPO/Intune/SCCM/MDM) y descubrimiento de endpoints no gestionados para facilitar su incorporación.
La solución debe operar sin dependencia de conexión permanente (protección local cuando el equipo está fuera de red), sincronizando eventos y políticas al reconectarse.
La solución debe garantizar telemetría cifrada entre agente y consola y permitir auditoría de cambios de configuración (quién, cuándo, qué).
La solución debe habilitar restauración/rollback cuando corresponda y mecanismos de auto-protección del agente (anti-tamper) para evitar su desactivación no autorizada.
La solución debe permitir definición de listas blancas y negras por hash, editor, ruta y reputación, así como listas de exclusión para evitar conflictos con aplicaciones críticas de la Entidad.
La solución debe cumplir con los lineamientos de soporte y ANS conforme a lo establecido en la Ficha Técnica.
Despliegue del agente en un grupo piloto y aplicación de políticas base.
Simulación controlada de detección (archivo de prueba) y verificación de acciones automáticas (bloqueo/cuarentena/log).
Verificación de actualización de motores/firmas y visibilidad de eventos en consola.
Prueba de integración con Vision One (XDR) y Sandbox: envío de artefacto a detonación y recepción de veredicto en consola.
Entrega de informe de puesta en marcha con capturas, políticas vigentes y evidencias.
Trend Vision One – Endpoint Security Pro - Protección Avanzada de Endpoints
La solución debe ofrecer todas las capacidades de Endpoint Security Essentials (antimalware, machine learning, firewall local, control de dispositivos, control de aplicaciones, DLP, prevención de intrusos, reputación web, virtual patching), más funciones avanzadas específicas de la edición Pro.
La solución debe incluir Cloud One Workload Security integrado en el mismo agente, para extender la protección hacia cargas de trabajo en entornos virtuales y de nube, con políticas unificadas.
La solución debe contar con File Integrity Monitoring (FIM) que permita monitorear en tiempo real los cambios en archivos críticos del sistema y aplicaciones, generando alertas centralizadas y evidencias para auditoría.
La solución debe ofrecer Intrusion Prevention System (IPS) a nivel de host con parchado virtual de vulnerabilidades, reduciendo el riesgo de explotación de fallos sin necesidad de aplicar parches inmediatos del fabricante del sistema operativo o de aplicaciones.
La solución debe incorporar un firewall de host avanzado, con control granular de tráfico entrante y saliente, segmentación por aplicación y capacidad de aplicar políticas diferenciadas por grupos.
La solución debe permitir respuestas automatizadas ante incidentes (ej. aislamiento de endpoint, bloqueo de proceso, eliminación de archivo malicioso), configurables desde la consola central.
La solución debe integrarse nativamente con Trend Vision One (XDR) para correlación de eventos entre endpoints, correo, red y nube, generando alertas enriquecidas y detecciones tempranas de ataques avanzados.
La solución debe incluir mecanismos de sandboxing integrado, en coordinación con el servicio Apex One Sandbox as a Service, para análisis de archivos sospechosos en entornos controlados.
La solución debe soportar integración con herramientas de SIEM mediante syslog o conectores nativos, enviando eventos de seguridad para consolidar la trazabilidad institucional.

ISO 14001:2015 BUREAU VERITAS Certification

Estamos certificados

La solución debe garantizar la disponibilidad de reportes especializados de cumplimiento (ejemplo: endpoints vulnerables, eventos IPS aplicados, integridad de archivos alterada, endpoints aislados), descargables y programables.
La solución debe ser administrable mediante consola SaaS multicliente de Trend Micro, con roles y permisos jerárquicos, autenticación de múltiples factores (MFA) y auditoría de cambios de configuración.
La solución debe garantizar actualizaciones automáticas y continuas de motores, firmas, políticas y módulos avanzados durante la vigencia de las licencias
La solución debe contar con auto-protección del agente (anti-tamper) para evitar su desactivación, modificación no autorizada o desinstalación por usuarios finales o malware.
La solución debe ser monomarca y no requerir agentes adicionales distintos al de Trend Micro para habilitar las funcionalidades avanzadas de seguridad.
Instalación del agente Pro en un grupo piloto de endpoints y validación de coexistencia con Essentials.
Simulación de vulnerabilidad en un endpoint y verificación de bloqueo mediante IPS (parchado virtual).
Generación de un cambio en un archivo crítico y validación de alerta en consola por File Integrity Monitoring.
Simulación de actividad sospechosa y verificación de acción de aislamiento automático del endpoint.
Validación de integración con Trend Vision One (XDR), evidenciando correlación de eventos.
Trend Vision One – Email & Collaboration Security Essentials - Protección de Correo y Plataformas de Colaboración
La solución debe integrarse de forma nativa con los servicios de correo electrónico institucional en la nube (ej. Microsoft 365 Exchange Online) y con las herramientas de colaboración (ej. Teams, OneDrive, SharePoint), sin necesidad de dispositivos adicionales ni agentes intermedios.
La solución debe proporcionar protección avanzada contra spam, phishing y spear-phishing, con análisis de reputación de remitentes, verificación de dominios (DMARC, DKIM, SPF) y bloqueo de correos fraudulentos.
La solución debe detectar y bloquear archivos adjuntos maliciosos utilizando múltiples capas de defensa: firmas, análisis de comportamiento, machine learning y sandboxing en la nube.
La solución debe incluir análisis de URLs en correos y documentos, verificando enlaces en tiempo real antes de permitir el acceso del usuario, con capacidad de reescritura dinámica de URL (URL rewriting) y protección contra redirecciones.
La solución debe ofrecer protección frente a Business Email Compromise (BEC) y ataques dirigidos, mediante análisis de patrones de comunicación, suplantación de identidad y detección de anomalías en el comportamiento de los remitentes.
La solución debe permitir la aplicación de políticas granulares por grupos o dominios, configurables desde consola SaaS, con opciones de cuarentena, bloqueo, entrega diferida o notificación al usuario.
La solución debe generar reportes centralizados de detecciones (correos bloqueados, URLs maliciosas, adjuntos sospechosos, ataques BEC), con exportación programada a PDF/CSV y visibilidad en la consola de Vision One.
La solución debe integrarse con Trend Vision One (XDR), enviando telemetría de correos, adjuntos y usuarios comprometidos, para correlacionar incidentes entre endpoints, red y correo.

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

ISO 14001:2015 BUREAU VERITAS Certification
icontec Carbono Neutro Certificado
Estamos certificados

La solución debe incluir capacidades de sandboxing para análisis de adjuntos sospechosos en entornos controlados, enriqueciendo los veredictos de seguridad de los mensajes.
La solución debe garantizar actualizaciones automáticas de motores y políticas antispam/antiphishing durante toda la vigencia de la licencia, sin costos adicionales.
La solución debe ofrecer acceso a un portal de autoservicio para usuarios finales, en el que puedan revisar sus correos en cuarentena, liberar mensajes legítimos y reportar posibles falsos positivos.
La solución debe asegurar la compatibilidad con normativas de privacidad y seguridad vigentes, evitando que el tráfico de correo de la Entidad se enrute fuera de los parámetros definidos por el fabricante.
Integración de la solución con el dominio institucional de correo en Microsoft 365.
Envío de un correo simulado con adjunto malicioso de prueba (archivo EICAR) y verificación de bloqueo en consola.
Envío de correo con enlace malicioso de prueba y verificación de neutralización mediante URL rewriting.
Simulación de correo de suplantación (spoofing) y validación de bloqueo mediante políticas DMARC/DKIM/SPF.
Validación de visibilidad de eventos en Trend Vision One (XDR) y de acceso de usuario al portal de autoservicio de cuarentena.
Trend Vision One – Cyber Risk Exposure Management (CREM) Essentials - Gestión de Exposición y Riesgo Cibernético
La solución debe proporcionar visibilidad continua de los activos de la Entidad (endpoints, servidores, aplicaciones y servicios en la nube), identificando vulnerabilidades críticas, configuraciones inseguras y superficies de exposición.
La solución debe generar una clasificación de riesgos priorizada, que permita identificar los vectores de ataque más probables y evaluar el impacto potencial de cada vulnerabilidad sobre los activos críticos institucionales.
La solución debe integrar la información de exposición con los módulos de Trend Vision One, correlacionando vulnerabilidades con incidentes de seguridad detectados en endpoints, red y correo.
La solución debe permitir la generación de informes periódicos y tableros dinámicos que muestren el nivel de riesgo global de la Entidad, tendencias en la superficie de ataque y la evolución de las acciones de mitigación.
La solución debe incluir un mecanismo de evaluación continua, sin depender exclusivamente de escaneos programados, asegurando la detección temprana de cambios en la postura de seguridad.
La solución debe ofrecer integración con fuentes de inteligencia de amenazas (Threat Intelligence) para contextualizar las vulnerabilidades encontradas frente a campañas activas a nivel global.
La solución debe permitir la definición de políticas y umbrales de riesgo para generar alertas automáticas al superar niveles críticos, facilitando la toma de decisiones temprana
La solución debe habilitar la exportación de reportes en formatos estándar (PDF, CSV, JSON) y la integración con SIEM para consolidar la información de riesgo en las herramientas existentes de la Entidad.
La solución debe operar como un servicio SaaS administrado por Trend Micro, accesible a través de credenciales seguras con autenticación multifactor, garantizando la confidencialidad y protección de la información evaluada.
La solución debe garantizar que la vigencia de la suscripción sea hasta el 30 de diciembre de 2028, asegurando continuidad en la visibilidad de riesgos durante todo el período contratado.

Conexión inicial de endpoints y servicios institucionales al módulo CREM.
Apex One – Sandbox as a Service Add-on - Análisis Avanzado de Archivos Sospechosos en Entorno Aislado
La solución debe permitir el análisis dinámico de archivos y objetos sospechosos en un entorno aislado (sandbox) en la nube del fabricante, evitando que amenazas desconocidas o de día cero afecten la infraestructura institucional.
La solución debe integrarse de forma nativa con los agentes de Trend Vision One Endpoint Security (Essentials y Pro) y con Email & Collaboration Security, para enviar automáticamente a sandboxing los archivos y adjuntos clasificados como sospechosos.
La solución debe ser capaz de analizar múltiples tipos de archivos: ejecutables, documentos ofimáticos, PDFs, scripts, archivos comprimidos y enlaces, detectando comportamientos anómalos y generando un veredicto de seguridad.
La solución debe incorporar técnicas de detección avanzada, incluyendo análisis de comportamiento, heurística, machine learning y detección de ransomware en etapa temprana.
La solución debe proporcionar resultados en forma de reportes detallados con indicadores de compromiso (IoCs), comportamiento observado, conexiones de red, modificaciones en el sistema y nivel de severidad asignado.
La solución debe enviar los veredictos generados de vuelta a los módulos de Endpoint y Email & Collaboration, para que tomen acciones de bloqueo, cuarentena o eliminación en función de la política definida.
La solución debe contar con capacidad de escalamiento automático hacia la plataforma Vision One (XDR), enriqueciendo las investigaciones con información sobre amenazas detonadas en sandbox.
La solución debe garantizar actualizaciones automáticas de las imágenes de sandboxing y motores de análisis, de acuerdo con lo dispuesto por el fabricante, durante la vigencia de la suscripción.
La solución debe operar bajo un modelo SaaS gestionado por Trend Micro, con acceso seguro, cifrado de la comunicación y aislamiento completo de los archivos analizados para garantizar la confidencialidad de la información.
La solución debe estar vigente hasta el 30 de diciembre de 2028, asegurando continuidad en el análisis de amenazas avanzadas.
Deep Discovery Inspector (DDI) – Software Only 1 Gbps - Detección de Amenazas en Red
La solución debe operar en modalidad software only, para ser desplegada en infraestructura de virtualización o servidores de la Entidad, sin incluir hardware físico.
La solución debe permitir la inspección de tráfico de red hasta 1 Gbps, detectando amenazas avanzadas, comunicaciones sospechosas y comportamientos maliciosos en protocolos comunes (HTTP, HTTPS, SMTP, SMB, DNS, entre otros).
La solución debe incorporar análisis basado en múltiples técnicas de detección: firmas, heurística, machine learning y correlación de patrones de tráfico, complementado con inteligencia global de amenazas (Smart Protection Network de Trend Micro)
La solución debe detectar y reportar actividades de comando y control (C&C), movimientos laterales, exfiltración de datos y ataques de día cero que intenten propagarse por la red interna o hacia Internet.
La solución debe integrarse de forma nativa con Trend Vision One (XDR) y con los módulos de endpoint y correo, permitiendo correlacionar eventos de red con incidentes en otros vectores.
La solución debe incluir capacidades de sandboxing integrado, detonando archivos extraídos del tráfico en entornos aislados para obtener veredictos de seguridad.

La solución debe generar reportes detallados de tráfico sospechoso, sesiones bloqueadas, IoCs detectados y correlación de amenazas, con exportación en formatos estándar (PDF, CSV, syslog) para integración con SIEM.
La solución debe permitir la configuración de alertas y notificaciones automáticas en tiempo real, ajustables según umbral de criticidad definido por la Entidad.
La solución debe garantizar actualizaciones automáticas y continuas de firmas, motores y modelos de detección durante la vigencia de la licencia.
La solución debe asegurar que la suscripción se extienda hasta el 30 de diciembre de 2028, garantizando la protección de la red institucional frente a amenazas persistentes.

FIRMA	
NOMBRE	**JULIO CESAR MANCIPE CAICEDO**
CARGO	Subdirector de Tecnologías de la Información (E)

Proyecto: Jorge Miguel Garcia Aguilar – Contratista STI 

Aprobó: Julio Cesar Mancipe – Asesor – Subdirector de Tecnologías de la información (E)

Carrera 68 A N.º 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.

www.supersalud.gov.co

Estamos certificados