CLAUSULADO DE ORDEN DE COMPRA

Orden No.	**ID CO1.PCCNTR.5037675**
Entidad contratante	**UNIDAD DE PLANEACIÓN MINERO ENERGÉTICA**
NIT	**830.000.282-1**
Contratista	**REDES TERCER MILENIO SAS – RTM SISTEMAS**
NIT	**NIT 805011332-8**
Representante Legal	**JUAN CARLOS CALDERON GARCÍA**

CLÁUSULAS

OBJETO: Adquirir una solución Endpoint antivirus para la UPME.

OBJETIVOS ESPECÍFICOS: EL CONTRATISTA deberá realizar los siguientes objetivos específicos:

- Adquirir el licenciamiento de una solución tipo MDR Complete de Sophos (Licenciamiento XDR + SOC) para protección antimalware de computadores y servidores de la Unidad que cuente con servicio de monitoreo 24x7 de caza y respuesta ante amenazas (SOC) para 350 dispositivos de cómputo por 1 año.
- Adelantar el proceso de instalación, configuración y puesta en producción de la solución adquirida en los 4 días calendario siguientes a la firma de la orden.
- Contar con las actualizaciones permanentes que libere el fabricante de la solución adquirida.
- Realizar transferencia de conocimiento hacia la Unidad en los términos del anexo técnico y la oferta presentada por el proveedor.
- Prestar el respectivo soporte técnico de la solución que permita: Prevenir, detectar y neutralizar software malicioso, a través de tres componentes a saber: prevención de intrusos, antimalware y firewall usado con filtro de conexiones entrantes y salientes, en los términos del anexo técnico emitido por la Unidad, así como de la oferta presentada por el proveedor.
- Cumplir con el anexo técnico presentado y la oferta presentada.

OBLIGACIONES ESPECÍFICAS: EL CONTRATISTA deberá realizar las siguientes obligaciones específicas:

- Entregar las 350 licencias del XDR (Endpoint Extendido) de Sophos para la protección de computadores (190 licencias) y servidores (160 licencias) de la unidad.
- Instalación y configuración del licenciamiento adquirido en la plataforma tecnológica de la Unidad dentro de los 4 días calendario siguientes a la firma de la orden.
- Servicio de monitoreo 24x7 de caza y respuesta ante amenazas (SOC) para la plataforma tecnológica de la Unidad, incluidas las 350 licencias adquiridas en este proceso de contratación por 1 año.
- Garantía y soporte técnico de fábrica por un (1) año.
- Soporte local por un (1) año de acuerdo con el anexo técnico.

Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
http://www.upme.gov.co

- Transferencia de conocimiento en los términos del anexo técnico de la oferta del proveedor.
- Entrega a satisfacción de la Unidad minero energético de los productos y servicios prestados.

ENTREGA DE PRODUCTOS: EL CONTRATISTA deberá entregar el siguiente bien tangible o intangible 350 licencias MDR Complete de Sophos (350 licencias de XDR + Servicio SOC), el cual se deberá ingresar a almacén.

OBLIGACIONES GENERALES DEL CONTRATISTA: EL CONTRATISTA deberá realizar las siguientes obligaciones generales:

- Cumplir el objeto de la orden.
- Cumplir con las condiciones y lineamientos ofertados en la propuesta.
- Ejecutar la orden dentro del plazo establecido, y bajo las condiciones técnicas y financieras definidas en el presente proceso.
- Presentar cuenta de cobro o facturación electrónica, si por ley está obligado a ello, dentro de los plazos definidos en la orden.
- Mantener vigente y al día durante la ejecución de la orden, la afiliación y aportes al sistema Integral de Seguridad Social Integral, Parafiscales y Sistema General de Riesgos Laborales.
- Las demás que le sean asignadas por el supervisor de la orden, en el marco de la orden.

OBLIGACIONES GENERALES DE LA UPME: La Unidad deberá realizar las siguientes obligaciones generales:

- Designar el supervisor de la orden.
- Efectuar un seguimiento efectivo al cumplimiento de las obligaciones del contratista/proveedor a través del supervisor de la orden.
- Autorizar el pago del valor de la orden de acuerdo con la forma establecida.
- Verificar el cumplimiento de las obligaciones del contratista frente al sistema General de Seguridad Social.
- Proporcionar toda la información que el contratista requiera para el cumplimiento de sus actividades contractuales.
- Velar por el cumplimiento de las obligaciones de la orden.

PLAZO: El plazo de la vigencia del licenciamiento y soporte será por el término de un (1) año, contado a partir de la entrega de las licencias, previa expedición del registro presupuestal. El plazo para la entrega de las licencias, será de treinta (30) días calendario de contado a partir de expedición del registro presupuestal.

VALOR: Esta Orden tiene un valor de **CIENTO CUARENTA Y UN MILLONES DOSCIENTOS NOVENTA Y CINCO MIL SETECIENTOS NOVENTA Y TRES PESOS ($141.295.793) M/CTE,** incluido IVA.

FORMA DE PAGO: LA UPME pagará el valor de la orden en UN (1) pago, así: previa radicación de la cuenta de cobro o factura electrónica correspondiente, si hay lugar,

Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
http://www.upme.gov.co

acompañada del certificado del pago de los aportes a la Seguridad Social Integral y Parafiscales, expedida por el Representante Legal o el Revisor Fiscal, según sea el caso, junto con la presentación del informe, y el certificado de cumplimiento expedido por el supervisor de la orden, donde coste el ingreso a almacén, así:

Número de pago	Porcentaje del valor	Momento del pago	Contra que se paga
Uno	**100%**	Luego del primer mes de ejecución de la orden	Entrega a satisfacción de la Entidad de las obligaciones específicas, productos y servicios.

PARÁGRAFO PRIMERO: Para presentar las cuentas de cobro de servicios objeto de la presente contratación, se debe tener en cuenta lo establecido en la Circular relativa a los trámites de Pago vigencia 2023, la cual debe estar acompañada del certificado del pago de los aportes a la Seguridad Social Integral, en la forma y términos indicados en la normatividad vigente, junto con el informe de avance o final, según el caso y, el certificado de cumplimiento y recibo a satisfacción por parte del supervisor. **PARAGRAFO SEGUNDO:** La factura deberá ser radicada en la oficina de correspondencia conforme la Circular relativa a los trámites de Pago vigencia 2023. **PARÁGRAFO TERCERO:** La factura se deberá expedir a nombre de la **UPME NIT 830.000.282-1**

IMPUTACION PRESUPUESTAL: El valor de la presente Orden se pagará con cargo al CDP No. 19823 del presupuesto de inversión 2023. **PARÁGRAFO:** Una vez realizado el registro presupuestal, se deberá liberar el valor no utilizado del respectivo CDP, cuando a ello hubiere lugar.

SUPERVISIÓN: La supervisión será ejercida por Claudia Marcela Beltrán Profesional Especializado Grado 15, asignado a la Oficina de Gestión de la Información, o quien designe el ordenador del gasto. **PARÁGRAFO:** En el caso que sea necesario cambiar de supervisor, está modificación no requerirá de la suscripción de una orden modificatoria.

PERFECCIONAMIENTO: La presente orden se perfecciona con la aprobación de las partes en la plataforma del SECOP II.

Elaboró: Jimena Hernández Olaya – Profesional Especializada GIT Gestión Jurídica y Contractual
Revisó: Natalia Bustamante Acosta – Coordinadora GIT Gestión Jurídica y Contractual
Laura Hincapié – Asesor Secretaria General.

Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
http://www.upme.gov.co

ANEXO TÉCNICO

Adquisición de licenciamiento de Antivirus EndPoint con MDR- MDR COMPLETE			
Ítem	**Características**	**Mínimo Exigido**	**Cumple (SI/NO)**
1	**Antivirus con MDR - MDR COMPLETE**		SI-MDR – MDR COMPLETE
2	**Versión**	El proveedor debe instalar, configurar y parametrizar a la UPME la última versión liberada y estable de la solución adquirida.	SI
3	**Tiempo de Garantía y Soporte**	1 año	SI
4	**Servicios a prestar durante la garantía y soporte del fabricante**	De Lunes a Sábado de 7:00 am a 7:00 pm. Atención máxima en cuatro horas a partir de la llamada de solitud de soporte. Solución de incidencia en ocho (8) horas a partir de la llamada de solicitud de soporte. Con esta adquisición el proveedor garantiza a la UPME que adelantará soportes de Actualización a la última versión de la solución sin costo adicional para la UPME, cada que dicho upgrade se libere, esto durante el tiempo de garantía y soporte contratado.	SI
5	**Cantidad de licencias**	**350 -** EndPoint Antivirus con EDR (Endpoint Detection Response). De las 350 licencias 160 son licencias para servidores y de estas últimas 5 son para servidores físicos.	SI
6	**Transferencia de conocimientos**	Realizar la transferencia de conocimiento de la solución a las tres (3) personas de la Unidad de Planeación Minero Energética UPME, designadas, con una intensidad horaria de mínimo 16 horas que les permita operar y atender idóneamente la operación del antivirus con EDR.	SI Se realizara capacitación de 6 jornadas, así: Las dos primeras sesiones virtuales serán de 3 horas, la tercera virtual por 4 horas, la cuarta virtual por 3 horas y la última sesión por 3 horas debe ser virtual. Sólo se puede adelantar una sesión por día. Adicional el próximo semestre se realizará Certificación técnica como administrador de Sophos Central en Bogotá sería 4 días se le otorgaría un váucher para la certificación presencial de 3 personas.
7	**Migración**	Realizar la migración del Endpoint CheckPoint de Harmony a la nueva solución, esto implica la instalación, configuración y puesta en funcionamiento de la nueva solución EndPoint en	SI

		la infraestructura tecnológica de la UPME. De las 350 licencias, 160 son para Servidores, 5 de ellos son servidores físicos. El proceso de Migración deberá garantizar la operatividad de la plataforma tecnológica de la UPME una vez instalado, en ese sentido se deben garantizar la disponibilidad de los aplicativos, los servicios tecnológicos, las herramientas y el software que tiene la Unidad (UPME) para atender el giro normal de sus actividades y operaciones. Esta migración debe adelantarse durante los 4 días siguientes a la firma del contrato, de requerirse más tiempo del señalado, favor informarlo en este estudio de mercado.	Migración completa, no incluye desinstalación de la solución anterior
8	**SOLUCIÓN ANTIVIRUS CON MDR – MDR COMPLETE**		
8.1	**Instalación y Configuración**	Instalación inicial de consola y agentes de antivirus con EDR y las actualizaciones, en todas las estaciones de trabajo físicas y virtuales, Servidores físicos y virtuales, Escritorios Virtuales y portátiles.	**si**
		El paquete de instalación debe entregarse como un instalador para los sistemas operativos:	**si**
		- Windows 8.1 32/64bit	**si**
		- Windows 10 32/64bit	**si**
		- Windows 11 64bit	**si**
		- Windows 2012 R2 y todas las versiones posteriores	**si**
		El Proveedor de la solución debe ser un canal autorizado por el fabricante.	**si**
		Para fines de escalabilidad, el producto debe permitir que cualquier componente o servicio se instale de forma independiente o en un método agrupado.	**si**
		Para propósitos de escalabilidad, el producto debe tener componentes dedicados para servicios de base de datos, servicios de comunicación, actualización y servicios web.	**si**
8.2	**Características Generales**	La solución deberá de permitir habilitar en un mismo agente las siguientes funcionalidades: o Endpoint Firewall o Control de aplicaciones o Cumplimiento en Endpoints o Protección de puertos (control periférico) o VPN de acceso remoto o Endpoint Anti-Virus: firmas conocidas, heurística o Análisis estático: prevención basada en el aprendizaje automático o Anti-Exploit o Protección contra phishing de día cero: Anti-phishing y prevención de re-uso de credenciales o Anti-Ransomware o Análisis de comportamiento: mutaciones de malware conocido, malware genérico	**Si cumplimos, pero en la parte de** o VPN de acceso remoto esto se maneja desde el firewall o el equipo de Borde

		desconocido, ataques sin archivos o Anti-Bot: detección de tráfico desde y hacia servidores de Comando y Control (C&C) maliciosos o Anti-Evasión: detección de técnicas de evasión o Colección y análisis forense o Informe automatizado de análisis forense de eventos	
		La solución integrada de firewall para EndPoint debe proporcionar mitigación adicional a través de la limitación de acceso en el EndPoint.	**si**
		La solución debe ser capaz de remediar la infección al menos de dos maneras: automatizado y manual.	**Si**
		La solución no debe tener un límite en la cantidad de clientes que la consola de administración puede administrar.	**Si**
		La solución deberá poder buscar los IoC (Indicadores de compromiso) proporcionados a través de la interfaz de usuario de gestión de EndPoint.	**Si**
		La solución debe tener la capacidad de verificar la configuración del registro en las máquinas localmente. Esto con el fin de verificar las actualizaciones y parches de Microsoft en varias versiones del sistema operativo Windows.	**Si**
		La solución deberá soportar al menos los siguientes sistemas operativos: o Windows 7 32/64bit o Windows 8.1 32/64bit o Windows 10 32/64bit o Windows 2008 R2 y todas las versiones posteriores	**Si**
		La solución deberá de poder funcionar en ambientes virtualizados de VDI	
		La solución debe poder trabajar en entornos distribuidos con ancho de banda limitado al proporcionar un servidor de administración secundario localmente en cada localización.	**Si**
		La solución debe ofrecer monitoreo detallado y análisis de logs a través de GUI dedicadas.	**Si**
		La solución debe proporcionar la capacidad de habilitar / deshabilitar de manera granular cada	**si**

		componente que sirve como un medio para aislar cualquier interferencia con otras aplicaciones.	
		Todas las acciones de gestión se deben registrar. ej. cambios de administración de políticas, aprovisionamiento de usuarios y máquinas, cambios de administradores en la administración, inicio / cierre de sesión de administrador, etc.	**Si**
		Todas las detecciones y protecciones de los EndPoint se deben loguear. .ej. detección y prevención maliciosa, Anti-Bot, (incluido el informe completo), informe de análisis de ataque forense, medidas correctivas y de cuarentena, etc.	**si**
		Las siguientes acciones deben de poder ser realizadas en el agente por los usuarios. o Ver eventos de seguridad o Ver análisis forense de eventos o Ver archivos en cuarentena o Liberar el archivo de la cuarentena (si lo permite la política) o Activar la actualización manual de firmas (por ejemplo, para AV) o Iniciar un análisis forense (si lo permite la política) o Restaurar archivos a la ubicación original / seleccionada después de un ataque de Ramsonwares	**si**
		Las alertas se deberán de poder configurar para ser enviadas como notificaciones por correo electrónico.	**si**
		El producto también deberá proporcionar alertas a los usuarios finales sobre cualquier infección detectada.	**si**
		La consola deberá proporcionar un estado inmediato y actualizado en cualquier host.	**si**
		El administrador deberá poder generar informes inmediatamente usando la consola o programarlos para que se ejecuten en el servidor.	**si**
		El firewall integrado en el EndPoint deberá proporcionar una política de firewall centralizada que permita el control granular para bloquear conexiones hacia y desde puertos específicos, sitios, e IPs.	**no**
		La solución deberá tener integrada la capacidad de controlar de manera granular los dispositivos periféricos y dispositivos de almacenamiento que se registran en el sistema. Todos los periféricos y accesos a dispositivos de almacenamiento se deben de loguear en el sistema.	**si**
		La solución debe de estar integrada con un servicio de inteligencia para recibir/compartir información de amenazas, esto deberá de poderse realizar utilizando un servicio público o privado.	**si**

		La solución deberá permitir a múltiples administradores conectarse en modo lectura/escritura y permitir que realicen acciones en el mismo servidor de administración simultáneamente	**si**
		El servidor de administración deberá permitir definir perfiles de administrador, donde cada perfil se crea a partir de un conjunto de permisos.	**si**
		Cada administrador deberá poder estar asignado a un perfil definido y tener su propio conjunto de permisos.	**si**
		Todas las acciones o configuraciones se deben poder realizar desde una única consola de administración.	**si**
		Los clientes deberán realizar mediciones de proximidad periódicamente para determinar qué servidor de políticas (en caso de tener varios) tiene mejor conectividad.	**si**
		Los agentes deberán de tener un mecanismo de heartbeat con el propósito de identificar si se ha realizado algún cambio en la política del cliente.	**si**
		Cuando existe una actualización en las políticas de los EndPoint, se deberá instalar únicamente los nuevos cambios (deltas) y no la policita completa.	**si**
		La comunicación entre el cliente y el servidor deberá manejase a través de protocolos https comunes.	**si**
		La solución se debe poder integrar fácilmente con herramientas de implementación de terceros, como SCCM.	**si**
		Los componentes de seguridad relevantes deberán de poder eliminarse mediante una opción de implementación de software o deshabilitarse mediante la política de despliegue.	**si**
		La desinstalación del cliente se debe poder proteger mediante una contraseña.	**si**
		Todos los componentes de los clientes deberán estar protegidos mediante un módulo de autoprotección que evita cualquier manipulación maliciosa de archivos de configuración, binarios o configuraciones de registro.	**si**
		La consola en sitio deberá aceptar los siguientes métodos de autenticación: o SecureID o Radius o Tacacs o OS Password o Active Directory	La autenticación se realiza nativa con doble factor de autenticación o con Office 365, aquí hace referencia a la autenticación o a la sincronización de usuarios ¿?
		La solución debe poder proteger las descargas web antes de que se descarguen en el EndPoint.	**Si**

		La cuarentena automática de los hosts infectados se deberá poder realizar en varios niveles: o Poner en cuarentena los procesos que se comunican con C&C: neutralizar la filtración de datos y el progreso del malware. o Poner en cuarentena la máquina infectada, evitando que se comunique, con el fin de evitar el movimiento lateral y la filtración de datos de los recursos de la red (por ejemplo, servidores de archivos). o La solución deberá tener la capacidad de desinstalar automáticamente todos los elementos del ataque en función del análisis forense automatizado.	**si**
		La solución deberá soportar capacidades de detección / protección del uso indebido de credenciales comunes, como pass-the-hash, robo de credenciales de memoria, keyloggers, robo de claves de cifrado, etc.	**si**
		Los archivos ingresados en cuarentena debido a un falso positivo deberán de poder ser recuperados fácilmente por un administrador para minimizar la interferencia.	**si**
		Las actualizaciones para mitigar los ataques activos y / o vulnerabilidades deberán ser efectivos de manera inmediata.	**si**
		Todas las acciones de respuesta (archivos de cuarentena, bloqueo de máquina, etc.) se deberán poder realizar offline.	**No** **Se puede deshabilitar o habilitar módulos pero la cuarentena se trata desde la consola por seguridad**
8.3	**Funcionalidades de Anti-Malware**	La solución de anti-virus debe de proporcionar una fuerte protección de primera línea estática y dinámica utilizando firmas y análisis de comportamiento	**si**
		Las actualizaciones de firmas de anti-virus deberán de poder ser extraídas utilizando servidores internos o un servicio público.	**Si**
		El módulo de Anti-Malware debe de proteger los dispositivos de todo tipo de amenazas de malware, desde gusanos y troyanos hasta adware y registradores de pulsaciones de teclas (keystroke loggers).	**si**
		La solución debe de permitir -Detectar actividad inusual: utilizando métodos de detección de comportamiento para proteger las computadoras de nuevas amenazas cuya información aún no se ha agregado a las bases de datos. -Habilitar los servicios de reputación en la nube para archivos, recursos web y procesos usando tecnologías en la nube para mejorar la precisión de las funciones de escaneo y monitoreo. -Habilitar protección web para evitar el acceso a sitios sospechosos y la ejecución de scripts	**si**

		maliciosos. Analizar archivos y ejecutables empaquetados transferidos a través de HTTP, y alertar a los usuarios si se encuentra contenido malicioso. -Protección de correo activando los escaneos de mensajes de correo electrónico cuando se pasan como archivos a través del sistema de archivos.	
		Anti-Malware debe de poder recibir actualizaciones de firmas de malware a intervalos regulares para asegurarse de que pueda buscar las amenazas más recientes.	**si**
		Anti-Malware debe de poder analizar las computadoras en busca de malware a intervalos regulares para asegurarse de que los archivos sospechosos sean tratados, puestos en cuarentena o eliminados.	**Si**
		Se debe de poder excluir el contenido de directorios o archivos confiables y ejecutables de programas confiables especificados del análisis de programaciones Anti-Malware	**si**
		Funcionalidades de Anti-Ransomware	**si**
		La solución debe tener la capacidad de evitar que los tipos de malware ransomware y cryptolocker puedan cifrar el sistema de archivos de un endpoint.	**si**
		En caso de que se detecte y bloquee un malware de tipo ransomware o cryptolocker después de que se haya iniciado el cifrado, la solución debe poder recuperar los archivos cifrados a su estado pre-cifrado.	**si**
		La detección, prevención y restauración de Anti-Ransomware deberá funcionar en todos los entornos, independientemente de la conexión a Internet.	**si**
		La solución deberá supervisar los cambios en los archivos en las unidades de usuario para identificar el comportamiento del ransomware, como el cifrado de archivos	**si**
8.4	**Protección de Phishing y Passwords**	La solución deberá poder bloquear el acceso a sitios de phishing bloqueando ataques de phishing desconocidos y de día cero dirigidos a las credenciales de los usuarios, escaneando todos los campos del formulario y verificando su validez.	**si**
		Cuando un usuario navega por un sitio web y antes de ingresar sus credenciales, el motor de anti-phishing deberá inspeccionar, identificar y bloquear los sitios de phishing	**si**
		Si el sitio se considera phishing, el usuario no podrá ingresar credenciales.	**si**

		Este motor debe ofrecer protección de día cero según las características del sitio, como las URL maliciosas conocidas. Incluso se deberán poder identificar sitios de phishing nuevos.	**si**
8.5	**Protección Anti-Bot**	La detección se debe basar en al menos dos capas al comparar las firmas de comunicación con una firma de comunicación maliciosa conocida y usar un servicio de inteligencia para identificar dominios o direcciones IP maliciosas a las que se accede.	**si**
		Una vez que se detecta una comunicación maliciosa, se debe poder bloquear la comunicación inmediatamente, cerrar el proceso y poner el archivo del proceso en cuarentena.	**si**
		La comunicación de C&C se debe de identificar y bloquear, evitando la acción del malware, el progreso del ataque y la filtración de datos.	**si**
		Las máquinas identificadas como infectadas deben poder ser aisladas de la red, lo que evita el movimiento lateral, el acceso a los datos en los servidores y las comunicaciones de C&C.	**si**
		Todas las acciones automáticas de cuarentena y remediación deberán poder limitarse a detecciones solo de alta confianza para minimizar el impacto de falsos positivos en los usuarios.	**si**
		Las capacidades de detección de Anti-Bot que se basan en la inteligencia en la nube deben poder funcionar en entornos online y offline, esto utilizando una nube privada para proporcionar información de inteligencia actualizada.	**si**
8.6	**Protección Anti-Exploit**	Debe poder detectar y prevenir el malware en la etapa Exploit	**SI**
		La solución debe de proteger contra amenazas de aplicaciones que explotan vulnerabilidades de memoria.	**Si**
		La solución debe de proteger aplicaciones ampliamente usadas como Microsoft Office, Adobe PDF Reader, 7zip, winrar, navegadores y Adobe Flash.	**Si**
		Debe utilizar al menos cuatro tecnologías para proteger contra exploits existentes y nuevos: o Import – Export Address Table Parsing o Return Oriented Programming o Stack Pivoting o VB Script God Mode	**Si**
8.7	**Análisis de Comportamiento**	La solución deberá de utilizar múltiples métodos de detección avanzados que no están basados en firmas. Por ejemplo, motores de comportamiento avanzados.	**Si**
		La solución debe de poder detectar y remediar diferentes formas de comportamiento malicioso. Cuando se detecta, generar un informe forense con reparación automática o manual.	**si**

		La solución deberá poder identificar y rastrear inyecciones de código malicioso en la memoria del proceso para detectar y prevenir la ejecución de malware sin archivos (Fileless malware). La solución también deberá poder identificar malware basado en el registro.	**Si**
		La solución deberá de tener la capacidad de detectar comportamientos anómalos o maliciosos que ocurren en el endpoint. Por ejemplo: o Lanzamientos anormales o Creaciones de archivos anormales o Ejecuciones de Hash Copy o Eliminaciones de archivos descartadas o Procesos anormales de ejecución o Cambio de privilegio o Eliminación de instantáneas de ransomware o etc.	**Si**
8.8	**Análisis Forense**	La solución deberá incluir dentro de la misma solución un módulo de análisis forense.	**Si**
		La solución deberá de supervisar la actividad de la red y asociar cada conexión con el proceso del sistema operativo que la generó.	
		La función forense deberá de poderse integrar con software externo anti-malware de terceros.	**Si**
		La solución deberá poder recopilar y almacenar datos forenses históricos de la actividad del sistema operativo.	**si**
		El administrador deberá poder controlar la cantidad de espacio en disco asignado para datos históricos forenses.	**No porque ya el espacio viene incluido en la nube**
		La solución deberá incluir un módulo de análisis forense que pueda analizar cualquier activador de detección para revelar el ataque completo y sus comportamientos maliciosos o sospechosos. Esto incluye la capacidad de rastrear las relaciones entre los componentes del ataque, las inyecciones de memoria, la actividad de key-logger, etc.	**Si**
		La solución deberá tener la capacidad de contener o remediar amenazas en sistemas host una vez detectados.	**Si**
		La recopilación y análisis forense deberá funcionar en todos los entornos, independientemente de la conexión a Internet.	**Si**
		El motor forense debe estar monitoreando el comportamiento de la aplicación y la actividad anómala. Una vez que cualquiera de los motores de seguridad del producto detecta actividad maliciosa, las actividades de protección y reparación deben poder activarse automáticamente (por ejemplo, poner en cuarentena el archivo ofensivo, poner en cuarentena el sistema, remediar y revertir la actividad de ataque).	**Si**

		La solución deberá de tener la capacidad de restaurar un host a un estado limpio como estaba antes de la presencia de malware.	**Si**
		Los resultados de análisis forense se deben de enviar inmediatamente al servidor de logs cuando se identifica un ataque.	**Si**
		El análisis forense debe incluir los accesos a archivos, claves de registro confidenciales utilizadas, creación de procesos, modificación de registros / archivos, todas las comunicaciones de red, actividad de inicio de sesión de usuarios, elevación de permisos, actividad de arranque del EndPoint, inyección y enganche de procesos, monitoreo de variables de entorno y más.	**Si**
		El proceso de análisis forense se debe iniciar automáticamente cuando se produce un evento de malware y proporcionar la siguiente información cuando aplique. o Eventos maliciosos: evidencia de comportamiento sospechoso detectado durante todo el ciclo de vida del ataque o Punto de entrada: cómo se inició el ataque, cómo entró y los elementos principales utilizados o Alcance del daño: una vez activado, la ruta del malware, su impacto en el negocio y qué datos se vieron comprometidos y / o copiados externamente o Hosts infectados: quién más o qué más se vio afectado	**Si**
		Basado en el registro de eventos de Windows, el módulo forense debe de poder analizar ataques, finalizar procesos, eliminar o poner en cuarentena los archivos, y hacer otras soluciones de ataque.	**Si**

Servicio de Monitoreo 24x7 de caza y respuesta ante amenazas

- La solución de monitoreo 24x7 se realiza por medio del SOC (Centro de operaciones de seguridad, por sus siglas en inglés) del fabricante de la solución de Endpoint sin la necesidad de instalar algún agente adicional en los equipos de cómputo.
- El equipo de analistas del SOC obtiene la información de los incidentes detectados por medio del mismo agente de antivirus de end point previamente instalado y debe de ser del mismo fabricante o proveedor de servicios de antivirus.
- El servicio de caza de amenazas notificara por medio de correo electrónico o llamada por teléfono a la (s) persona (s) asignadas por la institución del incidente detectado, según la criticidad del incidente.
- El servicio de caza de amenaza trabajara en conjunto con la (s) persona (s) asignadas por la institución para resolver el incidente en conjunto.
- Si la institución así lo determina, el servicio de caza de amenazas llevara a cabo las configuraciones necesarias a nivel del agente de end point para poder contener y mitigar el incidente detectado sin la intervención de la institución.
- Las acciones que el servicio de caza de amenazas puede realizar en las políticas del agente de end point de antivirus son:
    - Cambio de configuraciones
    - Aislar un end point
    - Bloquear archivos

- Ejecutar escaneos
- Bloquear sitios web, IP, CIDR
- Bloquear aplicaciones
- Uso de una terminal segura desde la misma consola de gestión basada en nube de la solución de end point y cifrado

- Entra de un reporte semanal con la información que contenga como mínimo los incidentes detectados de mayor criticidad y el estado de estos.
- El equipo de analistas de SOC hara revisiones de la salud y estado de la configuración de la consola de gestión basada en nube del módulo de antivirus para poder emitir recomendaciones acerca de mejoras pare evitar malas configuraciones.
- El equipo de analistas identificara la causa raíz de las amenazas para evitar futuros incidentes.
- El caso de que la institución lo solicite, el servicio de SOC es compatible con la telemetría de seguridad de proveedores como Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace, entre otros. Las fuentes de telemetría se utilizarán para ampliar la visibilidad de toda la infraestructura de la institución, generar nuevas detecciones de amenazas y mejorar la fidelidad de las detecciones de amenazas existentes, realizar búsquedas de amenazas y habilitar funciones de respuesta adicionales.
- El prestador de servicio de SOC entregara reportes semanales y mensuales que incluya información exhaustiva sobre las investigaciones de seguridad, las ciberamenazas y la postura de seguridad de la institución.
- El SOC tiene que designara a un responsable de respuesta a amenazas dedicado que colaborará con el personal que la institución designe en cuanto sea identificada una incidencia y deberá de trabajar en conjunto con la dependencia hasta que el incidente se resuelva.
- El servicio de SOC proporcionara recomendaciones proactivas para mejorar la postura de seguridad de la institución, realizar análisis de causa raíz para identificar los problemas subyacentes que han provocado el incidente.
- El servicio de SOC de caza de amenazas ofrecera orientación prescriptiva para resolver vulnerabilidades de seguridad a fin de que no puedan ser explotadas en el futuro dentro de la institución.
- El servicio incluye una sesión informativa de forma mensual en donde se mostrarán datos clave relativos a la información sobre amenazas más recientes y prácticas de seguridad recomendadas.

Requisitos Mínimos para la instalación de la Solución

- El end point antivirus soporta máquinas con arquitectura de 32 bits y 64 bits.

- El end point antivirus es compatible para su instalación en estaciones de trabajo con los sistemas operativos: Windows 7 en adelante, Mac OS X 10.15 en adelante y Linux Amazon Linux, Amazon Linux 2, CentOS 6, 7 y 8, Debian 9 y 10, Oracle Linux 6, 7 y 8, Suse 12 y 15, Ubunto 16 y 18 LTS.

- Es compatible para su instalación en servidores con los sistemas operativos: Windows server 2008 R2 en adelante y Linux Amazon Linux, Amazon Linux 2, CentOS 6, 7 y 8, Debian 9 y 10, Oracle Linux 6, 7 y 8, Suse 12 y 15, Ubunto 16 y 18 LTS.

Firma Representante Legal	
Nombre del Representante Legal	**Juan Calos Calderon**
Nombre de la Empresa	**Redes Tercer Milenio**
Teléfono de contacto de la Empresa	**3163420263**
Correo electrónico de la Empresa	**jucalder@rtm.com.co**
Propuesta válida por 1 mes	