ESPECIFICACIONES TÉCNICAS MINIMAS DE OBLIGATORIO CUMPLIMIENTO.

RENOVACIÓN DEL LICENCIAMIENTO Y SOPORTE DEL ENDPOINT SOPHOS CON MDR PARA ESTACIONES DE TRABAJO Y SERVIDORES DE LA AGENCIA DE DESARROLLO RURAL

Objeto: **ADQUIRIR, ACTUALIZAR E IMPLEMENTAR SOLUCIONES TECNOLÓGICAS QUE CONTRIBUYAN AL FORTALECIMIENTO DE LA INFRAESTRUCTURA TI, NETWORKING Y LOS SISTEMAS DE SEGURIDAD DE LA AGENCIA DE DESARROLLO RURAL – ADR**
LA AGENCIA DE DESARROLLO RURAL, actualmente cuenta con una solución de endpoint de seguridad orientado a proteger de manera constante de distintas amenazas en el entorno digital sobre los activos tecnológicos que posee, como lo son entre otros, pero sin limitarse a los servidores y equipos de cómputo. Por consiguiente, se considera necesario renovar la solución de endpoint de seguridad que le permitirá a la entidad cumplir con los siguientes objetivos y tareas: a) Proteger los servicios web, servidores, equipos de cómputo de la Agencia de software malicioso como, Ransomware, Virus, Gusanos entre otros. b) Reducción de riesgos en la prestación de los servicios digitales de la Agencia, teniendo en cuenta que estos servicios se prestan a través de plataformas web de cara internet lo que indica que están expuestos a múltiples vectores de amenaza. c) Asegurar el correcto funcionamiento de la entidad, reduciendo las probabilidades de infección por malware en los equipos de cómputo y servidores. d) Mantener la protección contra malware debidamente actualizada, teniendo en cuenta que una solución de seguridad sin actualización aumentará las probabilidades de sufrir ataques cibernéticos recientemente desarrollados. e) Monitoreo de los sistemas de información. La solución de seguridad permite verificar posibles amenazas detectadas con el objetivo de actuar rápidamente en caso de algún evento o incidente de seguridad.

En la ficha técnica se relacionan las especificaciones requeridas y son aquellas que determinan y precisan las características principales de los servicios a contratar y son de obligatorio cumplimiento.

A. CLASIFICACIÓN UNSPSC:

Ítem	Clasificación UNSPSC	Producto
1	43233200	Software de seguridad y protección
2	43222500	Equipo de seguridad de red
3	81111800	Servicios de sistemas y administración de componentes de sistemas

LA DESCRIPCIÓN DEL PRODUCTO ENDPOINT DE SEGURIDAD ES LA SIGUIENTE:

ESPECIFICACIONES	DESCRIPCION SERIAL/NOMBRE	Cantidad	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto
RENOVACIÓN DEL LICENCIAMIENTO Y SOPORTE DEL ENDPOINT SOPHOS CON MDR PARA ESTACIONES DE TRABAJO Y SERVIDORES DE LA AGENCIA DE DESARROLLO RURAL El oferente deberá suplir el licenciamiento por 1 año de la solución indicada	**ENDPOINT DE SEGURIDAD** es una categoría de software que incluye soluciones y medidas diseñadas para prevenir, detectar y responder a amenazas y ataques dirigidos a los dispositivos finales (Servidores, Equipos de cómputo o dispositivos móviles). Alguna de las tecnologías que incorpora son: Antivirus, antimalware, Firewall personal, HIDS, HIPS, IA de seguridad, Control de aplicaciones y navegación web entre otros.	**1**	

B. CONDICIONES TÈCNICAS REQUERIDAS POR ITEMS:

ÍTEM	ESPECIFICACIONES	DESCRIPCIÓN	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto

1	**VIGENCIA**	La renovación del licenciamiento es requerida por un periodo de 1 año en un esquema de soporte 7 x 24 con el oferente y fabricante. El licenciamiento por renovar es el siguiente: ✓ 500 Licencias de Endpoint - Central Managed Detection and Response complete- MDR . ✓ 75 Licencias de Endpoint para Seguridad - Central Managed Detection and Response complete- server ✓ 4 Licencias de Endpoint para Seguridad - Central Intercept X Advanced for Server with XDR (Con **soporte** extendido) ✓ 100 licencias de Central Device Encryption.	

ÍTEM	ESPECIFICACIONES	DESCRIPCIÓN	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto
		✓ Licenciamiento para integración del servicio de MDR con los 2 firewall Fortinet de la Agencia. ✓ Licenciamiento para la Integración del servicio de MDR con Office 365 a nivel de Management Activity y Microsoft Graph. La renovación del licenciamiento y los servicios de soporte deben tener una única fecha de vigencia, para el servicio de soporte ante el fabricante y soporte con partner (canal), la garantía, licenciamiento y actualizaciones para todos los productos, deberá aplicarse y entrar en vigor una vez caduque la anterior. **NOTA:** A partir del perfeccionamiento de requisitos de ejecución del contrato y con la firma del Acta de Inicio, el contratista tendrá tres (3) días para realizar la entrega del licenciamiento, e iniciar con el proceso de instalación y configuración.	
2	**DESPLIEGUE / ARQUITECTURA DE LA SOLUCIÓN TECNOLÓGICA**	La plataforma debe ofrecerse como un servicio de software en la nube (SAAS) y debe poder integrarse con las soluciones de seguridad existentes en la AGENCIA DE DESARROLLO RURAL. Los agentes de endpoint deben poderse instalar en servicios en la nube de la AGENCIA y en la red interna, sin que esto genere costos adicionales a la AGENCIA.	
3	**ESPECIFICACIONES TÉCNICAS PRINCIPALES DE LA HERRAMIENTA**	La solución debe incluir un módulo de protección web que incluya funciones como: filtrado activo de direcciones web, escaneado de contenido descargado y comprobación de la reputación de archivos descargados.	

		La reputación de descargas debe estar en la capacidad de calcular la fiabilidad de la descarga con base a la antigüedad, el origen, la prevalencia y el análisis de contenido profundo de los archivos.	
		Realizar el control de periféricos que permita controlar el acceso de periféricos y medios extraíbles.	
		Detectar malware con aprendizaje autónomo.	
		Escanear, detectar y eliminar en tiempo real cualquier tipo de malware (virus, troyanos, gusanos, adware y spyware.), macrovirus, virus de sector de arranque, programas maliciosos, Ransomware, phishing, rootkit, programas publicitarios, así como las aplicaciones potencialmente no deseadas.	

ÍTEM	ESPECIFICACIONES	DESCRIPCIÓN	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto
		Permitir el control de aplicaciones en donde permita al administrador detectar y bloquear posible software no permitido por la entidad.	
		Permitir la protección del registro de arranque y disco	
		La solución de contar con Interfaz de análisis antimalware	
		La solución de contener un recurso de detección de tráfico malicioso	
		Detectar y Prevenir los exploits que puedan llegar afectar el software o hardware de las estaciones de trabajo o servidores.	
		La solución debe estar en la capacidad de mitigar los adversarios activos para evitar el robo de credenciales y detectar el tráfico malicioso.	
		Permitir la Protección contra archivos de ransomware CryptoGuard (supervisión en la escritura de archivos).	
		Incluir consultas SQL en toda la infraestructura para la búsqueda de amenazas y la higiene de las operaciones de seguridad TI (Live Discover).	
		Incluir una Biblioteca de consultas SQL (consultas ya escritas totalmente personalizables) Detección y priorización de eventos sospechosos.	
		Detección y priorización de eventos sospechosos.	

		Permitir el almacenamiento de datos en disco de rápido acceso (hasta 90 días).	
		Investigar los casos de amenazas (Análisis de causa raíz).	
		Investigar el Análisis de malware con Deep Learning.	
		Permitir el Aislamiento de Endpoint a demanda.	
		Permitir Limpiar y bloquear en un solo clic	
		La solución debe permitir la integración con el Directorio activo de la Entidad y ser compatible con todas las configuraciones de este.	
		Tener capacidades de ejecución en equipos ubicados en sitios con poco ancho de banda y en equipos finales completamente de la red evitando hacer descarga de actualizaciones continuamente.	
		La solución propuesta debe poder evitar cifrados de disco causado por ransomware y modificación de archivos o registro de los dispositivos.	
		Para los servidores la solución debe permitir configurar políticas de acuerdo con las necesidades de la aplicación instalada, puertos y exclusiones para que no afecte el correcto funcionamiento del servidor y de la aplicación.	
		La solución debe permitir realizar cifrado de discos duros en el host.	

ÍTEM	ESPECIFICACIONES	DESCRIPCIÓN	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto
		La solución debe permitir configurar agentes separados para equipos de usuarios finales y servidores.	
		La solución debe funcionar con IPv4 e IPv6	
		Las licencias con soportes extendido de servidores y equipos de cómputo deberán ser compatible con SO Windows 10, Windows Server 2012 R2.	
		Disponer de una funcionalidad de protección contra amenazas tipo ransomware o similares con capacidad de protección no basada exclusivamente en firmas.	
4	**MODULO Y SERVICIOS MDR**	El servicio de MDR debe ser proveído directamente por el fabricante del EndPoint Sophos, y tener una disponibilidad de monitoreo y respuesta a amenazas 24 horas al día, 7 días a la semana, brindado por expertos que detectan y responden a los ataques cibernéticos dirigidos a sus computadoras, servidores, redes, cargas de trabajo en la nube, cuentas de correo electrónico y más.	

		El servicio de MDR se debe integrar con el firewall de la entidad (Fortinet) y correo electrónico (Office 365) – El proveedor debe incluir el licenciamiento de integración que sea necesario. Para lo cual se requiere: ✓ Licenciamiento para integración del servicio de MDR con los 2 firewall Fortinet de la Agencia. ✓ Licenciamiento para la Integración del servicio de MDR con Office 365 a nivel de Management Activity y Microsoft Graph.	
		El servicio de MDR deberá poder integrar telemetría de terceros Endpoint, firewall, identidad, correo electrónico y otras medidas de seguridad.	
		El servicio de MRD debe contar con un equipo de expertos que detenga los ataques avanzados dirigidos por humanos y pueda tomar medidas para neutralizar las amenazas antes de que puedan interrumpir sus operaciones comerciales o comprometer sus datos confidenciales.	
		El servicio de MDR deberá detectar más amenazas cibernéticas de las que las herramientas de seguridad pueden identificar por sí solas.	
		Debe contar con herramientas que bloqueen automáticamente el 99,98 % de las amenazas, lo que permite a los analistas de MDR centrarse en cazar a los atacantes más sofisticados que solo pueden ser detectados y detenidos por un humano altamente capacitado.	
		Debe poder tomar medidas de forma proactiva y proporcionar recomendaciones que reduzcan el riesgo para su organización.	
		Debe poder fusionar la tecnología de aprendizaje automático y el análisis de expertos para mejorar la búsqueda y detección de amenazas, una investigación más profunda de las alertas y acciones	

ÍTEM	ESPECIFICACIONES	DESCRIPCIÓN	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto
		específicas para eliminar las amenazas con velocidad y precisión.	
		Los objetivos de nivel de servicio (SLA) para garantizar que el equipo cumpla con las expectativas y brinde el mejor servicio de seguridad para proteger a la entidad deben ser: ✓ Tiempo objetivo para la creación de casos: 2 minutos desde la detección ✓ Tiempo objetivo para la acción de respuesta inicial: 30 minutos desde la creación del caso.	

		Debe tener un dashboard que muestre un resumen de las amenazas detectadas e investigadas recientemente.	
		Debe tener un banner de Acción requerida en el panel que se muestra cuando hay una notificación sobre un incidente o incidentes.	
		El dashboard también debe incluir lo siguiente: ✓ Mapa de calor de detecciones por hora del día (UTC), que muestra el nivel de detecciones cada hora. ✓ Detecciones totales por sistema operativo que muestra el número de detecciones para cada sistema operativo. ✓ Cuadro de técnicas de MITRE ATT&CK que muestra un desglose de los ataques según las clasificaciones utilizadas en la base de conocimiento de MITRE. ✓ Resumen de clasificación de detecciones que enumera los cinco tipos de comportamiento malicioso detectados con más frecuencia, junto con el número de cada uno. ✓ Dispositivos más investigados que muestra los dispositivos que hemos investigado con más frecuencia. ✓ Casos activos que enumera los casos de Managed Detection Response (investigaciones sobre amenazas potenciales) que están activos actualmente. ✓ Debe tener una sección de Historial de informes donde se pueda acceder a los informes semanales y mensuales y proporcionar información sobre investigaciones de seguridad, amenazas cibernéticas y postura de seguridad.	
		Referente al modo como el servicio responde en caso de amenaza, debe permitir personalizar que acciones de respuesta a amenazas debe realizar: ✓ Colaborar: El modo de respuesta a amenazas de Colaborar debe enviarle notificaciones de las actividades observadas y las recomendaciones correspondientes. El equipo de MDR debe investigar, pero no tomar medidas de respuesta sin nuestro consentimiento o participación. Este modo Colaborar, debe brindar la opción de que algunas acciones de respuesta las realice el equipo de MDR y otras las realice	

ÍTEM	ESPECIFICACIONES	DESCRIPCIÓN	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto

		nuestro equipo u otro socio (por ejemplo, un proveedor de servicios administrados de TI). ✓ Autorizar: El modo Autorizar respuesta a amenazas debe enviar notificaciones de las actividades observadas, pero el equipo de MDR gestionará proactivamente todas las acciones de contención en nuestro nombre e informará de las acciones tomadas. Con este modo se busca que el servicio de MDR maneje la mayor carga de trabajo posible, nos notifique las acciones de respuesta tomadas y solo nos escalen las cosas que requieran acciones específicas de nuestra parte.	
		Se debe proporcionar informes de inteligencia mensual con información sobre las últimas mejores prácticas de seguridad e inteligencia de amenazas.	
		Realizar Verificación constante del estado de la seguridad (Health Check)	
		Caza de amenazas dirigida por expertos (threat hunting)	
		Contención de amenazas (Threat containment): interrumpir los ataques, evitando su propagación.	
		El despliegue de agentes deberá permitir: ✓ Soportar máquinas con arquitectura de 32 bits y 64 bits; ✓ El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Mac OS X 14 en adelante, ✓ El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows 10 en adelante ✓ El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows server 2012 R2 en adelante.	
		El servicio MDR deberá contar con un equipo de operación con capacidad de ejecutar acciones sobre el EndPoint Sophos de la Agencia de Desarrollo Rural para contener y eliminar de forma remota las amenazas que se identifique.	
		Se deberá contar con un panel único para alertas en tiempo real, gestión de informes y que proporcione información sobre investigaciones de seguridad, amenazas cibernéticas, y la postura de seguridad de la Agencia de Desarrollo Rural.	
		El equipo de operaciones del servicio MDR deberá tener la capacidad de utilizar telemetría de otras herramientas con las que este conectada la solución, para realizar búsquedas proactivas de	

ÍTEM	ESPECIFICACIONES	DESCRIPCIÓN	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto
		amenazas e identificar comportamientos de atacantes.	
		Se deberá tener acceso telefónico directo por parte del personal de la Agencia de Desarrollo Rural al centro de operaciones de seguridad (SOC) para revisar posibles amenazas e incidentes activos. Disponibilidad 24/7/365.	
		El servicio de MDR deberá brindar un servicio de respuesta y contención de incidentes; en caso de que ocurra un incidente, se asignará un equipo responsable del servicio que colaborará con el equipo interno de ADR durante el proceso de investigación, hasta que el incidente sea resuelto.	
		El servicio de MDR deberá en dado caso de materializarse de un incidente, apoyar con la identificación y análisis de la causa raíz a fin de que no puedan ser explotadas en el futuro.	
		Se debe dar respuesta a incidentes a gran escala, eliminando las amenazas por completo apalancándose en el agente EDR/XDR del mismo fabricante.	
		El servicio debe brindar un respaldo o garantía de protección contra filtraciones de hasta $1 millón (USD) en gastos de respuesta ✓ La garantía debe aplicarse en caso de que se dé una pérdida irrecuperable de datos provocada por un incidente de ransomware en endpoints y servidores Windows y macOS que ejecuten la versión más reciente del Endpoint Protection del fabricante que brinda el servicio de MDR. ✓ La garantía de cubrir el reembolso de los gastos incurridos hasta 1000 USD por cada dispositivo atacado (Windows y macOS). La cobertura total debe ser de 1000 USD multiplicado por el número de dispositivos afectados, hasta un máximo de 1 millón USD. ✓ Al momento de presentar la oferta se debe incluir los términos y condiciones estipuladas por el fabricante de seguridad que prestará el servicio de MDR.	

ÍTEM	ESPECIFICACIONES	DESCRIPCIÓN	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto

5	**GESTIÓN Y ADMINISTRACIÓN DE LA HERRAMIENTA**	La solución deberá contar con las siguientes características de administración y reportes: ✓ La plataforma deberá poder ser administrada como SAAS vía HTTPS y debe ser compatible con los navegadores Chrome, Firefox y Edge. ✓ La plataforma deberá soportar idiomas español e inglés como mínimo. ✓ La plataforma deberá tener una consola del tipo dashboard en la cual se pueda personalizar varios tipos de gráficas y tablas, lo cual permita tener una visión global de las amenazas y vulnerabilidades identificadas. ✓ La plataforma deberá permitir generar y analizar estadísticas de las amenazas encontradas. ✓ La plataforma deberá ofrecer diferentes tipos reportes y dashboard predefinidos y deberá permitir crear reportes personalizados y enviarlos por correo. ✓ La consola debe permitir la sincronización con el directorio activo y la asignación de roles de administración de la consola a usuario del Directorio Activo, quienes para acceder a la consola lo harán con su correo electrónico y asignarán una contraseña, de igual manera se debe poder activar el Doble Factor de Autenticación, con el fin, de asegurar el acceso a la consola.	
6	**SERVICIOS PROFESIONALES DE SOPORTE TÉCNICO Y GARANTIA.**	A partir del perfeccionamiento de requisitos de ejecución del contrato y con la firma del Acta de Inicio, el contratista tendrá tres (3) días para realizar la entrega del licenciamiento, e iniciar con el proceso de instalación y configuración. El oferente (partner del fabricante) deberá realizar la Instalación, actualización y configuración de la herramienta y la activación del licenciamiento por 1 año.	
		En el proceso de instalación el contratista deberá garantizar que los servidores que no tienen salida a internet deberán garantizar la actualización de los agentes por un servidor relay o similar, esto hace parte del proceso de instalación, así mismo, el oferente será el primer nivel de atención para la AGENCIA DE DESARROLLO RURAL para el servicio de soporte, además el oferente será quien mediará cualquier interacción con fabricante en caso de ser necesario.	
		Presentar plan de trabajo y cronograma para realizar cada una de las actividades requeridas para el despliegue y aprovisionamiento del servicio, así como la activación de licenciamiento.	
		La plataforma deberá entregarse totalmente lista para usar y perfilada adecuadamente para los diferentes servicios internos o externos de la AGENCIA. Así mismo el oferente deberá acompañar a la AGENCIA en las actividades de instalación y configuraciones iniciales de la plataforma, análisis de los resultados y demás funcionalidades primarias de la plataforma.	

ÍTEM	ESPECIFICACIONES	DESCRIPCIÓN	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto
		El servicio de soporte debe incluir atención de incidentes sobre las plataformas ofertadas, acompañamiento y consulta sobre funcionamiento y/o configuración de los escaneos, despliegue de agentes o configuraciones de los servicios y requerimientos de soporte por cualquier medio (correo electrónico, sesiones remotas y atención en sitio en caso de requerirse) en horario 7/24/365/2. (Las 24 horas del día, los siete días de la semana, los 365 días del año, con un tiempo máximo de solución de dos (2) horas, soporte proactivo, reactivo. Todo con respecto a las plataformas ofertadas y objeto del presente contrato. Estos servicios de soporte y garantía no deben generar costos adicionales para la AGENCIA.	
		Si la plataforma ofrece nuevas funcionalidades, el oferente deberá realizar las inducciones y/o transferencias de conocimiento sin costo adicional para la AGENCIA.	
		Al finalizar cada visita correctiva y/o preventiva el contratista deberá generar un informe de servicio/acta en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones.	
		El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones. Estos valores no incurrirán en costos adicionales para la Agencia.	
7	**TRANSFERENCIA DE CONOCIMIENTO**	Se deberá ejecutar capacitación de mínimo 12 horas a las que se determinen por parte de la Agencia de Desarrollo Rural con respecto al uso, instalación y administración de la solución de software, sin que esto derive en costos adicionales para la ADR. El proveedor deberá proporcionar un certificado de asistencia a la transferencia a los asistentes y brindar acceso permanente a la documentación relacionada con la administración de la plataforma para consulta por parte de la Agencia. Así como suministra las memorias de la capacitación, documentos, diapositivas y grabación de las sesiones.	
8	**GESTIÓN DEL PROYECTO**	El oferente deberá definir un rol que haga las veces de enlace de proyecto con la Agencia, con quien se pueda tener un contacto directo para escalamiento de casos urgentes o consultas específicas. Adicionalmente, se deberá generar un cronograma de actividades donde se especifiquen responsables y metas específicas para el correcto despliegue del proyecto.	

ÍTEM	ESPECIFICACIONES	DESCRIPCIÓN	ESPECIFICACIONES OFERTADAS (DESCRIPCIÓN) Acepto / No Acepto
		Con el fin de garantizar el correcto uso y apropiación de las buenas prácticas dadas por el fabricante, el proponente cargara junto con la propuesta, una certificación emitida por el fabricante donde se evidencie que cuenta con el personal certificado en el manejo de la plataforma de seguridad ofertada, en particular el producto que es motivo de la adquisición objeto del presente proceso de selección. Este documento deberá ser expedido por el fabricante, y el mismo deberá estar vigente durante toda la ejecución del contrato. El proponente deberá adjuntar a su propuesta una certificación que lo acredite como partner en uno de los dos niveles más altos de la mayor categoría de la marca. Este documento deberá ser expedido por el fabricante, y el mismo deberá estar vigente durante toda la ejecución del contrato.	

Elaboró:

Comité Estructurador y Evaluador Técnico

Luis Enrique Paris García / Oficina de Tecnologías de la Información.

Yapharson Jopseph Zapata Dussan / Oficina de Tecnologías de la Información.

Aprobó:
Jhon Alexander Poveda Rodríguez/ Jefe de la Oficina de Tecnologías de la Información