

**ANEXO No. 1
FICHA TÉCNICA**

1. ESPECIFICACIONES TECNICAS

1.1 Identificación del bien o servicio a contratar utilizando el clasificador de bienes y servicios UNSPSC- v.14.080, hasta el cuarto nivel, así:

Segmento	Familia	Clase	Producto	Nombre
43000000	43230000	43233200	43233205	Software de seguridad de transacciones y de protección contra virus
81000000	81110000	81111800	81111801	Seguridad de los computadores, redes o internet.
81000000	81110000	81112200	81112208	Mantenimiento de software de protección y seguridad

1.2 ESPECIFICACIONES TÉCNICAS DEL BIEN O SERVICIO

OBJETO O DENOMINACIÓN DE BIEN O SERVICIO			
Renovación del Licenciamiento Antimalware para la ARN de acuerdo con las especificaciones del Anexo No. 1 "Ficha Técnica"			
DESCRIPCIÓN			
IDENTIFICACION DEL PRODUCTO	CREDITOS POR USUARIO	CANTIDAD 2026	TOTAL CREDITOS AÑO
End Point Security Essentials	65	2464	160.160,00
End Point Security Pro	300	20	6.000,00
Cyber Risk Exposure Management Core	20	2464	49.280,00
Total de créditos			215.440,00

El proveedor debe garantizar que la ARN tendrá servicio por un año.

Las licencias actuales tienen vigencia hasta el 26/06/2026, los créditos están calculados con la expectativa de uso por el termino de 12 meses, el cual incluye el soporte respectivo.

1. PROTECCIÓN ENDPOINT

Funcionalidades generales

- La solución de licenciamiento deberá estar listada como líder del cuadrante mágico de Gartner 2025 para la protección del punto final.
- La solución de licenciamiento debe contar con certificación de AV-Test.
- La solución de licenciamiento debe tener reconocimientos en cuanto a protección de Vulnerabilidades para endpoints.
- El fabricante de la solución de licenciamiento debe contar con equipo de investigación de vulnerabilidades de Zero Day adicionalmente debe ser reconocido por los estudios de Frost and Sullivan.
- La solución de licenciamiento debe estar ubicada mínimo por quinto año consecutivo en el cuadrante de líderes de Gartner para soluciones de Endpoint.
- La solución de licenciamiento debe permitir realizar escaneos de los endpoint de forma manual, programada y en tiempo real desde el agente instalado en los Endpoint.
- La solución de licenciamiento debe permitir realizar escaneos de los endpoint de forma manual, programada y en tiempo real desde el agente instalado en los Endpoint.
- La solución de licenciamiento debe utilizar métodos basados en firmas, heurísticos, conductuales y de reputación para defenderse de las distintas fases de un ataque. Esto incluye la protección en memoria, la prevención de ataques sin archivos y la monitorización de la integridad del sistema para garantizar una seguridad integral.
- La solución de licenciamiento debe proteger los puntos finales en cada etapa de un ataque con protección multicapa, IA y aprendizaje automático, y detección y respuesta nativas para proteger todas las partes de su infraestructura, incluidos los sistemas antiguos y los dispositivos IoT.
- La solución debe utilizar el aprendizaje automático predictivo y en tiempo de ejecución permitir evaluar las amenazas antes y durante su ejecución mediante el análisis del comportamiento y en memoria para bloquear amenazas sofisticadas como el ransomware y los ataques de día cero. Los algoritmos basados en IA permiten adaptarse continuamente a la nueva información sobre amenazas, mejorando así la protección.
- La solución de licenciamiento debe garantizar el cumplimiento normativo y proteger contra las amenazas a servidores y cargas de trabajo con control de aplicaciones, antimalware, servicio de reputación web, firewall, prevención de intrusiones, monitorización de la integridad e inspección de registros.
- La solución de licenciamiento debe permitir la protección de componentes de infraestructura, incluidos los sistemas heredados y los dispositivos IoT, para abordar las vulnerabilidades de los dispositivos más antiguos y menos seguros, y asegurar de que no representen puntos débiles en la postura de seguridad.
- La solución de licenciamiento debe consolidar múltiples herramientas y aplicaciones en una sola plataforma con flujos de trabajo automatizados.

- La solución de licenciamiento debe reducir la complejidad y la carga de gestionar múltiples proveedores y productos. Aprovechar una única interfaz para supervisar y controlar las políticas de seguridad, las configuraciones y las actualizaciones, y obtener una visibilidad completa de todas las actividades de los dispositivos.
- La solución de licenciamiento debe ofrecer soporte para entornos locales, en la nube, en la nube privada e híbridos con un agente flexible y ligero que se adapte a las necesidades cambiantes de la organización.
- La solución de licenciamiento debe tener la capacidad de aislar los equipos o ponerlos en cuarentena cuando se detecta algún ataque para evitar la propagación del ataque dentro de la red.
- La solución de licenciamiento debe permitir realizar una migración a versiones superiores de la misma conservando las configuraciones, incluida la base de datos.
- La solución de licenciamiento debe permitir la creación y aplicación de políticas a todas las máquinas, por perfil e individualmente para cada host y/o por grupos.
- La solución de licenciamiento debe tener la capacidad de brindar protección contra malware, virus de red, conexiones sospechosas, amenazas web, spyware, análisis de archivos adjuntos de correo, monitoreo de comportamiento, ataques combinados y ataques de día cero para equipos de punto final (Endpoint).
- Los agentes de endpoint deben ser instalados mediante instalación web, link de instalación por correo, instalación por script, instalación remota, y/o paquete de instalación.
- Los agentes deben requerir contraseña de administración para ser desinstalados de los equipos.
- Los agentes deben ser agrupados por NetBios, Directorio Activo, DNS y/o grupos personalizados.
- El agente debe tener la capacidad de eliminar los archivos sospechosos de forma automática.
- La solución de licenciamiento debe tener la capacidad de prevenir la ejecución de aplicaciones no deseadas o desconocidas en los endpoint.
- La solución de licenciamiento debe tener Motor antimalware de nueva generación con detección basada en firmas, reputación, machine learning y análisis de comportamiento para malware, ransomware, scripts y amenazas sin archivo.
- La solución de licenciamiento debe tener protección contra ransomware con capacidad de detección de comportamiento, bloqueo y recuperación/rollback de archivos afectados.
- La solución de licenciamiento debe tener análisis de comportamiento (behavior monitoring) que identifique y bloquee modificaciones sospechosas en sistema, registro, procesos, scripts y navegadores.
- La solución de licenciamiento debe tener sistema de reputación web y filtrado de URL para bloquear acceso a sitios maliciosos o sospechosos, integrando reputación de dominios y direcciones IP.
- Prevención de exploits y sistema de prevención de intrusiones en host (HIPS/HIDS) capaz de bloquear técnicas de explotación en aplicaciones y sistema operativo.
- Control de dispositivos (USB, almacenamiento extraíble, impresoras, etc.) y control de aplicaciones (permitir, bloquear, modo solo lista blanca).
- Firewall de host integrado o integración estrecha con el firewall del sistema para aplicar políticas de segmentación y control de tráfico saliente/entrante a nivel de endpoint.

- Integración nativa con una plataforma XDR para correlacionar eventos de endpoints con correo, red, identidades y nube, y permitir investigaciones consolidadas.
- Console única basada en la nube para despliegue de agentes, gestión de políticas, monitoreo de incidentes y generación de reportes técnicos y ejecutivos.
- Soporte para múltiples sistemas operativos (versiones actuales de Windows, macOS y varias distribuciones de Linux), incluyendo servidores y cargas virtuales.
- Los agentes deben tener la capacidad de conectarse a múltiples fuentes de actualización (patrones, firmas, url sospechosas, etc.), si alguna de estas es inaccesible para el agente.
- Los agentes de actualización deben buscar de forma automática las actualizaciones de firmas, componentes y distribuirlas a los agentes, estas actualizaciones deben realizarse en modo seguro utilizando comunicación SSL con el servidor del cual se descarga dicha información.

La consola de Administración deberá permitir las siguientes funcionalidades:

- Entorno de administración web compatible con Microsoft Internet Explorer, Mozilla Firefox y Google Chrome de todas las funcionalidades y servicios ofrecidos por la plataforma, así como el control de los agentes instalados en los endpoint ya sean físicos o virtuales.
- La consola de administración de la solución de licenciamiento debe proporcionar gráficos y estadísticas de distribución de la solución, distribución de políticas y agentes administrados.
- Proporcionar monitoreo continuo para visibilidad instantánea y completa del entorno, notificaciones en tiempo real de las actividades y eventos que ocurran; permitir la generación de reportes personalizables y desde el mismo dashboard de la consola de la solución de licenciamiento poder administrar entornos físicos, virtuales.
- Creación, modificación y eliminación de roles y usuarios para la administración de la misma.
- Habilidad de configurar permisos granulares, para delegar operaciones y trabajos específicos a diversos usuarios o grupos de usuarios, así como perfiles de auditoría que solo permitan visualizar datos pero sin la capacidad de modificar ninguna configuración.
- Capacidad de integrarse con Microsoft Active Directory para la administración de usuarios de acceso a la consola y realizar búsqueda de nuevas máquinas en el dominio.
- Contar con dashboards que permitan tener la visualización de los equipos administrados, que presenten alertas y que pueda ser personalizada por el administrador.
- La consola debe tener capacidad de estar en Nube y/o ambientes on premise, permitiendo tener un ambiente híbrido que permita administrar los agentes instalados en la red de equipos.
- La consola debe proporcionar la capacidad de administrar los usuarios para agregar o eliminar cuentas, restablecer contraseñas, cambiar permisos, configurar prioridad de políticas y buscar cuentas de usuario específicas.
- Agrupación los agentes en grupos para facilitar la configuración y administración de los mismos.
- Configuración de notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de los mismos.
- Tener un Dashboard que brinde información global sobre los agentes, eventos de reputación web, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.

- Consultar los Logs de instalación tanto del agente como el del servidor de administración.
- Visualizar estadísticas de históricos de actualizaciones de patrones de análisis de antivirus, antispymware, análisis de comportamiento, conexiones sospechosas, y exploits de los navegadores de internet.
- Visualizar los logs de los eventos sobre los equipos donde se encuentra instalado el agente, dichos eventos deben estar relacionados a temas de malware, spyware, Reputación web, conexiones sospechosas, archivos sospechosos, Command & Control Callbacks, Behavior Monitoring, Machine Learning, control de dispositivos, DLP, y escaneos.
- Capacidad en la consola de mostrar distintos gráficos para dar seguimiento al tráfico de correo y cuarentenas.
- Permitir a los administradores configurar la lista de excepciones, de los archivos detectados como maliciosos o sospechosos.

La solución de licenciamiento debe generar adicionalmente los siguientes reportes:

- Resumen gráfico de vulnerabilidades agrupadas por severidad encontradas en los endpoints y/o aplicación web instalas en los endpoints protegidos.
- Gráfico de tendencia en el tiempo (con la información de todos los escaneos realizados) de vulnerabilidades encontradas por aplicación web.
- Lista de vulnerabilidades clasificadas por nivel de severidad
- Lista de vulnerabilidades clasificadas por tipo de plataforma

1.1. Compatibilidad en sistemas operativos

Agente:

- Windows 10.
- Windows 11.
- macOS Sequoia 15
- macOS Sonoma 14
- macOS Ventura 13
- macOS Monterey 12
- macOS Big Sur 11
- macOS Tahoe

Servidor:

- Windows Server 2012 (6.2)
- Windows Server 2016 (10)
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

1.2. Firewall De Punto Final

La solución de licenciamiento deberá contener un firewall que proteja maquinas físicas, y/o virtuales administrados desde la misma consola, permitiendo sólo las comunicaciones requeridas entre ellos. Este filtrado debe ser bidireccional y hacerse al menos sobre los siguientes parámetros:

- La solución de licenciamiento debe permitir identificar las técnicas de escaneo de puertos como XMAS Scan, Null Scan, ACK Scan y tomar acciones al respecto.
- La solución de licenciamiento debe contar con firewall (reglas de conexiones de aplicación, IP, puerto y protocolo), reputación de archivos y/o reputación web.

1.3. Parcheo Virtual

Las brechas de seguridad descubiertas por medio de escaneo de recomendaciones deben ser protegidas de forma automática y transparente, interrumpiendo únicamente el tráfico malicioso y sin que se vean afectas las aplicaciones del sistema, contar con la posibilidad de aplicar automáticamente la protección para las vulnerabilidades a través de un perfil o por host y además el fabricante de la solución de licenciamiento debe reactivamente desplegar parches virtuales para vulnerabilidades críticas de Microsoft.

El parcheo virtual deberá contar con las siguientes funcionalidades:

- Permitir la aplicación de reglas para la protección de vulnerabilidades de forma automática posterior a un escaneo de vulnerabilidades.
- Permitir visualizar si una vulnerabilidad ya fue remediada o fue instalado el parche en su aplicación o sistema operativo.
- Crear tareas programadas para realizar escaneo de vulnerabilidades
- Aplicación de reglas de protección de vulnerabilidades se debe realizar sobre el tráfico de red, de forma transparente, sin generación de falsos positivos, sin afectar tráfico no anómalo y no deben requerir reinicio de máquinas, ni afectación del Sistema operativo, aplicaciones o código existente en el ambiente de la corporación.
- Debe estar en capacidad de generar parches virtuales para vulnerabilidades críticas de día zero para aplicaciones y sistemas donde todavía el fabricante no ha desplegado el parche oficial.
- Generar de forma inmediata parches de protección para vulnerabilidades en Sistemas Operativos que ya no son soportados.
- Identificar las vulnerabilidades y recomendar automáticamente reglas en base al sistema operativo y aplicaciones instaladas en cada uno de los servidores.

1.4. Data Loss Prevention

La solución de licenciamiento ofertada deberá mantener un monitoreo constate y una consola de administración WEB que permita la configuración de políticas e implementaciones, reportes de los equipos y actualizaciones. Debe contar con las siguientes funcionalidades para la prevención de fuga de información:

- Capacidad de prevenir y/o informar sobre la fuga o perdida de información sensible de la organización ya sea de forma accidental o deliberada.
- Identificar o configurar los activos digitales que se desean proteger.

- Crear políticas que limiten la transmisión o transferencias de activos digitales por los canales de comunicación convencionales (email y/o dispositivos externos).
- Brindar protección y aplicar políticas para transferencia de activos digitales mediante cliente de correo ya sea software o web.
- Brindar protección contra filtrado de datos sensibles y proporcionar un control de dispositivos, permitiendo configurar reglas o políticas para ser aplicadas a grupos o agentes individuales.
- Proporcionar identificadores de datos y/o plantillas para la creación de políticas.
- Capacidad de identificar o reconocer archivos ejecutables, documentos, gráficos vectoriales, archivos multimedia, archivos comprimidos, bases de datos, hojas de cálculo, presentación, archivos vinculados e incrustados, y/o archivos encriptados.
- Capacidad de localizar activos digitales almacenados en portátiles, equipos de escritorio, y servidores.
- Capacidad de proporcionar filtros de protección para canales de red como FTP o HTTP, canales de aplicaciones o periféricos con el mismo agente
- Capacidad de detectar datos estructurados y no estructurados.
- Integración con Directorio Activo y delegación de administración.
- La solución de licenciamiento debe contar con una herramienta que analice los activos digitales que se encuentran almacenados en los portátiles o computadores de escritorio aun así no estén conectados en la red de la organización.
- Las plantillas de identificación de activos digitales debe permitir combinar identificadores de datos (expresiones, atributos de archivos, huellas digitales, lista de palabras).
- La solución de licenciamiento debe permitir almacenar reportes y estos deben estar disponibles en formatos PDF, HTML, o Microsoft Excel.
- La herramienta de análisis local debe tener la capacidad de adquirir huellas digitales para los archivos almacenados en el equipo.
- Proveer una lista de palabras predefinidas para la validación de formularios como fecha de nacimiento, fecha de expiración, Nombres y apellidos, lugar de nacimiento, departamentos o ciudades y direcciones de domicilios.
- Proveer una lista de palabras que puedan identificar comandos o instrucciones en lenguajes de programación como C#, C/C++, COBOL, Java, Perl y VB.
- DLP a nivel de Email con la capacidad de descubrir y reportar violaciones a las políticas.
- DLP a nivel de SharePoint y One Drive, con la capacidad de descubrir y reportar violaciones a las políticas.

1.5. Control de aplicaciones

La solución de licenciamiento debe tener las siguientes funcionalidades de control de Aplicaciones:

- Bloquear o permitir aplicaciones de acuerdo a puntaje de seguridad propio del fabricante.
- Uso de protocolos TLS/SSL para la comunicación entre los agentes y el servidor de administración.
- Configuración del intervalo en el que los logs de los agentes son recolectados por el servidor de administración.

- Configuración del intervalo en el que los agentes actualizan las políticas consultando el servidor de administración.
- Capacidad de identificar o agrupar los logs por políticas, inventario de equipos, aplicaciones conocidas, acciones del administrador, mensajes de los agentes y mensajes del servidor.
- Debe permitir realizar búsquedas en los registros o logs, haciendo uso de filtros y permitir exportarlos en archivos con formato (CVS o XLSX).
- Tener capacidad de bloquear o permitir aplicaciones de acuerdo al path, hash o tipo de aplicación.

1.6 Consola de Administración

- Entorno de administración web compatible con Microsoft Internet Explorer, Mozilla Firefox y Google Chrome de todas las funcionalidades y servicios ofrecidos por la plataforma, así como el control de los agentes instalados en los endpoint ya sean físicos o virtuales.
- La consola de administración de la solución de licenciamiento debe proporcionar gráficos y estadísticas de distribución de la solución, distribución de políticas y agentes administrados.
- Consola de administración centralizada con panel de control unificado.
- Despliegue de agentes mediante políticas automatizadas.
- Soporte para sistemas operativos: Windows 10/11, Windows Server 2016/2019/2022, macOS 12+, Linux (Red Hat, Ubuntu, CentOS).
- Generación de reportes de cumplimiento y estado de seguridad.
- Integración con directorios corporativos (Active Directory / LDAP).
- Proporcionar monitoreo continuo para visibilidad instantánea y completa del entorno, notificaciones en tiempo real de las actividades y eventos que ocurran; permitir la generación de reportes personalizables y desde el mismo dashboard de la consola de la solución de licenciamiento poder administrar entornos físicos, virtuales.
- Creación, modificación y eliminación de roles y usuarios para la administración de la misma.
- Habilidad de configurar permisos granulares, para delegar operaciones y trabajos específicos a diversos usuarios o grupos de usuarios, así como perfiles de auditoría que solo permitan visualizar datos pero sin la capacidad de modificar ninguna configuración.
- Capacidad de integrarse con Microsoft Active Directory para la administración de usuarios de acceso a la consola y realizar búsqueda de nuevas máquinas en el dominio.
- Contar con dashboards que permitan tener la visualización de los equipos administrados, que presenten alertas y que pueda ser personalizada por el administrador.
- La consola debe tener capacidad de estar en Nube y/o ambientes on premise, permitiendo tener un ambiente híbrido que permita administrar los agentes instalados en la red de equipos.
- La consola debe proporcionar la capacidad de administrar los usuarios para agregar o eliminar cuentas, restablecer contraseñas, cambiar permisos, configurar prioridad de políticas y buscar cuentas de usuario específicas.
- Agrupación de los agentes en grupos para facilitar la configuración y administración de los mismos.
- Configuración de notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de los mismos.

- Tener un Dashboard que brinde información global sobre los agentes, eventos de reputación web, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.
- Consultar los Logs de instalación tanto del agente como el del servidor de administración.
- Visualizar estadísticas de históricos de actualizaciones de patrones de análisis de antivirus, antispysware, análisis de comportamiento, conexiones sospechosas, y exploits de los navegadores de internet.
- Visualizar los logs de los eventos sobre los equipos donde se encuentra instalado el agente, dichos eventos deben estar relacionados a temas de malware, spyware, Reputación web, conexiones sospechosas, archivos sospechosos, Command & Control Callbacks, Behavior Monitoring, Machine Learning, control de dispositivos, DLP, y escaneos.
- Capacidad en la consola de mostrar distintos gráficos para dar seguimiento al tráfico de correo y cuarentenas.
- Permitir a los administradores configurar la lista de excepciones, de los archivos detectados como maliciosos o sospechosos.

La solución de licenciamiento debe generar adicionalmente los siguientes reportes:

- Resumen gráfico de vulnerabilidades agrupadas por severidad encontradas en los endpoints y/o aplicación web instalas en los endpoints protegidos.
- Gráfico de tendencia en el tiempo (con la información de todos los escaneos realizados) de vulnerabilidades encontradas por aplicación web.
- Lista de vulnerabilidades clasificadas por nivel de severidad
- Lista de vulnerabilidades clasificadas por tipo de plataforma.

La solución de licenciamiento debe tener funcionalidades de XDR:

- La solución de licenciamiento de Predictive Machine Learning debe proporcionar protección fuera de línea sin conexión a Internet o no disponibilidad de acceso a la red.
- La solución de licenciamiento debe permitir monitorear, registrar y realizar investigaciones de seguridad actuales e históricas en sus diferentes puntos finales. Por medio de un panel debe permitir la investigación preliminar y de causa raíz de un incidente, permitiendo ubicar los puntos finales en riesgo antes de ejecutar el análisis de causa raíz en profundidad para identificar los vectores de ataque.
- La solución de licenciamiento debe ser líder en MITRE categoría de protección para garantizar la prevención temprana en el ciclo de vida del ataque.
- La solución de licenciamiento debe escale la investigación y búsqueda de amenazas visualizando todo el historial del ataque utilizando gráficos, asignaciones de MITRE ATT&CK y técnicas de búsqueda simplificadas.
- Debe permitir generar investigaciones preliminares para identificar rápidamente los puntos finales que son posibles candidatos para un análisis adicional. Una investigación preliminar utiliza metadatos del servidor para obtener resultados rápidamente.
- Debe permitir genera investigaciones detalladas que permitan realizar una investigación sobre el estado actual del sistema. Las investigaciones depectalladas se pueden configurar para que se ejecuten en períodos específicos y también admiten un conjunto más amplio de criterios mediante el uso de las reglas de OpenIOC y YARA.
- La solución de licenciamiento debe combinar diversas reglas, filtros y técnicas de análisis, incluido el apilamiento de datos y el machine learning, para mejorar la velocidad de detección y la precisión a la vez que reduce los falsos positivos en la entidad.

- La correlación de amenazas debe permitir conectar datos de actividad profunda en varios vectores de seguridad para una mayor detección e investigación.
- La solución de licenciamiento deberá permitir graficar toda la cronología de los eventos generados en una investigación por medio de un gráfico de anillos que muestra el número total de puntos finales clasificados ya sea estén relacionados, o no relacionados a otros procesos, en cola o cancelados. La información debe estar siendo actualizada en tiempo real y de forma automática mientras avanza una investigación.
- La solución de licenciamiento debe permitir la búsqueda de Indicadores de Compromiso (IoC) en búsqueda de comunicaciones específicas, actividad de registro, actividad de la cuenta autenticada en el sistema, procesos en curso.
- La solución de licenciamiento debe permitir la búsqueda de amenazas activas en el entorno utilizando diversos métodos de búsqueda múltiple, desde potentes consultas hasta sencillas búsquedas de texto, para identificar actividades sospechosas.
- La solución de licenciamiento debe poder integrarse con SIEM, SOAR, gestión de acceso por identidad, firewall, información sobre amenazas, gestión de servicios de TI y tecnologías de creación de tickets.
- La solución de licenciamiento debe tener la capacidad de funcionar en diversos vectores de seguridad, incluidos endpoints nativos, emails, servidores, redes, nubes, móvil, identidad y sensores de IoT y OT.
- La solución de licenciamiento debe permitir validar actividad sospechosa, investigar el ID de técnicas específicas de amenazas desconocidas y aprovechar la información automatizada para buscar continuamente nuevos indicadores de compromiso (IOC).
- La solución de licenciamiento debe permitir realizar análisis XDR a los datos de actividad recopilados de sus soluciones nativas para crear alertas accionables y correlacionadas, y perspectivas completas de incidentes.
- Protección contra ataques de exploits: controla los programas que demuestran un comportamiento anormal asociado con ataques de exploits.
- Aprendizaje automático: analiza archivos desconocidos de baja prevalencia al extraer características de los archivos para examinarlos utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso (es decir, malware / ransomware / amenazas de día 0).

2. PROTECCIÓN SERVIDORES

La solución de licenciamiento deberá incluir capacidades:

- Detección y Respuesta (EDR): Grabación continua de la telemetría del sistema (eventos de red, cambios en registro, ejecución de procesos) para análisis forense.
- Parcheo Virtual (HIPS): Capacidad de blindar vulnerabilidades conocidas antes de que se aplique el parche oficial del fabricante, operando a nivel de red (IPS).
- Análisis de Causa Raíz (RCA): Visualización del árbol de ejecución del ataque para identificar el punto de entrada (paciente cero) y la propagación lateral.
- Control de Aplicaciones: Capacidad de crear listas blancas (allow-listing) para permitir solo software autorizado en servidores o entornos críticos.
- Acciones de Respuesta: El administrador debe poder aislar hosts de la red, terminar procesos maliciosos o recolectar archivos sospechosos de forma remota desde la consola.

La solución de licenciamiento deberá incluir capacidades avanzadas de detección y respuesta:

- Funcionalidades completas de EDR/XDR: búsqueda de amenazas (threat hunting), consultas avanzadas sobre telemetría de endpoints, timeline de eventos, y capacidades de investigación forense ligera.
- Capacidad de respuesta remota en el endpoint: aislamiento de red del dispositivo, terminación de procesos maliciosos, eliminación de archivos, ejecución de scripts de remediación y cambios de políticas en tiempo real.
- Módulos avanzados de prevención de intrusiones para servidores y aplicaciones críticas, incluyendo protección de aplicaciones web, monitoreo de integridad e inspección de logs cuando aplique.
- Protección optimizada para entornos virtuales, VDI y nubes públicas, con opciones de agentes ligeros y/o awareness de virtualización para reducir impacto de desempeño.
- Telemetría enriquecida para XDR que incluya detalles de procesos, conexiones de red, cambios en el sistema, usuarios involucrados y contexto de autenticación.
- Integración ampliada con otras capas de seguridad gestionadas desde la misma consola (correo, red, nube, identidades), para construir incidentes compuestos y rutas de ataque completas.

3. GESTIÓN DE EXPOSICIÓN AL RIESGO

La solución de licenciamiento deberá incluir un módulo de gestión de exposición al riesgo cibernético con, al menos, las siguientes capacidades:

- Descubrimiento y mapeo automático de activos: endpoints, servidores, aplicaciones, servicios en nube, identidades y otros elementos relevantes, consolidando una vista única del entorno.
- Cálculo continuo de exposición y riesgo cibernético, priorizando vulnerabilidades y debilidades según criticidad del activo, explotabilidad y contexto de amenazas.
- Identificación y gestión de superficie de ataque externa.
- Gestión del riesgo de vulnerabilidad.
- Análisis de riesgo de exposición.
- Modelado de rutas de ataque y caminos probables que un atacante podría seguir, identificando puntos de entrada, movimientos laterales y activos críticos.
- Generación de un índice o puntuación de riesgo cibernético a nivel de organización, con paneles que permitan mostrar de forma sencilla la postura de riesgo a la alta dirección.
- Recomendaciones priorizadas de remediación, indicando controles técnicos y cambios de configuración específicos en endpoints, servidores, nube y otros componentes.
- Capacidad de orquestar y automatizar acciones de mitigación cuando sea posible (por ejemplo, aplicar políticas en endpoints, reforzar controles, aislar activos, abrir tickets).
- Mapas y reportes alineados a marcos de referencia (por ejemplo, NIST, ISO 27001, marcos de privacidad, etc.) con capacidad de exportar reportes listos para auditoría.
- Integración directa con la telemetría y las políticas de protección de endpoints para que los hallazgos de riesgo se traduzcan en cambios concretos de postura de seguridad.

La solución de licenciamiento debe proporcionar gestión continua de la superficie de ataque con las siguientes capacidades:

- Descubrimiento automático de activos internos y externos asociados a la organización.
- Evaluación de riesgo por activo basada en vulnerabilidades activas, configuraciones incorrectas y exposición en internet.

- Mapa visual de superficie de ataque con priorización de remediation por impacto potencial.
- Correlación con amenazas activas que explotan las vulnerabilidades identificadas.

La solución de licenciamiento debe proporcionar Métricas Ejecutivas con:

- Índice de riesgo organizacional con evolución histórica y tendencias.
- Desglose por departamento, ubicación geográfica o segmento de red.
- Dashboards personalizables para diferentes roles: CISO, SOC Manager, IT Operations.
- Exportación de reportes en formatos PDF, Excel y acceso vía API.

Gestión de Configuraciones Incorrectas

- Detección de configuraciones inseguras en sistemas operativos, aplicaciones y servicios cloud.
- Benchmarking contra CIS Benchmarks y mejores prácticas de la industria.
- Flujos de remediación guiada con priorización automática.

PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de dos **(2) meses** contados a partir de la fecha de la aprobación de la garantía, previa expedición del registro presupuestal y acta de inicio; periodo correspondiente a la entrega de la totalidad de los créditos del licenciamiento renovado, instalación, configuración, puesta en funcionamiento y transferencia de conocimiento.

Lo anterior, sin perjuicio de la garantía de soporte técnico y actualización que deberá prestarse por el contratista por un término de doce (12) meses, contados a partir de la entrega, instalación y puesta en funcionamiento del licenciamiento, para lo cual deberá tenerse en cuenta el vencimiento de las licencias de las que actualmente dispone la entidad, a saber.

1.3 ESPECIFICACIONES DEL SOPORTE TECNICO

SERVICIO DE IMPLEMENTACIÓN, INSTALACIÓN CONFIGURACIÓN Y PUESTA EN MARCHA DEL ANTIMALWARE

El servicio de soporte y asistencia técnica en sitio no genera costos adicionales para la ARN:

- Soporte técnico en sitio y remoto por demanda sin costo para la Entidad y de acuerdo con los ANS establecidos. Los cuales deben atenderse por la durabilidad de la adquisición de Licenciamiento Antimalware
- Instalación y migración de nuevas versiones o mejoras de la consola y el antimalware en cliente durante todo el plazo de ejecución del contrato. sin generar costos adicionales para la ARN, el mismo se extenderá **I** durante 12 meses para todos los productos renovados y adquiridos.

- Brindar soporte mediante dos (2) visitas anuales en las fechas que la supervisión establezca dentro del plazo de uso del licenciamiento (12 meses), con el fin de inspeccionar el uso del producto, en las cuales brindará recomendaciones del mismo, sin costo adicional para la entidad. Visita de soporte preventivo y monitoreo mensual durante el plazo de uso del licenciamiento sin costo para la Entidad.
- Soporte telefónico, remoto. sin generar costos adicionales para la ARN, en modelo 7X24.
- Implementación de políticas de seguridad informática que ayuden a las buenas prácticas de uso de información por parte del usuario final y que faciliten la eficiencia de la red.
- Entrega de reporte técnico, después de cada intervención del contratista y sin generar costos adicionales para la ARN.
- Servicio técnico prestado por personal certificado por el fabricante conforme a las certificaciones de distribuidor autorizado definidas en el numeral 8.3.4 del estudio previo y en corresponsabilidad y gestión por parte del contratista. sin generar costos adicionales para la ARN. El número de personas será el establecido por el contratista para dar cumplimiento de esta obligación.
- Para efectos de validación del licenciamiento con el que cuenta la entidad actualmente, la denominación para consultar con el fabricante es Agencia Colombiana para la Reintegración de Personas y Grupos Alzados en Armas ACR, hoy “Agencia para la Reincorporación y la Normalización, ARN”.

2. GARANTÍA Y SOPORTE TÉCNICO

-NIVELES DE SERVICIO ANS

Para el soporte por demanda y soporte reactivo, la Agencia, puede solicitar atención en cualquier día de la semana y horario, sin generar costos adicionales para la ARN. Según la severidad del incidente los tiempos de atención por parte del contratista son:

Severidad del Incidente	Tiempo de Respuesta
1	2 horas
2	3 horas
3	4 horas

Severidad 1: Significa un estado sin funcionamiento del producto que tiene impacto en un entorno de producción afectando la integridad y disponibilidad de los datos para el cual no hay una solución alternativa inmediata disponible, tal como (i) cuando la herramienta presenta fallas graves que no permiten la continuidad disponibilidad de los servicios tecnológicos o compromete evento de seguridad digital en algún componente de la infraestructura tecnológica de la Entidad; (ii) cuando la herramienta no permite generar el monitoreo, escaneo, búsqueda o detección, en mínimo 5 componentes tecnológicos, o problemas de la herramienta en procesos de instalación, actualización, configuración o migración asociados a la plataforma de antimalware.; (iii) cuando existe un incidente con la herramienta que compromete la disponibilidad y funcionalidad de un elemento que tenga la instalación del software de antimalware, cuando el software se instala o está en funcionamiento (es decir, un bloqueo del sistema, una pérdida o daño de la base de datos de la solución de licenciamiento o una pérdida de seguridad del sistema) y esto impacta en el funcionamiento continuo en un entorno de producción.

Severidad 2: Hace referencia al estado de alto impacto que, posiblemente, ponga en peligro un entorno de producción. El software puede funcionar, pero tiene restricciones, tales como (i) cuando se generan errores por desactualización de la herramienta; (ii) cuando se presentan errores de la herramienta; o (iii) cuando se presentan errores inesperados que no afectan del todo el funcionamiento, pero degradan el servicio.

Severidad 3: Significa un estado de bajo impacto que cuenta con la mayoría de las funciones de software todavía utilizables; no obstante, es necesaria alguna acción para brindar el servicio. Se refiere a (i) un problema o cuestión menor que no afecta la función de la herramienta, (ii) una sugerencia para las nuevas características o mejoras del producto de software.

En el caso de que el evento sea escalado al fabricante de la herramienta, se debe tener un tiempo de solución máximo de cuatro (4) horas bajo la modalidad 7X24. En este evento el CONTRATISTA deberá en todo momento realizar el seguimiento del caso escalado al fabricante y mantener informada a la Entidad de la solución de licenciamiento a dicho caso.

Este soporte no genera costo adicional para la ARN. La severidad será fijada por la ARN en la solicitud de servicio.

Proyectó Técnicamente: Fernando Caro – OTI

Revisó en lo Técnico: Merly Yolimar Parra Sosa - OTI