

FICHA TECNICA

DESCRIPCIÓN DEL OBJETO, SUS CARACTERÍSTICAS Y CONDICIONES TÉCNICAS MÍNIMAS DE OBLIGATORIO CUMPLIMIENTO

1. Objeto

Adquirir una solución de protección antivirus para los equipos de cómputo de la Entidad, incluyendo el licenciamiento y los servicios necesarios para su adecuada operación, con el propósito de fortalecer la seguridad de la información institucional y garantizar la continuidad de los servicios tecnológicos..

2. Requisitos funcionales mínimos

Descripción del bien o servicio a contratar:															
Con el fin de satisfacer la necesidad antes expuesta, se requiere contratar la renovación y adquisición del licenciamiento de la solución de Antivirus para 2.327 equipos .															
<table><tr><th>DESCRIPCIÓN</th><th>Cantidad</th></tr><tr><td>Computador Escritorio</td><td>1.643</td></tr><tr><td>Computador portátil</td><td>276</td></tr><tr><td>Computador Apple</td><td>51</td></tr><tr><td>Servidor Windows</td><td>287</td></tr><tr><td>Servidor Linux</td><td>70</td></tr><tr><td>Total</td><td>2.327</td></tr></table>	DESCRIPCIÓN	Cantidad	Computador Escritorio	1.643	Computador portátil	276	Computador Apple	51	Servidor Windows	287	Servidor Linux	70	Total	2.327	
DESCRIPCIÓN	Cantidad														
Computador Escritorio	1.643														
Computador portátil	276														
Computador Apple	51														
Servidor Windows	287														
Servidor Linux	70														
Total	2.327														
Durante un (1) año, incluidos los servicios de instalación, configuración, soporte y mantenimiento, mediante las siguientes características técnicas:															
Características mínimas de carácter mandatorio															
La existencia de un único motor antimalware.															
Para minimizar el consumo de recursos, los productos antimalware deben permitir la instalación de módulos personalizados.															
Teniendo en cuenta que el presente proceso contempla la implementación y operación de una solución de protección antivirus sobre activos críticos de la infraestructura tecnológica de la entidad, incluyendo entornos híbridos y en la nube, se hace necesario que los servicios asociados se presten bajo lineamientos de seguridad robustos y alineados con mejores prácticas internacionales. Lo anterior con el fin de garantizar la protección de la información, la integridad de los sistemas, el control adecuado de accesos y la mitigación de amenazas avanzadas que puedan afectar la continuidad operativa. En este sentido, el oferente deberá garantizar que sus servicios basados en infraestructura en la nube cuenten con procedimientos formalmente establecidos, documentados y operativos para la gestión segura de la información en entornos cloud. Para ello, el oferente deberá contar con certificación vigente en una norma internacional que establezca buenas prácticas de seguridad aplicables a servicios en la nube, incluyendo aspectos como la protección de datos, la responsabilidad															



compartida entre proveedor y cliente, el control de accesos, la segregación lógica de entornos y el monitoreo de recursos virtualizados.

Esta certificación respaldará el cumplimiento de estándares internacionales en la gestión de servicios en la nube, conforme a las políticas de seguridad de la entidad y en armonía con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia – MinTIC. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente.

Agente y consola únicos: Desarrollado desde cero como una solución de agente y consola únicos, que incorpora todas las tecnologías necesarias para proteger eficazmente los endpoints empresariales y detener todas las amenazas digitales. Elimina la necesidad de ejecutar varios agentes y simplifica significativamente la implementación y la operativa.

La solución propuesta deberá estar clasificada como líder en la categoría de "Seguridad de Endpoint" o "Endpoint Security", según el informe más reciente de The Forrester Wave.

Requisitos del sistema:

Sistemas operativos para estaciones de trabajo: Windows 11, windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3), Mac e iMac APPLE.

Tabletas y sistemas operativos integrados: Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7, Windows Embedded POSReady 2009, Windows Embedded Standard 2009, Windows XP Embedded con Service Pack 2, Windows XP Tablet PC Edition e IPAD APPLE.

Sistemas operativos de servidor: Windows Server 2016, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server.

Sistemas operativos dispositivos móviles: Apple iPhone y tabletas iPad (iOS 8.1+) Google Android smartphones y tabletas (4.1+)

La solución de EDR deberá estar incluida en el mismo agente del antivirus y deberá proveer mínimo las siguientes funcionalidades

Investigación y respuesta ante incidentes: La rápida priorización e investigación de incidentes, con línea de tiempos del ataque y salida en espacio aislado, permite que los equipos de respuesta ante incidentes reaccionen rápidamente y detengan los ataques en curso (respuesta con un solo clic).

Análisis integrado de riesgos en los endpoints: Analiza continuamente los riesgos utilizando cientos de factores para descubrir y priorizar los riesgos de configuración para todos sus endpoints, lo que permite la adopción automática de acciones de endurecimiento.

Protección modular por capas: Las tecnologías sin firmas, que incluyen aprendizaje automático avanzado local y en la nube, tecnologías de análisis del comportamiento, espacio aislado integrado y endurecimiento de dispositivos constituyen una protección por capas altamente eficaz contra las amenazas sofisticadas.

Análisis forense de los ataques de extremo a extremo: La visibilidad del ataque previa y posterior al incidente permite a los analistas de seguridad realizar análisis de causa raíz tanto en ataques bloqueados como en actividades sospechosas en curso.



Prevención y detección precisas de última generación con reparación automática: El mejor repertorio de medidas de prevención del mundo y sus capacidades de detección basadas en el comportamiento durante la ejecución detienen y evitan la ejecución de las amenazas avanzadas en la infraestructura de la empresa. Una vez que se detecta una amenaza activa, se pone en marcha la respuesta automática para bloquear daños posteriores o movimientos laterales.
SecOps integradas: Incorpora módulos que contribuyen a reducir la brecha entre la TI y las operaciones de seguridad. Disminuye el esfuerzo operativo necesario para minimizar el riesgo digital al reducir la superficie de ataque: control de apps, control de dispositivos y administración de parches.
Agente y consola únicos: Desarrollado desde cero como una solución de agente y consola únicos, que incorpora todas las tecnologías necesarias para proteger eficazmente los endpoints empresariales y detener todas las amenazas digitales. Elimina la necesidad de ejecutar varios agentes y simplifica significativamente la implementación y la operativa.
Cobertura multiplataforma y API de integración de terceros: Cubre todos los endpoints empresariales que ejecuten Windows, Linux o Mac, en infraestructuras físicas, virtualizadas o en la nube, y proporciona seguridad consistente en toda la infraestructura. Admite la integración con herramientas de operaciones de seguridad preexistentes (SIEMS, como por ejemplo Splunk) y tecnologías específicas de centros de datos (los principales hipervisores del mercado).
Administración e instalación remota:
Antes de la instalación, el administrador puede personalizar los paquetes de instalación incluyendo solo los módulos deseados: análisis basado en el comportamiento, cifrado completo del disco, firewall, control de contenido, control de dispositivos, control de aplicaciones, administración de parches.
La instalación se puede realizar de varias formas: Al descargar el paquete antimalware directamente a la estación de trabajo donde se instalará. Mediante la instalación remota, directamente desde la consola web.
La instalación en máquinas desde una ubicación remota se realizará utilizando un cliente instalado existente en estas ubicaciones para minimizar el tráfico WAN.
La consola de administración informará el número de estaciones de trabajo que tienen el antimalware instalado y el número de estaciones de trabajo que están desprotegidas.
La consola de administración incluirá en los paneles / widgets configurables del panel de control. El oferente deberá alinearse a las políticas de seguridad de la entidad, así como el modelo MSPI del Ministerio de las Telecomunicaciones de Colombia – Mintic, el prestador de servicio debe contar con certificación vigente en la norma de estándares internacionales del Sistema de Gestión de Seguridad de la Información en su versión más reciente para los procesos relacionados con seguridad y mesa de servicios, a fin de garantizar la calidad, gestión y mejora de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente.
La consola de administración incluirá información detallada sobre las estaciones de trabajo / servidores: nombre, IP, sistema operativo, módulos instalados, política aplicada, información de actualización, etc.
La consola de administración permitirá al administrador enviar una política para configurar todo el producto antimalware, tanto para estaciones de trabajo como para servidores.
La consola de administración permitirá dos tipos de cuentas, Administrador y Reportero, que pueden asignarse a qué grupos de usuarios pueden cambiar la configuración o generar informes.
La consola de administración incluirá una sección de registro donde se mencionarán todas las acciones, con información detallada: iniciar sesión, editar, crear, cerrar sesión, mover, etc.

La consola de administración deberá incluir un módulo de parchado de aplicaciones y sistemas operativos que pueda ejecutar tanto parchado virtual como real de las aplicaciones.
Las principales características y funcionalidades del antimalware y el módulo antispyware:
La consola de administración permitirá la posibilidad de crear un paquete único, utilizado para sistemas operativos de 32 bits y de 64 bits, MAC y Linux.
El administrador de la solución puede configurar el escaneo automático en tiempo real para que no analice archivos o archivos con un tamaño mayor que "x" MB.
El escaneo automático en tiempo real puede admitir escanear archivos con hasta 16 niveles de profundidad.
Escaneo heurístico del comportamiento y monitoreo de procesos.
Escaneo en la nube y tecnología de aprendizaje automático.
Tecnología anti-ransomware y anti-exploit.
Capacidad para detectar ataques sin archivos, incluidos aquellos que utilizan herramientas legítimas del sistema operativo, como Powershell o intérpretes de scripts. La solución no debe bloquear globalmente los scripts para lograr esto.
Capa de seguridad adicional de próxima generación, basada en heurísticas agresivas y tecnología de aprendizaje automático, para detectar y bloquear la nueva generación de ataques avanzados o dirigidos y malware sofisticado antes de la ejecución. Debe proporcionar: Clasificación de los tipos de ataque.
Posibilidad de informar únicamente sobre amenazas detectadas, sin bloquearlas. Capacidad para ajustar la agresividad de detección para cada categoría de ataque, con opciones para tomar medidas en detecciones de mayor confianza y también informar todas las demás detecciones de menor confianza. Al menos 3 niveles de detección estarán disponibles. Capacidad para realizar diferentes acciones sobre los archivos detectados y las amenazas basadas en la red.
Firewall:
El módulo se puede instalar / desinstalar de acuerdo con las preferencias del administrador.
Se debe permitir bloquear el análisis de puertos.
Se debe permitir o denegar la conexión compartida a internet.
Capacidad de mostrar o no notificaciones cuando se une un nuevo equipo a la red Wifi
Capacidad de tener un sistema de detección de intrusos IDS tuneable.
Debe permitir aplicar perfiles basados en nivel de confianza (De confianza, Hogar/Oficina, Publico, Insegura, Dejar que decida Windows)
Capacidad de realizar reglas para aplicaciones y conexiones
Control de Usuario:
Bloqueo del acceso a Internet para clientes específicos o grupos de clientes.
Bloqueando el acceso a ciertas aplicaciones.
Bloqueando el acceso a internet por ciertos periodos de tiempo.
Bloqueo de páginas web que contengan determinadas palabras clave.
Permitiendo el acceso a páginas web específicas especificadas por el administrador.
Restringir el acceso a ciertos sitios web por algunas categorías predeterminadas (por ejemplo, citas en línea, violencia, etc.).
Control de dispositivos:



Deberá prevenir la fuga de información confidencial y mitigar el riesgo de infecciones por malware derivadas del uso de dispositivos conectados.
Deberá implementar políticas de control que permitan definir reglas de bloqueo y excepciones aplicables a una amplia gama de dispositivos y tipos de conexión.
Deberá registrar y enviar información asociada a los eventos de conexión de dispositivos, incluyendo como mínimo: nombre del dispositivo, identificador de clase (ID de clase), fecha y hora de conexión.
Deberá contar con un catálogo predefinido de tipos de dispositivos, que incluya, entre otros: CD-ROM, dispositivos de imagen, unidades de cinta, puertos COM/LPT, dispositivos SCSI, impresoras, tarjetas de red (NIC) y dispositivos de almacenamiento tanto interno como externo.
Deberá soportar configuraciones diferenciadas de acceso y privilegios por tipo de dispositivo, permitiendo al menos los siguientes estados: permitido, bloqueado o personalizado conforme a las políticas definidas.
Análisis automático de Sandbox de archivos sospechosos:
La solución debe tener la capacidad de realizar un análisis en profundidad de los archivos sospechosos.
La solución debe tener la capacidad de enviar archivos de forma automática o manual a los servidores de sandbox.
La solución puede configurarse para permitir que los usuarios accedan a los objetos enviados o bloquearlos hasta que se devuelva el análisis.
La solución debe permitir diferentes acciones de remediación si un archivo enviado es una amenaza.
La solución debe tener la capacidad de usar un servidor proxy para el tráfico de la zona de pruebas.
La solución debe tener la capacidad de detonar archivos individualmente o en grupo.
La solución ofrece un informe detallado sobre los archivos enviados.
Anti Exploit Avanzado.
Debe proporcionar protección en ejecución contra intentos de explotación dirigidos a vulnerabilidades conocidas y desconocidas en aplicaciones de uso común.
Capacidad para agregar aplicaciones personalizadas y presentar una lista de aplicaciones predefinidas.
Administración del Riesgo
Se debe proporcionar un módulo para la administración del riesgo que proporcione indicadores de riesgo de todos los endpoints junto con la descripción de cada punto de riesgo y su correspondiente recomendación para mitigar la afectación por configuración.
Se debe tener la capacidad de resolver características de riesgo de forma automática con un botón de acción.
La administración de riesgo debe gestionar los diferentes puntos de riesgo a nivel de sistema operativo y a nivel de red. El oferente deberá garantizar que los servicios cuenten con procedimientos formalmente establecidos, documentados y operativos para la gestión de incidentes de seguridad de la información. Para ello, el oferente deberá contar con certificación vigente en la norma Gestión de Incidentes de Seguridad de la Información, la cual establece las mejores prácticas para el tratamiento de incidentes en todo su ciclo de vida: preparación, detección, evaluación, respuesta y aprendizaje. Esta certificación respaldará el cumplimiento de estándares internacionales en la gestión de incidentes, conforme a las políticas de seguridad de la entidad y en armonía con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y

las Comunicaciones de Colombia – MinTIC. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente.
Desde la Política de configuración y control de seguridad del sistema, se debe tener la opción de habilitar o deshabilitar el módulo de Administración del riesgo
Se tiene que contar con un programador en el cual se gestione el escaneo de riesgos de seguridad por días, semanas y horarios en específico.
Servicio de soporte
Soporte técnico con un nivel de servicio 8x5.
Asistencia inmediata a través del punto de contacto de soporte, disponible de lunes a viernes solo en días hábiles y en horario de 8:00 a.m. a 5:00 p.m. todo el año.
Asistencia vía telefónica, vía email, en sitio o remoto dentro de las 12 horas hábiles siguientes al reporte del problema para incidentes.
Escalar ante el fabricante los incidentes técnicos que no sean resueltos por su personal, sin que esto genere costo para la Entidad.
El oferente debe contar con una mesa de servicios y/o mesa de ayuda que esté certificada bajo la norma internacional vigente del Sistema de Gestión de Servicios en su versión más reciente, aplicable a los procesos de seguridad y soporte de servicios. Esta certificación asegurará la calidad, gestión y mejora continua de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida directamente al oferente por el ente certificador autorizado.
Transferencia de conocimiento para al menos dos funcionarios de TI en administración y manejo de las herramientas del antivirus.
PARTNER
El oferente debe ser como mínimo Partner del nivel más alto de la solución ofertada, garantizando amplia experiencia en el manejo de licenciamiento sobre las diferentes soluciones, garantizando -ANS- el menor tiempo de respuesta en el suministro de equipos y soporte. El proponente debe Anexar la Certificación del Fabricante junto a su propuesta la cual debe ser expedida a nombre de la entidad con fecha de expedición no superior a 30 días.

3. PERSONAL

El proponente deberá acreditar el siguiente equipo mínimo de trabajo para la ejecución del contrato, enfocado en la adecuada prestación del servicio de soporte técnico:

1. Coordinador de Soporte Técnico

- Profesional en ingeniería de sistemas, electrónica, telecomunicaciones o áreas afines.
- Posgrado y/o certificación en diseño y gestión de servicios de TI o gestión de servicios de TI o gerencia servicios de proyectos tecnológicos.
- Experiencia general de mínima de ocho (8) años contados a partir de la expedición de la Tarjeta Profesional, de los cuales al menos cinco (5) años de experiencia específica deben corresponder a la coordinación o gerencia

de proyectos de TI o gestión de servicios de soporte técnico o mesas de servicio.

- Certificaciones en PMP, ITIL V4 Foundation, ISO/IEC 27001:2022 Auditor Interno y Scrum Master.

2. Ingeniero de Soporte en Seguridad Informática

- Profesional en ingeniería de sistemas, electrónica, telecomunicaciones o afines.
- Posgrado en seguridad informática.
- Mínimo cinco (5) Años de Experiencia general contados a partir de la expedición de la T.P. y tres (3) años de experiencia específica en Proyectos de Seguridad Informática.
- Certificaciones en Auditor Interno ISO 27001:2022, Certificación ITIL V4, CEH (Certified Ethical Hacking)

3. Especialista en Seguridad Informática

- Ingeniero electrónico, sistemas o telecomunicaciones o afines.
- Posgrado en Seguridad de las Tecnologías de la Información y de las Comunicaciones y/o en Seguridad de Redes.
- Mínimo doce (12) años de experiencia específica en proyectos de seguridad informática, todas contadas a partir de la expedición de la T.P.
- Certificaciones en CISSP, CISM, CEH, CHFI, ISO/IEC 27032, CISA, CRISC, ISO 31000 Lead Risk Manager, Auditor Líder ISO 27001:2022 CQR, Auditor Interno ISO 22301, Auditor Interno ISO 27001:2013, COBIT 5 FC y ITIL FC .

El proponente deberá aportar las hojas de vida y los respectivos soportes que acrediten formación académica, experiencia y certificaciones exigidas.

4. PLAZO DE EJECUCIÓN:

El plazo de ejecución del contrato será de doce (12) meses, contados a partir de la fecha de inicio establecida en el acta de inicio o desde la activación de las licencias de la solución de protección antivirus, lo que ocurra primero, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.

Durante este periodo, el contratista deberá garantizar la vigencia de las licencias, la disponibilidad de las actualizaciones de seguridad y el correcto funcionamiento de la solución adquirida, conforme a las condiciones técnicas establecidas.

5. LUGAR DE EJECUCIÓN:

Bogotá D.C.: DAPRE – Calle 7 No. 6 -54